

L'indipendenza dell'Internal Auditor negli enti con finalità pubblicistiche

Giugno
2023

Sommario

1. Sintesi	4
2. Ruolo della figura dell'Internal Auditor	8
I modelli di riferimento:	
La Corporate Governance	8
Il modello delle tre linee	13
3. Indipendenza e obiettività della figura dell'Internal Auditor	17
La teoria dei costi di agenzia.....	17
Indipendenza organizzativa	18
I fattori che influenzano l'indipendenza	19
Competenza (Standard 1200).....	19
Aggiornamento professionale continuo (Standard 1230)	20
Pianificazione annuale degli incarichi (Standard 2010).....	20
Assegnazione delle risorse per l'incarico (Standard 2230).....	21
Svolgimento dell'incarico (Standard 2300).....	21
Outsourcing della Funzione di Internal Audit.....	21
Le limitazioni consentite all'indipendenza (standard 1112) – altri ruoli del RIA.....	22
4. Ruoli aggiuntivi del Responsabile Internal Audit	24
Responsabile Prevenzione Corruzione e Trasparenza.....	24
Indipendenza e autonomia.....	25
Compiti e Poteri del RPCT	26
Membro interno dell'Organismo di Vigilanza.....	26
Altri ruoli della seconda linea	29
Ulteriori figure di secondo livello	31
Condizioni e salvaguardie minime per l'indipendenza della funzione	31
5. Valutare l'indipendenza e l'obiettività	34
La definizione di indipendenza e obiettività.....	34
Indipendenza.....	35
Obiettività.....	38
Identificare la minaccia:	43
Valutare la significatività della minaccia:	43
Identificare i fattori di mitigazione:	43
Valutare minacce residue:	43
Gestire proattivamente la minaccia residuale:	44
Valutare la presenza di minacce non risolte:	44
Determinare le implicazioni di reporting e documentazione:.....	44
Review e monitoraggio:	44
Quality Assurance	45
6. Risultati del questionario	47
7. Conclusioni	53
Riferimenti bibliografici	56

Le opinioni espresse nel presente documento sono quelle degli autori e non impegnano in alcun modo le organizzazioni di appartenenza.





1. Sintesi

Il presente lavoro di ricerca è stato elaborato nell'ambito del Forum degli Internal Auditors (Forum IA), avviato dal Servizio Revisione Interna della Banca d'Italia e composto dalle funzioni di Internal Audit di qualificati enti e società appartenenti al settore pubblico, con l'obiettivo di condividere esperienze e *best practices*¹ sui temi della revisione interna. A tal fine, è stato costituito un Gruppo di Lavoro incaricato di redigere uno studio sull'indipendenza della Funzione di Internal Audit, analizzando la tematica sia da un punto di vista organizzativo, sia considerando gli aspetti che impattano direttamente e indirettamente sull'indipendenza e l'obiettività dell'Auditor².

La ricerca parte dal presupposto che i meccanismi di *corporate governance* rappresentano riferimenti fondamentali per garantire livelli minimi di indipendenza. Gli studi in materia hanno analizzato le relazioni e le modalità di interazione dei numerosi organi e funzioni che hanno un ruolo attivo all'interno del Sistema di Controllo e di Gestione dei Rischi (SCIGR) di un'organizzazione. Dall'analisi è emerso che la netta separazione delle tre linee di controllo e gestione dei rischi, mutate dall'omonimo modello, e la segregazione delle attività svolte dalla Funzione di Revisione Interna - terza linea - rappresentano principi fondamentali cui fare riferimento.

Infatti, l'indipendenza organizzativa della Funzione di Internal Audit rappresenta un elemento cruciale per l'efficacia dei meccanismi di *governance*

all'interno dell'organizzazione. L'indipendenza organizzativa è citata in diversi *standard* professionali dell'Institute of Internal Auditors (IIA):

1110 Indipendenza organizzativa: il Responsabile Internal Auditing deve riportare a un livello dell'organizzazione che consenta all'attività di Internal Audit il pieno adempimento delle proprie responsabilità. Il Responsabile Internal Auditing deve confermare al *Board*, almeno una volta l'anno, lo stato di indipendenza organizzativa dell'attività di Internal Audit;

1130 Condizionamenti dell'indipendenza o dell'obiettività: se indipendenza od obiettività sono compromesse o appaiono tali, le circostanze dei condizionamenti devono essere rese note ad appropriati interlocutori. La natura dell'informativa dipende dal tipo di condizionamento.

Tali *standard* mostrano come la scelta di un'appropriata linea di riporto per la Funzione di Internal Audit rappresenti uno dei requisiti fondamentali affinché possa essere garantito un adeguato livello di indipendenza organizzativa. Laddove tale linea di riporto non sia garantita, diviene necessario rendere note le circostanze dei condizionamenti che ne hanno impedito la piena applicazione. Solo a partire dal 2017, poi, è stato introdotto lo *Standard* 1112 che "deroga" al principio di indipendenza "assoluta", consentendo al Responsabile dell'Internal Audit (RIA) l'assunzione di ruoli e responsabilità addizionali rispetto

1 Oltre al Servizio di Revisione Interna della Banca d'Italia, partecipano al Forum IA i responsabili delle funzioni di Internal Audit dei seguenti enti: Agenzia del Demanio, Agenzia delle Dogane e dei Monopoli, Agenzia delle Entrate, Consob, INAIL, INPS, Istituto Poligrafico e Zecca dello Stato, Ivass.

2 Il Gruppo di Lavoro è composto da Rosaria Mosca - INAIL, Manuela Artemi e Velianna Numerico - INPS, Massimo Proietti, Antonella Giorgini, Fiore Coppola - Istituto Poligrafico e Zecca dello Stato e Sara Testella, Fabio Lupo - Banca d'Italia.



all'attività di Internal Auditing, imponendo nel contempo opportune misure di tutela atte a limitare i condizionamenti all'indipendenza o all'obiettività.

Lo standard 1112 recita: “Laddove il Responsabile Internal Auditing abbia, o si prevede abbia, ruoli e/o responsabilità che esulano dall'Internal Auditing, devono essere poste in essere opportune misure di tutela atte a limitare i condizionamenti all'indipendenza o all'obiettività”.

Anche la letteratura accademica ha diffusamente trattato il tema dell'indipendenza dell'Internal Auditor. L'importanza di tale argomento è evidenziata da alcuni autori che hanno persino paragonato l'indipendenza e l'obiettività per l'Internal Auditing al giuramento di Ippocrate per la medicina³. Per capire le ragioni di tale rilevanza occorre partire dai fondamenti ontologici della Funzione di Internal Audit, mediante la “teoria dei costi di agenzia”⁴. Essa identifica le organizzazioni come un nesso di contratti tra i proprietari di risorse economiche (principal) e i manager, ossia coloro che sono incaricati di gestire e controllare tali risorse (agenti). Gli agenti hanno più informazioni rispetto ai principali e tale asimmetria informativa impatta negativamente sulla capacità di questi ultimi di controllare che i manager agiscano nel loro interesse. La teoria assume che entrambi si comportino razionalmente e quindi massimizzino la propria funzione di utilità: ciò crea le condizioni per l'insorgere di comportamenti dettati da “moral hazard” in cui i manager sono indotti ad agire contro l'interesse dei principali⁵. Per la natura dell'attività svolta, inoltre, i manager sono in possesso di più informazioni rispetto

ai proprietari i quali, quindi, hanno limitate possibilità di svolgere un adeguato monitoraggio su di essi. L'Internal Audit rappresenta dunque il costo sostenuto dai proprietari per proteggere i propri interessi economici ed evitare il verificarsi dei casi sopra descritti. In virtù di questo, la responsabilità del controllo interno è assegnata al Board (espressione dei “principal”) a cui l'Internal Audit è chiamato a fornire assurance⁶. Se dunque la Funzione dell'Internal Audit è quella di tutelare gli interessi dei principali rispetto all'operato degli agenti, la sua indipendenza è un prerequisite indispensabile.

Il paper passa poi in rassegna i ruoli addizionali in altri ambiti che il Responsabile Internal Auditing può essere chiamato a svolgere e che possono avere impatti sull'indipendenza; ad esempio: Responsabile Prevenzione Corruzione e Trasparenza (RPCT Legge n. 190 del 2012), Membro interno dell'Organismo di Vigilanza (D.Lgs. 231/01), Data Protection Officer (DPO ai sensi del Regolamento Ue 2016/679), Dirigente Preposto sull'informativa finanziaria (DP L. 262/2005).

Viene inoltre proposto un *framework* per valutare il livello di indipendenza e di obiettività della Funzione di Internal Audit, a livello i) individuale, ii) di incarico, iii) di funzione, iv) di organizzazione e di v) professione al fine di permettere l'identificazione di situazioni di criticità e porre in essere eventuali misure correttive. In ogni modo, viene ribadito come la sede deputata a valutare il livello di indipendenza sia quella della *Quality Assurance Review* che periodicamente ogni Funzione di Internal Audit deve svolgere.

-
- 3 Mutchler J., Chang S. and Prawitt D. *Independence and Objectivity: a Framework for Internal Auditors*, IIA Research Foundation, Altamonte Springs, FL (2001).
 - 4 Per maggiori informazioni si veda Fama, E. F. Agency problems and the theory of the firm. *Journal of political economy*, vol. 88, No.2, pp. 288-307. Per un'applicazione della teoria all'Internal Audit vedasi inoltre Adams, M. B. Agency Theory and the Internal Audit. *Managerial Auditing Journal*, Vol. 9 No. 8, 1994 pp. 8-12 (1980).
 - 5 Ad es. garantendosi benefit eccessivamente elevati a discapito dei proprietari delle risorse economiche che sono stati chiamati ad amministrare.
 - 6 Christofer J., Sarens G., Leung P. A critical analysis of the independence of the Internal Audit function: evidence from Australia, *Accounting, Auditing & Accountability Journal*, Vol. 22 No. 2, pp. 200-220 (2009).



La trattazione teorica infine è stata confrontata con i risultati emersi da una survey condotta presso tutti i partecipanti al Forum. Dalle risposte emerge un elevato livello di indipendenza organizzativa: la Funzione di IA è una struttura organizzativa separata che riporta al Vertice nel 100% delle risposte; tale indipendenza è sancita nel mandato della funzione. Nel 66% dei casi il RIA riveste altri ruoli che esulano dall'Internal Audit: RPCT, membro dell'OdV o di altri Comitati (Comitato etico, Comitato Controlli e Rischi). Quanto al processo di definizione del piano di Audit, esso si basa nella maggior parte dei casi su un *risk assessment* svolto da diverse figure aziendali: nel 55% è la Funzione di Audit che lo effettua in maniera indipendente. Mentre in altri casi tale valutazione viene svolta attraverso l'apporto dei responsabili delle strutture, della Funzione di *Risk Management* o del Vertice

dell'Istituto. Quanto alla presenza di un Comitato di Audit all'interno dell'organizzazione, al quale l'Internal Audit riferisce funzionalmente, le percentuali si attestano al 33%.

In conclusione si può affermare che l'indipendenza dell'Internal Audit sia più un obiettivo a cui tendere che una condizione prestabilita: l'indipendenza, assicurata in primis da un corretto posizionamento all'interno dell'organigramma, può essere indebolita da molti fattori tra cui l'assegnazione al RIA, per obblighi normativi o per scelte organizzative, di altri ruoli che esulano dall'Internal Audit. In tutti i casi, è responsabilità del RIA porre in essere misure, organizzative o procedurali, che assicurino un adeguato livello di indipendenza della funzione quale elemento imprescindibile per dimostrare la sua credibilità e la capacità di fornire valore aggiunto all'organizzazione.





2. Ruolo della figura dell'Internal Auditor

(a cura di R. Mosca)

I modelli di riferimento: La Corporate Governance

Sul tema della *Corporate Governance* (governo d'impresa) e del sistema dei controlli interni sono intervenuti nel tempo strumenti di autodisciplina, di regolamentazione e norme che hanno promosso *standard*, modelli, regole volti a definire efficaci principi di governo e di controllo, anche con l'impulso di Enti sovranazionali (es. OECD, EU, EIOPA, EBA), che hanno contribuito a impostare un percorso di armonizzazione tra ordinamenti.

Pur nelle specificità dei diversi ambiti, nell'evoluzione di *standard*, modelli e regolamenti in tema di *governance* emergono tratti comuni nel disegno di un sistema di controllo sempre più orientato al governo dei rischi, nel riconoscimento del ruolo di rilievo svolto dal *Board* (o Consiglio di Amministrazione, o Organo Amministrativo) in tema di rischio e di controllo interno e della stretta relazione che si delinea tra organo di controllo e *Board*, oltre che nel principio di indipendenza della Funzione di *Internal Audit* (o revisione interna). L'organo amministrativo è trasversalmente riconosciuto responsabile della definizione delle linee di indirizzo e del monitoraggio dell'adeguatezza e dell'efficacia del sistema di controllo interno e di gestione dei rischi.

Di seguito alcuni riferimenti in tema di *governance* e di controllo interno (in particolare della Funzione di Audit) a livello di autoregolamentazione, di *standard*, regolamenti e normative.

Il Codice di Autodisciplina, pubblicato nel 1999 dal Comitato per la *Corporate Governance* di Borsa Italiana, aggiornato negli anni fino alla versione del gennaio 2020, rappresenta uno *standard* per le società quotate italiane. Definisce la *Corporate Governance* come “*il sistema delle regole secondo le quali le imprese sono gestite e controllate...*”⁷. Nel tempo e nelle revisioni che si sono succedute significative sono le disposizioni che hanno interessato il sistema del controllo interno, visto come “*uno degli snodi cruciali della governance di una società quotata*”⁸ e che sempre più si è incentrato sul concetto di rischio (“*la moderna concezione dei controlli ruota attorno alla nozione di rischi aziendali, alla loro identificazione, valutazione e monitoraggio*”⁹). È dall'edizione del 2011 che si fa più ampio riferimento alla Funzione di *Internal Audit* (o revisione interna) alla quale “*viene riconosciuta una spiccata indipendenza, che si esplica sia attraverso l'attribuzione di autonomi poteri di iniziativa nella predisposizione del piano di Audit e nell'attivazione dei singoli interventi, sia attraverso le modalità stabilite per la nomina, revoca e remunerazione del suo Responsabile. I poteri*

7 Comitato per la *Corporate Governance* delle Società Quotate, Rapporto Codice di Autodisciplina, 1999 pag. 18.

8 Comitato di *Corporate Governance*, *Codice di Autodisciplina*, 2011, art.7 - Commento.

9 *ibid*



riservati al Consiglio di Amministrazione in questa materia denotano l'esistenza di un vero e proprio rapporto gerarchico nei confronti del Responsabile della Funzione di Internal Audit"¹⁰. Nella più recente formulazione (2020), il sistema di controllo interno e di gestione dei rischi è definito come "l'insieme delle regole, procedure e strutture organizzative finalizzate ad una effettiva ed efficace identificazione, misurazione, gestione e monitoraggio dei principali rischi, al fine di contribuire al successo sostenibile della società"¹¹. Ampia l'estensione dei poteri riconosciuti al Consiglio di Amministrazione (Organo di Amministrazione nell'edizione 2020) che vanno dalla definizione delle linee di indirizzo del sistema di controllo interno e di gestione dei rischi, alla valutazione dell'adeguatezza di tale sistema, rispetto alle caratteristiche dell'impresa e al profilo di rischio assunto, e della sua efficacia. L'Organo di Amministrazione nomina e revoca il Responsabile dell'Internal Audit, ne definisce la remunerazione coerentemente con le politiche aziendali, assicura che sia dotato di risorse adeguate all'espletamento dei propri compiti¹². È stato osservato come dalle disposizioni del Codice - nelle revisioni che si sono succedute nel tempo - si configuri "il riconoscimento al Consiglio di Amministrazione del ruolo di figura apicale del sistema dei controlli, in coerenza con l'attività di alta amministrazione ad esso spettante"¹³.

Tra le Raccomandazioni relative all'Organo di Amministrazione quella di istituire al proprio interno comitati consiliari con funzioni istruttorie, propositive e consultive in materia di nomine, remunerazioni, controllo e rischi¹⁴. La previsione

dell'istituzione di comitati interni - organi non esecutivi a sostegno del Consiglio, funzionali a migliorarne l'efficacia e l'efficienza - è elemento ricorrente, se pure diversamente modulato, nell'evoluzione del quadro di orientamenti, standard e normative in tema di Corporate Governance, in linea anche con l'ampliamento delle competenze e delle responsabilità attribuite al Board.

Con riferimento alla Funzione di Internal Audit, il Responsabile è "incaricato di verificare che il sistema di controllo interno e di gestione dei rischi sia funzionante, adeguato e coerente con le linee di indirizzo definite dall'Organo di Amministrazione"¹⁵. Ne viene affermata la dipendenza gerarchica dall'Organo di Amministrazione, mentre è esclusa l'assunzione di responsabilità in aree operative ed è garantita la possibilità di accesso a tutte le informazioni utili per lo svolgimento dell'incarico. ("Il Responsabile della Funzione di Internal Audit non è responsabile di alcuna area operativa e dipende gerarchicamente dall'Organo di Amministrazione. Egli ha accesso diretto a tutte le informazioni utili per lo svolgimento dell'incarico"¹⁶).

Di Corporate Governance e di sistemi di controllo trattano i Principi di Corporate Governance dell'Organizzazione per la Cooperazione e lo Sviluppo Economico (OCSE). Formulati originariamente nel 1999¹⁷, sono stati oggetto di revisione nel 2004¹⁸ e nel 2015¹⁹. Forniscono indicazioni di riferimento per modelli di buon governo societario. Nei Principi OCSE la Corporate Governance "definisce la struttura attraverso cui vengono fissati gli obiettivi della società, vengono

10 ibid

11 Comitato di Corporate Governance, Codice di Corporate Governance, 2020, art.6 Principi.

12 Comitato di Corporate Governance, Codice di Corporate Governance, 2020, art 6 Raccomandazione 33.

13 Gasparri G., I controlli interni nelle società quotate. Gli assetti della disciplina italiana e i problemi aperti, Quaderni Giuridici Consob settembre 2013.

14 Comitato di Corporate Governance, Codice di Corporate Governance, 2020, art 3 Raccomandazione 16.

15 Comitato di Corporate Governance, Codice di Corporate Governance, 2020, art.6 Raccomandazioni 32.

16 Comitato di Corporate Governance, Codice di Corporate Governance, 2020, art.6 Raccomandazioni 36.

17 OECD - Organisation for Economic Cooperation and Development, OECD Principles of Corporate Governance, 1999.

18 OECD - Organisation for Economic Cooperation and Development, OECD Principles of Corporate Governance, 2004.

19 OECD - Organisation for Economic Cooperation and Development, G20/OECD Principles of Corporate Governance, 2015.



determinati i mezzi per raggiungere tali obiettivi e vengono controllati i risultati”.

Tra le responsabilità del Consiglio di Amministrazione quella di garantire l'integrità dell'informativa finanziaria, un *Audit* indipendente, sistemi di controllo adeguati, quali un sistema per la gestione del rischio, per il controllo finanziario e operativo, e la *compliance* verso norme e *standard* rilevanti (Cap VI – D7). Al Consiglio è attribuito un ruolo di *leadership* nel garantire efficaci strumenti di controllo del rischio, nel definire e far rispettare chiare linee di responsabilità, prevedendo l'istituzione di un *Internal Audit* a diretto riporto del Consiglio (Cap VI – D7).

In tema di gestione del rischio e di controllo interno, i Consigli di Amministrazione dovrebbero considerare l'istituzione di comitati consiliari, a supporto delle proprie funzioni, in particolare per l'*Audit* e, in ragione delle dimensioni aziendali e del profilo di rischio, per l'area di *Risk Management* (Cap VI – E2).

Nell'ambito dei settori bancario e assicurativo il tema della *governance* è trattato da Regolamenti, emessi dagli enti regolatori, da linee guida e da normative di settore ed assume caratteristiche specifiche.

Ispirata ai principi di *Corporate Governance* dell'OCSE del 1999 è la pubblicazione del documento *Enhancing Corporate Governance for Banking Organisations*, sempre nel 1999, da parte del *Basel Committee on Banking Supervision* (BCBS) “nell'intento di rinsaldare l'importanza per le istituzioni bancarie dei principi enunciati dall'OCSE...”²⁰. Anche la revisione del documento nel 2006 da parte del Comitato fa riferimento alla

revisione dei principi OCSE del 2004. Nel 2010 il Comitato di Basilea pubblica dei nuovi *Principles for enhancing Corporate Governance*²¹, “sottolineando espressamente, per la prima volta, la valenza sistemica della regolamentazione della *governance in ambito bancario*”²². Con la pubblicazione nel 2015 delle linee guida *Corporate Governance principles for banks*²³ si introducono significative novità in tema di governo societario e di sistemi di controllo e di rischio, la gestione del rischio è aspetto centrale della *governance* bancaria.

Nei principi le funzioni di controllo sono definite come “*those functions that have a responsibility independent from management to provide objective assessment, reporting and/or assurance. This includes the Risk Management function, the compliance function and the Internal Audit function*”. I responsabili di tali funzioni non dovrebbero svolgere un doppio ruolo (“*dual-hatting*”) e non dovrebbero avere responsabilità gestionali o finanziarie relative a linee di *business* operative (principi 6, 9, 10).

A garanzia di indipendenza, il riporto primario della Funzione di *Internal Audit* è al Consiglio (o al suo comitato per il controllo interno), al quale spetta anche la selezione, il controllo sui risultati e la revoca del Responsabile di tale Funzione (principio 10). La Funzione di *Audit* dovrebbe avere all'interno dell'organizzazione posizione, competenze, risorse e autorità tali da poter svolgere i propri compiti in modo efficace e obiettivo (principio 10).

A livello di ordinamento europeo la Direttiva 2013/36/UE (CRD IV), nel più ampio contesto delle norme sull'accesso all'attività degli enti creditizi e sulla vigilanza prudenziale, dedica una specifica sezione alle tematiche di *governance*. Prevede che

20 Basel Committee on Banking Supervision, *Enhancing corporate governance for Banking Organisations*, 1999.

21 Basel Committee on Banking Supervision, *Principles for Enhancing corporate governance*, 2010.

22 Frigeni, C. *La Governance Bancaria come Risk Governance: l'evoluzione della Regolamentazione internazionale ed europea dopo la crisi*, in OSSERVATORIO MONETARIO 1/2016, Associazione per lo Sviluppo degli Studi di Banca e Borsa, Università Cattolica del Sacro Cuore – Laboratorio di Analisi Monetaria, Capitolo II.

23 Basel Committee on Banking Supervision, *Corporate Governance Principles for Banks*, 2015.



gli enti (oggetto delle disposizioni) siano dotati di *“solidi dispositivi di governance, ivi compresa una chiara struttura dell’organizzazione con linee di responsabilità ben definite, trasparenti e coerenti, di processi efficaci per l’identificazione, la gestione, la sorveglianza e la segnalazione dei rischi ai quali sono o potrebbero essere esposti, e di adeguati meccanismi di controllo interno, ivi comprese valide procedure amministrative e contabili nonché politiche e prassi di remunerazione che riflettano e promuovano una sana ed efficace gestione del rischio”*²⁴.

Concorrono al processo di armonizzazione della disciplina a livello europeo gli orientamenti dell’Autorità Bancaria Europea (ABE) in tema di organizzazione e governance²⁵: *“...specificano i dispositivi, i processi e i meccanismi di governance interna che gli enti creditizi e le imprese di investimento devono attuare [...] al fine di garantire una gestione efficace e prudente dell’istituzione”*²⁶. Trovano applicazione secondo il criterio di proporzionalità, in funzione del profilo di rischio e del modello di business dell’ente.

Nelle indicazioni degli orientamenti, le funzioni di controllo interno dovrebbero includere una Funzione di Gestione dei Rischi, una Funzione di Conformità e una Funzione di Audit Interno. Le Funzioni di Gestione dei Rischi e di Conformità dovrebbero essere soggette a riesame da parte della Funzione di Audit Interno (paragrafo 19).

In tema di combinazione delle Funzioni di Controllo Interno, tenendo conto del principio di proporzionalità, è previsto che la Funzione di Gestione dei Rischi e la Funzione di Conformità possano essere combinate, mentre quella di Audit Interno non dovrebbe essere combinata con un’altra

Funzione di Controllo Interno (paragrafo 19.3).

I responsabili di tali funzioni dovrebbero essere stabiliti a un livello gerarchico adeguato che fornisca al Responsabile della Funzione di controllo l’autorità appropriata e il peso necessario per adempiere alle proprie responsabilità (paragrafo 19.1).

La Funzione di Audit, in particolare, dovrebbe valutare se il quadro di controllo interno dell’ente sia efficiente ed efficace; tra le altre cose dovrebbe valutare l’adeguatezza del quadro di governance dell’ente, l’adeguatezza, la qualità e l’efficacia dei controlli esercitati e delle segnalazioni effettuate dalle unità operative e dalle funzioni di gestione dei rischi e di conformità (paragrafo 22).

Nel quadro normativo nazionale, la circolare 285 del 17 dicembre 2013 (e successivi aggiornamenti) di Banca d’Italia, in un contesto di revisione e integrazione delle disposizioni di vigilanza in tema di governo d’impresa, recepisce le disposizioni della Direttiva CRD IV, tenendo conto degli standard internazionali del comitato di Basilea e delle raccomandazioni e orientamenti dell’Autorità bancaria europea.

Riconosce un ruolo strategico al sistema dei controlli interni, *“la cultura del controllo deve avere una posizione di rilievo nella scala dei valori aziendali”*; il sistema dei controlli interni è *“elemento di conoscenza per gli organi aziendali in modo da garantire piena consapevolezza della situazione ed efficace presidio dei rischi aziendali e delle loro interrelazioni”*.

Il Titolo IV della Parte Prima della circolare è dedicato alle disposizioni in tema di governo societario, controlli interni e gestione dei rischi.

24 Direttiva 2013/36/UE (CRD IV) del Parlamento europeo e del Consiglio “sull’accesso all’attività degli enti creditizi e sulla vigilanza prudenziale sugli enti creditizi e sulle imprese di investimento”, 26 giugno 2013, art. 74, paragrafo 1.

25 Autorità bancaria europea, Orientamenti ABE sull’organizzazione interna (GL44), 2011; EBA, Orientamenti sulla governance interna (EBA/GL/2017/11), 2018; EBA Orientamenti sulla governance interna (EBA/GL/2021/05), 2021.

26 EBA, Orientamenti sulla governance interna (EBA/GL/2017/11), 2018, pag. 3. Il riferimento è in conformità all’art. 74, paragrafo 3, della direttiva 2013/36/UE.



Prevede che siano istituite funzioni aziendali di controllo permanenti e indipendenti: di conformità alle norme (*compliance*), di controllo dei rischi (*Risk Management*), di revisione interna (*Internal Audit*).

Nella sezione relativa alle funzioni aziendali di controllo è previsto che, a garanzia di indipendenza, queste dispongano di autorità, risorse, competenze e accesso ai dati. I responsabili di tali funzioni “... sono collocati in posizione gerarchica e funzionale adeguata; in particolare, i responsabili delle funzioni di controllo dei rischi e di conformità alle norme sono collocati alle dirette dipendenze dell’organo con funzione di gestione o dell’organo con funzione di supervisione strategica; il Responsabile della Funzione di Revisione Interna è collocato sempre alle dipendenze dell’organo con funzione di supervisione strategica.” I responsabili delle funzioni di controllo “non hanno responsabilità diretta di aree operative sottoposte a controllo...”²⁷.

Importante il ruolo dell’organo con funzione di supervisione strategica²⁸ in tema di governo dei rischi e di controlli interni. È chiamato, tra l’altro, a definire e approvare: il modello di business, gli obiettivi di rischio e le politiche di governo dei rischi; le linee di indirizzo del sistema dei controlli interni. Ha il compito di nominare e revocare i responsabili delle funzioni aziendali di controllo (*Compliance*, *Risk Management*, *Internal Audit*). Approva il programma di attività, il piano di *audit*, annuale e pluriennale, della Funzione di Revisione Interna.

A livello normativo, in ambito assicurativo, la Direttiva europea 2009/138/CE (cd. *Solvency II*), come Basilea II per il settore bancario, pone l’attenzione sui temi della *governance*, del *Risk Management* e del Controllo Interno.

Il modello di *governance* e del sistema dei controlli è delineato dal Regolamento 38 del 2018 dell’IVASS²⁹, recante disposizioni in materia di governo societario, che ha sostituito (sviluppando) le logiche operative del Regolamento 20, attuativo dei principi della *governance* definiti nella Direttiva *Solvency II*.

Nel Regolamento 38 si parla di Funzione di *Internal Audit* (revisione interna) in staff al Consiglio di Amministrazione (denominato «organo amministrativo»). Rientra tra le cosiddette “funzioni fondamentali” del governo societario, costituite dalle funzioni di gestione dei rischi, verifica della conformità alle norme, *Internal Audit*, e dalla Funzione attuariale.

Sono costituite in forma di specifica unità organizzativa o, per le sole funzioni di gestione dei rischi, di conformità alle norme ed attuariale, anche mediante il ricorso a risorse appartenenti ad altre unità aziendali, tenuto conto della ridotta natura, portata e complessità dei rischi inerenti all’attività dell’impresa. In tale ultimo caso, l’indipendenza va assicurata attraverso la presenza di adeguati presidi che garantiscano la separatezza di compiti e prevengano conflitti di interesse. Anche quando non costituite in forma di specifica unità organizzativa riferiscono direttamente all’organo amministrativo (art.27).

La Funzione di Revisione Interna è incaricata di valutare e monitorare l’efficacia, l’efficienza e l’adeguatezza del sistema di controllo interno e delle ulteriori componenti del sistema di governo societario e le eventuali necessità di adeguamento, anche attraverso attività di supporto e di consulenza alle altre funzioni aziendali (art. 35).

È garantita l’indipendenza della Funzione di Revisione Interna dalle altre funzioni. In caso di collaborazione con le altre funzioni è, in ogni

27 Banca d’Italia, Circolare 285/2013, Parte Prima.IV.3.19).

28 Definito come “l’organo nel quale si concentrano le funzioni di indirizzo e/o di supervisione della gestione sociale” Circ. 285/2013, Parte Prima.IV.1.4).

29 IVASS Regolamento n. 38, 3 luglio 2018.



caso, evitata l'insorgenza di conflitti di interessi e garantita l'obiettività e l'indipendenza della Funzione di Revisione Interna (art. 35).

Nell'esercizio dell'attività di revisione e in sede di valutazione e segnalazione delle relative risultanze, la Funzione di Revisione Interna svolge i compiti ad essa assegnati con autonomia ed obiettività di giudizio, in modo da preservare la propria indipendenza e imparzialità, in coerenza con le direttive a tal fine definite dall'organo amministrativo [Consiglio di Amministrazione] (art. 36).

Il modello delle tre linee

La definizione di modelli di *governance* richiede l'individuazione delle responsabilità delle diverse componenti dell'organizzazione nella gestione e governo dei rischi. Uno schema generale di riferimento è stato elaborato nel cosiddetto modello delle "tre linee di difesa" sostenuto da organismi professionali come l'Institute of Internal Auditors (IIA), ma referenziato anche in contesti diversi.

In particolare, l'Institute of Internal Auditors ha inizialmente promosso il modello delle "tre linee di difesa" (2013)³⁰ che individua tre linee coinvolte nella gestione de rischi, ognuna delle quali svolge un ruolo:

- funzioni che hanno la "proprietà" e la gestione del rischio - i responsabili delle linee operative hanno la "proprietà" del rischio e costituiscono la prima linea di difesa; hanno la responsabilità di identificare, monitorare e controllare i rischi correlati alle attività svolte;
- funzioni che presidiano i rischi - costituiscono una seconda linea di difesa, variano in relazione al tipo di organizzazione, tipicamente prevedono una Funzione di Gestione del Rischio e una Funzione di Conformità;
- funzioni che forniscono una garanzia indipendente - è la terza linea di difesa in cui si colloca la Funzione di *Internal Auditing*; fornisce garanzia (*assurance*) indipendente sull'efficacia della *governance*, della gestione del rischio e dei controlli interni.

Lo stesso Codice di Autodisciplina, nella versione del 2011, fa riferimento all'attività della Funzione di Audit o di revisione interna, "...investita dell'attività di controllo "di terzo livello" [...]. "A un diverso livello si pongono le funzioni aziendali alle quali sono affidati i cosiddetti controlli "di secondo livello", volti a monitorare e gestire i rischi tipici aziendali, quali il rischio operativo, il rischio finanziario, il rischio di mercato, il rischio di (non) conformità, etc."³¹.

I principi di *Corporate Governance* per le Banche del Comitato di Basilea prevedono un modello a tre linee di difesa che vede le funzioni di *business* come prima linea, le Funzioni di *Compliance* e di *Risk Management* come controlli di secondo livello e la Funzione di *Internal Audit* come terzo livello di difesa, indipendente dalla prima e seconda linea. La terza linea di difesa consiste in una Funzione di Audit interno indipendente ed efficace³².

30 Institute of Internal Auditor The three lines of defense in effective risk management and control, 2013.

31 Comitato di Corporate Governance, Codice di Autodisciplina, 2011, art.7 - Commento.

32 Basel Committee on Banking Supervision, Corporate Governance Principles for Banks, 2015 Principle I (38-43).



Anche la Circolare 285 del 17 dicembre 2013 di Banca d'Italia distingue tra:³³

- controlli di linea (c.d. “controlli di primo livello”), diretti ad assicurare il corretto svolgimento delle operazioni, effettuati dalle stesse strutture operative;
- controlli sui rischi e sulla conformità (c.d. “controlli di secondo livello”), che prevedono che le funzioni preposte a tali controlli siano distinte da quelle produttive;
- revisione interna (c.d. “controlli di terzo livello”), finalizzata a individuare violazioni delle procedure e della regolamentazione e a valutare periodicamente la completezza, l'adeguatezza, la funzionalità (in termini di efficienza ed efficacia) e l'affidabilità del sistema dei controlli interni.

Successivamente, l'*Institute of Internal Auditors*, insieme alla *Committee of Sponsoring Organizations (COSO)*, ha redatto un lavoro congiunto con lo scopo di aiutare le organizzazioni a migliorare le proprie strutture di governance fornendo linee guida su come assegnare ruoli e responsabilità relativi al controllo interno, mettendo in relazione il modello delle tre linee di difesa con il *COSO Internal Control – Integrated Framework*³⁴ (2015). Lo studio rileva nello schema COSO una non chiara definizione di ruoli e responsabilità nella gestione dei rischi e dei controlli e individua nello schema a tre linee di difesa un possibile arricchimento dello schema COSO per definire un modello che descrive come attività e principi di gestione del rischio possano essere distribuite tra le tre linee di difesa.

Nel tempo non sono mancate proposte di evoluzione del modello a tre linee di difesa prevedendo, ad esempio, l'introduzione di ulteriori livelli di controllo. Il *Financial Stability Institute* ha pubblicato nel dicembre 2015 un *Occasional Paper* in cui propone per le istituzioni finanziarie un modello di controllo a quattro linee di difesa, individuando nelle autorità di vigilanza e nei revisori esterni un quarto livello di controllo, in virtù delle specifiche caratteristiche di governance di banche e assicurazioni³⁵.

Nel documento sono analizzati alcuni aspetti di debolezza del modello a tre linee evidenziando, ad esempio, come la prima linea di difesa, pur garantendo una migliore granularità e qualità dei controlli, per le conoscenze di “business”, possa essere meno incentivata su tali aspetti perché valutata su obiettivi di linea piuttosto che di controllo.

Da ultimo l'*Institute of Internal Auditors* ha rivisto il modello delle “tre linee di difesa” introducendo il modello delle “tre linee” (2020)³⁶, mantenendo il concetto delle linee per familiarità con il precedente, senza però voler denotare veri e propri elementi strutturali, bensì una differente definizione dei ruoli.

Il modello individua quattro ruoli chiave: organo di governo, *management* (prima e seconda linea), *Internal Audit* (terza linea) e fornitori esterni di “assurance” e definisce le relazioni tra questi (delega, *accountability*, *reporting*, comunicazione, allineamento, coordinamento e collaborazione).

33 Banca d'Italia Circolare 285 del 17 dicembre 2013 – Parte I Titolo IV Capitolo 3 Sezione I – Disposizioni preliminari e principi generali.

34 Leveraging COSO Across the three lines of defense by The Institute of Internal Auditors, Douglas J. Anderson, Gina Eubanks Research Commissioned by Committee of Sponsoring Organizations of the Treadway Commission Luglio 2015.

35 Financial Stability Institute, Arndorfer, I., Minto, A. : «The “four lines of defence model” for financial institutions - Taking the three-lines-of-defence model further to reflect specific governance features of regulated financial institutions», BIS, Occasional Paper N. 11, December 2015.

36 Institute of Internal Auditor The IAA's Three Lines Model An update of the Three Lines of Defense 2020.

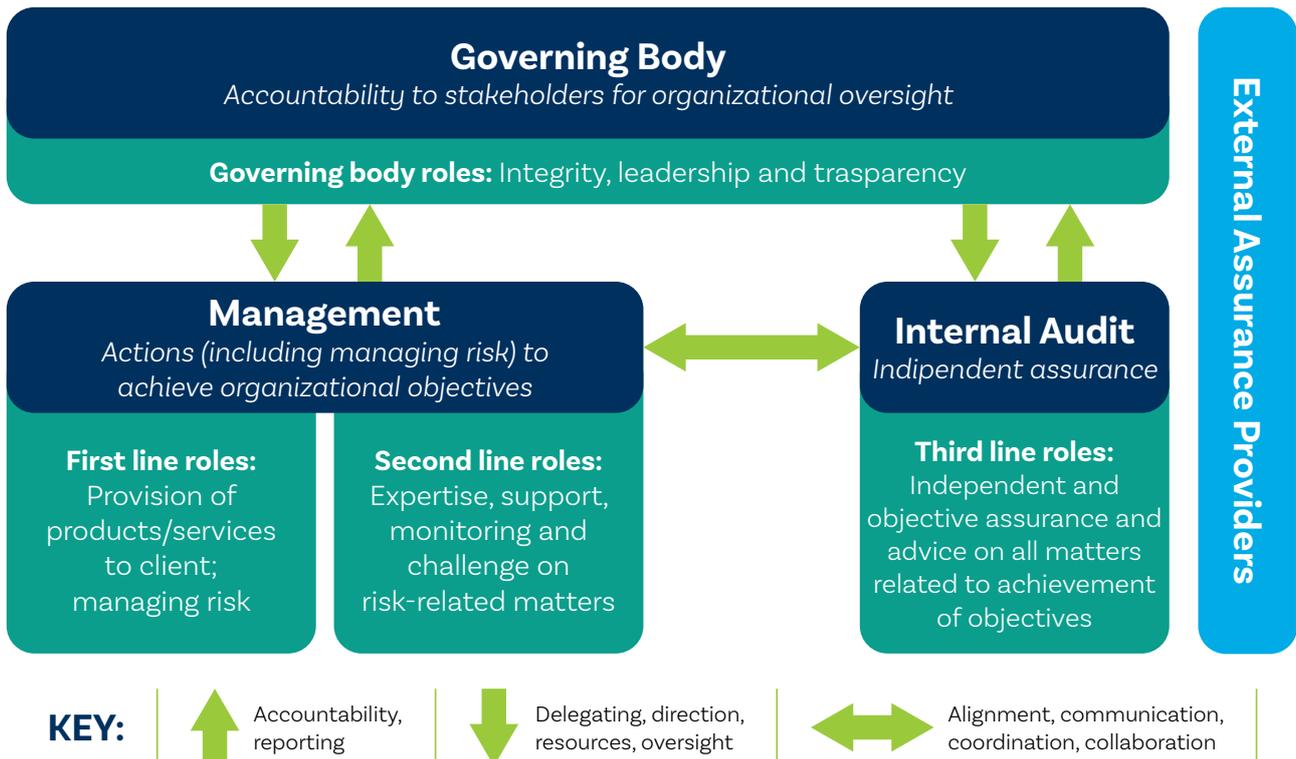


Figura 1 Fonte: The IIA's Three Lines Model An update of the Three Lines of Defense IIA (2020)

La sua applicazione si fonda su cinque principi³⁷, due dei quali riguardano il ruolo dell'Internal Audit e uno di questi attiene proprio all'indipendenza della terza linea: "Internal Audit's independence from the responsibilities of management is critical to its objectivity, authority, and credibility. It is established through: accountability to the governing body; unfettered access to people, resources, and data needed to complete its work; and freedom from bias or interference in the planning and delivery of Audit services".

37 Principio 1) Governance, 2) Governing body roles, 3) Management and first and second line roles, 4) Third line roles, 5) Third line independence, 6) Creating and protecting value.





3. Indipendenza e obiettività della figura dell'Internal Auditor

(a cura di S. Testella e F. Lupo)

La teoria dei costi di agenzia

La letteratura accademica ha diffusamente trattato il tema dell'indipendenza dell'Internal Auditor. L'importanza di tale argomento è evidenziata da alcuni autori che hanno persino paragonato l'indipendenza e l'obiettività per l'Internal Auditing al giuramento di Ippocrate per la medicina³⁸.

Per capire le ragioni di tale rilevanza occorre partire dai fondamenti ontologici della Funzione di Internal Audit, la cui esistenza è stata spiegata mediante la "teoria dei costi di agenzia"³⁹.

La teoria identifica le organizzazioni come un nesso di contratti tra i proprietari di risorse economiche (principali) e i manager (agenti), ossia coloro che sono incaricati di gestire e controllare tali risorse. Gli agenti hanno più informazioni

rispetto ai principali: tale asimmetria informativa impatta negativamente sulla capacità di questi ultimi di controllare che i manager agiscano nel loro interesse.

Entrambi i soggetti si comportano razionalmente, massimizzando la propria funzione di utilità: tale assunto crea le condizioni per il verificarsi di azioni dettate dal "moral hazard" quando, cioè, i manager sono indotti ad agire contro l'interesse dei principali⁴⁰. Analogamente, per la natura dell'attività svolta, i manager sono in possesso di più informazioni rispetto ai proprietari e possono con ciò impedire o limitare il monitoraggio svolto dai principali. L'Internal Audit rappresenta dunque il costo sostenuto dai proprietari per proteggere i propri interessi economici ed evitare il verificarsi dei casi sopra descritti. In virtù di questo, la responsabilità del controllo interno è assegnata al Board (espressione dei "principal") a cui l'Internal Audit è chiamato a fornire *assurance*⁴¹.

38 Mutchler, J., Chang, S. and Prawitt, D. Independence and Objectivity: a Framework for Internal Auditors 2001

39 Per maggiori informazioni si veda Fama, E. F. Agency problems and the theory of the firm. Journal of political economy, 88(2), 288-307 (1980). Per un'applicazione della teoria all'Internal Audit vedasi inoltre Adams, M. B. Agency Theory and the Internal Audit. Managerial Auditing Journal, Vol. 9 No 8, pp.8-12 MCB University Press 1994

40 Ad es. garantendosi benefit eccessivamente elevati a discapito dei proprietari delle risorse economiche che sono stati chiamati ad amministrare.

41 Christofer J., Sarens G., Leung P., A critical analysis of the independence of the Internal Audit function: evidence from Australia, Accounting, Auditing & Accountability Journal, Vol. 22 No. 2, pp.200-220 2009.



Se dunque la Funzione dell'Internal Audit è quella di tutelare gli interessi dei principali rispetto all'operato degli agenti, la loro indipendenza è un elemento imprescindibile.

Secondo la letteratura professionale, il ruolo dell'IA nella *governance* del settore pubblico è quello di ridurre i rischi inerenti in una relazione “mandante” – “rappresentante”. In base a tale tesi, “i funzionari pubblici – operando come rappresentanti del mandante – devono periodicamente rendere conto al mandante circa le modalità con cui hanno utilizzato e amministrato le risorse e in che misura gli obiettivi sono stati conseguiti⁴².

La ricerca accademica si è anche interrogata su una chiara definizione di indipendenza dell'Auditor. Utilizzando un modello principale-agente, Antle⁴³ definisce un Auditor (agente) indipendente quando decide autonomamente la sua strategia di azione rispetto al proprietario dell'organizzazione (principale). Sulla stessa linea, Simunic⁴⁴ argomenta che ogni situazione che alteri gli incentivi dell'Auditor in modo che egli sia più incline ad ignorare o occultare le risultanze del suo lavoro, rappresenta una diminuzione dell'indipendenza dell'Auditor. Tuttavia, la definizione del concetto di indipendenza rimane tuttora ambiguo e non chiaramente definito.

A fine di avere una visione più chiara e completa del concetto di indipendenza dell'Internal Auditor, si ritiene peraltro necessario fare riferimento alla letteratura professionale e alla normativa di settore. Bisogna quindi individuare i principali fattori che influenzano l'indipendenza, analizzare i modelli organizzativi che possano garantirla e definire gli strumenti che permettano di valutarne il livello per individuare e attuare eventuali interventi correttivi.

Indipendenza organizzativa

A dimostrazione dell'importanza dell'argomento, all'indipendenza organizzativa sono dedicati due *standard* di connotazione nel framework professionale emanato dall'*Institute of Internal Auditors*: il 1110 - Indipendenza Organizzativa e il 1130 - Condizionamenti dell'indipendenza o dell'obiettività.

Indipendenza organizzativa 1110: il Responsabile Internal Auditing deve riportare a un livello dell'organizzazione che consenta all'attività di Internal Audit il pieno adempimento delle proprie responsabilità. Il Responsabile Internal Auditing deve confermare al *Board*, almeno una volta l'anno, lo stato di indipendenza organizzativa dell'attività di Internal Audit.

Condizionamenti dell'indipendenza o dell'obiettività 1130: se indipendenza od obiettività sono compromesse sostanzialmente o apparentemente, le circostanze dei condizionamenti devono essere rese note ad appropriati interlocutori. La natura dell'informativa dipende dal tipo di condizionamento.

La ricerca accademica ha individuato alcuni fattori che influenzano negativamente il livello di indipendenza organizzativa dell'Internal Auditor.

Alcuni autori hanno cercato di studiare l'indipendenza della Funzione di Internal Audit mediante un'analisi empirica, analizzando le relazioni intercorrenti con il *management* e con il Comitato di Audit⁴⁵.

Tale ricerca ha individuato come possibile minaccia all'indipendenza le linee di reporting della Funzione di Internal Audit, qualora queste non

42 Il Ruolo dell'Auditing nella Governance del Settore Pubblico.

43 Antle, R. (1984). Auditor independence. *Journal of accounting research*, Vol. 22, No. 1, pp. 1-20.

44 Simunic, D. A. (1984). Auditing, consulting, and Auditor independence. *Journal of Accounting Research*, Vol. 22, No. 2, pp. 679-702.

45 Christofer J., Sarens G., Leung P., op cit.



siano conformi alle *best practices* che prevedono un riporto funzionale al Comitato di Audit (od organismo analogo) e amministrativo alla più alta carica esecutiva (ad es. Chief Executive Officer, Amministratore Delegato etc.).

Come seconda possibile minaccia è stata individuata composizione e competenze del Comitato di Audit. I membri, infatti, sono tenuti a possedere collettivamente le conoscenze tecniche, le capacità e l'esperienza per comprendere ed esercitare un'adeguata "*challenging*" sul lavoro svolto dalla Funzione di Internal Audit.

La terza minaccia attiene al potere di nominare, confermare e licenziare il RIA, che dovrebbe essere assegnato al predetto Comitato di Audit piuttosto che a cariche aziendali esecutive (ad es. *Chief Executive Officer*, Amministratore Delegato).

I fattori che influenzano l'indipendenza

Il concetto di indipendenza è un tema che non attiene esclusivamente alla collocazione organizzativa e alle linee di riporto della funzione, ma pervade tutti gli aspetti dell'attività di Audit. Di seguito si propone una lettura guidata degli *Standard* professionali IIA per evidenziare aspetti che possono avere un impatto indiretto sull'indipendenza della Funzione di Audit.

Competenza (*Standard 1200*)

L'indipendenza è condizionata dalla competenza⁴⁶: se l'Internal Auditor non ha conoscenze adeguate sulla materia oggetto di Audit, non può applicare uno spirito critico nel valutare le informazioni acquisite dalle unità di *business* sottoposte ad revisione.

Tale principio non richiede che l'Auditor debba possedere lo stesso livello di conoscenza del *business*, ma il grado necessario per poter svolgere efficacemente l'incarico di Audit.

Il rapporto tra competenza e indipendenza è stato studiato in letteratura soprattutto con riguardo alla revisione del reporting finanziario. Si giunge alla conclusione che indipendenza e competenza sono strettamente correlate: "l'effetto della competenza (indipendenza) dell'Internal Auditor sulla qualità del reporting finanziario dipende dalla sua indipendenza (competenza)"⁴⁷. Nello specifico, la letteratura mostra che la contemporanea presenza di indipendenza e competenza rappresenta una condizione necessaria per garantire un efficace monitoraggio del reporting finanziario da parte della Funzione di Internal Audit.

Gli *Standard* prevedono che qualora gli Internal Auditor non possiedano le conoscenze e le competenze necessarie per lo svolgimento di tutto o di parte dell'incarico, il RIA dovrebbe reperirle, internamente o esternamente⁴⁸. Tale previsione rafforza ancora di più il requisito imprescindibile per lo svolgimento di un incarico, sia esso di

46 1200 - Competenza e diligenza professionale: Gli incarichi devono essere effettuati con la dovuta competenza e diligenza professionale.
1210 - Competenza: Gli Internal Auditor devono possedere le conoscenze, capacità e altre competenze necessarie all'adempimento delle loro responsabilità individuali. L'attività di Internal Audit nel suo insieme deve possedere o dotarsi delle conoscenze, capacità e altre competenze necessarie all'esercizio delle proprie responsabilità.

Interpretazione:

Il termine competenza si riferisce complessivamente alle conoscenze, capacità e altre caratteristiche richieste agli Internal Auditor per adempiere efficacemente alle proprie responsabilità professionali. Questo include la valutazione della situazione attuale, dei trend e delle tematiche emergenti, allo scopo di consentire la formulazione di pareri e raccomandazioni pertinenti. Gli Internal Auditor sono incoraggiati a dimostrare la propria competenza conseguendo le opportune certificazioni e qualifiche professionali, come quella di "Certified Internal Auditor" e altre certificazioni rilasciate da "The Institute of Internal Auditors" e da altri organismi professionali riconosciuti.

47 Lawrence J. Abbott, Brian Daugherty, Susan Parker and Gary F. Peters Internal Audit Quality and Financial Reporting Quality: the joint importance of independence and competence - Journal of Accounting Research Vol. 54 No. 1 March 2016.

48 1210.A1 - Il Responsabile Internal Auditing deve dotarsi di opportuna assistenza e consulenza se gli Internal Auditor non possiedono le conoscenze, le capacità o altre competenze necessarie per lo svolgimento di tutto o di parte dell'incarico.



assurance o di consulenza: la conoscenza adeguata dell'oggetto della revisione.

A tal fine, alcune organizzazioni hanno introdotto programmi di rotazione delle risorse dall'Internal Audit alle funzioni di *business* e viceversa: in questa maniera la funzione è in grado di acquisire (internamente) competenze di *business* e allo stesso tempo di rilasciare nell'organizzazione conoscenze sul sistema dei controlli e di gestione dei rischi, in un connubio ad alto valore sinergico che genera un impatto positivo, da un lato sul livello di precisione e di utilità dei *findings* formulati dalla Funzione di Internal Audit e, dall'altro, sul grado di accettazione delle raccomandazioni da parte delle unità di *business*.

Peraltro, se da un lato i programmi di rotazione possono essere molto efficaci per consentire all'Internal Audit di raggiungere un livello di competenze adeguato, dall'altro richiedono una maggiore attenzione all'impatto che essi potrebbero avere sull'indipendenza dell'Auditor per la possibile comparsa di conflitti di interessi, attuali e potenziali. Essi potrebbero derivare dalla volontà dell'Auditor di cambiare ruolo e magari cercare una nuova opportunità professionale presso la struttura oggetto di revisione oppure dai legami che l'Auditor proveniente dall'unità di *business* possiede con la struttura di provenienza. In entrambi i casi, responsabilità del RIA è quella di assicurare con opportuni meccanismi ad es. di supervisione, di rotazione, di pianificazione, la mitigazione dei rischi derivanti da tali conflitti, per mantenere sempre un livello di obiettività e indipendenza adeguati.

Aggiornamento professionale continuo (Standard 1230)

Un adeguato livello di conoscenza deve essere non solo posseduto, ma anche mantenuto mediante un aggiornamento professionale continuo⁴⁹. L'aggiornamento professionale continuo richiede

risorse economiche e programmi di formazione e sviluppo. Un budget limitato o insufficiente potrebbe quindi impedire il raggiungimento del mix di conoscenze e competenze desiderato (e necessario), riducendo la capacità di svolgere con sufficiente autonomia di giudizio gli incarichi di Audit.

Pianificazione annuale degli incarichi (Standard 2010)

Lo *standard* prevede che “il Responsabile Internal Auditing deve predisporre un piano basato sulla valutazione dei rischi al fine di determinare le priorità dell'attività di Internal Audit in linea con gli obiettivi dell'organizzazione”.

L'interpretazione dello *standard*, formulata dall'IIA, suggerisce che per predisporre un piano *risk-based*, il Responsabile Internal Auditing deve consultarsi con il *senior management* e il *Board* per comprendere le strategie, i principali obiettivi di *business*, i rischi e i relativi processi di gestione. Il Responsabile Internal Auditing ha anche la responsabilità di rivedere sistematicamente tale piano per poterlo adeguarlo, laddove necessario, in risposta a eventuali cambiamenti intervenuti a livello di attività, rischi, operatività, programmi, sistemi e controlli dell'organizzazione.

A fini dell'indipendenza, la consultazione con il *senior management* può nascondere diverse insidie. Infatti, in assenza di fonti alternative, l'Internal Auditor potrebbe formulare un piano su informazioni parziali o incoerenti, inducendo l'esclusione di alcune aree o lo slittamento nel tempo di alcuni interventi. Il *senior management* potrebbe, ad esempio, confutare l'opportunità di un Audit adducendo argomentazioni legate ad attività in corso di svolgimento, sviluppi futuri, incompatibilità dei tempi, di fatto condizionando il RIA nella pianificazione degli Audit.

49 Standard 1230 - Aggiornamento professionale continuo: gli Internal Auditor devono migliorare le proprie conoscenze, capacità e altre competenze attraverso un aggiornamento professionale continuo.



I ricercatori Christofer, Sarens e Leung hanno confermato tali insidie, studiano l'atteggiamento di alcuni *top manager* che forniscono input al piano di Audit⁵⁰.

Assegnazione delle risorse per l'incarico (Standard 2230)

Il tema delle competenze ritorna anche nello *standard* di prestazione sull'assegnazione delle risorse all'incarico (2230) che ne definisce l'adeguatezza come "*l'insieme di conoscenze, capacità e altre competenze necessarie per dare esecuzione all'incarico*". Al concetto di competenza si aggiunge quindi anche quello di adeguatezza quantitativa delle risorse a disposizione. La scarsità di risorse potrebbe infatti impedire di raggiungere gli obiettivi dell'incarico nei tempi stabiliti, e quindi obbligare gli Auditor a limitare le analisi e/o a fare affidamento su analisi svolte dal business, con evidente impatti sull'indipendenza.

Svolgimento dell'incarico (Standard 2300)

Minacce all'indipendenza possono manifestarsi anche nella fase di svolgimento dell'incarico. Lo *standard* 2300 prevede infatti che l'Auditor corrobora le sue conclusioni con informazioni sufficienti, affidabili, pertinenti e utili⁵¹. A tal fine, l'Auditor deve aver accesso (indipendente e illimitato) a dette informazioni per svolgere in piena autonomia le analisi necessarie per raggiungere gli obiettivi dell'incarico di Audit.

Laddove non sia garantito un accesso autonomo per l'Internal Auditor, ma le informazioni siano acquisite per il tramite delle funzioni di *business*, si possono annidare pericoli per l'indipendenza dovuti a incompletezze, ritardi o impossibilità di lettura/interpretazione delle informazioni.

Per mitigare tali rischi può essere utile introdurre meccanismi che svincolino la proprietà dell'informazione e dei dati da chi effettivamente li genera all'interno dell'organizzazione, a vantaggio non solo dell'Internal Audit ma di una maggiore integrazione dei flussi informativi aziendali.

Outsourcing della Funzione di Internal Audit

Per garantire la piena efficacia della Funzione di Internal Audit, è indispensabile possedere il mix adeguato di competenze e conoscenze, per fornire servizi di Audit in linea con le aspettative degli stakeholder.

Garantire tale mix significa investire risorse ingenti per reclutare il personale, per formarlo e svilupparlo: risorse che non tutte le organizzazioni sono in grado di sostenere. Una possibile soluzione, soprattutto per le organizzazioni più piccole, è rappresentata dall'esternalizzazione (*outsourcing*) della Funzione di Internal Audit. La scelta di esternalizzare la Funzione di Revisione Interna è strettamente legata alla teoria dell'agenzia⁵² e più nello specifico alla teoria dei costi di

50 Christofer J., Sarens G., Leung P., op.cit.

51 2300 - Svolgimento dell'incarico Gli Internal Auditor devono raccogliere, analizzare, valutare e documentare informazioni sufficienti al raggiungimento degli obiettivi dell'incarico.

2310 - Raccolta delle informazioni

Gli Internal Auditor devono raccogliere informazioni sufficienti, affidabili, pertinenti e utili per conseguire gli obiettivi dell'incarico.

Interpretazione:

Le informazioni sono sufficienti quando sono concrete, adeguate e convincenti, così che, in base a esse, qualunque persona prudente e informata giungerebbe alle stesse conclusioni dell'Auditor. Le informazioni sono affidabili quando sono le migliori ottenibili attraverso l'uso di tecniche adeguate all'incarico. Le informazioni sono pertinenti quando sono coerenti con gli obiettivi dell'incarico e danno fondamento ai rilievi e alle raccomandazioni. Le informazioni sono utili quando aiutano l'organizzazione a raggiungere le proprie finalità.

52 Per maggiori informazioni si veda Fama, E. F. (1980). Agency problems and the theory of the firm. *Journal of political economy*, 88(2), 288-307.



transazione⁵³. Il mantenimento della funzione all'interno del perimetro dell'organizzazione rappresenta un meccanismo contrattuale che *permette il monitoraggio del management* da parte del *principal*. La scelta di mantenere all'interno dell'organizzazione l'Internal Audit, rende infatti soggetta questa funzione ad un controllo gerarchico interno all'organizzazione. Con *l'outsourcing* si fa affidamento alla disciplina di mercato, rinunciando alla dimensione del controllo gerarchico⁵⁴.

Tuttavia, esternalizzare (anche parzialmente) la Funzione di Audit potrebbe avere un impatto significativo sull'indipendenza dell'attività. Recenti studi accademici peraltro evidenziano che i principali vantaggi dell'esternalizzazione includono un più alto livello di indipendenza percepita, maggiore flessibilità, riduzione dei costi e un miglioramento della qualità della revisione interna⁵⁵. Nel caso concreto, tuttavia, il grado di esternalizzazione ottimale dipende da varie caratteristiche dell'organizzazione e delle attività svolte dalla Funzione di Revisione Interna fra cui: le dimensioni dell'organizzazione, il costo da sostenere per l'esternalizzazione, le soluzioni di *outsourcing* offerte dal mercato e la complessità delle attività che si intende esternalizzare⁵⁶. Non ultimo, a queste caratteristiche, si deve aggiungere l'indipendenza quale *driver* fondamentale per garantire l'efficacia della Funzione di Audit esternalizzata.

Le limitazioni consentite all'indipendenza (standard 1112) – altri ruoli del RIA

L'ultima revisione degli IPPF del 2017 ha introdotto lo Standard 1112 che, se da un lato consente delle deroghe al principio di indipendenza, dall'altro impone misure di tutela per limitarne i condizionamenti. Lo Standard recita infatti così: "Laddove il Responsabile Internal Auditing abbia, o si prevede abbia, ruoli e/o responsabilità che esulano dall'Internal Auditing, devono essere poste in essere opportune misure di tutela atte a limitare i condizionamenti all'indipendenza o all'obiettività".

Secondo l'interpretazione degli Standard "al Responsabile Internal Audit possono essere richiesti ruoli e responsabilità aggiuntive che esulano dall'Internal Auditing, come ad esempio la responsabilità per attività di *Compliance* o *Risk Management*. Tali ruoli e responsabilità possono condizionare, anche solo apparentemente, l'indipendenza organizzativa dell'attività di Internal Audit o l'obiettività individuale dell'Internal Auditor. Le misure di tutela sono quelle attività di supervisione, spesso intraprese dal *Board*, atte a indirizzare questi potenziali condizionamenti e possono comprendere attività come la valutazione periodica delle linee di riporto e delle responsabilità e lo sviluppo di processi alternativi per ottenere *l'assurance* sulle aree di responsabilità aggiuntive".

L'evoluzione organizzativa e normativa degli ultimi anni ha visto nascere nuove funzioni aziendali che, per il loro carattere di trasversalità e la necessità di terzietà rispetto al *business*, spesso sono state assegnate al Responsabile dell'Internal Audit, con riflessi negativi sulla piena indipendenza della funzione stessa. Nel prossimo paragrafo sono elencati alcuni di questi ruoli.

53 Williamson, O. E. (1979). Transaction-cost economics: the governance of contractual relations. *The Journal of Law and Economics*, 22(2), 233-261.

54 Spekle, R. F., Van Elten, H. J., & Kruijs, A. M. (2007). Sourcing of Internal Auditing: An empirical study. *Management Accounting Research*, 18(1), 102-124.

55 Barr R.H. and Chang S.Y., (1992). Outsourcing Internal Audits: A Boon or Bane? *Managerial Auditing Journal*, 8(1), 700-713.

56 Per maggiori informazioni si veda Spekle (2007, op. cit.).





4. Ruoli aggiuntivi del Responsabile Internal Audit

(a cura di M. Artemi e V. Numerico)

Responsabile Prevenzione Corruzione e Trasparenza

La figura del Responsabile Prevenzione Corruzione e Trasparenza (RPCT) è stata istituita dalla Legge 6 novembre 2012, n. 190 che stabilisce che ogni amministrazione/ente/società⁵⁷ approvi un Piano triennale della Prevenzione della Corruzione che valuti il livello di esposizione degli uffici al rischio e indichi gli interventi organizzativi necessari per mitigarlo. La predisposizione e la verifica dell'attuazione di detto Piano sono attribuite a un Responsabile della Prevenzione della Corruzione e della Trasparenza.

Quindi la nomina del RPCT è prevista in tutte le Pubbliche amministrazioni, nonché nei seguenti soggetti:

- enti pubblici economici e agli ordini professionali;
- società in controllo pubblico come definite dall'articolo 2, comma 1, lettera m), del decreto legislativo 19 agosto 2016, n. 175.

Sono escluse le società quotate come definite dall'articolo 2, comma 1, lettera p), dello stesso decreto legislativo, nonché le società da esse partecipate, salvo che queste ultime siano, non per il tramite di società quotate, controllate o partecipate da amministrazioni pubbliche;

- associazioni, fondazioni e enti di diritto privato comunque denominati, anche privi di personalità giuridica, con bilancio superiore a cinquecentomila euro, la cui attività sia finanziata in modo maggioritario per almeno due esercizi finanziari consecutivi nell'ultimo triennio da pubbliche amministrazioni e in cui la totalità dei titolari o dei componenti dell'Organo d'Amministrazione o di indirizzo sia designata da pubbliche amministrazioni.

La previsione di tale nuova istanza di controllo ha posto problemi di coordinamento con gli Organi deputati ai controlli interni già presenti nella P.A. e negli altri soggetti sopra indicati.

L'art 1, co. 7, della L. 190/2012, stabilisce che il RPCT è individuato dall'organo di indirizzo, di norma tra i dirigenti di ruolo in servizio, disponendo le

⁵⁷ In tale accezione sono ricomprese le pubbliche amministrazioni di cui all'articolo 1, comma 2, del D. Lgs. n. 165/2001, ai fini dell'adozione dei propri piani triennali di prevenzione della corruzione, e tutti gli altri soggetti di cui all'articolo 2-bis, comma 2, del D. Lgs. n. 33/2013, ai fini dell'adozione di misure di prevenzione della corruzione integrative di quelle adottate ai sensi del D. Lgs. n. 231/2001.



eventuali modifiche organizzative necessarie per assicurare funzioni e poteri idonei per lo svolgimento dell'incarico con piena autonomia ed effettività.

Nelle società e negli enti di diritto privato in controllo pubblico, tale scelta è rimessa all'organo di indirizzo della società/ente, Consiglio di Amministrazione o altro organo con funzioni equivalenti.

L'ANAC (Autorità Nazionale Anticorruzione) ha evidenziato, nel Piano Nazionale Anticorruzione del 2019 e nelle specifiche Linee guida pubblicate per le società e gli enti di diritto privato⁵⁸, che le funzioni di RPCT debbano essere svolte da un dirigente in servizio della società, stante il divieto, stabilito all'art. 1, co. 8, della l. 190/2012, di affidare l'attività di predisposizione del PTPCT a soggetti estranei all'amministrazione.

Nei casi in cui, per le ridotte dimensioni o per la scarsa presenza di dirigenti, non risultasse praticabile tale opzione, può essere nominato un dipendente non dirigente ma con idonee competenze (in tale caso è necessario motivare adeguatamente la scelta). In casi eccezionali può essere individuato quale RPCT un dirigente esterno (onere di congrua e analitica motivazione) o un amministratore privo di deleghe (nelle società/ente di diritto privato).

Negli enti locali, per specifica disposizione legislativa (art. 1, co. 7, l. 190/2012) il RPCT è individuato, di norma, nel segretario o nel dirigente apicale, salvo diversa e motivata determinazione. Nella prassi la nomina del segretario è la scelta più frequente anche se pone non pochi problemi relativamente al contemporaneo svolgimento di compiti gestionali.

Per quanto riguarda le unioni di comuni, è prevista la possibilità di nominare un unico Responsabile.

Indipendenza e autonomia

Il RPCT può esercitare con effettività le sue funzioni solo:

- in presenza di un elevato grado di autonomia e indipendenza;
- di un profilo integerrimo (ovvero non essere stato destinatario di provvedimenti giudiziari di condanna, né di provvedimenti disciplinari).

La L. 190/2012 non fornisce specifiche indicazioni sui requisiti soggettivi necessari per essere nominati RPCT. L'Autorità ha finora ritenuto che il RPCT debba essere selezionato tra quei soggetti che abbiano dato dimostrazione nel tempo di comportamento integerrimo e non siano stati destinatari di provvedimenti giudiziari di condanna, né di provvedimenti disciplinari.

Considerata la posizione di autonomia che deve essere assicurata al RPCT, e il ruolo di garanzia sull'effettività del sistema di prevenzione della corruzione, non appare coerente con i requisiti di legge la nomina di un dirigente che provenga direttamente da uffici di diretta collaborazione dell'organo di indirizzo, laddove esista un vincolo fiduciario.

Va evitato, per quanto possibile, che il RPCT sia scelto tra i dirigenti assegnati a uffici che svolgono attività nei settori più esposti al rischio corruttivo, come l'ufficio contratti o quello preposto alla gestione del patrimonio. In ogni caso la scelta è rimessa all'autonoma determinazione degli organi di indirizzo di ogni ente o amministrazione.

⁵⁸ Delibera n. 1064 del 13 novembre 2019 "PNA 2019" e delibera n. 1134 dell'8 novembre 2017 "Nuove linee guida per l'attuazione della normativa in materia di prevenzione della corruzione e trasparenza da parte delle società e degli enti di diritto privato controllati e partecipati dalle pubbliche amministrazioni e degli enti pubblici economici".



Compiti e Poteri del RPCT

Il RPCT svolge, nello specifico, le seguenti principali attività:

- predispone e sottopone il PTPCT all'Organo di indirizzo politico, ai fini della sua adozione entro il 31 gennaio di ogni anno;
- definisce procedure appropriate per selezionare e formare i dipendenti operanti in settori particolarmente esposti alla corruzione;
- verifica l'efficace attuazione del piano e la sua idoneità (incluso il monitoraggio sull'adempimento da parte dell'amministrazione degli obblighi di pubblicazione), nonché propone la modifica dello stesso (in caso di significative violazioni delle prescrizioni o di mutamenti nell'Organizzazione o nell'attività dell'amministrazione);
- verifica, di concerto con il Dirigente competente, dell'effettiva rotazione degli incarichi negli uffici preposti allo svolgimento delle attività nel cui ambito è più elevato il rischio di corruzione;
- individua il personale da inserire nei programmi di formazione;
- segnala all'organo di indirizzo, all'OIV, all'ANAC o all'ufficio di disciplina, le disfunzioni nell'attuazione delle misure in materia di prevenzione della corruzione e trasparenza;
- riceve e prende in carico le segnalazioni, attuando gli atti necessari ad una prima attività di verifica e di analisi delle segnalazioni ricevute (*whistleblowing*).

Membro interno dell'Organismo di Vigilanza

Il D.Lgs. 231/2001 introduce la responsabilità amministrativa per società, enti e organizzazioni, con o senza personalità giuridica. Per la prima volta nell'ordinamento italiano è prevista la responsabilità delle aziende per reati posti in essere da Amministratori, Dirigenti e/o Dipendenti nell'interesse o a vantaggio dell'azienda stessa.

Tale normativa, in vigore dal 4 luglio 2001, ha introdotto nell'ordinamento italiano, in conformità a quanto previsto anche a livello europeo, un nuovo regime di responsabilità denominata "da reato", derivante dalla commissione o tentata commissione di determinate fattispecie di reato nell'interesse o a vantaggio degli enti stessi.

Tra i reati compresi nel Decreto i più significativi sono quelli ai danni della sicurezza dei lavoratori, dell'ambiente, societari (false comunicazioni sociali, indebita restituzione conferimenti), nei confronti della pubblica amministrazione (truffa e corruzione). L'elenco dei reati che possono originare la responsabilità delle aziende è in continuo aggiornamento e ampliamento.

L'art. 6 del D. Lgs. 231/2001 richiede, in particolare, quale condizione per beneficiare dell'esimente dalla responsabilità amministrativa, che l'ente sia esonerato dalla responsabilità amministrativa nel caso sia in grado di provare di aver adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione (di seguito anche il «Modello») idonei a prevenire reati della specie di quello verificatosi; aver istituito un organo di controllo interno all'ente, dotato di autonomi poteri di iniziativa e di controllo, con il compito di vigilare sull'efficacia reale del Modello



(Organismo di Vigilanza, oppure OdV); in caso di reato vi sia stata la violazione fraudolenta del Modello da parte degli autori del reato; l'OdV, e gli altri soggetti incaricati della gestione e del controllo, abbiano operato con la necessaria diligenza.

Tale organismo, nominato dall'organo dirigente dell'ente, deve soddisfare i tre requisiti elaborati, in prima battuta, dalle linee guida delle principali associazioni rappresentative degli enti e successivamente confermati anche nei pronunciati di giurisprudenza, e segnatamente: autonomia ed indipendenza, professionalità, continuità d'azione.

Il Decreto non fornisce indicazioni specifiche in ordine alla composizione dell'Organismo di Vigilanza, limitandosi a richiedere che detto organismo sia interno all'ente e dotato di autonomi poteri di iniziativa e di controllo. Nel silenzio normativo, le associazioni rappresentative degli enti hanno rimesso all'ente la scelta relativa composizione dell'organismo, in forma monocratica o collegiale avendo riguardo alla dimensione e alla complessità organizzativa dell'ente stesso.

Le funzioni riservate dal D.Lgs.231/2001 all'OdV, posso riassumersi nei seguenti compiti di vigilanza:

- osservanza delle prescrizioni del Modello da parte dei destinatari, in relazione alle diverse tipologie di reati;
- reale efficacia ed effettiva capacità del Modello, in relazione alla struttura aziendale, di prevenire la commissione di reati e di illeciti;
- opportunità di aggiornamento del Modello, laddove si riscontrino esigenze di adeguamento dello stesso in relazione a mutate condizioni aziendali e/o eventuali modifiche normative;

- verifica dell'adozione di opportune iniziative finalizzate alla divulgazione e conoscenza del Modello e alla formazione e sensibilizzazione del personale sull'osservanza delle norme.

A differenza della L. 190/2012 che ha tratto ispirazione dal D.lgs. 231/2001 e ha specificato i requisiti soggettivi del RPCT, il Decreto non fornisce indicazione in merito ai requisiti personali dei membri, composizione, ecc. dell'OdV.

A tale mancanza di indicazioni, hanno sopperito negli anni le principali associazioni di categoria (Confindustria, Associazione dei componenti degli OdV, ecc.) che hanno pubblicato linee guida, paper, ecc. che danno indicazioni in tale ambito.

In particolare, le Linee Guida Confindustria per la costruzione dei modelli di organizzazione, gestione e controllo ai sensi del D. Lgs. n. 231/2001. hanno precisato alcuni aspetti specifici dell'Organismo di Vigilanza relativi a poteri e requisiti, autonomia ed indipendenza, professionalità e continuità d'azione.

In merito all'articolazione e composizione dell'Organismo di Vigilanza (monosoggettivo o plurisoggettivo) le Linee guida e la prassi consolidata, evidenziano che essa è direttamente correlata alla complessità strutturale dell'impresa (dimensioni, articolazione interna, dislocazione sul territorio, presenza su determinati mercati particolarmente a rischio, ecc.). In effetti non è possibile fissare limiti quantitativi, né in termini di fatturato, né di numero di dipendenti dell'impresa interessata, la complessità dell'organismo di controllo va infatti valutata caso per caso a seconda dei risultati dell'analisi dei rischi, dalla quale emergano quante aree, processi, funzioni devono essere assoggettate a controllo.

In linea generale, anche sulla base dell'esperienza applicativa finora maturata, è stato rilevato che le società di medio-grandi dimensioni si



orientano generalmente verso una composizione di tipo collegiale, che, nelle maggiori imprese italiane, risulta quello privilegiato, con ricorso a professionisti esterni di un certo “spessore”, affiancati a personale interno qualificato non operativo, in modo tale da garantire autonomia e professionalità.

Le realtà di più piccole dimensioni, invece, tendono ad optare per organismi monocratici, avvalendosi di un professionista esterno. La scelta di un membro interno, infatti, nel caso di OdV composto da un solo soggetto, lederebbe il requisito di autonomia e indipendenza, come più volte sottolineato dalla giurisprudenza.

Dai risultati di una recente indagine “D.Lgs. 231/01 Indagine nell’ambito delle società quotate – 13a edizione», condotta nel 2020 da Pricewaterhousecoopers (PWC) su un campione di 221 società, emergono aspetti che confermano tali tendenze⁵⁹.

In particolare, tale indagine ha evidenziato che circa il 93% delle società quotate campionate ha optato per una composizione collegiale dell’Organismo di Vigilanza, confermando in tale caso la presenza del Responsabile Internal Auditing tra i membri interni dell’OdV, nel 45% dei casi.

La composizione dell’OdV collegiale

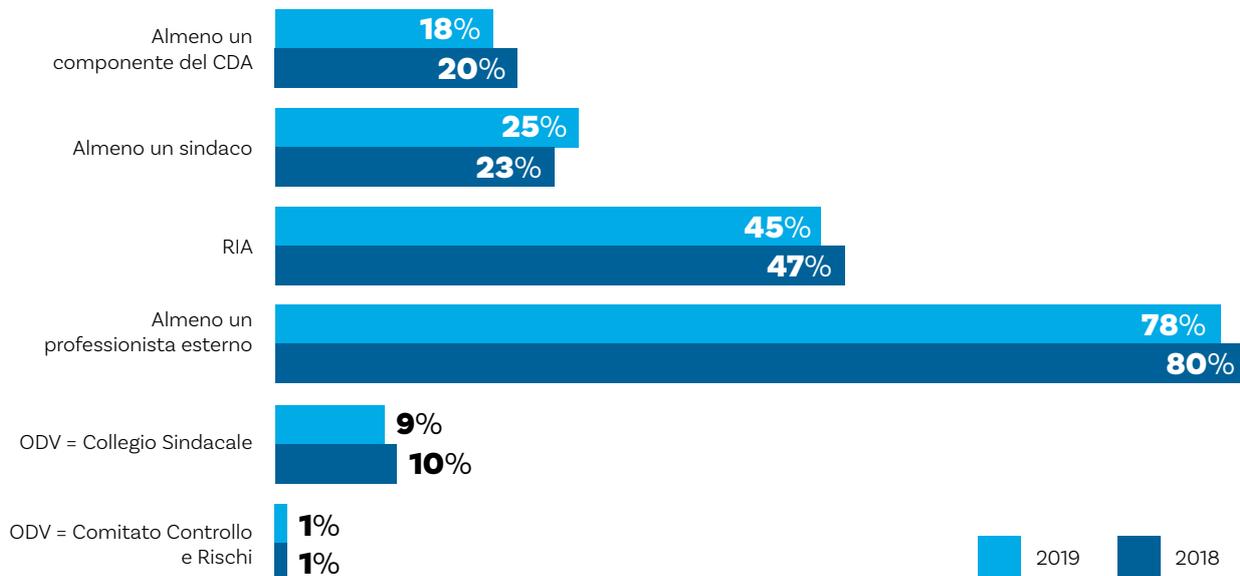


Figura 2 D.Lgs. 231/01 Indagine nell’ambito delle società quotate 2020- 13a edizione, Pricewaterhousecoopers (PWC)

59 Pwc: D.Lgs. 231/01 Indagine nell’ambito delle società quotate Anno 2020 - 13a edizione <https://www.pwc.com/it/it/services/risk-assurance/assets/docs/dlgs231-2021.pdf>.



Altri ruoli della seconda linea

Tra le funzioni tipiche della seconda linea possono essere incluse:

- la Funzione di Gestione dei Rischi (*Risk Management*) che facilita e monitora l'implementazione di regole efficaci di gestione dei rischi da parte del *management* operativo, supporta i process owner dei rischi nella definizione dei livelli di esposizione al rischio e riferisce informazioni adeguate riguardanti il rischio in tutta l'organizzazione" [IIA, 2013];
- la Funzione di *Compliance*, per monitorare vari rischi specifici connessi all'inosservanza delle leggi e dei regolamenti applicabili all'organizzazione. Spesso in una sola organizzazione coesistono numerose funzioni di *compliance*, che sono responsabili del monitoraggio della *compliance* di specifici rischi, quali la salute e sicurezza, la supply chain, il monitoraggio ambientale o della qualità [IIA, 2013];
- una Funzione di Controllo Interno che supporta il *management* nell'identificazione dei rischi più significativi di ciascun processo e nella definizione e attuazione dei controlli preventivi e correttivi volti a mitigare i rischi individuati;
- etica aziendale e tutela aziendale: funzioni con professionisti che si concentrano sulla comunicazione e sulla erogazione di formazione sul codice di condotta dell'azienda, sulla supervisione del processo di segnalazione (*whistleblowing*) e sulla promozione della consapevolezza sulle tematiche connesse alle frodi. Un team di specialisti può essere dedicato al follow-up su potenziali casi di frode.

Sotto quest'ultimo profilo e soprattutto in realtà aziendali di medie/piccole dimensioni, ove il rischio frode risulta essere quasi sempre interno, la funzione dell'antifrode può difatti essere fatta rientrare in quella di Audit, con relativa responsabilità in capo al RIA e gestita con il medesimo approccio metodologico, rappresentando il *fraud Audit* una specifica tipologia di Audit.

Situazione ben diversa, invece, è quella che si riscontra in Enti o aziende di grandi dimensioni, generalmente erogatori di servizi, ove il rischio di frode esterna supera di gran lunga quello di frode interna. È il caso, ad esempio, di INPS che per il suo ruolo istituzionale di ente erogatore di prestazioni sociali di vario tipo, risulta spesso tra i soggetti passivi del reato di cui all'art. 640bis c.p.

In questi casi, la strada seguita già da qualche anno dall'Istituto Nazionale della Previdenza Sociale è stata quella di svincolare la funzione antifrode da quella di Audit, lasciando quest'ultima nell'esclusivo ambito del controllo di III livello, attribuendo invece all'antifrode una posizione "specialistica" e di intelligence all'interno dell'Ente, dotata pertanto di maggiore incisività, nonché di uno specifico *know-how* in tema di strategia di *fraud management*.

Le organizzazioni implementano queste funzioni per garantire che i processi e i controlli siano correttamente progettati, in atto e operino in modo efficace e per mitigare i rischi identificati.

Soprattutto nel settore non finanziario, quando non ci sono requisiti specifici del regolatore in relazione all'istituzione di funzioni specifiche e separate di gestione dei rischi e di *compliance*, le diverse attività possono essere spesso unite insieme.



Nella pratica, infatti, i confini tra le attività relative all'Internal Auditing, la gestione dei rischi e la compliance non sempre risultano così ben definiti.

In tali casi si pone l'interrogativo su come gestire correttamente tale situazione di commistione tra funzioni di seconda linea con l'Internal Audit e, in tal caso, come e in base a quali circostanze e condizioni questo può risultare accettabile e non lesivo dell'indipendenza e obiettività della stessa Funzione di Internal Auditing.

Le considerazioni gestionali (che possono indurre le organizzazioni a introdurre una integrazione delle funzioni sopra riportate) possono essere sintetizzati come segue:

- ottimizzazione dello *span of control*, ovvero la limitazione del numero di interlocutori che riferiscono al *Board* sulle attività di *assurance*;
- efficienza, in termini di controllo dei costi connessi alla prestazione di servizi di *assurance*, sicuramente più efficiente quando i diversi prestatori di attività di assicurazione sono integrati in un'unica funzione.

L'unione di queste funzioni potrebbe semplificare tale controllo, ridurre la duplicazione delle attività. Ciò può favorire la supervisione unificata del sistema di controllo, richiedendo l'utilizzo di un numero inferiore di risorse rispetto a una situazione nella quale le attività sono distribuite tra funzioni separate.

Se c'è separazione, il coordinamento tra le funzioni potrebbe risultare condizionato dalla volontà dei *manager* di collaborare, mentre sarebbe maggiormente garantito nell'ipotesi di riporto a una figura univoca di responsabile:

- ragioni storiche: l'organizzazione potrebbe essere il prodotto di sviluppi successivi; con le attività che risultano gradualmente ampliate e assegnate a un unico dipartimento/funzione;

- sinergia, ovvero creazione di forme di migliore collaborazione e cooperazione, riunendo le funzioni sotto un'unica responsabilità.

Ciò può comportare un approccio più olistico alle attività del GRC (*Governance, Risk Management e Compliance*) guidato da una visione condivisa. Inoltre, la visione e la strategia sarà eseguita da un gruppo di professionisti con mentalità e competenze simili e complementari. Questo potrebbe essere percepito dal *management* come più efficace di una separazione delle funzioni.

Inoltre, una funzione più ampia potrebbe facilitare la pianificazione dei percorsi di carriera delle risorse, poiché in uno staff più ampio possono essere offerte maggiori opportunità di sviluppo. Infine, la combinazione di diverse responsabilità in un unico ruolo di leadership potrebbe risultare maggiormente attrattivo per potenziali professionisti qualificati ed esperti.

Maturità: il ruolo dell'Internal Audit può anche dipendere dal livello di maturità non ancora ottimale dei processi e dei controlli dell'organizzazione. L'Internal Audit può svolgere un ruolo (temporaneo) di supporto nella progettazione delle metodologie e delle attività di GRC (*Governance, Risk Management e Compliance*) all'interno della propria organizzazione.

Sopra sono state elencate le motivazioni antitetiche alla netta separazione delle tre linee e alla segregazione delle attività svolte dalla Funzione di Revisione Interna. Vale la pena sottolineare che la letteratura professionale e i modelli di *governance* presentati nel capitolo 1 propendono per una indipendenza "piena" della Funzione di Internal Audit: qualora tale caratteristica non sia realizzabile nel breve termine, essa è comunque da intendersi come obiettivo a cui tendere.



Ulteriori figure di secondo livello

Il *Data Protection Officer* (di seguito DPO) è una figura introdotta dal GDPR (Regolamento generale sulla protezione dei dati 2016/679), pubblicato sulla Gazzetta Ufficiale europea L. 119 del 4 maggio 2016.

La norma prevede che tutti gli enti pubblici ed alcune categorie di aziende private nominino un soggetto qualificato che si occupi in maniera esclusiva della protezione dei dati personali, aggiornandosi sui rischi e le misure di sicurezza.

L'art. 39 del Regolamento europeo elenca i seguenti principali compiti del DPO:

- a.** informare e fornire consulenza al titolare del trattamento o al Responsabile del trattamento nonché ai dipendenti che eseguono il trattamento, in merito agli obblighi derivanti dal Regolamento, nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
- b.** sorvegliare l'osservanza del Regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del Responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- c.** fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;
- d.** cooperare con l'autorità di controllo;
- e.** fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento dei dati.

In relazione alle similitudini che contraddistinguono sia il RIA che il DPO (la necessaria indipendenza e autonomia nello svolgimento delle attività rispettive attività di verifica e monitoraggio; il ruolo di consulente; il riporto al Vertice dell'organizzazione; l'assenza di responsabilità operative; l'attività di verifica risk based; la possibilità di esternalizzazione dell'attività; ecc.), alcune organizzazioni hanno individuato il RIA anche come DPO (es. Enav Spa), oppure hanno inserito quest'ultimo all'interno della Funzione Internal Auditing (es. Poligrafico e Zecca dello Stato spa).

Tale scelta appare motivata dalla necessità di consentire al DPO di svolgere il proprio ruolo con la necessaria indipendenza e autonomia (che all'interno di altre Direzioni, ad esempio Legale, non sarebbero tali), nonché dalla possibilità di poter operare una integrazione delle rispettive attività di verifica sui processi che prevedono trattamenti di dati personali, evitando duplicazioni e oneri eccessivi nei processi di controllo, come già indicato per le altre funzioni di secondo livello (*compliance* e *risk manager*).

Condizioni e salvaguardie minime per l'indipendenza della funzione

Viene da chiedersi a questo punto se il ruolo del DPO, così come quello di *Compliance* e *Risk Management*, possa essere assolto dal RIA. È parere di chi scrive, che due figure non siano incompatibili per una serie di ragioni intrinseche nel ruolo del RIA, da un lato, e del DPO, del Responsabile *Compliance* e *Risk Management* dall'altro, sebbene debbano essere attuati alcuni meccanismi per non intaccare l'obiettività ed evitare conflitti di interesse tenendo



in considerazione anche le altre responsabilità attribuite/attribuibili allo stesso RIA (responsabilità in ambito D.Lgs. 231/01, *Risk Management*, Anticorruzione/RPC, attività legate alla *compliance*, etc.). Premettendo infatti che il ruolo del DPO è da considerarsi assimilabile ad un controllo di II livello, la necessità di autonomia e indipendenza sarebbero di certo assicurate dal RIA, laddove questo rispetti le prescrizioni degli *Standard* professionali e sia posto a diretto riporto del CdA, assicurando in tal modo anche il dialogo con il vertice. La familiarità con il tema dei rischi è essenziale per le diverse figure e le metodologie di *risk assessment* e di definizione di un piano delle verifiche *risk based* sono per tutte un presupposto per condurre la propria attività, in accordo con quanto richiesto dagli *Standard* di riferimento e dalle specifiche regolamentazioni (es. GDPR). Laddove sia necessario introdurre nel Piano di Audit, ad esempio, un intervento sul sistema della protezione dei dati nel suo complesso all'interno dell'organizzazione, sarà opportuno intervenire tramite, ad esempio, il ricorso ad interventi in *outsourcing* per garantire obiettività e indipendenza di giudizio.

Tuttavia, volendo evitare assegnazioni di funzioni in *outsourcing* anche in un'ottica di contenimento della spesa pubblica e nell'intento di preservare, al contempo, l'obiettività e l'indipendenza del RIA senza incorrere in situazioni di potenziale conflitto di interessi come quella riportata nell'esempio sopra menzionato, altra strada percorribile potrebbe essere quella di incardinare il DPO all'interno di Strutture, appositamente costituite e ricomprendenti altri controlli di secondo livello, quali *Risk Management* e *Compliance*. Tale *modus operandi* è stato scelto da INPS a seguito delle recenti azioni di manutenzione organizzativa di cui alla Deliberazione del CdA 137/2022.

Tale soluzione sembrerebbe infatti includere in modo più razionale le attività del DPO (aventi in realtà una natura mista di *assessment* e di *compliance*) tra quelle genericamente assimilabili alla valutazione e alla gestione dei rischi e ben concilierebbe l'esigenza di autonomia del DPO con l'indipendenza e l'obiettività dell'IA, titolare invece del controllo di III livello.





5. Valutare l'indipendenza e l'obiettività

(a cura di M. Proietti, A. Giorgini, F. Coppola)

La definizione di indipendenza e obiettività

In un sistema in continua evoluzione rispetto alle tematiche di *Corporate Governance*, gli Internal Auditors sono chiamati ad affrontare molti cambiamenti e diverse opportunità, tra i quali il complesso e pervasivo uso della tecnologia, la necessità di competenze nuove e in continuo mutamento, l'adozione di strutture organizzative meno gerarchiche, la domanda di servizi in via di espansione nonché la crescente competizione e globalizzazione delle organizzazioni in cui la funzione opera. La professione dell'Internal Auditor comporta, quindi, lo sviluppo di nuove strategie per cogliere questi mutamenti, l'adozione di approcci maggiormente proattivi nell'erogazione della vasta gamma di servizi, nonché una generale rivisitazione del modello di Internal Auditing. Al tempo stesso queste dinamiche, se da un lato rappresentano un'interessante opportunità di crescita professionale, dall'altro espongono la funzione a rischi di indipendenza e obiettività.

In considerazione della circostanza che le organizzazioni, sia del settore pubblico sia privato,

si stanno sviluppando in termini di dimensioni e influenza, si assiste a una crescente e generale esigenza di "accountability", un trend che aumenta il focus sulle attività di Auditing, come "pietra angolare" del sistema di governance.

In tale contesto assume rilevanza la definizione di un processo che gestisca i rischi di conformità agli standard internazionali della professione, valutando in particolare, attraverso un *framework* di riferimento, il rispetto dei requisiti di indipendenza e obiettività a livello individuale, di incarico di Audit, organizzativo e, infine, a livello professionale.

Un primo aspetto del processo di valutazione di indipendenza e obiettività è rappresentato dalla comprensione delle stesse definizioni, analizzando eventuali elementi di ambiguità o intercambiabilità nell'utilizzo dei diversi termini. L'aggiornamento degli Standard internazionali della professione, entrati in vigore a partire da gennaio 2017, ha chiarito e rafforzato le definizioni di "indipendenza" e "imparzialità", trattandosi di concetti estremamente differenti, nonché ha previsto la possibilità che il Responsabile Internal Auditing rivesta ruoli addizionali (Standard 1112).



In termini di misurazione, il requisito di indipendenza è maggiormente “valutabile” rispetto a quello dell’obiettività, tenuto conto che il primo è principalmente riferito alla Funzione/ Direzione Internal Auditing nella sua totalità, mentre il secondo è relativo essenzialmente alle modalità con cui ogni singolo Auditor assicura la responsabilità e il controllo nella conduzione della sua attività professionale.

Un modello di valutazione dell’indipendenza della Funzione Internal Auditing non può, quindi, prescindere da un’analisi congiunta degli aspetti che possono potenzialmente minare il requisito di obiettività, considerato che entrambi gli elementi assicurano la credibilità delle attività condotte e dei risultati emersi.

Indipendenza

Nel tenere in considerazione i fattori che impattano sull’indipendenza, occorre contestualizzare lo specifico ruolo che la Funzione di Internal Auditing riveste all’interno dell’organizzazione alla luce di fattori quali la dimensione dell’azienda, l’ambito di attività, la struttura societaria e l’ambiente normativo di riferimento. In alcune realtà, il lavoro degli Internal Auditor è confinato a progetti di “assurance” e “consulenza” per il *management*, mentre in altre il *management* è solo uno dei destinatari dell’attività di Auditing. In alcune realtà organizzative, inoltre, le attività di “assurance” e “consulenza” della funzione possono essere fornite a vari gruppi all’interno o all’esterno dell’organizzazione, quali ad esempio l’organo di governo (Consiglio di Amministrazione), organi di vigilanza o revisori esterni, clienti e fornitori. Lo specifico ruolo dell’attività dell’Internal Auditing all’interno dell’organizzazione ne determina sia l’appropriata struttura di responsabilità e il relativo livello di riporto gerarchico/funzionale, sia il grado di “affidabilità” atteso nei servizi di “assurance”

e “consulenza” erogati. In generale, quanto più è elevato il livello di riporto, tanto maggiore è l’ambito potenziale di incarichi che possono essere condotti dalla struttura di Internal Audit senza minare l’indipendenza rispetto alle entità destinatarie dell’attività di Audit.

Nel rivedere e valutare lo status organizzativo di una Funzione di Internal Auditing, l’organo di governo dovrebbe considerare i fattori che ne influenzano l’indipendenza, tra i quali:

- il livello di reporting del Chief Audit Executive (di seguito CAE) all’interno dell’organizzazione;
- l’accesso del CAE alle informazioni in tutta l’organizzazione e all’organo di governo;
- il processo decisionale di assunzione e/o rimozione del CAE e di emissione/approvazione del mandato di Internal Auditing, con eventuale coinvolgimento dell’organo di governo;
- le modalità di definizione del budget della funzione, del perimetro di attività (es. Piano di Audit), nonché la remunerazione e il mantenimento del CAE, con eventuale coinvolgimento dell’organo di governo;
- il coinvolgimento diretto, la supervisione, la revisione e il follow up dell’organo di governo nelle attività della Funzione Internal Auditing.

Questi fattori dovrebbero essere “contestualizzati” rispetto alle aspettative dell’organizzazione e di tutti gli stakeholders della funzione per comprendere il livello di *assurance* atteso dalle attività di Internal Auditing. Quando una Funzione Internal Auditing ha un sufficiente status organizzativo e un’adeguata autonomia, le parti interne ed esterne all’organizzazione stessa possono riporre maggiore fiducia sull’abilità della funzione di gestire le minacce di indipendenza rispetto al lavoro svolto. Analogamente, il CAE deve essere libero da ogni forma di significativa interferenza che



potrebbe influenzare la capacità del singolo Auditor nell'assumere decisioni indipendenti riguardo agli incarichi di Audit e alle attività di reporting.

Si riporta di seguito un elenco, esemplificativo seppur non esaustivo, di fattori di mitigazione e salvaguardia a presidio delle minacce di indipendenza della Funzione Internal Auditing in un'organizzazione.

Posizione organizzativa e policy: i ruoli dell'Auditor e della Funzione di Internal Auditing sono chiaramente definiti da un'adeguata posizione organizzativa, da un mandato formalizzato, da una politica aziendale ai vari livelli indirizzata alla gestione delle relazioni della funzione con i clienti interni, tutti elementi che rappresentano dei presidi interni rispetto a potenziali influenze e/o intimidazioni degli Auditor. Analogamente, concorrono a tal fine tutti quei documenti aziendali strumentali alla promozione dello status della Funzione Internal Auditing all'interno dell'organizzazione, quali il Codice Etico dell'organizzazione, il Mandato del Comitato per il controllo interno, la *mission* formalizzata dell'attività di audit, gli audit report e/o altre comunicazioni ufficiali della Funzione di Internal Auditing e, infine, sezioni dedicate all'interno del portale aziendale.

Ambiente di controllo - Forte sistema organizzativo di governance: un ambiente che supporti nella sua totalità il sistema di controllo interno e gestione dei rischi (di seguito SCIGR) incoraggia gli Auditor a condurre, con maggiore efficacia, la propria attività e riportare le risultanze senza restrizioni e/o timori di ritorsioni per opinioni negative e/o osservazioni critiche. Un componente significativo dell'ambiente di controllo è rappresentato dal Comitato per il controllo interno, CdA e/o altri organi di governo che sono cruciali nell'assicurare l'indipendenza della Funzione Internal Auditing e dei singoli componenti.

Mandato di Internal Audit: la formalizzazione di un mandato di Internal Audit che chiaramente definisca le responsabilità della funzione, il livello di autorità e le attività di reporting, nonché l'accesso illimitato alle informazioni, alle figure aziendali e/o ai dati/archivi rappresenta un elemento di promozione dell'indipendenza, tenuto conto del livello approvativo in capo all'organo di governo. In particolare, l'attività di supervisione del suddetto organo di governo sul rispetto del mandato, nonché in relativo potere decisionale nell'assunzione, valutazione, definizione dei compensi e cessazione del CAE possono rafforzare il grado di indipendenza della funzione.

Politiche di assunzione e compensazione: le politiche e il processo di assunzione del personale, anche nelle ipotesi di reclutamento interno, garantiscono un'adeguata salvaguardia dell'indipendenza. Per esempio, un sistema di screening, in fase di selezione dei potenziali candidati, può assicurare l'esclusione di potenziali conflitti di interesse⁶⁰ con l'organizzazione che esporrebbero al rischio di minare l'indipendenza dell'intera funzione. Anche le pratiche di compensazione/riconoscimento di premi possono essere strutturate, affinché la retribuzione degli Auditor sia indipendente dalle *performance* delle unità organizzative oggetto di revisione.

Outsourcing: quando le strutture e i meccanismi interni non risultano essere efficaci per gestire le minacce all'indipendenza, l'esternalizzazione del servizio ad un provider esterno può rappresentare un'adeguata soluzione per garantire il rispetto di tale fondamentale attributo della Funzione di Internal Audit.

60 Per esempio, in tale fase rientra l'analisi di tutte le forme di interesse di un potenziale candidato verso la Società come detenzione di azioni/obbligazioni, attuali rapporti lavorativi o di business con l'organizzazione anche riferiti a situazioni pregresse, etc.



Ai fini dell'identificazione e valutazione completa delle minacce di indipendenza in relazione a tutti i livelli di coinvolgimento dell'Auditor si presenta di seguito un framework di riferimento.

MANAGED INDEPENDENCE FRAMEWORK	
LEVEL	ISSUES
I. Individual	<ul style="list-style-type: none">• Management of auditor independence• Reporting relationship of the auditor
II. Engagement	<ul style="list-style-type: none">• Review auditor independence• Access to information• Freedom from influence or control by audit client
III. Internal Audit Activity	<ul style="list-style-type: none">• Ensure independence is managed (including third-party outsourcing)• Organizational placement• Strong charters
IV. Organization	<ul style="list-style-type: none">• Management interest in, and support of, independence• Human resources policies (e.g., hiring, firing, promoting)• Level of audit committee involvement
V. Profession	<ul style="list-style-type: none">• Standards-setting, education, and enforcement• Active promotion of independence management• Monitoring of profession level results• Certification

Figura 3 Fonte: IPPF - Practice Guide "Independence and objectivity" IIA (October 2011)

Il Livello I descrive gli aspetti riferiti al singolo Internal Auditor. Una componente chiave dell'indipendenza è la relazione di riporto gerarchico dell'Internal Auditor.

Il Livello II descrive il coinvolgimento a livello di incarico di Audit. Su questo piano, l'elemento cruciale è rappresentato dal grado di influenza e/o controllo del cliente di Audit sull'attività.

Il Livello III descrive la questione a livello di Funzione di Internal Auditing. Il CAE è responsabile di riportare qualsiasi minaccia, residuale e/o non risolta, al Comitato di controllo interno, all'organo di governo e/o agli appropriati livelli organizzativi per

garantire che l'indipendenza sia adeguatamente gestita a livello di singolo incarico, proponendo eventualmente l'esternalizzazione dello stesso nell'eventualità il rischio non possa essere gestito in modo appropriato all'interno.

Il Livello IV descrive le questioni a livello organizzativo. È opportuno che si stabiliscano policy atte ad assicurare che gli Auditor siano liberi nel condurre gli Audit e riportare i risultati senza interferenza. A tali fini, il CAE dovrebbe essere attivamente coinvolto nel Comitato di Audit e/o organi simili per assicurare il più alto livello di indipendenza all'attività di Audit.



Il Livello V descrive il punto di vista della professione e analizza il ruolo da parte degli organi professionali come l'IIA o AIIA. Queste strutture esterne possono definire *standard* e/o linee guide che concorrono a migliorare la capacità dell'Internal Auditor di garantire l'indipendenza della funzione e supportare le organizzazioni nello stabilire, al proprio interno, l'appropriato e l'adeguato livello di indipendenza della funzione, definendo gli opportuni flussi di comunicazione e le relazioni di reporting gerarchico-funzionale. Nei settori finanziari o in altri settori industriali regolamentati, la più alta soglia di *accountability* potrebbe richiedere l'emissione di documenti formali e pubblici sulla revisione dell'indipendenza della funzione. In altri contesti, l'adozione di una normativa ad hoc e la previsione di flussi formali di revisione spesso forniscono un rafforzamento addizionale alla conformità agli *standard* internazionali.

Obiettività

Per garantire una *performance* professionale e riportare delle decisioni imparziali, gli Internal Auditor devono essere capaci di gestire le minacce all'obiettività. Questa abilità rappresenta anche un importante segnale per l'organo di governo, per gli azionisti e le terze parti che possono fare affidamento sui risultati di *assurance* dell'Internal Audit circa la valutazione e funzionamento dello SCIGR, nonché la *compliance* e altri aspetti rilevanti per l'organizzazione. I principali fattori che possono minacciare l'obiettività possono essere i seguenti: la pressione sociale, gli interessi economici, le relazioni personali, la familiarità, le preferenze culturali, razziali e di genere, le distorsioni cognitive, la carenza di segregazione nella revisione dell'attività di Audit, le minacce di intimidazione nonché le minacce per altri interessi (sostegno/avversione per il destinatario dell'Audit).

Si descrivono sinteticamente di seguito i fattori che, in modalità anche latente e/o non espressa, potrebbero incidere sull'imparzialità del singolo

Auditor, affinché se ne comprenda in modo consapevole l'effetto di tali eventi e si identifichino le minacce per la successiva gestione.

Pressione sociale: tali minacce si verificano quando un Auditor è esposto o percepisce di essere esposto a pressioni da parti esterne. Elementi da considerare sono: le aspettative di Auditor esterni o delle autorità di regolamentazione in merito ai risultati di Audit, le osservazioni di Audit sollevate inavvertitamente o erroneamente dall'Auditor in passato, i condizionamenti che potrebbero portare l'Auditor a trascurare elementi sospetti, l'approccio del tipo "questo è il modo in cui l'abbiamo sempre fatto" (etichettato come "groupthink" nella letteratura comportamentale), la coercizione esplicita o occulta da parte dei clienti di Audit o di altre parti interessate.

Interesse economico: questa minaccia può sorgere nel caso in cui l'Auditor abbia un interesse economico rispetto alle prestazioni dell'organizzazione, qualora si tratti di un'attività di verifica riguardante una struttura o una risorsa che possa successivamente prendere decisioni che influiscano direttamente sul rapporto di lavoro del singolo Auditor. In tali casi, l'Auditor può temere che significativi risultati negativi che dovessero emergere dall'attività di Audit potrebbero mettere a repentaglio il futuro dell'organizzazione, nonché il proprio.

Relazioni personali e familiarità: tali minacce si verificano se l'Auditor è un amico o parente del Responsabile o delle risorse della struttura destinataria dell'Audit, ovvero se sussistono tra di essi rapporti professionali di lunga data. L'Auditor potrebbe essere eccessivamente comprensivo, o condizionato da pregiudizi positivi rispetto al cliente di Audit.

Preferenze di razza, cultura, genere: tali minacce potrebbero ad esempio indurre l'Auditor, in un'organizzazione multidivisionale, ad essere parziale o pregiudizievole nei confronti di clienti che si trovano in determinate sedi estere.



Distorsioni cognitive: questa minaccia può derivare da inconsci e non intenzionali pregiudizi psicologici nell'interpretazione delle informazioni. Ad esempio, se l'Auditor assume una prospettiva eccessivamente critica, potrebbe sottovalutare gli aspetti positivi, mentre una visione facilitatrice eccessivamente positiva potrebbe comportare la mancata considerazione di informazioni negative. Inoltre, un Auditor potrebbe avere idee preconcepite e tendere a cercare evidenze che le confermino.

Mancanza di segregazione nelle attività di verifica ("self-review"): tali minacce occorrono quando l'Auditor effettua la review delle proprie carte di lavoro o delle proprie attività svolte in un precedente incarico di Audit o consulenza. Ad esempio, un Auditor potrebbe revisionare, ripetutamente o in anni consecutivi, la stessa struttura organizzativa, oppure potrebbe fornire servizi di consulenza circa l'implementazione di un sistema o di azioni correttive che successivamente dovrà verificare. Tali esempi rappresentano situazioni in cui l'Auditor potrebbe potenzialmente operare in modo meno critico o accorto, dovendo rilevare errori o carenze nel proprio lavoro.

I possibili fattori di mitigazione che possono ridurre o eliminare le minacce di obiettività sono riportati nell'elenco di seguito, pur trattandosi di un'elencazione esemplificativa e non esaustiva.

Incentivi (premi, disciplina): l'adozione di un sistema di riconoscimento e/o sistema disciplinare, all'interno dell'organizzazione, che premi o penalizzi eventuali comportamenti conformi o difformi agli standard aziendali, sia della Funzione di Internal Auditing sia dell'intera organizzazione, rappresenta un deterrente alle minacce di obiettività. Per esempio, un ambiente che riconosca il valore aggiunto di un ragionamento critico e obiettivo o penalizzi pregiudizi può incoraggiare il valore dell'obiettività in tutte le sue forme. Gli stessi incentivi economici, il tempo libero addizionale, l'adozione di programmi di lavoro flessibili e/o

altri riconoscimenti positivi possono essere utilizzati per incoraggiare e premiare il pensiero obiettivo. Allo stesso modo, penali e/o sanzioni che impattano sulla revisione delle performance, ritardi nelle promozioni o altri avanzamenti o richieste di formazione addizionali potrebbero essere strumentali a scoraggiare la mancanza di obiettività. Analogamente, la modalità di impostazione e gestione dei programmi di premialità e/o di disciplina sono rilevanti e devono essere condotti in modo professionale e bilanciato affinché l'ambiente di controllo venga percepito come positivo e di supporto.

Gestione del team di Audit: il coinvolgimento di membri diversi del team di Audit può diffondere e/o eliminare potenziali minacce all'obiettività del singolo professionista, garantendo una prospettiva addizionale alle attività di verifica. Questa visione addizionale può controbilanciare le potenziali minacce dovute alla familiarità, alle relazioni personali, alla self-review e/o alle altre minacce dell'obiettività che possono riguardare parte o tutto il team di Audit.

Rotazione/riassegnazione: la rotazione nell'assegnazione degli Audit può ridurre il grado di familiarità o self-review. Ci sono differenti tipi di rotazione, inclusa la rotazione di tutto lo staff da un Audit a un altro, la rotazione di alcuni membri del team, nonché il mantenimento dello staff di Audit su un incarico ripetuto, ruotando però il lavoro svolto all'interno dello staff.

Formazione: l'implementazione di uno strutturato programma formativo, con adeguati mezzi e approcci, migliora l'obiettività. Pertanto, la formazione può anche aiutare gli Auditor nel riconoscere le potenziali minacce all'obiettività, così come garantire che le stesse possano essere ridotte e/o efficacemente e tempestivamente gestite all'adeguato livello organizzativo.



Supervisione/revisione: un'attenta supervisione degli Auditor e un'accurata *review* del lavoro svolto possono incoraggiare lo staff ad approcciare alle questioni di Audit in maniera obiettiva, tenuto conto che essi stessi sono responsabili dei loro giudizi. Le ricerche dimostrano che la responsabilità è un fattore importante per migliorare i giudizi e ridurre le influenze in un'attività di Auditing.

Quality Assesement: le *review* interne ed esterne di una Funzione di Internal Audit, dei servizi erogati, dei processi e delle procedure possono garantire maggiormente una gestione efficace delle minacce di obiettività e il mantenimento costante della professionalità all'interno della funzione. Il monitoraggio continuo e le revisioni periodiche delle attività di Auditing possono facilitare la gestione di processi secondo gli standard professionali, nonché l'implementazione delle attività, da parte dello staff di Audit, in accordo alle procedure e alle policy definite.

Politiche di assunzione: le politiche di assunzione possono migliorare la probabilità che il personale sia libero da preconcetti e capace di fornire giudizi obiettivi nella gestione un incarico di Internal Audit. Per esempio, lo screening può assicurare che potenziali candidati non presentino conflitti di interesse che minacciano la loro obiettività.

Outsourcing: esternalizzare le attività di Auditing potrebbe essere appropriato laddove vi siano conflitti di interessi noti e/o apparenti che potrebbero ostacolare il giudizio degli Auditor e/o creare potenziali distorsioni.

Si presenta di seguito un framework per gestire le minacce dell'obiettività a tutti i livelli di coinvolgimento degli Auditor.

MANAGED OBJECTIVITY FRAMEWORK	
LEVEL	ISSUES
I. Individual	<ul style="list-style-type: none"> • Management of auditor objectivity • Management of professionalism
II. Engagement	<ul style="list-style-type: none"> • Review auditor objectivity • Review auditor professionalism and the audit process
III. Internal Audit Activity	<ul style="list-style-type: none"> • Rotation of employees on jobs • Ensure objectivity is managed (including third-party outsourcing) • Review hiring practices
IV. Organization	<ul style="list-style-type: none"> • Management interest in objectivity • Human resources policies (hiring, firing, promoting) • Quality assurance reviews
V. Profession	<ul style="list-style-type: none"> • Standards-setting, education, and enforcement • Active promotion of objectivity management • Monitoring of profession-level results • Certification
FOUNDATION: NEED FOR OBJECTIVITY	

Figura 4 Fonte: IPPF - Practice Guide "Independence and objectivity" IIA (October 2011)



Il Livello I descrive le questioni a livello di singolo Internal Auditor, rappresentando il punto e/o il livello nel quale le minacce di obiettività sono identificate e proattivamente gestite. La professionalità dell'Internal Auditor (ad es. competenza, integrità e l'uso della diligenza professionale) è misurata in questo livello in quanto la stessa garantisce la necessaria obiettività richiesta al singolo professionista.

Il Livello II descrive le questioni a livello di incarico. Su questo piano si svolge una *review* dell'obiettività dell'Internal Auditor così come una *standard review* delle pratiche di Audit, delle procedure e dei giudizi riportati. Un'appropriata supervisione dello staff di Audit e una sistematica *review* del lavoro di Audit possono assicurare che i risultati di Auditing siano imparziali e non siano influenzati in alcun modo da giudizi precedenti.

Il Livello III descrive le questioni a livello di Funzione Internal Auditing. Questo è il punto nel quale il CAE è chiamato ad assumere delle iniziative per migliorare l'obiettività (es. rotazione degli Auditor tra gli incarichi). Il CAE potrebbe anche essere responsabile di riportare qualsiasi minaccia residuale non mitigata alla obiettività sia al Comitato interno sia alle parti interessate, assicurando che l'obiettività sia appropriatamente gestita in tutti gli incarichi.

Il Livello IV descrive la questione a livello organizzativo, in quanto la Funzione di Internal Auditing deve essere dotata dell'opportuna libertà e/o autonomia per gestire appropriatamente minacce di obiettività. È opportuno che si stabiliscano policy atte a garantire che gli Auditor non siano penalizzati nell'affrontare i problemi e/o identificare eventuali questioni all'interno dell'organizzazione, prevedendo se del caso un eventuale supporto attivo del *management*.

Il Livello V analizza la questione a livello professionale e coinvolge le attività di organizzazioni e organi come AIIA o IIA. Questi organi professionali possono definire gli *standard* e le linee guide che

incrementino strumenti di presidio dell'obiettività, offrendo certificazioni per migliorare la professionalità e rafforzare l'obiettività dell'Auditor e garantirne la promulgazione. Tali istituti possono contribuire ad assicurare la qualità e i controlli in merito all'obiettività nel processo di Audit, quale la *Quality Assurance peer review*. In alcuni contesti, l'introduzione o la previsione di normative specifiche spesso offre rafforzamenti addizionali alla conformità professionale. In aggiunta, i programmi formativi possono essere offerti per focalizzarsi sul miglioramento dell'obiettività e sul supporto degli Auditor alla identificazione e comprensione delle minacce alla formulazione di giudizi obiettivi.

Ai fini di un'analisi completa del framework occorre considerare le possibili combinazioni di minacce, su più livelli e su più piani, nonché la presenza contestuale e concomitante di diverse categorie di rischio.

A livello di singolo Auditor, il team può essere chiamato a fornire dei servizi di *control self-assessment*, tali da comportare una collaborazione diretta con i rappresentanti delle strutture destinatarie dell'Audit. Le minacce potrebbero aumentare in queste circostanze, come in quelle di *self-review*, nel momento in cui gli Auditor agiscono come facilitatori e vengono successivamente assegnati a rivedere il relativo SCIGR in un incarico di Audit. In tale fase potrebbe verificarsi anche la minaccia di pressione sociale, laddove gli Auditor "facilitatori" percepiscano la pressione di non "violare la fiducia" riposta nel *self-assessment* da parte dei partecipanti che dichiarano apertamente le debolezze del loro sistema. In questo contesto, un Auditor potrebbe essere preoccupato che future attività di *self-assessment* siano minate da osservazioni di Audit negative. Pertanto, quando un Auditor assume un ruolo di facilitatore, lo stesso può creare un legame stretto con alcuni clienti di Audit attraverso lo sviluppo di relazioni interpersonali che potrebbero essere difficili da gestire in fase di Audit. In altri casi, gli Auditor potrebbero sviluppare una inconsapevole distorsione cognitiva a causa di un



positivo ruolo di facilitatore adottato nel processo di self-assessment, attraverso un'interpretazione delle informazioni sui clienti di Audit molto più positiva rispetto a un approccio obiettivo e di ricerca informazioni di conferma/validazione.

A livello di attività, alcuni Internal Auditor intravedono nello svolgimento di alcuni incarichi, come i servizi di consulenza e di control *self-assessment*, la possibilità di minare l'obiettività dell'attività e rappresentare un fattore di conflitto. Per esempio, se un'attività di Auditing fornisce dei servizi estensivi di consulenza aziendale, le minacce di obiettività possono aumentare nella forma di *self-review* e familiarità. Le minacce di mancata segregazione possono aumentare anche quando l'Internal Auditor è prima coinvolto nell'implementazione del sistema informativo a livello aziendale, e poi nella *review* dello stesso sistema. In generale, l'erogazione di servizi di consulenza non compromette di per sé l'obiettività, in particolare se l'Auditor è coinvolto principalmente in ruolo consulenziale (un Internal Auditor non potrebbe essere coinvolto in un processo decisionale) e non c'è ragione di presupporre che l'obiettività dell'Internal Auditor sia automaticamente compromessa. Un Internal Auditor e un'attività di Internal Audit professionale, all'interno di un contesto/quadro sopra descritto, dovrebbero essere capaci di riconoscere le potenziali minacce all'obiettività nella gestione di successivi incarichi di Audit, valutando i fattori di mitigazione e adottando le appropriate azioni per ridurre o eliminare le minacce residuali all'obiettività.

In generale si osserva che l'Auditor può solamente gestire le minacce individuali, seppur in alcuni casi possano essere presenti molteplici minacce su

vari piani, per i quali occorre individuare specifici fattori di mitigazione nonché strumenti correttivi o preventivi per gestire i rischi riferiti alle diverse situazioni. Pertanto, è fortemente raccomandato un approccio comprensivo e integrato nell'identificare, valutare e gestire potenziali minacce.

L'indipendenza e l'obiettività sono necessarie per garantire l'efficacia dei servizi di Internal Auditing; ciascuna di esse deve essere gestita efficacemente per garantire la conformità del servizio agli *standard* professionali. In questa sezione si descrive un processo per gestire le minacce di indipendenza e obiettività a livello organizzativo, di incarico e a livello personale, richiedendo agli Internal Auditor di identificare le minacce alla loro indipendenza o obiettività. È quindi richiesto agli Internal Auditor di valutare e mitigare queste minacce e valutare se essi possono essere indipendenti e obiettivi, tenuto conto dei passi intrapresi per mitigare le minacce identificate.

Il *framework* per l'indipendenza riconosce l'indipendenza come primario aspetto organizzativo e strutturale. Il *framework* per l'obiettività riconosce l'obiettività principalmente come uno "stato mentale". La valutazione delle minacce di indipendenza e obiettività e la loro mitigazione o gestione è rappresentata da un processo di auto-valutazione condotto dagli Internal Auditor. I *framework* si fondano principalmente sulla professionalità del CAE e dei singoli Auditor. Gli Internal Auditor devono accettare le responsabilità per gestire e informare sulle minacce della propria indipendenza e obiettività.



La tabella seguente presenta un diagramma di processo per gestire le minacce di indipendenza e obiettività.

PROCESS FOR MANAGING THREATS TO INDEPENDENCE OR OBJECTIVITY							
Identify Threat	Assess Significance of Threat	Identify Mitigating Factors	Assess Residual Threat	Proactively Manage Residual Threat	Assess Presence of Unresolved Threats	Determine Reporting and Disclosure Implications	Review and Monitoring
->	->	->	->	->	->	->	->

Figura 5 Fonte: IPPF – Practice Guide “Independence and objectivity” IIA (October 2011)

Identificare la minaccia:

Identificare la minaccia: la prima responsabilità degli Auditor all’interno di un processo che gestisce l’indipendenza e l’imparzialità è quella di identificare possibili minacce a questi elementi caratterizzanti la professione. Qualsiasi situazione o circostanza che potrebbe indebolire la capacità degli Internal Auditor di agire liberamente o senza pregiudizio deve essere identificata come una minaccia. Anche eventuali rischi apparentemente non significativi dovrebbero essere individuati in questa fase. Tali situazioni potrebbero derivare, seppur non siano limitati ad esse, da potenziali debolezze di reporting o organizzative o personali o finanziarie o di assegnazione dei compiti. Le minacce identificate dagli Auditor dovrebbero essere rese note al CAE al fine di garantire una gestione proattiva della questione emersa. L’identificazione delle minacce può essere supportata dai fattori di influenza e dai framework riportati nei paragrafi 0 e 0.

Valutare la significatività della minaccia:

la seconda fase del processo richiede agli Auditor di valutare la significatività di ogni minaccia all’indipendenza o obiettività identificata nella fase precedente. La valutazione di tali aspetti riguarda l’analisi di quali tipologie di servizi siano impattate da tali minacce e se le stesse, seppur insignificanti, potrebbero intensificarsi con il tempo. La valutazione di tale significatività dovrebbe essere considerata sia nel quadro delle immediate e contingenti circostanze presenti, sia nei previsti o ragionevoli potenziali cambiamenti delle circostanze future.

Identificare i fattori di mitigazione:

a seguito della identificazione e valutazione della significatività delle minacce di indipendenza o obiettività, gli Internal Auditor potrebbero identificare specifici fattori di mitigazione al fine di attenuare le minacce. Fattori di mitigazione potrebbero includere, ma non essere limitati, alle seguenti azioni: supporto del Comitato interno, questioni di sicurezza del lavoro, capitale reputazionale e penali legali o professionali. Gli Internal Auditor dovrebbero aver cura di identificare i fattori di mitigazione rilevanti atti a garantire che le minacce possano essere limitate e, in caso di esito positivo, valutare la modalità per limitare il più possibile che il rischio di indipendenza o obiettività possa essere compromesso. L’identificazione dei fattori di mitigazione può essere supportata dai relativi elenchi riportati nei paragrafi 0 e 0.

Valutare minacce residuali:

dopo aver identificato i fattori di mitigazione per le relative minacce di indipendenza o obiettività, un Internal Auditor deve poi determinare se questi fattori siano sufficientemente mitigativi delle minacce nello svolgimento dell’attività di Audit, al fine di ridurre al minimo il rischio di Audit non efficaci. L’Internal Auditor deve essere cauto nell’evitare di presupporre che tali fattori abbiano adeguatamente mitigato tutti i rischi di indipendenza e obiettività e dovrebbe svolgere un assessment dalla prospettiva delle figure che fanno affidamento sui giudizi dell’Internal Auditor. Nei casi in cui le minacce residuali siano significative, o l’Internal Auditor non sia



pienamente sicuro della propria indipendenza o obiettività, la valutazione dovrebbe essere svolta o rivista dal CAE o, laddove necessario, dal *senior management* e/o comitato interno.

Gestire proattivamente la minaccia residuale:

le minacce all'indipendenza o obiettività possono essere non adeguatamente compensate dai fattori di mitigazione che dovrebbero essere opportunamente gestiti dagli Auditor (per quanto possibile) per assicurare che gli incarichi siano svolti senza interferenza o pregiudizio. Tra i possibili strumenti utilizzati per gestire le minacce residuali all'indipendenza o obiettività si include, ad esempio, uno strutturato Mandato della Direzione, una *review* di terze parti, una separazione dei compiti e delle attività di Audit, nonché una esternalizzazione del lavoro ad altre parti.

Valutare la presenza di minacce non risolte:

in questa fase, gli Auditor devono rivedere ogni minaccia residuale che potrebbe non essere stata adeguatamente risolta attraverso l'identificazione dei fattori di mitigazione o gli sforzi manageriali. L'Auditor dovrebbe determinare se le significative minacce non mitigate o gestite persistano, e valutare se è ancora possibile svolgere il lavoro. In molti casi, potrebbe essere raccomandabile informare gli utilizzatori dei servizi circa le minacce non risolte, prima di iniziare il lavoro di Audit. Se, dopo una seria considerazione e consultazione, la decisione è quella di condurre l'incarico nonostante le minacce non risolte alla indipendenza e obiettività, le implicazioni devono essere attentamente riportate.

Determinare le implicazioni di reporting e documentazione:

i fattori di mitigazione e gli step intrapresi per gestire le minacce di indipendenza e obiettività devono essere adeguatamente documentati per fornire un'accurata traccia degli sforzi dell'Auditor per raggiungere tali *standard*. Questa tracciabilità fornirà valide informazioni all'organo di governo della Società e alla *review* professionale del team

di QA. Inoltre, qualora si decidesse di intraprendere il lavoro anche in presenza di minacce irrisolte alla indipendenza e obiettività, gli Auditor dovranno riportare i dettagli della situazione agli appropriati livelli organizzativi (es. *senior management*, comitato interno di controllo e rischi, Consiglio di Amministrazione o organo equivalente) e tenere traccia delle minacce suddette nei relativi Audit report.

Review e monitoraggio:

per ogni incarico di Audit, il CAE dovrebbe condurre una complessiva *review* dell'attività di Audit e dello staff coinvolto per determinare se l'indipendenza e obiettività siano efficacemente gestite. Questo potrebbe richiedere l'accettazione di incarichi compatibili con il ruolo dell'attività di Internal Audit nell'organizzazione. In aggiunta, il CAE dovrebbe rivedere e monitorare il processo di gestione delle minacce di indipendenza e obiettività per i singoli incarichi di Audit. Il Comitato interno o organi simili sono essi stessi parte del processo di *review* e monitoraggio. Infine, la professione di Internal Auditor richiede una strutturata attività di *quality assessment* delle attività condotte.

In conclusione, la valutazione dell'indipendenza e obiettività è un processo iterativo nel quale il CAE definisce un approccio metodologico per indirizzare in maniera adeguata le potenziali minacce, in particolare quelle non mitigate e/o irrisolte, garantendo in ogni caso la tracciabilità delle azioni e decisioni intraprese, con un flusso di reporting al Comitato di controllo interno e/o simili organismi indipendenti. Laddove, invece, i membri del Comitato interno e/o il *top management* possono, di fatto, rappresentare essi stessi degli elementi che concorrono a minare l'indipendenza e obiettività, la migliore alternativa può essere quella di rifiutare l'esecuzione dell'Audit. In generale, se il problema è sistemico, l'Internal Auditor e/o il CAE dovrebbe adeguatamente valutare se e come la propria professionalità e il sottostante impegno all'integrità possano essere influenzati dal rimanere nell'organizzazione.



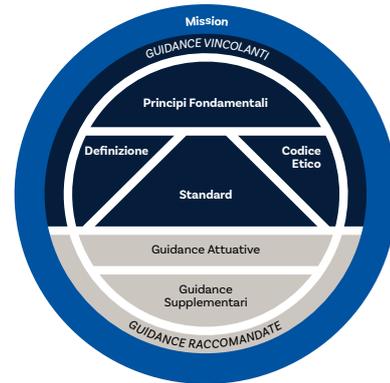
Quality Assurance

In linea con le migliori prassi internazionali, l'attività di Internal Auditing ha l'obiettivo di supportare il Board e il management nell'adempimento delle proprie responsabilità in tema di adozione e miglioramento dei sistemi di controllo interno aziendali, nonché nell'identificazione, valutazione, gestione e controllo dei rischi di business. È per tale ragione che la natura, l'estensione e la qualità dei servizi offerti dalla funzione, assumendo rilevanza nel contesto di un efficace sistema di Corporate Governance, devono essere periodicamente sottoposti ad una valutazione esterna indipendente che ne attesti l'adeguatezza e supporti il miglioramento continuo.

Tale linea di indirizzo è prevista anche dagli Standard Internazionali per la Pratica Professionale dell'Internal Auditor cui le funzioni di Internal Audit dovrebbero adeguarsi, secondo cui:

- il Responsabile Internal Audit deve sviluppare e mantenere un programma di assicurazione e miglioramento qualità che copra tutti gli aspetti dell'attività di Internal Auditing e ne verifichi continuamente l'efficacia. Tale programma comprende valutazioni periodiche interne ed esterne ed attività di monitoraggio continuo;
- l'Internal Auditing deve adottare un processo di monitoraggio e valutazione dell'efficacia complessiva del programma di qualità. Il processo deve includere valutazioni sia interne sia esterne dell'attività;
- le valutazioni esterne, come le *Quality Assurance Review*, devono essere condotte almeno ogni cinque anni, da Auditor esterni all'organizzazione, qualificati e indipendenti⁶¹.

IPPF International Professional Practices Framework



Il processo di "Quality Assurance" mira a valutare la conformità dell'attività di Internal Auditing agli International Professional Practices Framework (IPPF) e può rappresentare un efficace momento di confronto sul grado di rispondenza, in particolare, dei requisiti di indipendenza e obiettività previsti a livello professionale. Dall'attività di Quality Assessment possono emergere punti di forza o debolezze/opportunità di miglioramento e in generale, un parere di conformità della Funzione agli Standard professionali.

L'approccio metodologico con cui condurre le attività di "Quality Assurance Review" è definito nel "Quality Assessment Manual" il quale descrive la mappa dei tools di riferimento relativi a:

- preparazione e fasi preliminari (Tool A);
- questionari e Guide per le interviste (Tool B e C);
- aree Tematiche, quali IA Governance, IA Staff, IA Management e IA Process (Tool D);
- valutazione e comunicazione dei risultati (Tool E e F).

Per aspetti di dettaglio, si rimanda al "Quality Assessment Manual for the Internal Audit Activity - 2017 IPPF Aligned".

61 Standard 1300 - Programma di Assurance e Miglioramento della Qualità: "Il Responsabile Internal Auditing deve sviluppare e sostenere un programma di assurance e miglioramento della qualità che copra tutti gli aspetti dell'attività di Internal Audit". Standard 1310 - Requisiti del programma di Assurance e Miglioramento della Qualità: "Il programma di assurance e miglioramento della qualità deve includere valutazioni sia interne che esterne".





6. Risultati del questionario

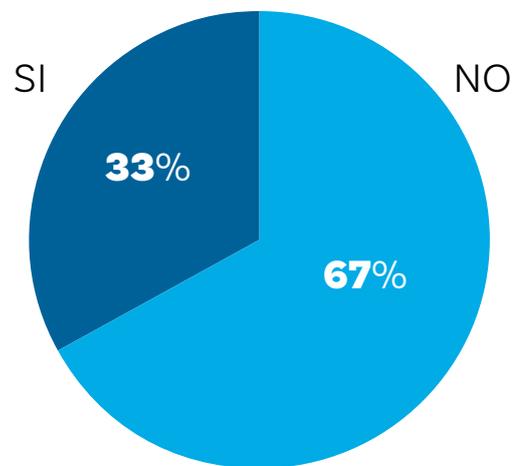
Gli autori hanno somministrato un questionario ai partecipanti al Forum IA per rilevare il livello di indipendenza della Funzione di Internal Audit e i fattori che la condizionano.

Dalle risposte emerge che tutte le funzioni di Internal Audit degli enti interpellati sono conformi allo *Standard* sull'indipendenza organizzativa poiché sono unità organizzative separate e dipendenti dal Vertice dell'Organizzazione a cui la funzione riferisce direttamente.

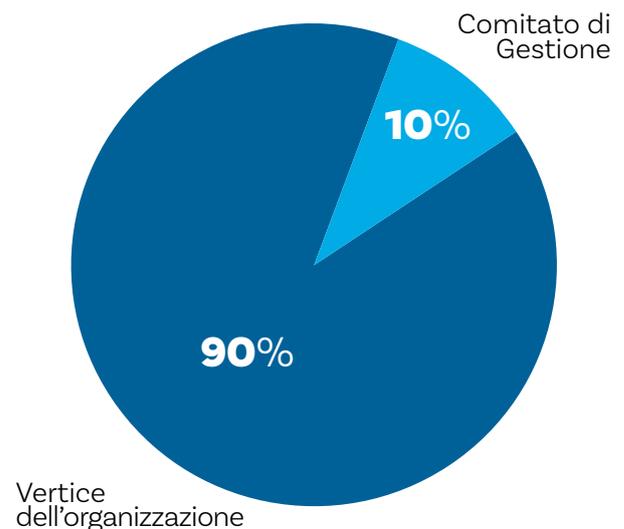
Nel testo sono stati più volte richiamati alcuni fattori che condizionano positivamente l'indipendenza, tra cui la presenza e il reporting funzionale al Comitato di Audit: il 33% del campione esaminato dichiara di avere un Comitato di Audit, e nel 22% dei casi al Comitato partecipano anche membri esterni all'Organizzazione.

Nel 66% dei casi il RIA riveste altri ruoli che esulano dall'Internal Audit: RPCT, membro dell'OdV o di altri Comitati (Comitato etico, Comitato Controlli e Rischi). Quanto ai programmi di ottenimento delle certificazioni internazionali, essi sono diffusi nel 20% dei casi. Il Processo di definizione del piano di Audit si basa nella maggior parte dei casi su un *risk assessment*, quello che differenzia le risposte è l'autore di tale valutazione dei rischi: nel 55% l'IA in maniera indipendente, in altri coinvolgendo un gruppo di lavoro, i responsabili delle strutture, la Funzione di *Risk Management* o il Vertice dell'Istituto o un mix di tutte le soluzioni).

È presente un Comitato di Audit o simile?

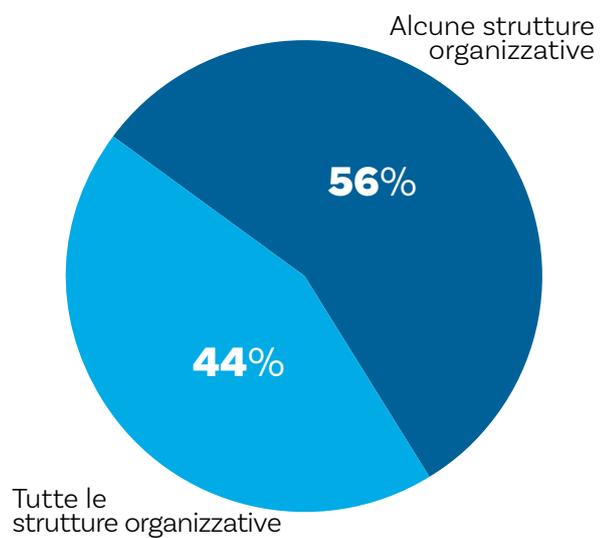


Da chi è nominato il Responsabile Internal Audit RIA?

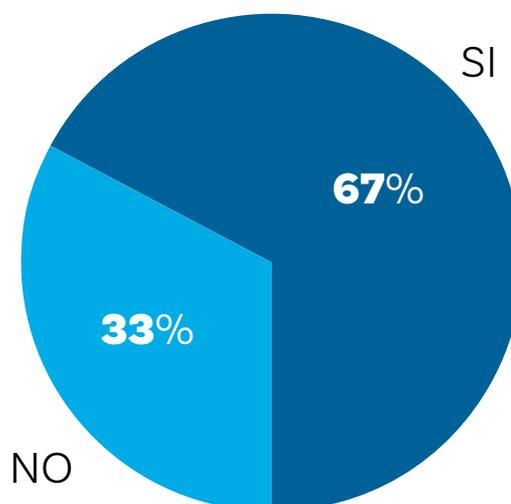




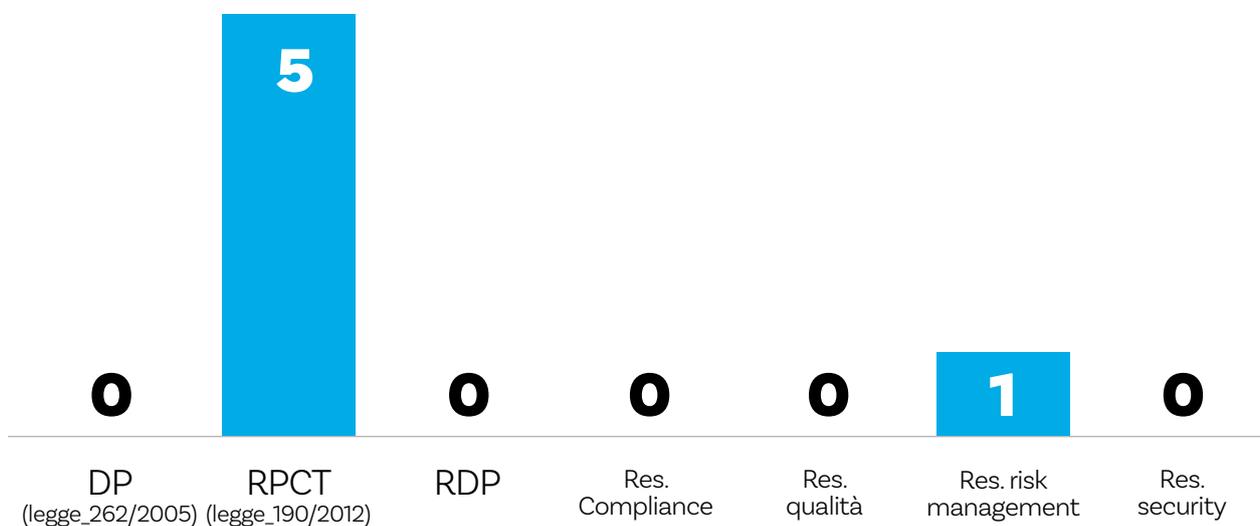
Da cosa è composto l'universo di Audit?



Il RIA riveste altre cariche all'interno dell'organizzazione?

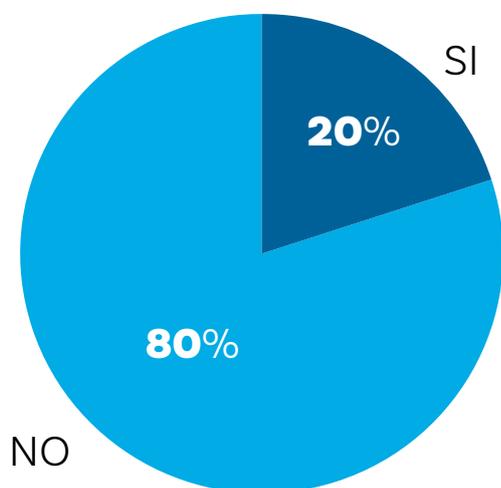


Quali altre cariche riveste il RIA?

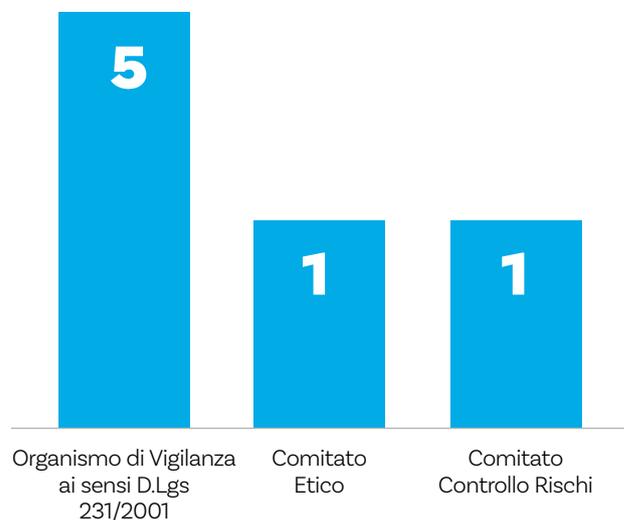




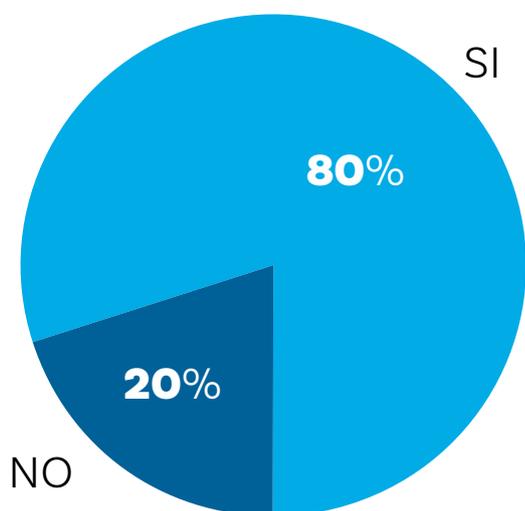
Il RIA è membro di qualche Organismo/Comitato interno all'organizzazione?



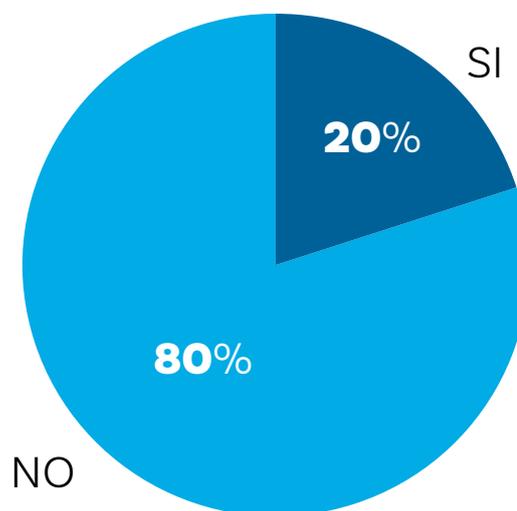
A quale Comitato partecipa il RIA?



E' in essere un piano di formazione per gli addetti della Funzione di Internal Audit?

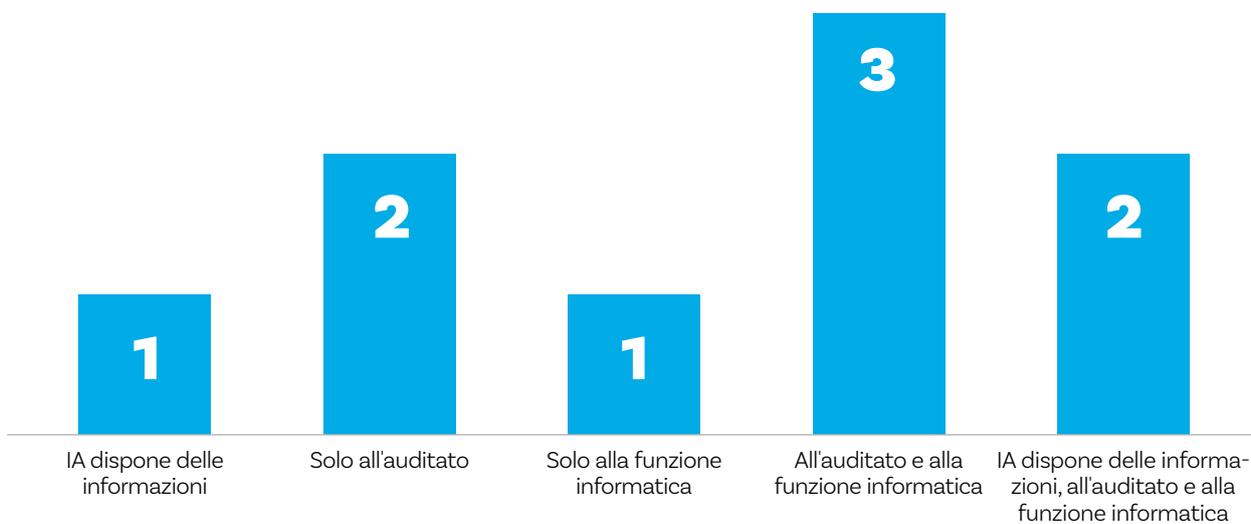


La Funzione di Internal Audit ha in essere programmi per il conseguimento delle Certificazioni internazionali (ad es. Certified Internal Auditor)?

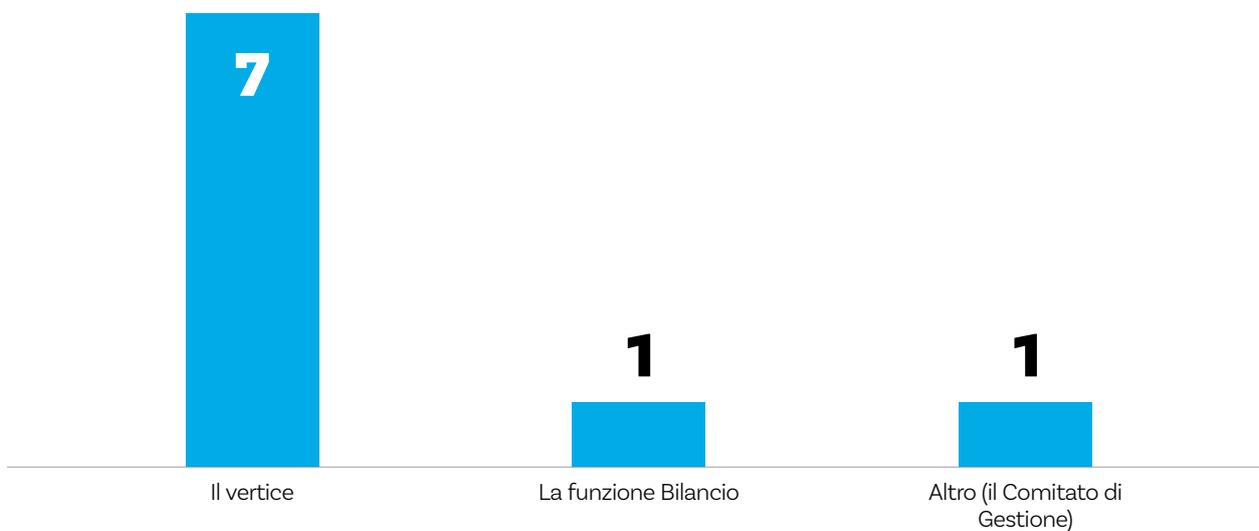




L'IA a chi chiede le informazioni necessarie per lo svolgimento di un incarico di Audit?

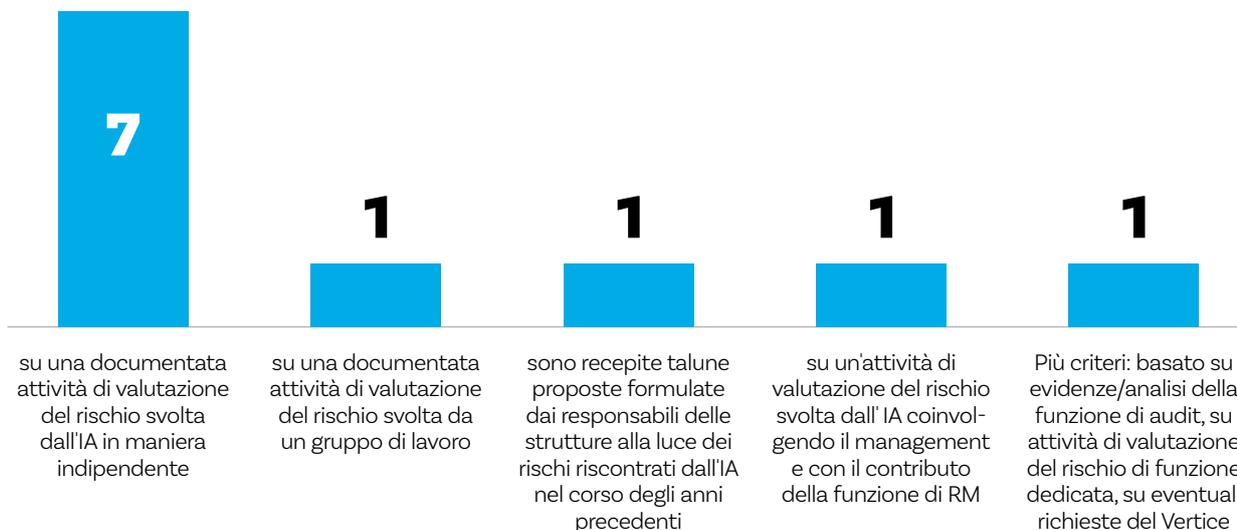


Chi approva il budget della funzione di IA?



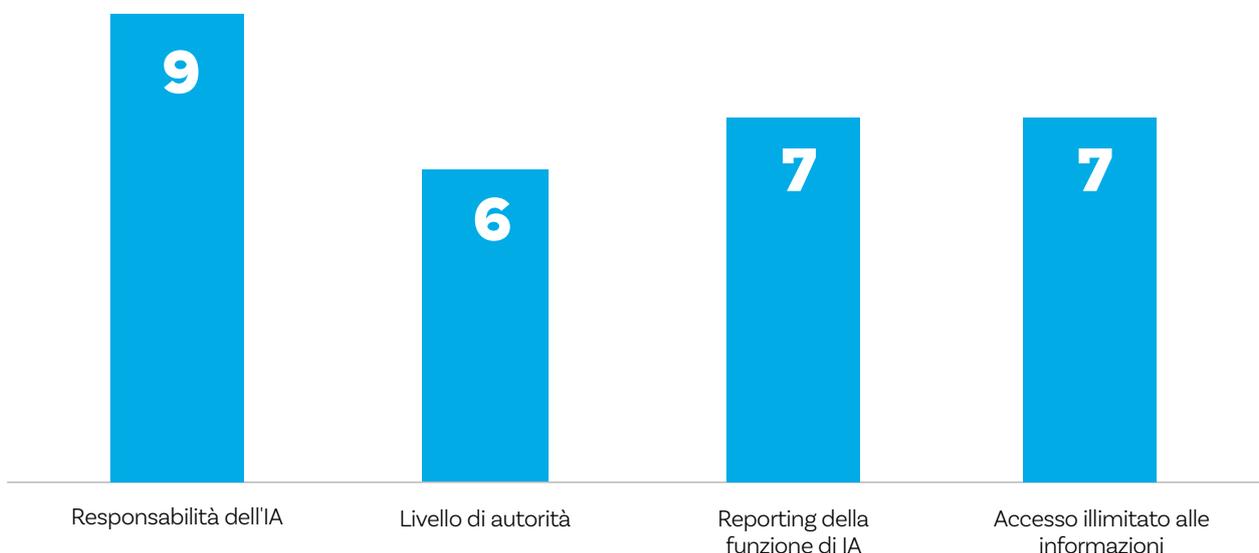


Su cosa è basato il piano di Audit?



Tutti i partecipanti hanno risposto che le attività della Funzione di Internal Audit sono definite in un mandato formalizzato e periodicamente rivisto e approvato dal Vertice dell'Organizzazione.

Cosa comprende il mandato dell'IA?







7. Conclusioni

(a cura del gruppo di Lavoro)

Il presente lavoro ha esaminato i principali riferimenti normativi, la letteratura professionale ed i contributi accademici in tema di indipendenza dell'Internal Auditor, al fine di fornire delle linee guida agli enti con finalità pubblicistiche per valutare il proprio livello di indipendenza: alla trattazione teorica è stata affiancata una rilevazione delle soluzioni organizzative e gestionali adottate dai partecipanti all'indagine.

L'analisi svolta dal gruppo di lavoro parte dal presupposto che i meccanismi di *Corporate Governance* ricoprono un ruolo di fondamentale importanza al fine di garantire l'indipendenza della Funzione di Internal Audit. Nello specifico, il modello delle tre linee rappresenta un importante punto di riferimento. Una chiara e netta separazione delle tre linee e la segregazione delle attività svolte dalla Funzione di Revisione Interna rientrano fra i principali presupposti per garantire l'indipendenza degli Internal Auditor. Tuttavia, una corretta implementazione del modello delle tre linee rappresenta una condizione necessaria ma non sufficiente per garantire adeguati livelli di indipendenza.

Risulta dunque necessario interrogarsi sui principali fattori che influenzano l'indipendenza dell'Internal Auditor. Attraverso una rilettura degli *standard* professionali di riferimento, alla luce dei risultati evidenziati dai principali contributi accademici, il presente lavoro mostra che vari elementi possono influenzare sia in modo positivo sia in negativo il livello di indipendenza. Più precisamente, le linee di riporto della Funzione di Revisione Interna, la composizione del Comitato di Audit, e la scelta

della figura cui assegnare il potere di nominare, confermare e licenziare il capo della Funzione di Revisione Interna rappresentano possibili minacce all'indipendenza. Altri fattori chiave sono:

- il livello di competenza degli Internal Auditor;
- l'interazione con il *management* durante il processo di pianificazione dell'Audit;
- l'assegnazione delle risorse per l'incarico di revisione;
- l'autonoma capacità di attingere a informazioni affidabili e intellegibili da parte dell'Auditor, (anche senza il supporto della prima o della seconda linea).

Nel caso in cui non sia possibile governare opportunamente questi fattori per migliorare il livello di indipendenza, un possibile rimedio è rappresentato dall'esternalizzazione totale o parziale della Funzione di Internal Audit.

Il tema dell'indipendenza diviene ancor più delicato nell'ipotesi in cui il RIA assuma ruoli aggiuntivi rispetto al tradizionale ruolo di capo della Funzione di Internal Audit. Indagini svolte da alcune grandi società di consulenza, così come i risultati del questionario auto-somministrato dal gruppo di lavoro, mostrano che il RIA spesso ricopre ruoli aggiuntivi di responsabile per la prevenzione della corruzione e trasparenza e di membro dell'Organismo di Vigilanza. Si noti a tal proposito che tali ruoli possono essere considerati come appartenenti alla seconda linea piuttosto che alla terza. Sebbene non possa



configurarsi una netta incompatibilità fra queste figure, risulta necessaria l'attuazione di opportuni meccanismi di salvaguardia per evitare che venga intaccata l'indipendenza ed obiettività della Funzione di Internal Audit.

Al fine di promuovere un innalzamento dei livelli di indipendenza della Funzione di Internal Audit, risulta cruciale l'identificazione di opportuni strumenti che siano in grado di valutarli e di identificare opportune aree di miglioramento. Il presente lavoro propone dunque un processo di valutazione dell'indipendenza ed obiettività che consta delle seguenti fasi:

- identificazione della minaccia;
- valutazione della significatività della minaccia;
- identificazione dei fattori di mitigazione;
- valutazione delle minacce residuali;
- gestione proattiva della minaccia residuale;
- determinazione delle implicazioni di reporting e documentazione;
- revisione e monitoraggio.

Analogamente, il processo di *Quality Assurance* rappresenta un momento fondamentale per innalzare ulteriormente i livelli di indipendenza ed obiettività della Funzione di Internal Audit. In tale ottica, il processo di *Quality Assurance* mira a valutare la conformità dell'attività di Internal Auditing agli *International Professional Practices Framework* (IPPF) e può rappresentare un efficace momento di confronto sul grado di rispondenza agli *standard* di indipendenza e obiettività stabiliti a livello professionale.

La rilettura degli *standard* professionali e della normativa di riferimento, l'analisi della letteratura professionale e accademica in materia, hanno posto in luce gli aspetti più importanti che possono influenzare l'indipendenza di una Funzione di Internal Audit. Il presente lavoro propone delle considerazioni generali per introdurre nelle stesse funzioni un processo teso a rafforzare il livello di detta indipendenza, sebbene il dibattito su tali temi, soprattutto nel settore pubblico, non possa ancora considerarsi esaurito, per l'insorgenza di fattori quali gli aggiornamenti normativi, l'introduzione di nuove figure aziendali e mutati assetti di *governance*.





Riferimenti bibliografici

Abbott L. J., Daugherty B., Parker S., and Peters G. F. - *Internal Audit Quality and Financial Reporting Quality: the joint importance of independence and competence.* Journal of Accounting Research Vol. 54 No. 1, pp. 3-40 (2016).

Adams, M. B. - *Agency Theory and the Internal Audit.* Managerial Auditing Journal, Vol. 9 No. 8, 1994 pp. 8-12.

Associazione Italiana Internal Auditors - AIIA - *Approccio Integrato al Sistema di Controllo Interno ai fini di un efficace ed efficiente governo d'impresa,* Corporate Governance Paper 2008

Associazione Italiana Internal Auditors - AIIA - *Il Ruolo dell'Auditing nella Governance del Settore Pubblico* 2008

Associazione Italiana Internal Auditors - AIIA - *Approccio integrato al sistema di controllo interno* 2009

Associazione Italiana Internal Auditors - AIIA - *La Revisione del Sistema di Governo Societario nel settore assicurativo: prime riflessioni,* 2017

Antle, R. (1984) - *Auditor independence.* Journal of accounting research, Vol. 22, No. 1, pp. 1-20.

Barr, R.H. and Chang, S.Y., (1992) - *Outsourcing Internal Audits: A Boon or Bane?* Managerial Auditing Journal, Vol. 8, No. 1, pp. 700-713

Banca d'Italia - *Disposizioni di vigilanza per le banche* Circolare n. 285 del 17 dicembre 2013

Basel Committee on Banking Supervision - *Enhancing corporate governance for Banking Organisations,* 1999

Basel Committee on Banking Supervision - *Principles for Enhancing corporate governance,* 2010

Basel Committee on Banking Supervision - *Corporate Governance Principles for Banks,* 2015

Carciello J.V., Eulrich M, Masli A., Wood D.A. (2017) - *The Value to Management of Using the Internal Audit Function as a Management Training Ground.* Accounting Horizons, Vol. 32, No. 2, pp. 121-140

Christofer J., Sarens G., Leung P., (2009) - *A critical analysis of the independence of the Internal Audit function: evidence from Australia,* Accounting, Auditing & Accountability Journal, Vol. 22 No. 2, pp. 200-220

Consob - *Regolamento adottato con delibera n. 20307 del 15 febbraio 2018 e aggiornato con le modifiche apportate dalla delibera n. 21755 del 10 marzo 2021 recante norme di attuazione del TUF in materia di intermediari.*

Consob - *Testo Unico della Finanza Decreto legislativo 24 febbraio 1998, n. 58 Aggiornato con le modifiche apportate dalla L. n. 238 del 23.12.2021*

Comitato Corporate Governance - *Codice di Corporate Governance* 2020

EBA – European Banking Authority - *Final Report on Guidelines on Internal Governance under Directive 2013/36/EU, July 2021 (EBA/GL/2021/05) che abroga il precedente EBA/GL/2017/11 del 26 September 2017*

Fama, E. F. (1980) - *Agency problems and the theory of the firm.* Journal of political economy, Vol. 88, No. 2, pp. 288-307



Financial Stability Institute, Arndorfer, I., Minto, A. - «The “four lines of defence model” for financial institutions - Taking the three-lines-of-defence model further to reflect specific governance features of regulated financial institutions», BIS, Occasional Paper N. 11, December 2015

Frigeni, C. - *La Governance Bancaria come Risk Governance: l'evoluzione della Regolamentazione internazionale ed europea dopo la crisi*, in OSSERVATORIO MONETARIO 1/2016, Associazione per lo Sviluppo degli Studi di Banca e Borsa, Università Cattolica del Sacro Cuore - Laboratorio di Analisi Monetaria, Capitolo II

Gasparri G. - *I controlli interni nelle società quotate. Gli assetti della disciplina italiana e i problemi aperti*, Quaderni Giuridici Consob Settembre 2013

Institute of Internal Auditor - *The three lines of defense in effective risk management and control*, IIA Research Foundation, Altamonte Springs, FL 2013

Institute of Internal Auditor - *Practice Guide Independence and objectivity* 2011

Institute of Internal Auditor - *The IAA's Three Lines Model An update of the Three Lines of Defense* 2020

Institute of Internal Auditor - *Quality Assessment Manual for the Internal Audit Activity* 2017 IPPF Aligned

Institute of Internal Auditors: *Standard internazionali per la pratica professionale dell'Internal Auditing International Professional Practice Framework (IPPF)* 2017

Institute of Internal Auditors - *Leveraging COSO across the three lines of defense* by, Douglas J. Anderson, Gina Eubanks Research Commissioned by Committee of Sponsoring Organizations of the Treadway Commission Luglio 2015.

Messier Jr, W. F., Reynolds, J. K., Simon, C. A., & Wood, D. A. (2011) - *The effect of using the Internal Audit function as a management training ground on the external Auditor's reliance decision*. The Accounting Review, Vol. 86, No.6, pp. 2131-2154

Mutchler, J., Chang, S. and Prawitt, D. - *Independence and Objectivity: a Framework for Internal Auditors*, IIA Research Foundation, Altamonte Springs, FL (2001)

OECD – Organisation for Economic Cooperation and Development (1999) - *Principles of Corporate Governance*

OECD – Organisation for Economic Cooperation and Development (2015) - *G20/OECD Principles of Corporate Governance*

Pricewaterhousecoopers D.Lgs. 231/01 - *Indagine nell'ambito delle società quotate 2020- 13ª edizione*. Pricewaterhousecoopers, Milano 2020

Protiviti-Lattanzio - *Il responsabile per la Prevenzione della Corruzione e Trasparenza: attore del sistema di controllo interno*. Protiviti-Lattanzio, Milano 2018

Rose, A. M., Rose, J. M., & Norman, C. S. - *Is the objectivity of Internal Audit compromised when the Internal Audit function is a management training ground?* Accounting & Finance, Vol. 53, No. 4, pp. 1001-1019 (2013)

Simunic, D. A. - *Auditing, consulting, and Auditor independence*. Journal of Accounting Research, Vol. 22, No. 2, pp. 679-702 (1984).

Spekle, R. F., Van Elten, H. J., & Kruis, A. M. - *Sourcing of Internal Auditing: An empirical study*. Management Accounting Research, Vol. 18, No. 1, pp. 102-124 (2007)

Williamson, O. E. - *Transaction-cost economics: the governance of contractual relations*. The journal of Law and Economics, Vol. 22, No. 2, pp. 233-261 (1979)



Associazione Italiana
Internal Auditors

via San Clemente, 1 - 20122 Milano
www.iiaweb.it