

Proteggere e accrescere il valore nelle aziende del SSN: il ruolo della funzione di Internal Audit

Anessi Pessina E., Cantù E., Langella C., Persiani N.

Position Paper CERISMAS



VITA E PENSIERO

POSITION PAPER



Centro di Ricerche e Studi in Management Sanitario (CERISMAS) – Eugenio Anessi Pessina, Componente del Consiglio Direttivo CERISMAS e Professore Ordinario di Economia Aziendale, Università Cattolica del Sacro Cuore, Milano; Elena Cantù, Vicedirettore CERISMAS e Professore Associato di Economia Aziendale, Università Cattolica del Sacro Cuore, Milano; Cecilia Langella, Responsabile Area Sistemi Contabili CERISMAS e ricercatore di Economia Aziendale, Università Cattolica del Sacro Cuore, Milano; Niccolò Persiani, professore ordinario di Economia Aziendale, Università degli Studi di Firenze.

Si prega di citare il position paper come segue: Anessi Pessina et al. (2025), *Proteggere e accrescere il valore nelle aziende del SSN: il ruolo della funzione di Internal Audit*, Vita e Pensiero, Milano, ISBN: 978-88-343-5958-7

Proteggere e accrescere il valore nelle aziende del SSN: il ruolo della funzione di Internal Audit

Anessi Pessina E., Cantù E., Langella C., Persiani N.

Position Paper CERISMAS



VITA E PENSIERO

www.vitaepensiero.it

Le fotocopie per uso personale del lettore possono essere effettuate nei limiti del 15% di ciascun volume dietro pagamento alla SIAE del compenso previsto dall'art. 68, commi 4 e 5, della legge 22 aprile 1941 n. 633.

Le fotocopie effettuate per finalità di carattere professionale, economico o commerciale o comunque per uso diverso da quello personale possono essere effettuate a seguito di specifica autorizzazione rilasciata da CLEARedi, Centro Licenze e Autorizzazioni per le Riproduzioni Editoriali, Corso di Porta Romana 108, 20122 Milano, e-mail: autorizzazioni@clearedi.org e sito web www.clearedi.org

© 2025 Vita e Pensiero - Largo A. Gemelli, 1 - 20123 Milano
ISBN 978-88-343-5958-7

Indice

I.	Lo sviluppo della funzione di Internal Audit: quadro concettuale di riferimento	8
II.	L'Internal Audit nelle aziende sanitarie pubbliche italiane: stato dell'arte e linee di tendenza	13
	2.1. I risultati della ricerca sulle "Scelte e pratiche aziendali relative all'introduzione e allo sviluppo della funzione di Internal Audit nelle aziende sanitarie pubbliche italiane"	13
	2.2. Evidenze emerse nella Community of Practice per esperti di Internal Audit in sanità	18
III.	Raccomandazioni per lo sviluppo e il consolidamento della funzione di Internal Audit nel SSN	22
IV.	Riflessioni conclusive	33
	Appendice A – Attività di ricerca e formazione svolte da Cerismas sull'Internal Audit in sanità	34
	Bibliografia	36

I. Lo sviluppo della funzione di Internal Audit: quadro concettuale di riferimento

La funzione di Internal Audit (di seguito IA) è nata nel settore privato e ha assunto un ruolo di rilievo nel sistema di *corporate governance* soprattutto in seguito agli scandali finanziari di inizio XXI secolo.

Caratterizzata inizialmente da un approccio prettamente ispettivo, la funzione nel tempo ha visto crescere le proprie responsabilità, fino a proporsi come alleato proattivo del *management* nella prevenzione e gestione di svariate tipologie di rischio quali, per esempio, rischi strategici, operativi, di *compliance*, di *reporting*, di frode, informatici (Mihret & Grant 2017). Tale evoluzione è coerente con la definizione stabilita dall'associazione professionale degli *internal auditor*, che configura l'IA come: “attività indipendente e obiettiva di *assurance* e consulenza, finalizzata al miglioramento dell'efficacia e dell'efficienza dell'organizzazione, [che] assiste l'organizzazione nel perseguimento dei propri obiettivi tramite un approccio professionale sistematico, che genera valore aggiunto in quanto finalizzato a valutare e migliorare i processi di *governance*, di gestione dei rischi e di controllo” (IIA 2024).

Nel complessivo sistema di controllo interno e di gestione dei rischi (SCIGR) di un'azienda, l'IA si configura come funzione di controllo di terzo livello. Per SCIGR si intende “l'insieme delle regole, delle procedure e delle strutture organizzative” predisposte dalla direzione e “volte a consentire l'identificazione, la misurazione, la gestione e il monitoraggio dei principali rischi. Tale sistema è integrato nei più generali assetti organizzativi e di governo” dell'azienda e “concorre ad assicurare (i) la salvaguardia del patrimonio sociale, (ii) l'efficienza e l'efficacia dei processi aziendali, (iii) l'affidabilità delle informazioni fornite agli organi sociali e al mercato, (iv) il rispetto di leggi e regolamenti nonché dello statuto sociale e delle procedure interne” (Borsa Italiana 2018, § 7). La definizione ben evidenzia

come la corretta impostazione del SCIGR e la garanzia del suo funzionamento rientrino tra le responsabilità della Direzione Aziendale. Il SCIGR è tipicamente organizzato su tre livelli di controllo (CoSO 1992; 2013). Al primo livello si collocano i controlli predisposti e attuati dal personale aziendale che pone in essere l'attività o esercita una funzione di coordinamento, nel rispetto dei propri obiettivi e responsabilità. Si tratta di controlli di carattere procedurale, informatico, comportamentale, amministrativo-contabile ecc., insiti nei processi operativi e finalizzati a presidiare i rischi derivanti dall'ordinaria attività aziendale, assicurando il corretto svolgimento di tale attività. Al secondo livello si posiziona un insieme di controlli trasversali focalizzati su specifiche aree di rischio. I controlli di secondo livello sono affidati a funzioni aziendali dedicate e distinte da quelle operative. Tali funzioni concorrono a definire le politiche di governo e il processo di gestione dei rischi, nonché le metodologie di identificazione e valutazione dei rischi stessi. Con riferimento alle aree di rischio di propria competenza, inoltre, provvedono a individuare idonei controlli e garantirne l'applicazione, a verificare il disegno e il funzionamento dei controlli di primo livello, a verificare la corretta applicazione delle normative e delle disposizioni interne finalizzate a prevenire e mitigare i rischi. Infine, il terzo livello, affidato all'IA, ha la responsabilità di fornire garanzie sul disegno e sulla funzionalità complessiva del SCIGR attraverso valutazioni indipendenti e obiettive. L'IA, pertanto, si propone non solo come sistema per l'analisi dei processi, la loro valutazione e il loro sviluppo, ma anche, e soprattutto, come sistema di valutazione della capacità dell'azienda di identificare e mitigare i propri rischi, attraverso un approccio non solo difensivo ma anche proattivo, garantendo la coerenza, la sistematicità e il corretto funzionamento del complessivo SCIGR.

* * *

Nelle amministrazioni pubbliche, l'introduzione dell'IA, nell'accezione sopra delineata, è più recente. Ciò nonostante, la funzione è stata caricata di aspettative ancora maggiori che nel settore privato. La letteratura internazionale di *Public Administration* attesta la crescente gamma e complessità delle responsabilità attribuite alla funzione IA. Di conseguenza, l'*internal auditor* viene descritto come una

sorta di *factotum* (Roussy & Perron 2018), dedito a una molteplicità di attività (formalmente e informalmente assegnategli) che lo portano a svolgere una pluralità di ruoli, da “scudo protettivo e custode dei segreti aziendali” a “consulente, guida e innovatore” (Roussy 2013). Significativamente, la medesima letteratura e, più di recente, anche gli organismi professionali evidenziano l'impossibilità di trasporre automaticamente alle amministrazioni pubbliche strutture e sistemi di controllo tipici del settore privato. Ciò a causa delle caratteristiche distintive delle amministrazioni pubbliche quali la molteplicità di attori, interessi, responsabilità, rapporti d'agenzia e, conseguentemente, strutture di *governance* e relazioni di *accountability* stratificatesi nel tempo (Borgonovi 1984; Hyndman et al. 2014; Ellwood & Garcia-Lacalle 2016; Langella et al. 2021; IIA 2024).

Più recentemente, la letteratura ha anche evidenziato come, di fronte a crisi economiche, climatiche, sociali, sanitarie, ecc., il settore pubblico sia “*the ultimate bearer of major societal risks*” e debba essere in grado non solo di gestire questi rischi, ma anche di anticiparli (Roberts 2020). Questa caratterizzazione sottende un'evoluzione del concetto di rischio (Spira & Page 2003) che va ben oltre i rischi tipici del contesto di impresa (Black 2005).

Nella pubblica amministrazione italiana, il superamento del tradizionale approccio al controllo, incentrato sul controllo preventivo di legittimità e sulle verifiche di conformità (Borgonovi 1988), è stato avviato negli anni Novanta, anche per l'influenza esercitata dal contesto internazionale e, in particolare, dall'iniziativa di *Public Internal Financial Control* promossa dalla Commissione Europea. Con il d.lgs. 286/1999, il legislatore delegato ha riformato i controlli interni delle amministrazioni pubbliche, definendone i quattro pilastri: controllo strategico, controllo di gestione, controllo di regolarità amministrativa e contabile, valutazione della dirigenza (Pavan & Fadda 2013). I provvedimenti normativi che si sono susseguiti hanno, tuttavia, generato un quadro frammentato e disorganico, spesso caratterizzato dal mancato coordinamento tra i diversi organi di controllo nonché dall'assenza di un orientamento alla gestione dei rischi (Fadda & Paglietti 2016), sviluppatosi “per aggiunta progressiva di componenti” (Cantù 2014, p. 35) e senza una regia complessiva di sistema (Langella et al. 2023).

* * *

All'interno del settore pubblico italiano, un caso particolarmente interessante di sviluppo della funzione di IA è rappresentato dal Servizio Sanitario Nazionale (SSN), anche per le riflessioni svolte e le iniziative avviate nell'ultimo decennio.

Le aziende sanitarie si caratterizzano per la compresenza di diverse tipologie di rischio – tra cui si annoverano, a titolo non esaustivo, quello clinico, di sicurezza sui luoghi di lavoro, di *compliance*, corruttivo, di *reporting*, di sicurezza informatica (Brusoni et al. 2014). Ciò si è tradotto nella progressiva introduzione e stratificazione (Cantù 2014) di strumenti di controllo sia propri del tradizionale modello burocratico sia di matrice tipicamente aziendale, ciascuno disciplinato da una specifica normativa, da proprie metodologie e da propri canali di comunicazione. Si pensi, in particolare, ai tipici controlli di secondo livello presenti nelle aziende sanitarie pubbliche: controllo di gestione, prevenzione della corruzione e trasparenza, antiriciclaggio, prevenzione e protezione dei lavoratori, *privacy*, *data protection officer* ecc. Suddetti controlli si sono, quindi, sviluppati e consolidati secondo una logica di tipo funzionale, per “silos” non comunicanti.

In anni più recenti, l'assenza di una gestione integrata dei rischi e la conseguente necessità di sistematizzazione del complessivo sistema dei controlli interni ha trovato una possibile risposta nella funzione di IA. In quanto terzo livello di controllo, l'IA si propone come funzione in grado di revisionare i processi aziendali in un'ottica di sviluppo e di valutare la capacità dell'azienda di prevenire e mitigare in ottica integrata i propri rischi (Trincherò et al. 2023; Cantù et al. 2024).

Una significativa spinta per l'introduzione dell'IA nelle aziende sanitarie pubbliche italiane è derivata dai Percorsi Attuativi della Certificabilità (PAC) dei bilanci (DM 17/09/2012; DM 01/03/2013). In quanto “programmi d'azione finalizzati al raggiungimento degli standard organizzativi, contabili e procedurali necessari a garantire la certificabilità dei bilanci”, i PAC hanno richiesto alle aziende sanitarie un attento riesame delle proprie procedure amministrativo-contabili, offrendo un'occasione per la riprogettazione dei processi, la riorganizzazione delle responsabilità, nonché la sistematizzazione e il consolidamento del sistema dei controlli (Anessi Pessina et al. 2011; Persiani 2012; Langella et al. 2022).

Seppur con ampie differenze interregionali, la conclusione dei PAC ha lasciato alle aziende sanitarie pubbliche che hanno investito

in modo più sostanziale sul “percorso” una significativa eredità, che comprende tra l’altro: un sistema sufficientemente organico di procedure amministrativo-contabili formalizzate; un insieme di controlli interni basati sui principi della tracciabilità dei dati e della segregazione delle funzioni; la percezione della certificazione del bilancio come mezzo e non come fine; più in generale, una nuova sensibilità verso le tematiche del controllo interno e della gestione dei rischi, nonché la consapevolezza di dover ridefinire la *governance* dei controlli al fine di una loro integrazione e razionalizzazione (Cantù 2014; Langella et al. 2022).

Tale necessità di sistematizzazione, richiamata anche da strumenti di programmazione integrata quali il PIAO, ha favorito l’istituzione e lo sviluppo della funzione di IA. Infatti, da una parte, l’IA risponde alle esigenze di supervisione del processo di aggiornamento continuo delle procedure amministrativo-contabili nonché di potenziamento del SCIGR; dall’altra, le procedure e i controlli sviluppati nell’ambito dei PAC hanno rappresentato un utile punto di partenza per una più completa e sistematica mappatura dei rischi e dei controlli.

Ad oggi, l’introduzione e lo sviluppo della funzione di IA non sono avvenuti in maniera uniforme nel SSN. Particolarmente dirimente è stato il ruolo della Regione, cruciale per imporre o incoraggiare l’istituzione della funzione, accrescerne la legittimazione, dare impulso alle fasi di pianificazione, svolgimento, coordinamento, monitoraggio e consolidamento degli *audit* (Langella et al. 2023; Anessi Pessina et al. 2024). Il capitolo II presenta lo stato dell’arte e le linee di tendenza dell’IA nelle aziende sanitarie pubbliche italiane, come emergono da due iniziative di Cerismas: una recente ricerca in tema di “Scelte e pratiche aziendali relative all’introduzione e allo sviluppo della funzione di Internal Audit nelle aziende sanitarie pubbliche italiane” (Anessi Pessina et al. 2024) e la “Community of Practice per esperti di Internal Audit in sanità”¹.

¹Per maggiori dettagli si veda: <https://www.cerismas.com/formazione/learning-by-doing/community-of-practice-esperti-internal-audit>

II. L'Internal Audit nelle aziende sanitarie pubbliche italiane: stato dell'arte e linee di tendenza

2.1. *I risultati della ricerca sulle “Scelte e pratiche aziendali relative all'introduzione e allo sviluppo della funzione di Internal Audit nelle aziende sanitarie pubbliche italiane”*

A fine 2022, Cerismas ha effettuato una mappatura della funzione di IA nelle aziende sanitarie pubbliche italiane. I dati sono stati raccolti attraverso la somministrazione di un questionario *online* indirizzato ai responsabili aziendali della funzione di IA. Gli indirizzi *e-mail* sono stati raccolti attraverso una ricerca manuale sui siti *web* delle singole aziende. Per 102 aziende non è stato possibile reperire l'indirizzo *e-mail* del responsabile aziendale della funzione di IA, verosimilmente perché la funzione non era ancora stata istituita. In totale, quindi, sono stati raccolti gli indirizzi *e-mail* dei responsabili della funzione di IA di 114 aziende, pari al 53% della popolazione di riferimento.

Il questionario è stato compilato da 62 rispondenti, con un tasso di risposta pari al 54%. Nella distribuzione geografica dei rispondenti prevalgono le aziende del nord Italia (77%), con una forte rappresentanza dei Servizi Sanitari Regionali (SSR) di Lombardia, Veneto ed Emilia-Romagna. Seguono il sud e le isole (18%), mentre poche risposte sono pervenute dal centro Italia (5%). La metodologia della ricerca e i relativi risultati sono stati dettagliatamente illustrati in un articolo pubblicato nella rivista *Azienda Pubblica* (Anessi Pessina et al. 2024). La Tabella 1 sintetizza i principali punti di forza e di debolezza della funzione di IA nelle aziende sanitarie pubbliche italiane come emergono dai risultati della ricerca.

Tabella 1 - *Principali punti di forza e di debolezza della funzione di IA nelle aziende sanitarie pubbliche italiane*

Punti di forza	Punti di debolezza
Direzione o coordinamento da parte della Regione: sostiene la legittimazione della funzione, consente la condivisione di un linguaggio e una metodologia di lavoro e, in base alle configurazioni assunte, può anche favorire l'indipendenza della funzione. Creazione di gruppi interaziendali, fondamentali per le fasi di pianificazione e svolgimento degli <i>audit</i>, nonché per la condivisione di un linguaggio e una metodologia di lavoro. Frequente posizionamento organizzativo in staff alla Direzione Generale. Coinvolgimento e supporto della Direzione Generale: sostiene la legittimazione della funzione e ne tutela l'indipendenza. Profilo qualificato dei responsabili dell'IA in termini di <i>background</i> formativo e professionale. Ampliamento degli ambiti di attività della funzione. Collaborazione con altre unità organizzative aziendali (gruppi di lavoro multidisciplinari).	Scarsità di risorse a disposizione. Mancata istituzione di un'unità organizzativa specificamente ed esclusivamente dedicata alle attività di IA. Commistione di ruoli, con affidamento al responsabile IA di altri incarichi all'interno dell'azienda. Frequente coinvolgimento dell'IA in attività gestionali. Scarsità di collaborazione e di flussi informativi da e verso gli altri organi di controllo aziendale. Terminologia, metodologie e strumenti di lavoro propri dell'IA non sempre pienamente agiti.

Fonte: adattato da Anessi Pessina et al. (2024).

Innanzitutto, la ricerca conferma l'influenza esercitata dalla Regione. La variabilità delle risposte fornite dalle aziende, infatti, diminuisce all'interno del medesimo SSR o di gruppi di SSR per certi versi

assimilabili (per esempio, le Regioni in Piano di Rientro). Il *commitment* della Regione emerge, quindi, come cruciale per accrescere la legittimazione della funzione di IA. L'esistenza di una regia regionale nelle fasi di pianificazione, di svolgimento degli *audit*, di coordinamento ed eventuale monitoraggio e di consolidamento dei risultati può dare un notevole impulso allo sviluppo della funzione nonché, in base alle configurazioni assunte, anche contribuire a garantirne l'indipendenza (*infra*). La ricerca evidenzia, inoltre, il significativo contributo al consolidamento della funzione che deriva dalla costituzione di gruppi di lavoro interaziendali, anche multidisciplinari, per la condivisione di un linguaggio e di una metodologia di lavoro.

Sempre con riferimento alla *governance*, ma in una prospettiva aziendale, è apprezzabile la scelta, relativamente diffusa (50% delle aziende che hanno istituito una funzione dedicata di IA), di un posizionamento organizzativo in staff alla Direzione Generale, come tra l'altro previsto dagli standard professionali. Questo posizionamento tutela l'indipendenza della funzione e ne favorisce la legittimazione, soprattutto in presenza di un forte coinvolgimento e supporto da parte della Direzione stessa nella definizione del piano di *audit* (punteggio medio attribuito dai rispondenti: 6,8 su 10), nella condisione delle risultanze e delle azioni da intraprendere (6,8) nonché nella fase di *follow up* (6,4).

Dall'analisi è emerso, inoltre, un profilo molto qualificato dei responsabili dell'IA dal punto di vista del *background* sia formativo (il 95% dei rispondenti ha conseguito un titolo di studio pari o superiore alla laurea magistrale) sia professionale (in media, 5 anni di esperienza pregressa di IA in sanità, seppur con un'elevata variabilità). Molto frequente risulta anche l'investimento in percorsi formativi su tematiche rilevanti per l'IA (l'89% dei rispondenti vi ha preso parte negli ultimi tre anni).

Analogamente a quanto testimoniato dalla letteratura internazionale, la funzione si è evoluta nel tempo, ampliando gli ambiti del proprio ruolo e della propria attività. Il 66% dei rispondenti dichiara di svolgere attività di *assurance* e il 49% attività di consulenza. Combinando le risposte relative ai due ambiti di attività, circa un terzo dei rispondenti (31%) svolge attività sia di *assurance* sia di consulenza, mentre un altro terzo (34%) si focalizza sull'*assurance* e il 18% sulla consulenza. La gamma di *audit* svolti all'interno di un'azienda

(Tabella 2), inoltre, comprende solitamente due (41%) o tre (20%) tipologie, mentre più rare sono le aziende che si focalizzano su una sola tipologia di *audit* (16%) o che, al contrario, svolgono una gamma di *audit* ancora più ampia (12%). In particolare, agli *audit* di tipo *compliance* ed eventualmente *financial* – tradizionalmente diffusi nella pubblica amministrazione – si è aggiunto l'*operational audit*. Quest'ultimo si caratterizza per l'elevato contenuto consulenziale volto a valutare, mediante analisi di processo trasversali alle funzioni aziendali, l'effettiva possibilità di conseguimento degli obiettivi prefissati, nonché l'efficacia e l'efficienza nella realizzazione degli stessi.

Infine, l'ampliamento del ruolo e delle attività dell'IA ha inevitabilmente richiesto un maggior coordinamento con le altre unità organizzative aziendali, anche attraverso la creazione di gruppi di lavoro multidisciplinari, per la mappatura dei processi e la valutazione dei rischi e dei controlli. Questo risultato è particolarmente significativo vista l'importanza delle relazioni di collaborazione con i soggetti *auditati* per un efficace esercizio della funzione di IA.

Tabella 2 - *Ambiti di attività della funzione di IA nelle aziende sanitarie pubbliche italiane*

Ambiti di attività	Percentuale
<i>Operational audit</i>	70%
<i>Compliance audit</i>	67%
<i>Financial audit</i>	41%
<i>Fraud audit</i>	15%
<i>IT audit</i>	11%
Compresenza di più tipologie	Percentuale
1 tipologia di <i>audit</i>	16%
2 tipologie di <i>audit</i>	41%
3 tipologie di <i>audit</i>	20%
4 tipologie di <i>audit</i>	10%
5 tipologie di <i>audit</i>	2%

Fonte: Anessi Pessina et al. (2024).

L'analisi, però, ha messo in luce anche una serie di aspetti che necessitano di essere potenziati.

Innanzitutto, è frequente l'assenza di personale dedicato a tempo pieno e in modo esclusivo all'attività di IA; anche il personale destinato solo parzialmente alla funzione è mediamente molto limitato.

Questo spiega, tra l'altro, alcune inadeguatezze rilevate nell'assetto organizzativo, quali la mancata istituzione, nella maggioranza del campione, di un'unità organizzativa specificamente ed esclusivamente dedicata alle attività di IA (61%) o, ancora più significativamente, la commistione di ruoli (74%). Il responsabile dell'IA, infatti, ricopre frequentemente anche altri incarichi all'interno dell'azienda, vedendosi affidate responsabilità relative a controlli di secondo livello (quali, ad esempio, prevenzione della corruzione e trasparenza, qualità e accreditamento, rischio clinico, *data protection officer*) o, addirittura, di primo livello (quali, ad esempio, ufficio personale, URP). Ciò genera, tra l'altro, potenziali problemi di indipendenza e obiettività della funzione di IA. Particolarmente critico, inoltre, è il frequente (33% dei rispondenti) coinvolgimento diretto dell'IA nella gestione in termini, per esempio, di svolgimento di attività di controllo di primo e secondo livello, di assunzione di decisioni inerenti alle azioni da intraprendere per fronteggiare i rischi, di modifica e aggiornamento delle procedure aziendali.

Un'ulteriore criticità riguarda la relazione con gli altri organi aziendali di controllo. Sorprende, infatti, la scarsità di collaborazione e di scambi informativi. Gli altri organi aziendali di controllo esercitano un peso marginale nella definizione dei contenuti del piano di *audit*, nell'identificazione delle fasi e delle attività, nella valutazione dei rischi e dei controlli. Inoltre, non sono generalmente previste forme strutturate di condivisione degli esiti dei controlli e delle eventuali azioni di miglioramento.

Infine, le metodologie e gli strumenti di lavoro propri dell'IA non vengono sempre pienamente agiti (Tabella 3). In questa fase di sviluppo della funzione e coerentemente con la necessità di legittimarne il ruolo, è fondamentale consolidare le conoscenze e le abilità professionali in termini, per esempio, di valutazione del rischio inerente e residuo, analisi del disegno dei controlli, impostazione e svolgimento dei test sull'effettivo funzionamento dei controlli stessi.

Tabella 3 - *Metodologie e strumenti di lavoro impiegati dalla funzione di IA nelle aziende sanitarie pubbliche italiane*

Metodologie e strumenti di lavoro	Percentuale
Conseguimento di certificazioni in tema di <i>audit</i>	8%
Definizione del piano di <i>audit</i> fondata su una mappatura dei processi aziendali prioritari e dei relativi rischi	89%
Valutazione separata dei concetti di rischio inerente e rischio residuo	54%
Valutazione dei rischi in termini di probabilità e impatto	79%
di cui valutazione separata dei due aspetti	58%
di cui valutazione congiunta dei due aspetti	42%
Classificazione delle tipologie di rischio	66%
Analisi e valutazione del disegno dei controlli	71%
Attività di test per la verifica dell'effettivo funzionamento dei controlli	59%

Fonte: Anessi Pessina et al. (2024).

2.2. *Evidenze emerse nella Community of Practice per esperti di Internal Audit in sanità*

La Community of Practice si configura come un'aggregazione informale di attori che, in determinati contesti sociali e organizzativi, si costituiscono spontaneamente attorno a pratiche di lavoro comuni. Nell'ambito della Community si sviluppa solidarietà sui problemi, condividendo scopi, saperi pratici, significati e linguaggi. Si generano, per questa via, processi di apprendimento individuale e collettivo e si arricchiscono le competenze spendibili per il raggiungimento degli obiettivi attesi dal ruolo ricoperto. Le Communities of Practice si alimentano di contributi reciproci legati alla consapevolezza di partecipare a un'impresa comune, scambiando e acquisendo repertori condivisi di linguaggi, *routine* d'azione, storie, valori, strumenti e oggetti specifici che caratterizzano le diverse esperienze e convergo-

no in un comune riconoscimento di conoscenze da impiegare e di azioni da intraprendere nei rispettivi contesti di appartenenza.

A partire da settembre 2021, Cerimas ha sviluppato la “Community of Practice per esperti di Internal Audit”, finalizzata a promuovere – sulla base di un pervasivo confronto e interazione reciproca – processi di apprendimento individuale e organizzativo. La Community offre agli *auditor* un luogo di confronto, di dibattito e di crescita comune che, in ossequio agli standard internazionali della professione, valorizza la specificità del settore sanitario e propone soluzioni ai molteplici problemi che lo caratterizzano.

Nello specifico, i membri della Community, anche tramite l’interazione con esperti del settore e della professione, hanno fatto emergere alcune tematiche di particolare rilevanza per lo sviluppo della funzione nelle aziende sanitarie italiane.

In primo luogo, esiste un’avvertita necessità di disegnare *risk model* aziendali che guidino un ripensamento e una riprogettazione del sistema dei controlli. Come già precedentemente accennato, i controlli esistenti sono il risultato di una progressiva stratificazione che in molti casi non ha seguito l’evoluzione dei rischi da presidiare. Tali controlli, inoltre, vengono spesso interpretati e svolti in modo prevalentemente adempimentale. Un’interessante evoluzione in tal senso è la revisione attualmente in corso in alcune Regioni relativamente alle procedure PAC. Tipicamente, nella prima stesura, le procedure PAC sono state redatte fotografando la situazione esistente, quindi senza rimettere in discussione il disegno e l’effettivo funzionamento dei controlli. Più recentemente, alcune Regioni hanno promosso una riflessione sui rischi sottostanti a ciascuna fase procedurale in modo da valutare ed eventualmente rafforzare l’adeguatezza dei controlli stessi. Ciò costituisce un significativo passaggio da un sistema *control oriented* ad uno *risk oriented*.

In questo ripensamento, una necessità di particolare rilievo è mettere a sistema le attività dei controlli di secondo livello in una prospettiva di *combined assurance*. Tradizionalmente, infatti, nelle aziende sanitarie le funzioni di controllo di secondo livello si sono configurate come “silos” non comunicanti, ciascuna con proprie specificità in termini di normativa di riferimento, pianificazione delle attività, tecniche di analisi dei processi, dei rischi e dei controlli, contenuti

e destinatari della reportistica. Ne derivano significative lacune e sovrapposizioni.

Tra le funzioni di controllo di secondo livello, meritano un'attenzione particolare i rapporti tra l'IA e il rischio clinico e la prevenzione della corruzione e trasparenza. Rispetto al rischio clinico, i processi di prevenzione, diagnosi, cura e riabilitazione sono tradizionalmente visti come dominio pressoché esclusivo dei professionisti dell'area sanitaria. Di conseguenza, frequentemente il rischio clinico e il relativo sottosistema dei controlli restano esclusi dal perimetro dell'IA. Almeno in termini di impatto, tuttavia, il rischio clinico rappresenta uno dei principali rischi a cui l'azienda sanitaria è esposta. Quanto alla prevenzione della corruzione e trasparenza, è significativo il fatto che la normativa in molti passaggi attribuisca a questa funzione caratteristiche proprie di un terzo livello di controllo, generando evidenti sovrapposizioni con le responsabilità dell'IA. Diventa, quindi, essenziale distinguere i due ruoli oppure assegnare al Responsabile IA anche il ruolo di Responsabile della prevenzione della corruzione e della trasparenza².

Un ulteriore aspetto di attenzione è rappresentato dalla frequente scelta nelle aziende di coinvolgere direttamente l'IA nella gestione dei rischi emergenti. Negli ultimi anni ne hanno rappresentato degli esempi i rischi legati alla *privacy* o alla rendicontazione dei progetti PNRR.

Da ultimo, rispetto alle modalità di lavoro, appare forte l'esigenza di standardizzare gli strumenti di programmazione e di *reporting* dell'attività e di potenziare le tecniche per lo svolgimento degli *audit*. Tipicamente, gli standard professionali definiti a livello nazionale o internazionale rispondono a questa esigenza. Gli standard attuali, tuttavia, sono definiti con riferimento ai contesti normativi e regolatori delle imprese e ai loro assetti di *governance*, organizzativi e di finanziamento. Solo recentemente l'*Institute of Internal Auditors* (IIA),

² Quest'ultima scelta viene esplicitamente suggerita nel documento "Governance delle Funzioni di Controllo nel Settore Pubblico" (Comitato per il Settore Pubblico di AIIA 2020, p. 18) e giustificata sottolineando che essa sarebbe: "[i]n linea con le indicazioni dell'ANAC in materia, che nel PNA 2018 raccomanda di «promuovere l'interazione e il coordinamento delle strutture preposte e valuta positivamente le scelte volte ad attribuire l'incarico di RPCT al responsabile dell'Audit o di altra struttura che svolge controlli interni»".

nell’emanazione dei nuovi standard professionali (IIA 2024), ha riconosciuto l’importanza di declinare le peculiarità di esercizio della funzione di IA nel settore pubblico. A livello europeo, il *Public Sector Committee* della *European Confederation of Institutes of Internal Auditing* ha recentemente pubblicato un documento che discute le principali modifiche, i nuovi requisiti, le interpretazioni specifiche e alcune raccomandazioni pratiche per facilitare l’implementazione dei *Global Internal Audit Standards* nel settore pubblico (ECIIA 2024).

* * *

Complessivamente, dunque, la funzione di IA può generare un significativo valore aggiunto per le aziende sanitarie. A tal fine, tuttavia, necessita di venire ulteriormente sviluppata e consolidata. Dalle evidenze qui presentate, nonché dalle altre attività di ricerca e formazione svolte da Cerismas sul tema (Appendice A), emergono alcune raccomandazioni al riguardo, presentate nel successivo capitolo III.

III. Raccomandazioni per lo sviluppo e il consolidamento della funzione di Internal Audit nel SSN

1. La funzione di IA deve mantenersi indipendente e obiettiva.

L'indipendenza e l'obiettività rappresentano caratteristiche definitorie e irrinunciabili dell'IA. Per tutelarle, occorre innanzi tutto un opportuno posizionamento organizzativo, in staff alla Direzione Generale o, se presente, al Consiglio di Amministrazione o a un organo equivalente. Come accennato in precedenza, all'indipendenza possono contribuire anche la presenza di un coordinamento regionale e l'effettuazione di *audit* da parte di gruppi di lavoro interaziendali.

Una fonte di tutela spesso ancora sottovalutata nelle aziende sanitarie pubbliche italiane, inoltre, è rappresentata dai *Global Internal Audit Standards* predisposti dall'*Institute of Internal Auditors* (IIA 2024). I *Global Internal Audit Standards* sono un insieme di principi e linee guida che regolano la pratica professionale dell'IA a livello internazionale. Si articolano in 5 sezioni, 15 principi e 52 standard. Indipendenza e obiettività sono, appunto, due dei principi e vengono definiti rispettivamente come la "libertà da condizionamenti che possono minacciare la capacità della funzione Internal Audit di assolvere alle proprie responsabilità senza pregiudizi o distorsioni" e "l'attitudine di imparzialità che consente agli Internal Auditor di formulare giudizi professionali, adempiere alle proprie responsabilità e realizzare il Purpose dell'Internal Auditing senza compromessi". La necessità di aderire ai *Global Standards* ha, tra l'altro, proprio lo scopo di aiutare l'*internal auditor* a resistere a eventuali pressioni indebite.

Significativamente, lo Standard 6.2 stabilisce che il responsabile della funzione di IA debba "sviluppare e mantenere aggiornato l'*Internal Audit Charter*, che deve specificare almeno i seguenti punti": (i) la finalità dell'IA; (ii) l'impegno ad aderire ai *Global Internal Audit Standards*; (iii) il mandato di *audit*, comprensivo dell'ambito e delle

tipologie di servizi di *audit*, nonché delle responsabilità del *Board* nel supportare la funzione di IA; (iv) il posizionamento organizzativo dell'IA. L'approvazione formale, da parte della Direzione Aziendale, del mandato di *audit* e del più complessivo *Internal Audit Charter* rappresenta dunque un'ulteriore fondamentale modalità per tutelare l'indipendenza della funzione di IA.

Infine, è doveroso ricordare che la mancanza di personale dedicato a tempo pieno e in modo esclusivo all'attività di audit, con la conseguente commistione di ruoli rischia inevitabilmente di compromettere, almeno in parte, l'indipendenza e l'obiettività della funzione di IA nelle aziende sanitarie pubbliche. Da qui la necessità di riflettere sulle strategie per garantire un adeguato dimensionamento organizzativo, eventualmente anche individuando *auditor* con un ruolo sovra-aziendale.

* * *

2. *La funzione di IA deve svolgere attività di assurance e consulenza, ma non deve essere coinvolta nella gestione.*

I *Global Internal Audit Standards* prevedono espressamente che l'IA svolga attività di *assurance* e consulenza (IIA 2024) ed è, quindi, essenziale che l'IA delle aziende sanitarie ricopra entrambi i ruoli.

L'attività di *assurance* è definita come “attestazione volta ad aumentare il livello di fiducia degli *stakeholder* nei processi di *governance*, *risk management* e controllo di un'organizzazione riguardo ad un'attività, un tema, una situazione oggetto di *audit*, rispetto ai criteri stabiliti” (IIA 2024). Al riguardo, l'IA deve comunque proporsi in modo collaborativo, evitando di adottare atteggiamenti ispettivi.

L'attività di consulenza ha acquisito crescente centralità nel modo in cui la professione stessa si percepisce e si propone. Nelle aziende sanitarie pubbliche, la consulenza svolta dall'IA è essenziale per diffondere la cultura e gli strumenti di identificazione e valutazione dei rischi e dei controlli, a maggior ragione nella fase iniziale di ridisegno complessivo del SCIGR.

Il coinvolgimento dell'Internal Audit nella gestione, invece, non

è condivisibile. Le debolezze del SCIGR non possono essere superate ricorrendo a una “supplenza” da parte dell’IA.

Almeno in parte, il coinvolgimento nella gestione scaturisce dall’assenza di personale interamente dedicato all’IA e dall’affidamento di ulteriori incarichi al responsabile dell’IA. Rispetto a queste criticità organizzative, una possibile risposta è ravvisabile nell’esperienza di quei SSR che hanno deciso di accentrare o comunque coordinare a livello regionale la funzione di IA. In Veneto, per esempio, la Regione (tramite Azienda Zero) pianifica, gestisce, coordina, monitora e consolida il processo di *auditing* dell’intero SSR. In Emilia-Romagna, il ruolo della Regione è meno pervasivo, ma comunque fondamentale per la pianificazione e il coordinamento interaziendale. Una gestione sovra-aziendale del processo di *audit* consente di creare gruppi di lavoro interaziendali di *internal auditor* specializzati, con potenziali benefici anche in termini di indipendenza della funzione di IA. Allo stesso tempo, va ricordato che i rischi e le responsabilità regionali non sono perfettamente sovrapponibili ai rischi e alle responsabilità aziendali. È quindi necessario che, anche nell’ambito di una gestione sovra-aziendale del processo di *audit*, la Direzione Aziendale continui a rappresentare un riferimento importante nella pianificazione delle attività di *audit* e nella gestione delle relative risultanze.

* * *

3. La funzione di IA non deve diventare l’ennesima sovrastruttura di controllo ma deve generare valore aggiunto per l’azienda.

Potenzialmente la funzione di IA può generare significativo valore aggiunto per l’azienda. Prevenire e mitigare i rischi, infatti, è nell’interesse dell’azienda, del suo *management* e dei suoi professionisti. Sono loro a subire le conseguenze di eventuali eventi avversi. È, quindi, nel loro interesse evitare che tali eventi si manifestino e, nel caso, limitarne gli effetti negativi. Laddove tali eventi si verificano, inoltre, è nel loro interesse poter dimostrare di aver adottato e attuato soluzioni che avrebbero ragionevolmente dovuto prevenire o mitigare il rischio.

Peraltro, uno degli approcci più innovativi alla gestione dei rischi incoraggia una prospettiva proattiva che vede i rischi non solo come minacce, bensì anche come opportunità di miglioramento.

Naturalmente, non è, invece, nell'interesse dell'azienda, del suo *management* e dei suoi professionisti aggiungere un ulteriore “mattoncino” o “silo” al SCIGR senza coordinarlo con quanto già esiste, per sole finalità isomorfe e con la possibilità di creare l'ennesima “soluzione in cerca di problemi”.

Per generare valore aggiunto, inoltre, l'IA deve tenere sempre in considerazione l'economicità dei controlli. Le risorse sono necessariamente scarse e vanno impiegate in misura proporzionale ai rischi. È, inoltre, essenziale evitare duplicazioni e sovrapposizioni di controlli. Allo stesso tempo, azzerare i rischi è impossibile. Uno dei benefici che la funzione di IA può offrire, tuttavia, è una maggiore consapevolezza circa i rischi che l'azienda non sta presidiando e, quindi, implicitamente sta accettando.

Al riguardo, è anche opportuno ribadire che la definizione della “propensione al rischio” (ossia, la disponibilità ad accettare qualche livello di rischio, che può anche essere diverso per aree di rischio diverse e/o per ambiti di attività diversi) spetta alla Direzione Aziendale e non all'IA. Un elemento forse meno evidente è che le metriche di valutazione dei rischi in termini di probabilità e di impatto (per esempio, quando un impatto è da ritenersi “molto elevato”) riflettono la propensione al rischio dell'azienda e devono quindi essere definite in accordo con la Direzione Aziendale.

* * *

4. La funzione di IA non deve sostituirsi ai controlli di primo e secondo livello. Deve, invece, contribuire a rafforzarli e coordinarli.

Come detto, la funzione di IA si caratterizza spesso per la scarsità di collaborazione e di scambi informativi con gli altri organi di controllo aziendale. Ciò forse anche perché percepisce una certa debolezza dei controlli di primo e secondo livello. Al riguardo, però, la soluzione non può essere che l'IA si faccia direttamente carico dei controlli di primo e secondo livello. È, inoltre, necessario evitare che,

con l'introduzione dell'IA, i soggetti deputati ai controlli di primo e secondo livello si percepiscano (anche opportunisticamente) come sollevati dalle proprie responsabilità. Tutto ciò, infatti, sarebbe in evidente contraddizione con la qualificazione dell'IA quale controllo di terzo livello. Suddette criticità evidenziano la necessità di distinguere e chiarire meglio il ruolo, rispettivamente, dei controlli di primo, secondo e terzo livello. In particolare, il terzo livello deve sviluppare una visione strategica ed essere in grado di tracciare le interdipendenze per garantire un approccio integrato alla *governance* e alla gestione dei rischi.

D'altra parte, la sistematizzazione e il coordinamento del complessivo SCIGR costituisce un obiettivo prioritario della funzione di IA. Al riguardo, significativi benefici possono derivare dall'applicazione della tecnica del *Control Risk Self Assessment* (di seguito CRSA) e, in particolare, dello strumento del *workshop* (Cantù et al. 2024). Il CRSA è definito dall'*Institute of Internal Auditors* (IIA 1999) come una tecnica di autodiagnosi, strutturata e analitica, basata su un approccio collaborativo, che utilizza le conoscenze e le competenze di dirigenti e altri soggetti operativi coinvolti in un dato processo al fine di: (i) identificare gli obiettivi prioritari e i rischi che ne ostacolano il conseguimento; (ii) valutare il sistema di controllo in essere, mettendone in luce le eventuali debolezze; (iii) determinare il livello di accettabilità dei rischi, coerentemente con la realizzazione degli obiettivi aziendali, e mantenere i rischi individuati al di sotto di tale soglia; (iv) fornire indicazioni per lo sviluppo di azioni di miglioramento al fine di ridurre i rischi emersi dall'autodiagnosi (Dittmeier 2011). Tra gli strumenti per la conduzione del CRSA, il più utilizzato è il questionario, che propone una serie di domande volte a focalizzare l'attenzione dei partecipanti sull'individuazione e la misurazione dei rischi e dei controlli (Allegrini & D'Onza 2003). Meno frequente è la metodologia del *workshop*, che prevede lo svolgimento di riunioni strutturate tra *management* e altri soggetti operativi coinvolti al fine di far emergere, attraverso l'analisi e la discussione, conoscenze, percezioni e giudizi dei partecipanti sui rischi, sulle loro cause e sulle possibili conseguenze, nonché sull'adeguatezza dei controlli esistenti in relazione a un determinato obiettivo o processo. Rispetto al questionario, il *workshop* incentiva maggiormente la partecipazione e la collaborazione, offrendo un'occasione per superare la visione

per “silos”, fornire una visione strategica d’insieme a tutto il personale coinvolto, comprendere le ricadute del proprio lavoro su quello degli altri, confrontarsi in un contesto neutrale, contemperare i diversi interessi in gioco, presidiare adeguatamente le varie tipologie di rischio, raggiungere una valutazione condivisa dei rischi, definire puntualmente i controlli (e i relativi *owner*), identificare le eventuali necessità di un loro potenziamento o depotenziamento, accrescere la responsabilizzazione del personale e migliorarne la motivazione, sviluppare un approccio sistemico e relazioni sinergiche. Nell’ambito dei *workshop*, l’IA svolge un ruolo quasi “maieutico”, pianificando e conducendo le attività e aiutando così il gruppo di lavoro a valutare obiettivi, rischi e controlli secondo una metodologia comune, a far emergere azioni di miglioramento condivise, nonché a individuarne le responsabilità. Lo sviluppo di una comune metodologia di valutazione dei rischi e dei controlli, in particolare, dovrebbe rappresentare una priorità per l’IA delle aziende sanitarie.

In prospettiva, infine, un possibile approccio ancora più avanzato è quello della *combined assurance*, in cui l’IA coordina la propria attività con quella di altre funzioni di controllo, per ridurre la frequenza e la ridondanza degli *audit*, accrescendo così l’efficienza della copertura di *assurance* e della comunicazione verso la Direzione Aziendale.

* * *

5. La funzione di IA deve dedicare particolare attenzione alla copertura dei complessivi rischi aziendali.

Si è detto che l’IA, quale controllo di terzo livello, deve valutare, rafforzare e coordinare i controlli di primo e secondo livello. Ciò facendo, l’IA non deve però mai dare per scontato che il sistema dei controlli esistenti copra tutti i rischi rilevanti a cui l’azienda è esposta. Le dinamiche di azienda e di ambiente, infatti, possono far sorgere nuovi rischi che sfuggono al sistema dei controlli esistenti. Ciò a maggior ragione in un contesto, quale quello del SSN, in cui i controlli sono frammentati e storicamente stratificati. Per esempio, alcuni rischi molto rilevanti rispetto ai quali il sistema si è recentemente trovato evidentemente impreparato sono le pandemie, la *cybersecurity*

and data security, il rischio idrogeologico e il rischio di aggressioni al personale sanitario.

L'IA, quindi, deve sempre disporre di un aggiornato catalogo dei rischi, anche attraverso il confronto con i colleghi del settore sanitario e di altri settori. Deve, inoltre, porsi sistematicamente domande che si possono esemplificare come segue: “quali sono i cinque rischi fondamentali a cui l'azienda deve far fronte?”; “quali sono i cinque rischi fondamentali a cui l'azienda dovrà far fronte tra tre anni?”.

* * *

6. Il rischio clinico e il relativo sottosistema dei controlli non possono restare permanentemente esclusi dal perimetro su cui l'IA esercita le funzioni di controllo di terzo livello.

Nelle aziende sanitarie pubbliche, i processi di prevenzione, diagnosi, cura e riabilitazione sono stati tradizionalmente visti come dominio esclusivo dei professionisti e della loro “autonomia professionale”. Un limite significativo dei processi di aziendalizzazione della sanità italiana è consistito proprio nella focalizzazione sui pur importanti elementi “di contorno” (gli assetti istituzionali, le strutture organizzative, i meccanismi operativi di pianificazione, programmazione e controllo nonché, seppur in misura minore, di gestione del personale). Solo più recentemente, con lo sviluppo delle funzioni di *supply chain*, logistica e *operations*, il *management* ha iniziato ad affrontare direttamente le questioni attinenti ai “processi produttivi” aziendali.

La stessa criticità rischia ora di riproporsi rispetto alla funzione di IA. Nel settore pubblico, il rispetto delle norme è la modalità fondamentale di perseguimento delle finalità istituzionali, il che giustifica il rilievo attribuito ai rischi di *compliance*. In molte aziende sanitarie pubbliche, l'introduzione della funzione di IA rappresenta uno sviluppo dei PAC, il che spiega la particolare attenzione ai rischi di tipo *financial* e *reporting*. Inoltre, la limitatissima disponibilità di risorse impone, nel breve periodo, che l'IA si focalizzi solo su alcune tipologie di rischio. Di qui, tra l'altro, anche il frequente posizionamento organizzativo della funzione di IA in staff alla Direzione Amministrativa (nella ricerca presentata al capitolo II, il 38% delle aziende che

hanno istituito una funzione dedicata di IA) anziché alla Direzione Generale, nonché la frequentissima (87%) scelta, come responsabile dell'IA, di persone che avevano ricoperto, in precedenza, incarichi di tipo amministrativo anziché sanitario.

A regime, però, è impensabile che il rischio clinico e il relativo sottosistema dei controlli restino esclusi dall'*audit universe* dell'IA. Almeno in termini di impatto, infatti, il rischio clinico è tra i principali rischi a cui l'azienda sanitaria è esposta. Naturalmente, ciò non significa che l'IA debba sostituirsi ai controlli di primo e secondo livello specificamente deputati a governare il rischio clinico. Significa, però, che l'IA dovrà progressivamente estendere il proprio ambito di attività per esercitare, anche nei confronti del rischio clinico e del relativo sottosistema dei controlli, le funzioni di *assurance* e di consulenza proprie del terzo livello di controllo.

* * *

7. La funzione di IA deve avere legittimazione normativa nazionale.

Ad oggi, l'istituzione e lo sviluppo della funzione di IA sono il frutto di scelte aziendali e, solo in alcuni casi, di iniziative regionali. L'auspicio è che, come, tra l'altro, già avvenuto per altri organi di controllo, all'IA venga dato un riconoscimento normativo nazionale volto a garantirne il rigore di applicazione e il corretto posizionamento organizzativo. La funzione di IA sembra, infatti, ben rappresentare la logica conseguenza di un percorso nazionale che, seppur con diverse tempistiche, persegue il rafforzamento e l'*assurance* del sistema dei processi di *governance*, di *risk management* e di controllo.

* * *

8. La professione di IA deve trovare riconoscimento anche ai fini concorsuali.

La definizione di IA (IIA 2024) richiede indipendenza, obiettività e un approccio professionale e sistematico. A tal fine, l'IA deve possedere un'ampia gamma di conoscenze e competenze tecniche e

relazionali. Questi requisiti devono essere tenuti in debita considerazione nell'individuazione dei soggetti a cui affidare la funzione di IA e, quindi, anche nei procedimenti concorsuali volti a selezionare i nuovi *auditor* delle aziende sanitarie. Da questo punto di vista diventa fondamentale sviluppare percorsi formativi (e, in prospettiva, certificazioni professionali) che attestino tali requisiti con specifico riferimento al settore pubblico. Ne discende, inoltre, che la posizione di *internal auditor* non dovrebbe essere assegnata come “incarico aggiuntivo”.

* * *

9. Per la funzione di IA è essenziale la legittimazione, nel duplice significato di “legittimarsi” ed “essere legittimata”.

La funzione di IA deve legittimarsi e “conquistarsi ‘un posto al tavolo’, ossia diventare un attore la cui opinione è tenuta in significativa considerazione” (Fountain 2016). A tale fine, la funzione deve apportare valore aggiunto e saper comunicare il valore aggiunto che apporta. La legittimazione va perseguita nei confronti della Direzione Aziendale, degli altri organi di controllo (a partire dalle funzioni deputate ai controlli di secondo livello) e dei soggetti *auditati*. Ciò non è semplice anche perché, solitamente, la Direzione Aziendale ha poco tempo ed energie da dedicare; gli altri organi di controllo hanno maggiore familiarità ed esperienza dell'IA nelle aree di propria competenza e hanno anch'essi accesso diretto alla Direzione Aziendale; i soggetti *auditati* potrebbero non essere necessariamente ferrati sui temi dei rischi e dei controlli e potrebbero manifestare forme di resistenza sia nei confronti di una funzione piuttosto recente quale l'IA sia verso l'assoggettamento al controllo in quanto tale. Di conseguenza, l'IA deve possedere e applicare: (i) conoscenze, capacità e competenze tecniche; (ii) competenze relazionali e di comunicazione; nonché (iii) integrità professionale. Deve, inoltre, rafforzare significativamente le fasi di *reporting* e *follow-up*, sapendo distillare le informazioni rilevanti in base alla tipologia di destinatari e insistendo sull'effettiva implementazione delle azioni di miglioramento. In merito, sarebbe auspicabile potenziare gli investimenti in formazione,

organizzare strutturati momenti di confronto interaziendale, nonché instaurare forme di collaborazione con le associazioni professionali, anche per il conseguimento di certificazioni. Da ultimo, ma non per importanza, risulta fondamentale l'allineamento strategico: l'IA deve essere un alleato nel conseguimento degli obiettivi e della missione aziendale, capace di integrarsi nell'organizzazione, spendersi su rischi emergenti e supportare il miglioramento generativo.

Allo stesso tempo, la Regione e la Direzione Aziendale devono legittimare la funzione di IA all'interno dell'azienda, per esempio dotandola di adeguate risorse professionali e finanziarie, partecipando alla definizione del piano di *audit*, dedicando attenzione alla fase di condivisione delle risultanze degli *audit* e di definizione delle azioni da intraprendere, sostenendo la cogenza delle raccomandazioni formulate e attribuendo particolare rilievo agli esiti dei *follow-up*.

* * *

10. La Regione deve svolgere un ruolo di “regia” nello sviluppo della funzione di IA nelle aziende sanitarie pubbliche.

Lo sviluppo della funzione di IA nel SSN è avvenuto in maniera differenziata sul territorio nazionale. Ciò anche per l'influenza esercitata da ciascuna Regione sulle proprie aziende. Negli ultimi venti anni, i SSR si sono progressivamente evoluti verso assetti caratterizzati da logiche collaborative e di programmazione centralizzata, in cui la Regione esercita un ruolo di capogruppo. Questi assetti presentano forti differenze interregionali. In base alla natura e all'intensità delle prerogative di governo esercitate dalla capogruppo e, conseguentemente, al potere, all'autonomia e alle responsabilità lasciate alle singole aziende sanitarie pubbliche, Cantarelli et al. (2017) identificano tre possibili tipologie di “gruppo sanitario pubblico regionale”, distinguendo tra capogruppo di pianificazione, capogruppo strategica e capogruppo direzionale. La capogruppo di pianificazione si focalizza sulla pianificazione degli obiettivi di sistema e sulla relativa allocazione delle risorse, lasciando alle aziende responsabilità strategiche e gestionali. La capogruppo strategica assume, oltre ai compiti di pianificazione, anche quelli di definizione delle strategie, lasciando

alle aziende solo la responsabilità gestionale. Infine, la capogruppo direzionale ha funzioni di pianificazione e definizione non solo delle strategie, ma anche delle procedure che le aziende devono applicare, limitandone così notevolmente l'autonomia. Naturalmente, questa classificazione va incrociata con quella che distingue le Regioni in base all'eventuale assoggettamento ai Piani di Rientro (Cuccurullo et al. 2010).

I peculiari e differenziati assetti di *governance* dei “gruppi sanitari pubblici regionali” influenzano inevitabilmente la configurazione assunta dalla funzione di IA e consentono di sperimentare diversi modelli di pianificazione, gestione e coordinamento dell'attività di *audit* svolta a livello aziendale. In ogni caso, però, affinché la funzione si sviluppi nelle aziende sanitarie pubbliche è essenziale che la Regione fornisca un esplicito impulso in tal senso. Anche nei gruppi privati, del resto, la funzione di IA è generalmente accentrata o, comunque, coordinata a livello della capogruppo (Allegrini & D'Onza 2003; Arena & Azzone 2007).

IV. Riflessioni conclusive

In conclusione, pare importante ribadire che nelle aziende sanitarie, come in ogni azienda, la presenza di un adeguato sistema di controllo interno e di gestione dei rischi è responsabilità della Direzione e non dell'IA.

Se la normativa, europea, italiana e regionale spinge sempre di più verso il potenziamento dei sistemi di controllo, la qualità della Direzione Aziendale verrà sempre più frequentemente valutata sulla base di questo aspetto. Al riguardo, la funzione di IA potrà offrire un essenziale contributo attraverso le proprie attività di *assurance* e consulenza.

Le raccomandazioni elencate in questo documento rappresentano tutte occasioni perché l'IA possa svolgere tale ruolo, in modo obiettivo e indipendente, generando un significativo valore aggiunto per le aziende sanitarie.

Appendice A - Attività di ricerca e formazione svolte da Cerismas sull'Internal Audit in sanità

Ricerca istituzionale Cerismas

- “La funzione di Internal Audit nel SSN” (2022-2024)

Corsi di formazione “elective”

- “La funzione di Audit Interno nelle aziende sanitarie” (sette edizioni, dal 2018)

Corsi di formazione “learning by doing”

- “Community of Practice per esperti di Internal Audit in sanità” (tre edizioni, dal 2021)

Progetti “ad hoc”

- Fondazione Don Carlo Gnocchi Onlus: Progetto di formazione “Il sistema di controllo interno: dai controlli di primo livello all'Internal Auditing” (2024)
- Regione Lombardia: Progetto di “Assistenza tecnica per la sperimentazione di metodologie e procedure di controllo interno nelle aziende sanitarie pubbliche in esito al Percorso Attuativo della Certificabilità dei bilanci” (2023-2025)
- Regione Lombardia: Progetto di “Assistenza tecnica per la manutenzione del Percorso Attuativo della Certificabilità dei bilanci delle Aziende sanitarie pubbliche, della Gestione Sanitaria Accentrata e del Consolidato SSR” (2020-2022);
- Regione Emilia-Romagna: Progetto di “Affinamento del Sistema di Controllo Interno delle aziende sanitarie della Regione Emilia-Romagna” (2021-2023)
- Regione Liguria: Progetto di “Affidamento dei servizi in ambito di sistemi informativi gestionali e sistemi di gestione dei proce-

dimenti amministrativi in favore degli enti del servizio sanitario” (2020-2023)

- Regione Abruzzo: *Training on the job* rivolto ai Servizi di Internal Audit all’interno del progetto di “Affidamento di servizi professionali di supporto nell’attuazione dell’art. 79” (2019-2021)
- ATS Insubria: Progetto formativo “Sviluppo della Funzione di Internal Auditing” (2018)

Bibliografia

Allegrini M., D'Onza, G. (2003), Internal Auditing and Risk Assessment in Large Italian Companies: an Empirical Survey, *International Journal of Auditing*, 7, pp. 191-208

Anessi Pessina E., Cantù E., Langella C. (2024), Scelte e pratiche aziendali relative all'introduzione e allo sviluppo della funzione di Internal Audit nelle aziende sanitarie pubbliche italiane, *Azienda Pubblica*, 37(1), pp. 15-45

Anessi Pessina E., Cantù E., Persiani N. (2011), Armonizzazione contabile e revisione dei bilanci nelle aziende sanitarie pubbliche, in Anessi Pessina E., Cantù E. (a cura di), *L'Aziendalizzazione della Sanità in Italia. Rapporto OASI 2011*, Milano: Egea, pp. 469-494

Arena M., Azzone, G. (2007), Internal audit departments: adoption and characteristics in Italian companies, *International Journal of Auditing*, 11 (2), pp. 91-114

Black J. (2005), The emergence of risk-based regulation and the new public risk management in the United Kingdom, *Public Law*, 3, pp. 510-546

Borgonovi E. (1984), Il sistema contabile degli istituti pubblici: caratteristiche, valutazione, prospettive, in AA.VV., (a cura di), *Studi e Ricerche della Facoltà di Economia e Commercio dell'Università di Parma*, Bologna: Patron, pp. 49-81

Borgonovi, E. (1988), I concetti di controllo burocratico e controllo manageriale nella pubblica amministrazione, *Azienda Pubblica*, 1(1), pp. 11-30

Borsa Italiana, Comitato per la Corporate Governance (2018), *Codice di autodisciplina*

Brusoni M., Trincherò E., Vescia, M. (2014), La gestione del rischio in sanità: elementi organizzativi e gestionali, in Aleo S., De Matteis R., Vecchio G. (a cura di), *La responsabilità in ambito sanitario*, Padova: Cedam, pp. 1151-1194

Cantarelli P., Lega F., Longo F. (2017), La regione capogruppo sanitaria: assetti istituzionali e modelli organizzativi emergenti, in CERGAS - Bocconi

(a cura di), *Rapporto OASI 2017. Osservatorio sulle Aziende e sul Sistema sanitario italiano*, Milano: Egea, pp. 363-381

Cantù E. (2014), *Il bilancio delle Aziende di Servizi Sanitari*, Milano: Egea

Cantù E., Langella C., Vannini I.E. (2025), Making sense of the internal audit function: towards internal controls integration and organizational learning, *Financial Accountability and Management*, e12413

Comitato per il Settore Pubblico di AIIA (2020), *Governance delle Funzioni di Controllo nel Settore Pubblico*, Associazione Italiana Internal Auditors – AIIA

CoSO (1992), *Internal Control – Integrated Framework*, Jersey City: Committee of Sponsoring Organizations of the Treadway Commission

CoSO (2013), *Internal Control – Integrated Framework*, New York: Committee of Sponsoring Organizations of the Treadway Commission

Cuccurullo C., Ferrè F., Lega F. (2010), I Piani di Rientro della spesa sanitaria: un’analisi comparative, in Cantù E. (a cura di), *L’aziendalizzazione della sanità in Italia. Il Rapporto OASI 2010*, Milano: Egea, pp. 225-260

Dittmeier C.A. (2011), *Internal Auditing: Chiave per la corporate governance*. Milano: Egea

ECIIA (2024), *Implementing the Global Internal Audit Standards in the European Public Sector – Practical guidance*, Public Sector Committee Project, European Confederation of Institutes of Internal Auditing

Ellwood, S., Garcia-Lacalle, J. (2016), Examining audit committees in the corporate governance of public bodies, *Public Management Review*, 18(8), pp. 1138-1162

Fadda I., Paglietti P. (2016), La lotta alla corruzione: più controlli interni e meno adempimenti, *Azienda Pubblica*, 28(1), pp. 81-96

Fountain L. (2016), *Leading the Internal Audit Function*, Auerbach

Hyndman N., Liguori M., Meyer R. E., Polzer T., Rota S., Seiwald J. (2014), The translation and sedimentation of accounting reforms. A comparison of the UK, Austrian and Italian experiences, *Critical Perspectives on Accounting*, 25(4-5), pp. 388-408

IIA (1999), *Control and Risk Self Assessment, Professional Briefing Note n. 14*, London: Institute of Internal Auditors United Kingdom and Ireland

IIA (2024), *Global Internal Audit Standards*, The Institute of Internal Auditors

Langella C., Anessi-Pessina E., Cantù E. (2021), What are the required qualities of auditors in the public sector?, *Public Money & Management*, 41(6), pp. 466-476

Langella C., Vannini I.E., Persiani N. (2023), What are the determinants of internal auditing (IA) introduction and development? Evidence from the Italian public healthcare sector, *Public Money & Management*, 43(3), pp. 268-276

Langella C., Vannini I.E., Persiani N., Marciacano M. (2022), L'Internal Auditing nel Servizio Sanitario Nazionale: l'esperienza della Regione Veneto e della Regione Emilia-Romagna, *Mecosan*, 123, pp. 7-27

Mihret D.G., Grant B. (2017), The role of IA in corporate governance: a Foucauldian analysis, *Accounting, Auditing & Accountability Journal*, 30(3), pp. 699-719

Pavan A., Fadda I. (2013), I controlli interni per il buon andamento del settore pubblico italiano, *Azienda Pubblica*, 26(4), pp. 431-449

Persiani N. (2012), Il controllo contabile del bilancio degli enti del S.s.n.: verso la certificabilità dei dati e dei bilanci, *Ragiusan*, 344, pp. 28-36

Roberts A. (2020), The Third and Fatal Shock: How Pandemic Killed the Millennial Paradigm, *Public Administration Review*, 80(4), pp. 603-609

Roussy M. (2013), Internal auditors' roles: From watchdogs to helpers and protectors of the top manager, *Critical Perspectives on Accounting*, 24(7-8), pp. 550-571

Roussy M., Perron, A. (2018), New Perspectives in Internal Audit Research: A Structured Literature Review, *Accounting Perspectives*, 17(3), pp. 345-385

Spira L.F., Page M. (2003), Risk management: The reinvention of internal control and the changing role of internal audit, *Accounting, Auditing & Accountability Journal*, 16(4), pp. 640-661

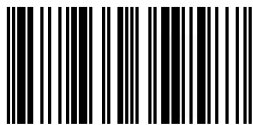
Trinchero E., Falivena C., Rappini V., Notarnicola E., Lecci F. (2023), Internal Auditing in Sanità: stato dell'arte e prospettive evolutive, in CERGAS - Bocconi (a cura di), *Rapporto OASI 2023*. Milano: Egea

Il Centro di Ricerche e Studi in Management Sanitario (CERISMAS) è un'associazione senza scopo di lucro costituita nel 2000 su iniziativa dell'Università Cattolica del Sacro Cuore e della Fondazione IRCCS Istituto Neurologico Carlo Besta.

La mission di CERISMAS è promuovere lo sviluppo dei sistemi manageriali a supporto dei processi clinico-assistenziali e amministrativi delle organizzazioni sanitarie e socio-sanitarie attivando e valorizzando il networking tra e con le aziende associate e privilegiando attività di ricerca, formazione e progetti sul campo, che siano focalizzate su contenuti e metodologie innovativi, sviluppate attraverso un rapporto fiduciario con un management orientato al cambiamento e finalizzate a generare concrete ricadute organizzative.

La formula istituzionale dell'Associazione adottata da CERISMAS, sin dalla sua costituzione, ha consentito al Centro di mettere a fattor comune con le aziende associate il rigore del metodo nell'attività di ricerca e la rilevanza dei temi indagati, che sono vicini ai "problemi reali" in una concretezza guidata e stimolata da coloro che operano sul campo.

Le competenze di CERISMAS coprono l'intero spettro del management sanitario, con particolare riferimento ai sistemi di pianificazione, programmazione e controllo, all'organizzazione aziendale e alla gestione del personale, alla logistica, ai sistemi contabili, ai processi di leadership e gestione del cambiamento.



9788834359587



VITA E PENSIERO

Progetto: studio grafico Andrea Musso