Università di Genova

MIPA
Master di II livello in
Innovazione nella Pubblica Amministrazione

## Università degli studi di Genova

## DIPARTIMENTO DI SCIENZE POLITICHE E INTERNAZIONALI

## Master di II livello in Innovazione nella Pubblica Amministrazione (MIPA)
## III edizione – a.a. 2022/2023

# LA FUNZIONE INTERNAL AUDIT E LA GOVERNANCE DEL SETTORE PUBBLICO

*-Un nuovo supporto ai processi di innovazione-*


Relatore

*Chiar.mo Prof. Luca Gandullia*

Correlatore

*Ing. Federico Grasso - ARPAL*

*Ing. Dario Lagostena - ARPAL*

Candidata

*Cinzia Barbieri*

***Ringraziamenti***

Ringrazio il Chiar.mo Prof. Luca Gandullia e la D.ssa Simona Tirasso, per avermi guidata e supportata in questo mio percorso accademico.

Un sentito grazie ad AIIA (Associazione Italiana Internal Auditors) per l'accesso alle informazioni, indispensabili alla realizzazione della mia tesi.

Ringrazio ARPAL, in particolare l'Ing. Federico Grasso e l'Ing. Dario Lagostena, per avermi dato la possibilità di svolgere il mio lavoro di tesi in una dimensione interessante e dinamica, che mi ha permesso di mettermi in gioco e fare un'esperienza che sarà preziosa per il mio futuro.

Alla mia famiglia, i miei amici, i miei compagni di Master ed a tutti quelli che hanno incrociato la loro vita con la mia, lasciandomi qualcosa di buono, in questo percorso intenso ed entusiasmante.

# INDICE

# INTRODUZIONE

Il presente lavoro ha l'obiettivo di riepilogare la "Governance" del sistema dei controlli e gestione dei rischi ("SCIGR"), attualmente presente nei principali cluster del Settore Pubblico, e di delineare le possibili evoluzioni dello stesso che consentano la creazione e lo sviluppo di una *Funzione Internal Audit (FIA)* [1]. Tale Funzione dovrà avere caratteristiche fondanti trasversali rispetto alle diverse realtà del Settore, ma coerenti con le caratteristiche specifiche e gli obiettivi evolutivi di ciascuna PA.

In particolare, l'attuazione del PNRR, con il carico di lavoro che ha comportato, ha messo alla prova le organizzazioni pubbliche ed ha riportato l'attenzione sulle tematiche dell'efficacia e dell'efficienza nel settore pubblico; l'analisi riguarda anche il sistema dei controlli che a volte appesantisce il funzionamento della macchina pubblica [2].

In alcuni casi le pubbliche amministrazioni hanno istituito funzioni di controllo a seguito ad iniziative autonome (per esempio in INPS e Agenzia delle Entrate), in altri sono state formalizzate con regolamenti e leggi, come per esempio in Regione Lombardia [3]. La situazione attuale, comunque, non sembra adeguata ai compiti che attendono, anche in prospettiva, il settore pubblico. Infatti, la crescente attenzione dei cittadini e la richiesta di servizi di maggiore qualità hanno attribuito ai sistemi di controllo interno e gestione dei rischi un ruolo chiave nella governance delle PA. Inoltre, l'attribuzione ai manager pubblici di obiettivi da raggiungere e risorse da gestire richiede il supporto di una funzione competente ed indipendente sul fronte dei controlli, come, peraltro, accade da tempo nel privato.

Ad oggi si percepisce quindi la necessità di abbandonare il modello di natura ispettiva (verifiche ex-post sui singoli atti) e passare ad un controllo preventivo sulla gestione, quindi a sistemi di controllo interno articolati per linee di difesa con approccio risk based, fondati su delle best practice

internazionali. Si tratta quindi di promuovere l'istituzione di una funzione di controllo interno (indipendente rispetto ai soggetti interni ed esterni all'organizzazione), che assicuri integrità e accountability, coordinandosi con i diversi attori dell'organizzazione pubblica. Compito della funzione di controllo interno diventa quindi quella di collaborare con l'organizzazione pubblica al fine di costruire un sistema di controllo e gestione dei rischi adeguato agli obiettivi, individuando i rischi che potrebbero impedirne il raggiungimento (per esempio in termini economici, di soddisfacimento dei bisogni dei cittadini e dei tempi di attuazione di politiche pubbliche). Tale tipologia di controllo porterebbe un effetto positivo sulla fiducia di cittadini e degli stakeholder.

Nel presente lavoro di tesi si descriverà quindi la Funzione di Internal Audit (FIA) come strumento per assicurare il corretto funzionamento del Sistema di Controllo Interno, presentando anche una simulazione di preparazione di un Piano di Audit e successiva esecuzione di un audit su uno specifico processo di ARPAL.

# Capitolo 1
# La Governance delle Funzioni di Controllo nel Settore Pubblico

## 1.1 Il sistema dei controlli interni nella PA

Negli anni i controlli interni delle PA italiane sono stati oggetto di interventi normativi che hanno contribuito ad indirizzare le scelte organizzative e definire i modelli di Control Governance da adottare. L'evoluzione principale della normativa in tema di controlli interni nella PA può essere riassunta nella seguente tabella [4,11].

| Normativa | Oggetto |
|---|---|
| Legge n. 5026/1869 | Legge di contabilità e finanza pubblica. Nascita del controllo interno. |
| Regio Decreto n. 2440/1923 | Attribuzione al Tesoro del controllo di legittimità, contabile e di proficuità della spesa. |
| Decreto Presidente Repubblica 748/1972 | Riforma della dirigenza statale. |
| Legge n.241/1990; Legge 142/1990 | Disciplina procedimento ammnistrativo; riforma poteri degli Enti Locali |
| Decreto Legislativo n.29/1993 | Introduzione del controllo interno nella PA. |
| Decreto legislativo n.286/1999 | Riordino e potenziamento dei controlli interni nella PA |
| Decreto Legislativo n.267/2000 | Disciplina dei controlli interni negli enti locali. |
| Decreto Legislativo n.150/2009 | Nuova disciplina dei controlli interni nelle Amministrazioni Pubbliche. |
| Legge n.213/2012 (ex D.lgs. n.174/2012) | Sistema dei controlli interni negli enti locali: controllo sulla regolarità ammnistrativa e contabile. |

***Tabella 1**: L'evoluzione principale della normativa in tema di controlli interni nella PA.*

Dati i numerosi interventi normativi sopra citati è emersa l'esigenza di individuare modalità e strumenti per valutare l'adeguatezza del SCI (Sistema Controllo Interno) da adottarsi in ambito pubblico, caratterizzato dalle sue particolari regole, procedure e strutture organizzative. Con tale fine, nel 2019 è stato istituito un Tavolo Tecnico relativo al SCI nella PA, promosso da Regione Lombardia [5,6]. In occasione della prima edizione del Tavolo (2019-2020) sono stati discussi i diversi modelli di riferimento internazionali per la rappresentazione del SCI, per arrivare all'elaborazione di un *Modello di Control Governace* per il contesto pubblico che si basa su tre linee di difesa. Nella seconda edizione del Tavolo (2020-2021), eseguita una ricognizione del SCI nel settore privato, si è individuato,

come standard maggiormente aderente alle finalità del settore pubblico, quello pubblicato dalla Committee of Sponsoring Organizations of the Treadway Commission - COSO, denominato "Internal Control - Integrated Framework" (ICIF), noto anche come "*CoSO Report*". Tale Standard persegue lo scopo di determinare l'entità del rischio che la PA è disposta ad accettare per creare valore per i suoi stakeholder. Il CoSO identifica 5 componenti (ambiente di controllo, valutazione dei rischi, attività di controllo, informazione e comunicazione, monitoraggio) che a loro volta vengono declinate in 17 principi che rappresentano gli elementi del SCI, fornendo così indicazioni al management riguardo alla progettazione, implementazione e gestione, ed alla valutazione della sua efficacia.

Di seguito si elencano le principali funzioni di controllo comuni agli enti del Settore Pubblico che, sebbene siano preposte a diverse tipologie di controllo, operano a presidio del complessivo sistema di controllo interno.

Le Funzioni di controllo presenti in tutti i cluster pubblici sono [7]:

- *Responsabile della Prevenzione della Corruzione e della Trasparenza*
- *Responsabile della Protezione dei dati*
- *Corte dei Conti*
- *Pianificazione e Controllo di Gestione*
- *Organismo Indipendente di Valutazione della performance (escluso il cluster delle Imprese / società pubbliche)*

### *1.1.1 Il modello delle "Tre linee di difesa"*

Il Sistema dei Controlli Interni nel suo complesso, sia in riferimento al suo "*disegno*" che al relativo funzionamento, è articolato nei tre "*livelli di difesa*" rappresentati in Figura 2.

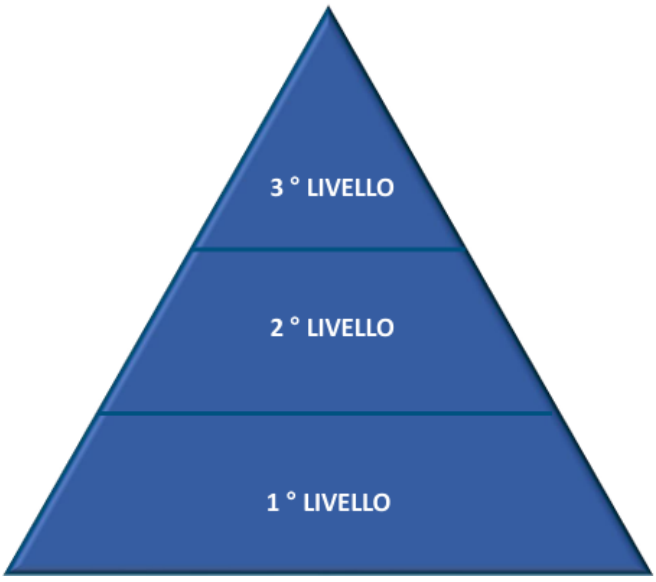


***Figura 2**: Struttura dei tre livelli di difesa* [4].

- *I Livello*: definisce e gestisce i controlli insiti nei processi operativi: controlli/verifiche svolti sia da chi mette in atto una determinata attività, sia da chi ne ha la responsabilità di supervisionare;
- *II Livello*: presidia il processo di individuazione, valutazione, gestione e controllo dei rischi legati all'operatività garantendone la coerenza rispetto agli obiettivi: Risk Management, Compliance Officer, Controllo di Gestione, DPO (Privacy), ecc.;
- *III Livello*: sono controlli di competenza dell'Internal Auditing: fornisce l'«assurance» complessiva sul disegno e il funzionamento del Sistema di Controllo Interno attraverso valutazioni indipendenti.

Le prime due linee operano attraverso uno schema di responsabilità nella gestione delle attività finalizzate al raggiungimento degli obiettivi dell'organizzazione e dei rischi intrinseci, che possono comprometterne il raggiungimento, con intervento diretto per la I linea o con ruolo di

consulenza e controllo per la II linea. La terza linea, con ruolo di assurance sull'adeguatezza ed efficacia della Governance del sistema di gestione rischi, deve essere attribuita a una Funzione Internal Audit, prevista con normativa esterna e/o interna, il cui responsabile può ricoprire anche il ruolo di Responsabile della prevenzione della corruzione e della trasparenza. In relazione al terzo Livello, essendo quindi necessaria l'effettiva indipendenza della funzione Internal Audit, a garanzia dell'obiettività e autonomia della funzione stessa verso i soggetti interni ed esterni, non è possibile l'affidamento a Responsabili di attività operative, anche quella della Funzione di Internal Audit. L'Internal Audit fornisce direttive per il miglioramento dei controlli di secondo livello. Tutte e tre le linee operano in collaborazione per la tutela degli interessi degli stakeholder interni ed esterni all'organizzazione [8].

## 1.2 Il rapporto tra il sistema dei controlli interni, la gestione dei rischi e la Funzione Internal Audit

Nel documento *"Metodologie e buone pratiche per la creazione e la protezione del valore pubblico"* [8] si definisce il SCIGR (Sistema di Controllo Interno e di gestione dei Rischi) come *"un sistema integrato, volto a fornire una ragionevole garanzia sul raggiungimento di:*

- *obiettivi operativi relativi all'efficacia e all'efficienza (performance, finanziari e patrimoniali);*
- *obiettivi di reporting interno ed esterno, con riferimento all'informativa finanziaria e non finanziaria;*
- *obiettivi di compliance relativi alla conformità a leggi, regolamenti, contratti, ecc."*

L'Internal Audit è una funzione indipendente e oggettiva all'interno del SCIGR, con il compito e la responsabilità di:

- *verificare l'operatività e l'idoneità del SCIGR*, attraverso un piano di audit;

• *facilitare l'integrazione tra gli organismi di governance, di management e di controllo*, favorendo il coordinamento e lo scambio delle informazioni."

Nel documento *"La Vision dell'Internal Auditing nel settore Pubblico"* [1], si definisce l'Internal Auditing come *"un'attività indipendente e obiettiva di assurance e consulenza, finalizzata al miglioramento dell'efficacia e dell'efficienza dell'organizzazione. Assiste l'organizzazione nel perseguimento dei propri obiettivi tramite un approccio professionale sistematico, che genera valore in quanto finalizzato a valutare e migliorare i processi di gestione dei rischi, di controllo e di governance".*

La FIA è quindi finalizzata a migliorare i processi di governance ben descritti dal *Modello di Public Value Governance* (PVG), di seguito rappresentato, che consente di governare l'ente in funzione del Valore Pubblico (VP).

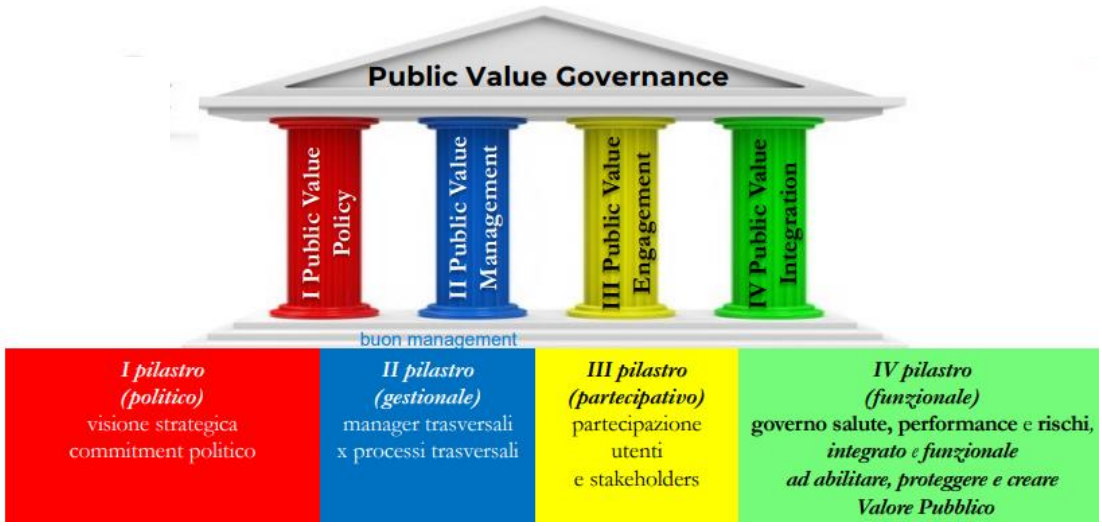


***Figura 1**: Modello di Public Value Governance* (PVG) [8]

Osservando Fig.1 si possono individuare gli specifici contributi della FIA al VP, riferendosi ai quattro pilastri del Modello [7]:

- ✓ **<u>per garantire e supportare</u>**:

• la governance (I pilastro)
• il management (II pilastro)
• gli stakeholders (III pilastro)

- ✓ **<u>per abilitare, proteggere e creare</u>**: in merito alla compliance, all'adeguatezza e alla funzionalità dell'integrazione amministrativa, informativa (IV pilastro).

# Capitolo 2

# Il ruolo e la gestione della Funzione Internal Audit nel Settore Pubblico

La natura del settore pubblico determina un contesto complicato per l'applicazione della FIA a causa del diverso grado di autonomia, azione, controllo, regolamentazione, accountability riscontrabili nei vari livelli territoriali nei quali si articola la PA (es. nazionale regionale, locale).
La FIA s'inserisce in questo contesto volendo rappresentare un fattore chiave per supportare le istituzioni pubbliche a tutti i livelli, esercitando il proprio ruolo di coordinamento e supervisione per raggiungere obiettivi di:

- ✓ *tutelare l'interesse pubblico*
- ✓ *assicurare trasparenza*
- ✓ *favorire l'innovazione*
- ✓ *coordinare il complessivo sistema di controlli interni ed esterni*
- ✓ *incrementare l'affidabilità e credibilità*

*"In particolare, per poter affrontare la sfida delle crisi reputazionali, la FIA dovrà svolgere un ruolo proattivo nel monitorare e mitigare tutti i rischi che possono impattare negativamente sulla reputazione della PA."*

La FIA dovrà quindi integrare il rischio reputazionale nei processi di valutazione del rischio complessivo, che maggiormente incide sul processo di creazione di fiducia degli stakeholder.

## 2.1 I pilastri dei Global Internal Audit Standards

I *Global Internal Audit Standards,* pubblicati il 9 Gennaio 2024 [9], intendono guidare la professione di Internal Auditing a livello mondiale rappresentando la base per valutare e migliorare la qualità dell'operato della funzione stessa.

L'Internal Auditing svolge un ruolo fondamentale nel migliorare la capacità di un'organizzazione di servire il pubblico interesse, ed i relativi Global Internal Audit Standards stabiliscono principi, requisiti, indicazioni ed esempi per la pratica della Funzione IA a livello globale.

Gli Standard sono organizzati in cinque Sezioni:

- *Sezione I*: Purpose dell'Internal Auditing;
- *Sezione II*: Etica e professionalità;
- *Sezione III*: Governo della funzione Internal Audit;
- *Sezione IV*: Gestione della funzione Internal Audit;
- *Sezione V*: Svolgimento delle attività di Internal Auditing

### *2.1.1 Gestione della Funzione Internal Audit*

Il CAE ha la responsabilità di gestire la funzione Internal Audit in conformità ai Global Internal Audit Standards, realizzare una pianificazione strategica, ottenere e impiegare risorse adeguate, costruire relazioni, comunicare con gli stakeholder e garantire lo svolgimento delle attività di auditing ed il miglioramento delle performance della funzione.

La pianificazione strategica del CAE deve inoltre essere in linea con le aspettative del Board, del Top Management e degli altri stakeholder chiave.

Quando il CAE determina gli obiettivi strategici e le iniziative a supporto, è necessario che assegni ad ogni attività delle priorità e delle tempistiche. La strategia di Internal Audit dovrebbe essere adattata ogni volta che si verificano cambiamenti negli obiettivi strategici dell'organizzazione o nelle aspettative degli stakeholder.

Per implementare la strategia, attuare il piano di Audit, ed essere conformi agli Standard, le metodologie dovranno, per esempio, documentare l'approccio della funzione Internal Audit rispetto alle seguenti attività [9]:

- *valutare rischi dell'organizzazione;*
- *sviluppare e aggiornare il piano di Audit;*
- *conservare e rilasciare documenti e altre informazioni, secondo le linee guida dell'organizzazione e i requisiti normativi o di altro tipo pertinenti;*
- *monitorare e confermare l'attuazione delle raccomandazioni degli Internal Auditor e/o dei piani d'azione indicati dal management;*
- *garantire la qualità e il miglioramento della funzione Internal Audit.*

Un metodo di predisposizione del piano di Audit consiste nell'organizzare, le aree potenzialmente oggetto di audit all'interno dell'Ente, in un *Audit Universe* per facilitare l'identificazione e la valutazione dei rischi. Un audit universe è più utile quando si basa sulla comprensione degli obiettivi e delle iniziative strategiche dell'organizzazione ed è allineato con la struttura o il framework dei rischi dell'organizzazione.

Inoltre, per svolgere un piano di audit dovrebbero essere tenuti in debita considerazione i rischi, come quelli relativi all'etica, alle frodi, all'information technology, alle relazioni con le terze parti e alla non conformità ai requisiti normativi, che possono essere legati a più di un business unit o di un processo e che possono richiedere una valutazione più complessa.

Per creare il piano di Audit, il CAE considera il livello di rischio identificato in ciascuna delle aree potenzialmente oggetto di audit rispetto al livello noto di efficacia del controllo. Ad influenzare il piano di Audit sono anche le richieste avanzate dal Board e dal Top Management, la copertura di assurance prevista in tutta l'organizzazione, gli incarichi richiesti da leggi o regolamenti.

Quando definisce il piano di Audit, il CAE dovrebbe considerare [9]:

- *incarichi previsti da leggi o regolamenti;*
- *incarichi critici per la mission o la strategia dell'organizzazione;*
- *aree e attività con un significativo livello di rischio;*

• *se tutti i rischi significativi hanno una copertura sufficiente da parte dei fornitori di assurance;*
• *servizi di advisory e richieste ad hoc;*
• *il tempo e le risorse necessarie per ogni potenziale incarico;*
• *i potenziali benefici di ogni incarico per l'organizzazione, ad esempio il potenziale contributo dell'incarico al miglioramento della governance, del risk management e dei processi di controllo dell'organizzazione.*

### *2.1.2 Svolgimento delle attività di Internal Auditing*

Gli Internal Auditor devono acquisire un'adeguata conoscenza dell'attività oggetto di audit per valutarne i rischi rilevanti.
Gli Internal Auditor devono esaminare le informazioni raccolte per comprendere il disegno dei processi.
Per raccogliere informazioni, gli Internal Auditor possono:
• esaminare i risk assessment svolti di recente dalla funzione Internal Audit, dal management o dai fornitori esterni di servizi;
• esaminare le carte di lavoro degli incarichi precedenti;
• esaminare i riferimenti pertinenti, quali le linee guida dell'IIA o di altri organismi e le leggi e i regolamenti applicabili al settore;
• prendere in considerazione le categorie di rischio rilevanti dell'organizzazione, tra cui strategico, operativo, finanziario e di compliance;
• visitare fisicamente le sedi o le strutture dell'attività oggetto di audit;
• esaminare siti web, i database e i sistemi;
• acquisire informazioni tramite interviste, discussioni;
Gli Internal Auditor possono costruire un grafico, un foglio excel, una matrice di rischi e controlli, una descrizione dei processi o un altro strumento per documentare i rischi e i controlli implementati per gestirli.
I rischi da affrontare durante l'incarico dovrebbero essere classificati in ordine di priorità in base alla significatività.

### *2.1.3 Criteri di valutazione*

L'Internal Auditor deve individuare i criteri più adatti da utilizzare per valutare gli aspetti dell'attività oggetto di audit definiti negli obiettivi e nell'ambito dell'incarico. Tali criteri vengono utilizzati dall'organizzazione per valutare l'efficacia e l'efficienza dei processi di governance, risk management.

Criteri adeguati sono essenziali per identificare le differenze tra lo stato desiderato e la condition, che rappresentano i rilievi potenziali.

Esempi di criteri adeguati includono:

- criteri interni (policy, procedure, key performance indicator o obiettivi specifici dell'attività);
- criteri esterni (leggi, regolamenti e clausole contrattuali);
- pratiche autorevoli (framework, Standard, linee guida e benchmark specifici per un settore, un'attività o una professione);
- prassi organizzative consolidate;
- aspettative basate sul disegno di un controllo;
- procedure che potrebbero non essere formalizzate.

Gli Internal Auditors dovrebbero verificare se l'organizzazione ha adottato o chiaramente definito un livello di controllo soddisfacente.

### *2.1.4 Programma di lavoro*

Gli Internal Auditor possono creare il programma di lavoro collegando i rischi e i controlli identificati nell'attività di risk assessment con i test da svolgere.

Il livello di analisi e di dettaglio applicato durante la fase di pianificazione varia a seconda della funzione Internal Audit e dell'incarico in questione. Il programma di lavoro dovrebbe indicare la metodologia utilizzata per la definizione della popolazione (come universo di riferimento), poi la dimensione del campione analizzato. La valutazione dell'adeguatezza del disegno dei controlli potrebbe essere completata nella fase di pianificazione dell'incarico, in quanto aiuta gli Internal Auditor a identificare chiaramente i controlli chiave da sottoporre a ulteriori test per verificarne l'efficacia.

Carte di lavoro a supporto dello sviluppo del programma di lavoro, quali:

- risk and control matrix con disegno dei test da effettuare;
- mappe o descrizioni dei processi di controllo;
- note sulla valutazione dell'adeguatezza del disegno del controllo;
- pianificazione di test aggiuntivi;
- verbali, note o documentazione delle riunioni di pianificazione durante le quali sono state definite attività e modalità operative.

### *2.1.5 Raccolta delle informazioni per l'analisi e la valutazione*

Le modalità per raccogliere informazioni per le analisi possono prevedere:

• interviste o questionari alle persone coinvolte nell'attività;

• osservazione diretta di un processo;

• acquisizione della conferma o della verifica delle informazioni da parte di una persona indipendente dall'attività oggetto di audit;

• ispezione o analisi di evidenze fisiche come documenti, magazzini o attrezzature;

• accesso diretto ai sistemi dell'organizzazione per osservare o estrarre dati;

• collaborazioni con gli utenti e gli amministratori di sistema per ottenere i dati.

Gli Internal Auditor dovrebbero comprendere e utilizzare tecnologie che migliorino l'efficienza e l'efficacia delle analisi, come le applicazioni software che consentono di testare un'intera popolazione piuttosto che solo un campione.

### *2.1.6 Raccomandazioni e piani d'azione*

Gli Internal Auditor devono decidere se sviluppare raccomandazioni, richiedere piani d'azione al management o collaborare con il management stesso per concordare azioni al fine di:

• risolvere le differenze tra i criteri stabiliti e le condition;

• mitigare a un livello accettabile i rischi identificati;

• indirizzare la root cause del rilievo;

• rafforzare o migliorare l'attività oggetto di audit.

Nell'elaborare le raccomandazioni, gli Internal Auditor devono discuterne con il management coinvolto nell'attività oggetto di audit.

## 2.2 L'applicazione dei Global Internal Audit Standards nel Settore Pubblico

Sebbene i Global Internal Audit Standards si applichino a tutte le funzioni Internal Audit, gli Internal Auditor nel settore pubblico operano in un ambiente politico caratterizzato da strutture di governance, organizzative e di finanziamento che possono differire da quelle del settore privato. La natura di tali strutture e le relative condizioni possono essere influenzate dalla giurisdizione e dal livello di articolazione del settore pubblico in cui opera la funzione Internal Audit (nazionale, locale, ecc.).

Il CAE deve essere consapevole delle leggi e/o dei regolamenti che incidono sulla capacità della funzione Internal Audit di conformarsi pienamente a tutte le disposizioni degli Standard.

Sebbene alcune di queste situazioni non soddisfino i requisiti di indipendenza previsti dai Global Internal Audit Standards, l'istituzione di un Audit Committee composto da membri pubblici, indipendenti dal management, può salvaguardare l'indipendenza e fornire supervisione, consulenza e feedback continui.

L'elenco seguente descrive situazioni in cui le leggi e/o i regolamenti possono influenzare la capacità delle funzioni Internal Audit nel settore pubblico di conformarsi agli Standard [9]:

• *quando le leggi e/o i regolamenti fungono da Mandato dell'Internal Audit, il CAE potrebbe non avere l'autorità o la capacità di apportare modifiche;*

• *le leggi e/o i regolamenti sulla divulgazione al pubblico possono disciplinare i tipi di documenti che devono essere resi pubblici e quelli che non possono essere resi pubblici;*

• *le leggi e/o i regolamenti possono richiedere alle funzioni Internal Audit nel settore pubblico di presentare i risultati dell'Internal Audit in occasione di incontri pubblici;*

• *nel settore pubblico l'audit esterno è spesso previsto per legge. In alcune giurisdizioni, l'autorità di un'istituzione superiore di controllo (per esempio Corte dei Conti) può sostituirsi a quella della funzione Internal Audit e le*

*funzioni Internal Audit possono essere tenute a seguire la pianificazione come stabilito ed a svolgere lavori congiunti.*

Inoltre, gli Internal Auditor nel settore pubblico hanno molteplici stakeholder, tra cui la collettività all'interno della giurisdizione ed i funzionari eletti. Per servire adeguatamente i propri stakeholder, gli Internal Auditor possono prendere in considerazione anche il contributo della collettività durante la pianificazione e l'esecuzione dei servizi di Internal Audit.

# Capitolo 3

# L'applicazione della Funzione Internal Audit ad un processo di ARPAL

Nel presente capitolo viene simulata la predisposizione di un Piano di Audit e la successiva esecuzione di un audit, per un singolo processo aziendale di ARPAL, di competenza dell'Unità Operativa Rischio Tecnologico. In particolare, il processo analizzato prevede l'effettuazione, sia per clienti privati che pubblici, di verifiche tecniche ad impianti soggetti a controlli periodici. Tali verifiche son finalizzate alla tutela della salute e della sicurezza in ambienti di lavoro e di vita, come previsto dalla normativa regionale (L.R. 20/06).

Di seguito si elencano le attività che si svolgono in questo processo, corredate con le diverse normative che le regolano:

A. *Verifiche su apparecchi di sollevamento (D.Lgs. 81/08)*
B. *Verifiche su apparecchi a pressione (D.Lgs. 81/08 e al D.M. 329/04)*
C. *Verifiche di impianti elettrici (D.P.R. 462/01)*
D. *Verifiche su ascensori e montacarichi (D.P.R. 162/99)*
E. *Verifiche su impianti termici (D.Lgs. 81/08 e D.M. 01/12/1975).*

Nel caso in esame si applicheranno le indicazioni dei *Global Internal Audit Standards,* riassunti nel Capitolo 2, al fine di predisporre di un Piano di Audit ed una successiva attività di audit su quello specifico processo considerato [9,10].

## 3.1 Definizione di un Piano di Audit

Il Piano di audit verrà realizzato sulla base delle priorità individuate in funzione:

1. del Risk Assessment;
2. dei risultati di Audit esistenti;
3. delle interviste con il Management per la definizione del contesto aziendale;
4. della compliance esistente (modifiche di Normative, Regolamenti esterni al Gruppo)

Sulla base dei quattro punti precedenti si identifica e si struttura un *Audit Universe*, che prevede la determinazione, misurazione e gestione dei principali rischi legati al mancato raggiungimento delle seguenti categorie di obiettivi:

- efficacia ed efficienza delle attività operative;
- attendibilità delle informazioni di bilancio;
- conformità alle leggi ed ai regolamenti in vigore

La definizione del risk assesment si basa sulla costruzione di una metrica che considera l'impianto normativo, l'informativa fornita dal management ed un'analisi integrata dei rischi.
In particolare, tale elaborazione è stata effettuata sia considerando i rischi esistenti, già elencati nell'attuale PIAO aziendale, sia valutando ulteriori rischi, individuati in attività analoghe svolte all'interno di altre Agenzie facenti parte, come ARPAL, del Sistema Nazionale Protezione Ambiente (SNPA), quindi con paragonabili mission ed obiettivi strategici.
L'approccio risk-based adottato porta ad analizzare tutti i rischi associati al processo, di seguito elencati in funzione delle varie tipologie (ICT, compliance, financial, operational) e graduati da una valutazione su tre livelli (1=basso, 2=medio, 3=alto), generando così una matrice di valutazione del rischio inerente per ogni attività esaminata.

| Descrizione del Rischio | Tipologia | Valutazione del rischio inerente |
|---|---|---|
| **R1**: Corruzione, imparzialità, conflitto d'interesse | compliance | 2 |
| **R2**: Esercizio discrezionalità tecnica | compliance, operational | 2 |
| **R3**: Insoddisfazione cliente | operational | 1 |
| **R4**: Mancato pagamento fattura | financial, ICT | 1 |
| **R5**: Mancato raggiungimento obiettivi performance del personale | operational, compliance, | 1 |
| **R6**: Mancato raggiungimento obiettivi strategici | operational, compliance, financial ICT | 2 |
| **R7**: Non adeguata comunicazione con imprese | ICT, operational, compliance, financial | 2 |
| **R8**: Non adeguata interoperabilità tra i software di rendicontazione attività, protocollo, gestione contabilità | ICT, financial | 2 |
| **R9**: Mancata efficacia probatoria verbali di verifica trasmessi | ICT, compliance | 1 |
| **R10**: Mancata fatturazione | ICT, financial | 1 |
| **R11**: Trasparenza, pubblicità, reputation dell'Agenzia | ICT, compliance | 2 |

***Tabella 2:*** *Analisi dei rischi connessi alle attività* ***Verifiche su apparecchi di sollevamento****.*

| Descrizione del Rischio | Tipologia | Valutazione del rischio inerente |
|---|---|---|
| **R1**: Corruzione, imparzialità, conflitto d'interesse | compliance | 2 |
| **R2**: Esercizio discrezionalità tecnica | compliance, operational | 2 |
| **R3**: Insoddisfazione cliente | operational | 1 |
| **R4**: Mancato pagamento fattura | financial, ICT | 1 |
| **R5**: Mancato raggiungimento obiettivi performance del personale | operational, compliance, | 1 |
| **R6**: Mancato raggiungimento obiettivi strategici | operational, compliance, financial ICT | 1 |
| **R7**: Non adeguata comunicazione con imprese | ICT, operational, compliance, financial | 1 |
| **R8**: Non adeguata interoperabilità tra i software di rendicontazione attività, protocollo, gestione contabilità | ICT, financial | 2 |
| **R9**: Mancata efficacia probatoria verbali di verifica trasmessi | ICT, compliance | 1 |
| **R10**: Mancata fatturazione | ICT, financial | 1 |
| **R11**: Trasparenza, pubblicità, reputation dell'Agenzia | ICT, compliance | 1 |

***Tabella 3:*** *Analisi dei rischi connessi alle attività* ***Verifiche su apparecchi a pressione****.*

| Descrizione del Rischio | Tipologia | Valutazione del rischio inerente |
|---|---|---|
| **R1**: Corruzione, imparzialità, conflitto d'interesse | compliance | 2 |
| **R2**: Esercizio discrezionalità tecnica | compliance, operational | 2 |
| **R3**: Insoddisfazione cliente | operational | 1 |
| **R4**: Mancato pagamento fattura | financial, ICT | 1 |
| **R5**: Mancato raggiungimento obiettivi performance del personale | operational, compliance, | 1 |
| **R6**: Mancato raggiungimento obiettivi strategici | operational, compliance, financial ICT | 2 |
| **R7**: Non adeguata comunicazione con imprese | ICT, operational, compliance, financial | 2 |
| **R8**: Non adeguata interoperabilità tra i software di rendicontazione attività, protocollo, gestione contabilità | ICT, financial | 2 |
| **R9**: Mancata efficacia probatoria verbali di verifica trasmessi | ICT, compliance | 1 |
| **R10**: Mancata fatturazione | ICT, financial | 1 |
| **R11**: Trasparenza, pubblicità, reputation dell'Agenzia | ICT, compliance | 1 |

***Tabella 4**: Analisi dei rischi connessi alle attività **Verifiche di impianti elettrici**.*

Una volta effettuata l'analisi dei rischi delle tre tipologie di attività oggetto di studio, al fine di classificare le aree di priorità da inserire nel piano di audit, si è definita un'ulteriore metrica caratterizzata da 3 livelli di valutazione, analoghi ai precedenti, ma riferiti ad una verifica di compliance, alle risultanze delle interviste con il Top management ed a quelle derivanti da precedenti audit.

La graduazione è così strutturata:

- Livello 1= ritenuto dal Management poco soggetto a rischi, non presenti rilevi negativi di precedenti audit, rispetto di conformità a leggi, regolamenti, contratti, policy, procedure e altri requisiti.
- Livello 2= ritenuto dal Management mediamente soggetto a rischi, presenti alcuni rilevi negativi di precedenti audit, limitato rispetto di conformità a leggi, regolamenti, contratti, policy, procedure e altri requisiti.
- Livello 3= ritenuto dal Management molto soggetto a rischi, non conformità rilevata da precedenti audit, tendenziale non rispetto di conformità a leggi, regolamenti, contratti, policy, procedure e altri requisiti.

Le risultanze di tali valutazioni sono espresse in tabella 5 dove si riportano sia il dettaglio degli score attribuiti ai singoli parametri valutati, che il grado finale di priorità assegnato, riassunto nella riga "*Score totale*" (determinato con somma semplice), che restituisce l'ordine di priorità delle aree da sottoporre a successivo specifico audit.

**ATTIVITA': A - *Verifiche su apparecchi di sollevamento***

| Attività | Risk Assessment | Interviste al Top management | Compliance | Altri Audit | Score |
|---|---|---|---|---|---|
| **R1** | 2 | 2 | 1 | 1 | 6 |
| **R2** | 2 | 2 | 1 | 1 | 6 |
| **R3** | 1 | 2 | - | - | 3 |
| **R4** | 1 | 2 | 1 | 1 | 5 |
| **R5** | 1 | 1 | 1 | 1 | 4 |
| **R6** | 2 | 3 | 1 | 1 | 7 |
| **R7** | 2 | 3 | - | - | 5 |
| **R8** | 2 | 3 | - | - | 5 |
| **R9** | 1 | 1 | 1 | - | 3 |
| **R10** | 1 | 2 | 1 | 1 | 5 |
| **R11** | 2 | 2 | 1 | 1 | 6 |
| | | | | Score totale | **55** |

***Tabella 5**: Classificazione, con ordine di priorità, delle attività* A - *Verifiche su apparecchi di sollevamento, da sottoporre ad audit.*

**ATTIVITA': B -** ***Verifiche su apparecchi a pressione***

| Attività | Risk Assessment | Interviste al Top management | Compliance | Altri Audit | Score |
|---|---|---|---|---|---|
| **R1** | 2 | 1 | 1 | 1 | 5 |
| **R2** | 2 | 2 | 1 | 1 | 6 |
| **R3** | 1 | 1 | - | - | 2 |
| **R4** | 1 | 2 | 1 | 1 | 5 |
| **R5** | 1 | 1 | 1 | 1 | 4 |
| **R6** | 1 | 1 | 1 | 1 | 4 |
| **R7** | 1 | 1 | - | - | 3 |
| **R8** | 2 | 3 | - | - | 5 |
| **R9** | 1 | 1 | 1 | - | 3 |
| **R10** | 1 | 2 | 1 | 1 | 5 |
| **R11** | 1 | 2 | 1 | 1 | 5 |
| | | | | Score totale | **47** |

***Tabella 6****: Classificazione, con ordine di priorità, delle attività* B - *Verifiche su apparecchi a pressione, da sottoporre ad audit.*

**ATTIVITA': C - *Verifiche di impianti elettrici***

| Attività | Risk Assessment | Interviste al Top management | Compliance | Altri Audit | Score |
|---|---|---|---|---|---|
| **R1** | 2 | 2 | 1 | 1 | 6 |
| **R2** | 2 | 2 | 1 | 1 | 6 |
| **R3** | 1 | 1 | - | - | 2 |
| **R4** | 1 | 2 | 1 | 1 | 5 |
| **R5** | 1 | 1 | 1 | 1 | 4 |
| **R6** | 2 | 2 | 1 | 1 | 6 |
| **R7** | 2 | 1 | - | - | 3 |
| **R8** | 2 | 3 | - | - | 5 |
| **R9** | 1 | 1 | 1 | - | 3 |
| **R10** | 1 | 2 | 1 | 1 | 5 |
| **R11** | 1 | 2 | 1 | 1 | 5 |
| | | | | Score totale | **50** |

***Tabella 7**: Classificazione, con ordine di priorità, delle attività* C - *Verifiche di impianti elettrici, da sottoporre ad audit.*

Tale valutazione, da riportarsi nel Piano di audit, viene utilizzata per identificare le aree da sottoporre a specifico audit nell'anno successivo, che, nel caso in esame, interesserà, con frequenza annuale l'attività A, mentre con frequenza biennale le attività B e C. Il piano per l'anno successivo viene così definito e validato dal management di riferimento.

## 3.2 Esecuzione di un audit

L'esecuzione dell'audit ha previsto lo svolgimento delle seguenti fasi, realizzate attraverso l'estrazione di informazioni sia in modo automatico che manuale attraverso l'utilizzo di tecnologie ICT (applicativi: SIMPA, FOLIUM, SIFORMA):

a) acquisizione analisi dei rischi effettuata al paragrafo precedente;
b) mappatura dei controlli interni esistenti ed identificazione degli eventuali controlli mancanti;
c) esecuzione test di verifica di robustezza dei controlli esistenti (TOD-Test sul Disegno del Controllo; TOE-Test di Efficacia Operativa);
d) formulazione di rilevi di audit ("*finding*");
e) raccolta, da parte dell'audit team, di tutti i rilevi condivisi con il Management, e formulazione di suggerimenti (azioni correttive) che diventano una guida per il Management per definire gli Action Plan. Quest'ultimi, a loro volta, andranno condivisi con l'audit team in quanto volti alla riduzione del rischio residuo.

Una volta identificati e valutati i rischi di cui al precedente paragrafo, si è proceduto ad eseguire la mappatura dei controlli, operata sulla base:

i. della caratterizzazione delle tipologie di controllo presenti: direttivo, preventivo, concomitante, successivo;
ii. di specifiche caratteristiche dei controlli quali: chi lo svolge, con che frequenza, in che cosa consiste e come viene documentato;
iii. dell'esistenza di controlli chiave/non chiave, documentabili/non documentabili.

Nella seguente tabella si riporta la mappatura dei controlli esistenti e mancanti. Tutti i controlli esistenti sono documentabili attraverso estrazione autonoma e manuale di dati, tramite l'utilizzo di alcuni applicativi ufficiali di ARPAL, che permettono l'acquisizione di informazioni di rendicontazione di performance del personale, contabile, gestionale, di formazione, ed anche specifici dati relativi alle anagrafiche dei clienti ed

informazioni tecniche relative alla conduzione ed all'esito delle verifiche impiantistiche svolte da personale di Agenzia.

In tabella 8 vengo evidenziati i controlli esistenti con funzione di **controlli chiave** (in verde i controlli chiave e senza colorazione i controlli non chiave) ed i controlli **mancanti** (azzurro). La distinzione tra controlli chiave/non chiave risulta importante in quanto, in caso di fallimento di un controllo chiave, sarebbe più difficile mitigarne il rischio associato.

| Tipologia di Rischio | Nome Controllo | Tipologia di Controllo | Responsabile controllo | frequenza controllo |
|---|---|---|---|---|
| **R1** | **C1** | conclusivo, direttivo | Responsabile U.O. Rischio Tecnologico | ad ogni conclusione di corsi di formazione, ed annualmente |
| **R2** | **C2** | direttivo, concomitante | Responsabile U.O. Rischio Tecnologico | mensile |
| **R3** | **C3** | - | | |
| **R4** | **C4** | preventivo, successivo, cross-organizzativo | Responsabile Settore Risorse Finanziarie, Responsabile U.O. Rischio Tecnologico | bimestrale, annuale |
| **R5** | **C5** | concomitante, conclusivo | Responsabile U.O. Rischio Tecnologico | mensile ed annuale |
| **R6** | **C6** | concomitante, successivo, conclusivo | Responsabile U.O. Rischio Tecnologico | mensile ed annuale |
| **R7** | **C7** | direttivo | Responsabile U.O. Rischio Tecnologico | bimestrale |
| **R8** | **C8** | - | | |
| **R9** | **C9** | concomitante | Responsabile U.O. Rischio Tecnologico | mensile |
| **R10** | **C10** | preventivo, successivo, cross-organizzativo | Responsabile Settore Risorse Finanziarie, Responsabile U.O. Rischio Tecnologico | bimestrale, annuale |
| **R11** | **C11** | direttivo | Responsabile Settore Acquisizione Gestione Risorse | annuale |

***Tabella 8**: Mappatura dei controlli esistenti e mancanti, con indicazione di quelli chiave evidenziati in verde.*

Una volta valutati i controlli esistenti e mancanti, si effettuano i test di verifica sulla robustezza dei controlli esistenti.

I test eseguiti sono sostanzialmente di due topologie TOD (Test sul Disegno del Controllo) e TOE (Test di Efficacia Operativa, che di norma si esegue durante il processo). Una volta eseguito il test TOD, se lo stesso risulta "positivo" (quindi risulta efficacie), si può proseguire verso un'ulteriore fase di testing, che prevede di ripetere lo stesso test su un campione di analisi più ampio (divenendo test TOE), permettendo così di verificare l'efficacia del test su tutta la popolazione di campioni. Qualora il test TOD non avesse un esito positivo, evidenziando così una criticità, si potrebbe procedere con un test "di sostanza".

In Tabella 9, vengono indicate le diverse tipologie di test eseguite sui controlli esistenti, ed il loro esito. L'esecuzione di entrambi i test è stata sperimentata solo sul controllo C7 che ha evidenziato l'opportunità di ampliare il campione oggetto di test.

| Nome Controllo | Tipologia di Test | Esito Test |
|---|---|---|
| **C1** | TOD | positivo |
| **C2** | TOD | positivo |
| **C4** | TOD | positivo |
| **C5** | TOD | positivo |
| **C6** | TOD | positivo |
| **C7** | TOD-TOE | positivo |
| **C9** | TOD | positivo |
| **C10** | TOD | positivo |
| **C11** | TOD | positivo |

***Tabella 9**: Elenco e risultanze dei Test svolti sui controlli esistenti.*

Conclusa la fase di testing si è proceduto alla valutazione del Rischio Residuo che ha permesso di definire i contenuti dell'Action Plan di seguito esplicitato.

Nel caso in esame il testing ha fatto emergere:

a) la mancanza di due controlli, riferiti ai rischi R3 ed R8. Entrambi i controlli risultano, ad oggi, controlli non chiave, in quanto l'interoperabilità contemporanea tra tutti i sistemi software presenti in Agenzia (R8) non è condizione necessaria al raggiungimento degli obiettivi strategici, e la soddisfazione del cliente (R3) viene comunque monitorata attraverso prassi organizzative consolidate che ad oggi non necessitano di formalizzazione;
b) l'opportunità di garantire una maggiore uniformità nella gestione del rapporto con i clienti attraverso la predisposizione di una più dettagliata procedura interna sulla "gestione del rapporto con il cliente" (R7).

Gli elementi finora identificati contribuiscono alla valutazione che l'auditor deve effettuare in merito al rischio residuo, per il quale va predisposto un Action Plan, la cui implementazione andrà verificata, l'anno successivo, dalla funzione di audit, per conseguente follow up del Piano di audit.
L'esecuzione dell'audit si conclude con la redazione di un documento, denominato *audit report*, che presenta una valutazione sul sistema di controllo interno, e che è supportato dai *finding* identificati dall'auditor. Ciascun finding deve presentare gli elementi:

1. *condizione* (che cosa è successo)
2. *causa* (cosa ha determinato la discrepanza)
3. *criterio* (quali sono i principi da rispettare per un corretto controllo)
4. *impatto* (che impatto ha generato la problematica riscontrata)
5. *raccomandazione* (proposta per risolvere la "condizione" di cui al precedente punto 1), con l'indicazione di un Action Plan costruito sugli elementi di criticità emersi).

Il giudizio di sintesi, nonché la sintesi dei finding più salienti, varranno condivisi nelle riunioni periodiche con gli organi di controllo (incluso Audit Commitee).

# Capitolo 4

# Delineare una visione per la Funzione Internal Audit

Le analisi dello stato attuale della funzione IA, nelle diverse tipologie di amministrazioni del Settore Pubblico, hanno portato alla determinazione di un possibile percorso evolutivo della funzione, strutturato in diversi step, sulla base dei livelli di maturità di partenza delle singole PA [1].

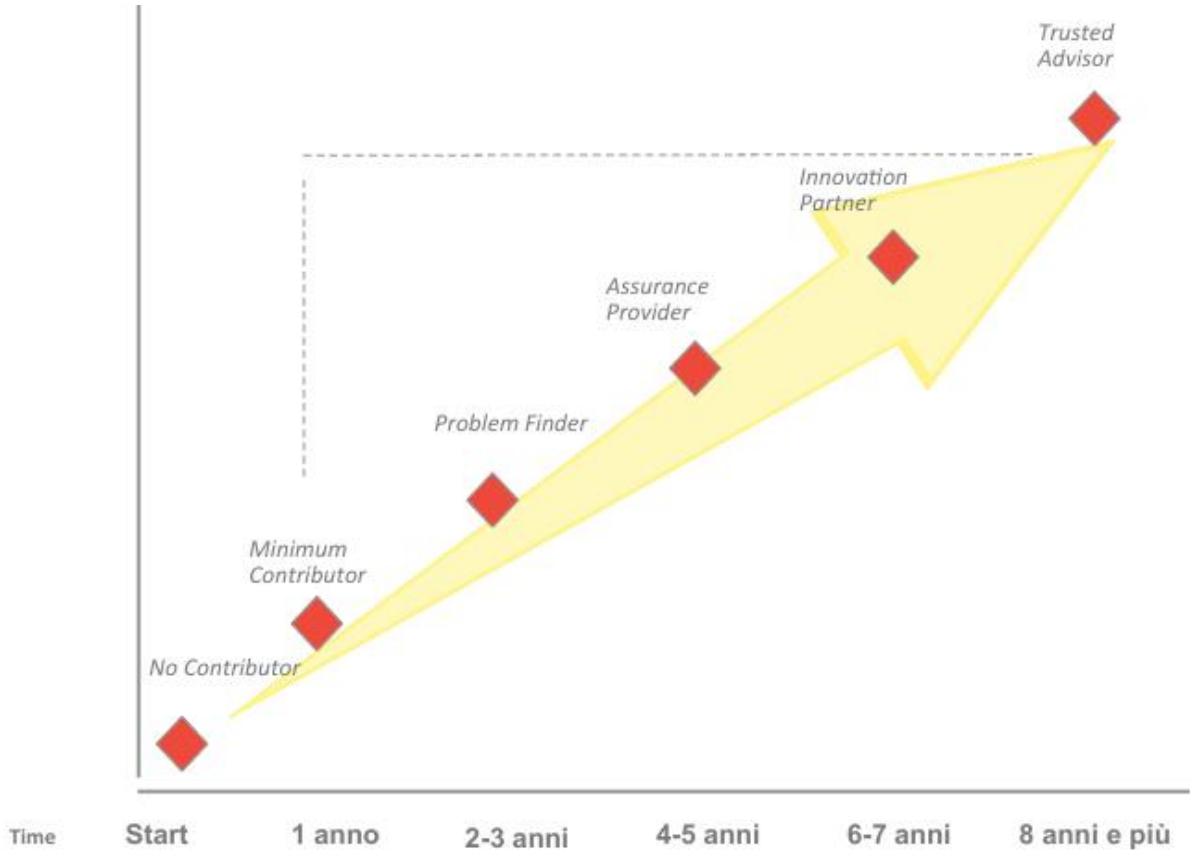


***Figura 3:*** *Time line evolutiva della Funzione IA [1].*

I diversi livelli del "Maturity Model", rappresentati in figura 3, sono stati definiti in funzione dell'eventuale presenza e specifica attività che l'IA svolge nell'organizzazione, come di seguito specificato:

*1. No Contributor: assenza di una Funzione IA all'interno dell'organizzazione;*

*2. Minimum Contributor: presenza di una Funzione IA focalizzata su tematiche specifiche di compliance, legalità e prevenzione della corruzione peculiari alla propria organizzazione;*

*3. Problem Finder: Funzione IA tesa principalmente ad analizzare problemi e criticità, al fine di supportare il Management nella definizione di azioni correttive finalizzate a garantire l'efficacia ed efficienza dei processi aziendali;*

*4. Assurance Provider: la Funzione IA mira a fornire un'assurance obiettiva, indipendente e risk based, sull'efficacia ed efficienza del Sistema di Controllo Interno dell'organizzazione, anche Regolamentazione normativa;*

*5. Innovation Partner: la Funzione IA assume un ruolo attivo nel promuovere e attuare i processi di innovazione e di coordinamento con le altre funzioni aziendali, che si identificano come Assurance Provider, e con il sistema dei controlli esterni;*

*6. Trusted Advisor: la Funzione IA, quale indipendente fornitore di servizi professionali di assurance, consulenza e coordinamento del complessivo sistema dei controlli a supporto della Governance dell'Ente, viene identificata come interlocutore affidabile, trasparente e indipendente dagli stakeholder interni ed esterni.*

Per aumentare il livello di maturità della Funzione di Internal Audit, è necessario attivare le leve di seguito riportate [1]:

- *Regolamentazione della normativa: integrazione e adeguamento della normativa esterna specifica e applicabile all'entità e di quella interna all'organizzazione;*
- *Competenze professionali: inserimento, nell'organico della Funzione IA, di profili professionali caratterizzati da un mix di competenze*

*specialistiche, diversificate in considerazione delle specificità dell'organizzazione;*

- *<u>Dimensionamento:</u> dimensionamento della Funzione IA in coerenza con la complessità e l'articolazione territoriale dell'organizzazione;*
- *<u>Infrastrutture:</u> implementazione di piattaforme tecnologiche (es. Data Analytics, Data Mining, Machine learning, ecc.) che consentano alla Funzione IA di attivare processi volti ad una valutazione dinamica e costante dei rischi dell'organizzazione.*

Tale assetto consente di comprendere quali siano le variabili chiave da implementare per migliorare il livello di maturità di una FIA, dato il suo specifico punto di partenza.

# Conclusioni

Le considerazioni sul modello di Governance del sistema di controllo e sul ruolo della Funzione Internal Audit non possono prescindere dal processo evolutivo, innescato anche dalla crisi pandemica, richiesto al Settore Pubblico. In un momento storico in cui, mediante l'attuazione dei progetti del piano Next Generation EU, l'impatto potenziale della spesa pubblica avrà una dimensione considerevole, il Settore Pubblico si troverà a dover svolgere un ruolo strategico che, per essere efficace, richiederà una evoluzione della Governance di tutto il Settore Pubblico.

L'analisi del contesto attuale e prospettico evidenzia, quindi, l'opportunità di istituire e sviluppare una Funzione Internal Audit in linea con il modello proposto al paragrafo 4, in modo da favorire i processi di innovazione, di contrasto alla corruzione, di trasparenza, e di un più efficiente utilizzo delle risorse e dei beni pubblici, nonché un rafforzamento della credibilità e affidabilità della Pubblica Amministrazione nel suo complesso.

L'utilizzo del Maturity Model consente la definizione di un livello di partenza tipico di ciascuna organizzazione, dato il proprio contesto di riferimento, e la definizione del "*Livello Target*", sulla base degli obiettivi definiti, agendo attraverso un'opportuna combinazione di fattori abilitanti (quali regolamentazione normativa, mix competenze, infrastrutture), attraverso un percorso di implementazione graduale. Le modifiche e integrazioni normative al sistema di controllo esistenti devono costituire uno stimolo per l'implementazione della FIA, seguendo il percorso già intrapreso nel settore privato ed in parte di quello pubblico.

Essendo la FIA centrale nell'assicurare il corretto funzionamento del SCI, ci si aspetta che sia in grado di determinare i rischi aziendali più importanti e di effettuare una pianificazione che identifichi chiaramente le azioni correttive da intraprendere.

In quest'ottica predittiva si mette il settore Pubblico in condizione di poter prendere decisioni adeguate anche in contesti caratterizzati da forti incertezze geopolitiche, tecnologiche, regolamentari e dalla crescente concorrenza.

È auspicabile, pertanto, che si attivi prioritariamente il Dipartimento della Funzione Pubblica/Ministero PA, al fine di promuovere la costituzione e lo sviluppo della Funzione Internal Audit [7,9].

# Glossario

*estratto da: Global Internal Audit Standards - pubblicati il 9 Gennaio 2024 - The Institute of Internal Auditors*

**Attività oggetto di Audit** – L'oggetto di un incarico di Internal Audit. Alcuni esempi: un'area o una funzione, un'operazione, un processo o un sistema.

**Assurance** – 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.

**Board** – Il massimo organo di governo, quale: • un Consiglio di Amministrazione; • un Audit Committee; • un Consiglio Direttivo o di fiduciari; • un gruppo di funzionari eletti o nominati politicamente; • un altro organo che abbia autorità sulle funzioni di governance rilevanti. In un'organizzazione che prevede più di un organo di governo, il termine "Board" si riferisce all'organo o agli organi autorizzati a conferire alla funzione Internal Audit autorità, ruolo e responsabilità appropriate. Laddove non esista nessuno dei precedenti, "Board" dovrebbe essere riferito a un gruppo di soggetti o alla persona che agisce come massimo organo di governo dell'organizzazione, ad esempio il CEO.

**Compliance** – Conformità a leggi, regolamenti, contratti, policy, procedure e altri requisiti.

**Chief Audit Executive (CAE)** – La persona che ha la responsabilità di gestire effettivamente le attività della funzione Internal Audit e di garantirne la qualità dei servizi in conformità con i Global Internal Audit Standards. Job title e/o responsabilità specifiche possono variare da un'organizzazione all'altra.

**Controllo** – Qualsiasi azione intrapresa dal management, dal Board o da altri soggetti per gestire i rischi e aumentare le possibilità di conseguimento degli obiettivi e dei traguardi stabiliti.

**Criteri** – Detti anche "criteri di valutazione", definiscono, nell'ambito di un incarico, le caratteristiche attese ("to-be") delle attività oggetto di audit.

Funzione Internal Audit – Un singolo individuo o un gruppo di individui responsabili di fornire servizi di assurance e advisory a un'organizzazione.

**Governance** – L'insieme dei processi e delle strutture implementate dal Board per produrre informazioni, indirizzare, gestire e monitorare le attività dell'organizzazione nel raggiungimento degli obiettivi.

**Impatto** – Il risultato o l'effetto di un evento. Un evento può avere un impatto positivo o negativo sulla strategia o sugli obiettivi di business di un'organizzazione

**Internal Auditing** – L'Internal Auditing è un'attività indipendente e obiettiva di assurance e advisory, finalizzata al miglioramento dell'efficacia e dell'efficienza dell'organizzazione. 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 risk management e di controllo.

**Internal Audit Charter** – Un documento formale, che include il Mandato della funzione di Internal Audit e il suo posizionamento all'interno dell'organizzazione, i flussi informativi, l'ambito di copertura, le tipologie di attività e altre specifiche

**Matrice di rischio e controllo** – Strumento che facilita lo svolgimento delle attività di Internal Auditing, permettendo la correlazione tra obiettivi aziendali, rischi, processi di controllo e informazioni chiave.

**Piano di Audit** – Un documento, sviluppato dal Chief Audit Executive, che identifica gli incarichi e gli altri servizi di Internal Auditing che si prevede di svolgere durante un determinato periodo. Il piano dovrebbe essere risk-based e dinamico e riflettere adeguamenti tempestivi in risposta ai cambiamenti che interessano l'organizzazione

**Rischio** – Un evento incerto che può influire positivamente o negativamente sul raggiungimento degli obiettivi.

**Rischio inerente** – L'insieme dei fattori di rischio interni ed esterni in assenza di attività di controllo.

**Rischio residuo** – La parte di rischio inerente che permane dopo aver attuato le azioni di prevenzione, mitigazione e controllo.

**Risk assessment** – L'insieme delle azioni volte a individuare e analizzare i rischi rilevanti per capirne gli impatti sul raggiungimento degli obiettivi di un'organizzazione. La significatività dei rischi viene generalmente valutata in termini di impatto e probabilità.

**Risk management** – L'insieme delle azioni volte a identificare, valutare, gestire e controllare potenziali eventi o situazioni, al fine di fornire una reasonable assurance sul raggiungimento degli obiettivi dell'organizzazione.

**Settore pubblico** – Enti governativi, agenzie, istituzioni, imprese e altri enti controllati o finanziati con fondi pubblici, che erogano programmi e servizi o forniscono beni al pubblico.

**Top Management** – Il più alto livello di dirigenza di un'organizzazione che è in ultima analisi responsabile nei confronti del Board per l'esecuzione delle decisioni strategiche dell'organizzazione; in genere è un gruppo di persone che include il Chief Executive Officer.

# BIBLIOGRAFIA

**[1]** MASSIMO PROIETTI: *"La Vision dell'Internal Auditing nel settore Pubblico"* - AIIA COMITATO PER IL SETTORE PUBBLICO - Luglio 2020

**[2]** MASSIMO PROIETTI: *"Per far correre la PA servono controlli preventivi" - AIIA*

**[3]** Legge Regione Lombardia n.13/2018

**[4]** MASSIMO PROIETTI: *"L'internal audit nel settore pubblico"* - Seminario AIIA del *23 Novembre 2023*

**[5]** ALESSANDRO CENCIONI, ENRICO GASPARINI, ENRICO GUARINI- Articolo a cura dei componenti del Tavolo di Lavoro - *"Il Passo avanti della Lombardia"* – IA n.121 Aprile/Giugno 2024

**[6]** ENRICO GUARINI - Università di Milano _Bicocca *"Perché e come la Lombardia può diventare un benchmark"* –IA n.121_ Aprile/Giugno 2024-

**[7]** ENRICO DEIDDA GAGLIARDO *"Metodologie e buone pratiche per la creazione e la protezione del valore pubblico" – Seminario AIIA "L'Internal Audit nel settore Pubblico: stato dell'arte e prospettive" - 23 Novembre 2023*

**[8]** GOVERNANCE DELLE FUNZIONI DI CONTROLLO NEL SETTORE PUBBLICO - COMITATO PER IL SETTORE PUBBLICO DI AIIA - DICEMBRE 2020

**[9]** GLOBAL INTERNAL AUDIT STANDARDS - THE INSTITUTE OF INTERNAL AUDITORS- 09GENNAIO 2024

**[10]** *Audit Methodologies Internal Audit Function: End-to-End Process* - Seminario svolto nell'ambito del Lab. PA - UNIVERSTITÀ DI GENOVA - DIPARTIMENTO DI SCIENZE POLITICHE INTERNAZIONALI- 02/03/2024

**[11]** AIIA Comitato per il Settore pubblico - Project Leader: Dott.Massimo Proietti - "*Governance delle Funzioni di Controllo nel Settore Pubblico*" - Dicembre 2020