

# **REGOLAMENTO PER L'ATTIVITÀ DI INTERNAL AUDIT NELLA FONDAZIONE**

## SOMMARIO

Premessa .....	3
Art. 1 Scopo .....	3
Art. 2 Ambito di Applicazione.....	3
Art. 3 Riferimenti .....	3
Art. 4 Organizzazione .....	4
Art. 5 Ruoli, Funzioni e Responsabilità.....	4
Art. 6 Collaborazioni con altre Fondazioni IRCCS lombarde in tema di I.A. ....	5
Art.7 Tipologia dei controlli.....	5
Art. 8 Metodologia .....	6
Art. 9 Rapporti e Comunicazioni .....	7
Art. 10 Obbligo di denuncia .....	7
Art. 11 Formazione e aggiornamento .....	7
Art. 12 Codice di Condotta .....	7
Art. 13 Confidenzialità delle Informazioni .....	7
Art. 14 Protezione dei Dati Personali.....	7
Art. 15 Norma di rinvio .....	7

## Premessa

Il Regolamento per l'attività di Internal Audit della Fondazione IRCCS Istituto Nazionale dei Tumori (di seguito in breve "Fondazione") è stato emanato con deliberazione del CDA n. 281F del 22 dicembre 2015 in attuazione della D.G.R. 23 dicembre 2014, n. X/2989 (paragrafo 2.3.6.4 dell'Allegato B - "Regole di sistema 2015 - ambito sanitario"), con cui Regione Lombardia ha stabilito di inserire nella Rete di Internal Audit tutti gli Enti Sanitari. L'attuale Regolamento è già stato oggetto di una prima revisione con deliberazione del CDA n. 161F del 29 gennaio 2018.

L'Internal Audit (di seguito in breve "I.A."), secondo la **definizione** validata dall'organizzazione mondiale cui fa riferimento l'Associazione Italiana Internal Auditors (A.I.I.A.), è *"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 aggiunto in quanto finalizzato a valutare e migliorare i processi di gestione dei rischi, di controllo e di governance"*.

Il presente Regolamento si ispira ai Principi e Standard etici e professionali emanati dall'Institute of Internal Auditors (I.I.A.), a cui la Funzione di I.A. fa riferimento, riportati per esteso nel Piano di Audit.

Il focus dell'attività di I.A. è assicurarsi che il sistema di controllo interno e di gestione dei rischi (SCI-GR) sia adeguato e operi in modo efficace.

## Art. 1 Scopo

Il presente Regolamento disciplina le procedure, le metodologie e gli strumenti di lavoro utilizzati per l'attività di I.A., con l'obiettivo di definire la metodologia per assistere il management nell'identificazione, mitigazione e monitoraggio dei rischi e dei relativi controlli.

## Art. 2 Ambito di Applicazione

I destinatari del Regolamento sono la Direzione Strategica, il Responsabile della Funzione di Internal Audit (di seguito in breve "Responsabile I.A."), il Team di Auditor (di seguito in breve "Team I.A."). L'Internal Audit si applica a tutte le aree operative dell'azienda sanitaria, inclusi i processi clinici, amministrativi, finanziari e informatici. Tutte le unità organizzative sono soggette a revisione.

## Art. 3 Riferimenti

- D.Lgs. 286/1999 e D.Lgs. 150/2009 dettano disposizioni per il riordino e il potenziamento dei controlli nella Pubblica Amministrazione;
- Legge Regionale n. 17 del 4 giugno 2014, definisce la Funzione di Internal Audit quale strumento necessario alla valutazione dell'efficacia del sistema dei controlli interni, mediante la verifica dei processi, delle procedure e delle operazioni, e dei sistemi di gestione e di controllo aziendali ai fini di identificare, mitigare e/o correggere gli eventuali rischi presenti nell'organizzazione;
- D.G.R. n. X/2989 del 23 dicembre 2014, avente per oggetto "Determinazioni in ordine alla gestione del servizio socio sanitario regionale per l'esercizio 2015", che, al paragrafo 2.3.6.4 dell'Allegato B) "Regole di sistema 2015: ambito sanitario", ha prescritto, tra l'altro, agli Enti Sanitari di approvare un proprio Regolamento di Internal Audit ispirato ai principi e criteri enunciati dal Manuale di Internal Auditing regionale o, alternativamente, di adottare il Manuale stesso;
- Legge regionale n. 13 del 28 settembre 2018 istituisce l'Organismo Regionale per le Attività di Controllo (ORAC) introducendo una rilevante novità nell'ambito del sistema dei controlli della Giunta e degli enti del sistema regionale, in particolare ORAC prevede il coordinamento della rete degli uffici di Internal Audit degli Enti del sistema Regionale, assicurando adeguate forme di impulso, la condivisione di buone pratiche e la dotazione di strumenti finalizzati a rafforzarla;

- D.G.R. n. XI/1046 del 17 dicembre 2018, avente per oggetto “Determinazioni in ordine alla gestione del servizio sociosanitario per l’esercizio 2019” che ha confermato l’allocazione della Funzione di I.A. a un livello dell’organizzazione idoneo ad assicurare autonomia della Funzione stessa, indipendenza di giudizio e obiettività delle rilevazioni, stabilendo le date di invio dei documenti alla Direzione Generale Welfare e alla Struttura Audit;
- D.G.R. n. XI/6278 dell’11 aprile 2022 “Linee guida regionali per l’adozione dei piani di organizzazione aziendale strategici (POAS)”, che al capitolo II, punto 1. Internal Auditing, prevede che *“la Funzione di Internal Auditing sia allocata nella Direzione Generale, al fine di assicurare autonomia, indipendenza di giudizio e obiettività delle rilevazioni, nonché in ragione del ruolo del Direttore di attuare una netta segregazione delle funzioni con conseguente esclusione della sovrapposizione dell’incarico di Responsabile I.A., con lo svolgimento di attività di controllo di primo livello e, in generale, con incarichi di tipo gestionale”*. La DGR definisce anche le compatibilità di incarichi, fermo restando l’elettività dell’incarico esclusivo, è fatta salva la possibilità di cumulo degli incarichi ritenuti affini, a patto di adeguata assegnazione di risorse formate, a garanzia dell’assolvimento dei propri compiti;
- D.G.R. n. XI 6387 del 16 maggio 2022 avente per oggetto: “Determinazione in ordine agli indirizzi di programmazione per l’anno 2022”, che descrive nell’allegato 9: “La Funzione di Internal Auditing”;
- Piano di Organizzazione Aziendale Strategico (POAS) 2022-2024, approvato con D.G.R n. XI/6811 del 2 agosto 2022.

Più in generale, i riferimenti normativi seguiti dall’Internal Audit includono in ogni caso le determinazioni in ordine agli indirizzi di programmazione del SSR (cosiddette regole di sistema regionali), e le relazioni/raccomandazioni di ORAC che costituiscono un quadro di riferimento per l’attività di audit.

#### **Art. 4 Organizzazione**

Il Piano di Organizzazione Aziendale Strategico (POAS) 2022-2024, approvato con D.G.R n. XI/6811 del 2 agosto 2022 - in conformità alle Linee Guida regionali di cui alla D.G.R. n. XI/6278 dell’11 aprile 2022- pone la “Funzione di Internal Auditing - Sistema controlli interni” in capo alla Direzione Generale della Fondazione.

Alla relativa Funzione aziendale, per svolgere il suo compito in modo obiettivo, è garantita la necessaria autonomia, libera da limitazioni, e l’accesso a tutte le informazioni necessarie allo svolgimento delle attività. Alla Funzione è preposto un Responsabile I.A., incaricato dal Direttore Generale in via esclusiva, ovvero in base a criteri di affinità degli ulteriori incarichi, competente per le funzioni di verifica e miglioramento dei controlli interni, al fine di una corretta gestione dei rischi aziendali.

Il Responsabile I.A. è coadiuvato da un Team I.A., nominato annualmente nell’ambito del Piano annuale di Internal Audit, in base alle competenze richieste dalla verifica dei processi pianificati. I componenti del Team I.A. sono impegnati solo per il tempo necessario allo svolgimento dell’audit, in accordo con il Direttore della struttura di appartenenza.

Il Team I.A. può essere integrato, per esigenze contingenti, con professionalità ulteriori, anche esterne alla Fondazione, se necessarie alle specifiche attività di controllo.

#### **Art. 5 Ruoli, Funzioni e Responsabilità**

##### Il Direttore Generale:

- a) è Responsabile dell’attuazione del Regolamento in oggetto e delle disposizioni organizzative e gestionali atte ad assicurare l’esercizio della Funzione di I.A., nel rispetto delle scadenze indicate da Regione Lombardia;
- b) approva il Piano annuale di Internal Audit e la programmazione pluriennale;
- c) riferisce al Consiglio di Amministrazione i contenuti del Piano annuale;
- d) affida la responsabilità della Funzione di I.A. a un Dirigente/Funziionario che, per esperienza, capacità e affidabilità, possieda i requisiti idonei ad assolvere i compiti propri della Funzione di I.A.;

- e) garantisce alla Funzione di I.A. la necessaria autonomia e indipendenza, secondo i principi costitutivi dell'attività;
- f) individua e assegna alla Funzione di I.A. le risorse necessarie per adempiere al mandato;
- g) promuove lo sviluppo delle competenze in materia di I.A. alle professionalità assegnate alla Funzione di I.A.

#### Il Responsabile I.A.:

- a) è incaricato di verificare che il sistema di controllo interno di gestione dei rischi (SCI) sia adeguato e funzionante;
- b) riferisce al Direttore Generale in merito all'adeguatezza dell'assetto organizzativo della funzione;
- c) redige il Piano annuale di Internal Audit, basandosi sulle c.d. "Regole del sistema sociosanitario lombardo", annuali, sulle eventuali indicazioni della Struttura di Audit regionale, sulle raccomandazioni ORAC, e sugli obiettivi strategici di Internal Audit condivisi con il Direttore Generale;
- d) nomina i componenti del Team I.A., con lettera di incarico su base annuale;
- e) assicura lo svolgimento delle attività programmate all'interno del Piano di Audit adottato, assegnando competenze e tempo/operatore adeguati al raggiungimento dell'obiettivo di audit, sorvegliando lo svolgimento efficiente ed efficace delle attività di audit e di follow-up;
- f) riferisce al Direttore Generale gli esiti delle verifiche, tramite l'attività di reporting e relaziona annualmente sull'efficacia e adeguatezza della Funzione I.A., e delle eventuali necessità di miglioramento;
- f) valuta le proposte di azioni migliorative.
- g) propone l'attivazione di supporti esterni, qualora ve ne sia bisogno per carenza di competenze necessarie al Team I.A., per l'esecuzione degli interventi di audit;
- h) avanza proposte di modifiche regolamentari o altri suggerimenti volti a superare le difficoltà riscontrate;
- i) progetta lo sviluppo delle competenze proprie e del Team I.A., sia nell'ambito del Piano di Formazione Aziendale INT, che nel contesto della formazione extra sede;
- j) è componente d'ufficio del Comitato di Coordinamento dei Controlli interni della Fondazione (di seguito in breve "CCCi").

#### Il Team I.A.:

- a) esegue le attività di audit;
- b) raccoglie, ordina e archivia le evidenze che documentano le attività di audit;
- c) collabora con il Responsabile I.A. alla redazione dei verbali degli audit e dei rapporti preliminari e finali;
- d) al termine di ciascun intervento di audit aggiorna la documentazione per eventuali successivi follow-up;
- e) collabora con il Responsabile I.A. alla revisione del Regolamento;
- f) contribuisce all'aggiornamento e alla valutazione del modello di "Risk Assessment", secondo i risultati degli interventi di audit;
- g) partecipa agli specifici corsi di formazione e/o aggiornamento.

### **Art. 6 Collaborazioni con altre Fondazioni IRCCS lombarde in tema di I.A.**

Al fine di assicurare l'indipendenza e l'obiettività della Funzione I.A., l'attività di audit può essere svolta in collaborazione e interscambio con la corrispondente Funzione e Team I.A. ad essa collegata, di altre Fondazioni IRCCS pubbliche lombarde, mediante stipula di appositi accordi.

### **Art. 7 Tipologia dei controlli**

L'attività di I.A. si esplica secondo le seguenti tipologie di verifiche:

- a) **audit di conformità (compliance audit)**: conformità alle leggi e ai regolamenti in vigore; conformità dei comportamenti alle procedure e alle prassi interne; adeguatezza e chiarezza delle stesse alle esigenze operative;
- b) **audit operativo (operational audit)**: efficacia ed efficienza delle attività operative e dei processi per monitorare il rispetto degli obiettivi;
- c) **audit finanziario/contabile (financial audit)**: attendibilità delle informazioni di bilancio (e salvaguardia del patrimonio finanziario).

**Follow-up**: rilevazione dell'effettiva realizzazione delle azioni concordate a seguito di osservazioni formulate durante interventi precedenti.

## Art. 8 Metodologia

Il processo di Internal Audit si articola nelle fasi di pianificazione, attuazione e comunicazione (reporting), a fini della valutazione di adeguatezza e funzionamento del Sistema di Controllo Interno e Gestione del Rischio (SIC-GR).

L'identificazione e valutazione del rischio (Risk Assessment), rappresenta l'analisi preliminare utile per la stesura del Piano di Audit, che può essere definito dal Responsabile I.A., o derivato dai Modelli Organizzativi contenenti le mappature dei processi sensibili già presenti a vario titolo nella Fondazione. La pianificazione costituisce la fase successiva e consiste nell'individuazione dei processi da sottoporre ad audit nell'ambito di un Piano (di seguito in breve "Piano I.A.") predisposto con periodicità almeno annuale. Il Piano annuale di Internal Audit è approvato con Decreto del Direttore Generale.

I requisiti minimi del Piano I.A. consistono nelle specifiche di:

- a) processo e/o procedura oggetto di audit;
- b) tipo e obiettivo dell'audit;
- c) criteri di valutazione;
- d) strumenti di supporto e di rilevazione;
- e) modalità di comunicazione agli interessati del calendario e delle specifiche del singolo audit;
- f) individuazione del responsabile e/o referente interno alle strutture interessate per la fase di istruttoria e verifica sul campo;
- g) modalità di comunicazione dei risultati agli interessati e alla Direzione Generale;
- h) definizione delle attività di formazione programmate per la Funzione I.A.
- i) principi etici declinati dall'I.I.A.

L'attuazione dell'audit consiste in:

- analisi della documentazione che disciplina il processo verificato, intesa sia come norme esterne legislative e tecniche, che regole interne documentate;
- intervista ai soggetti coinvolti, al fine di conoscere il contesto e le prassi consolidate, nonché chiarire eventuali dubbi emersi dall'analisi documentale;
- campionamento, in base a criteri di significatività o di opportunità.

La fase finale dell'audit si realizza con la redazione di:

- un rapporto provvisorio di audit per la condivisione delle osservazioni emerse, che sarà trasmesso alle strutture coinvolte nell'audit, con esplicitazione dei tempi di risposta per eventuali considerazioni di parte;
- il rapporto definitivo di audit, alla luce delle considerazioni pertinenti, sarà trasmesso al Direttore Generale e agli altri interessati.

Il rapporto può determinare un piano di miglioramento le cui azioni sono sottoposte a un follow-up per il monitoraggio/verifica delle azioni correttive. Per ciascun intervento di audit viene creato e conservato, con garanzia di riservatezza, un fascicolo contenente tutte le evidenze atte a documentare l'attività svolta.

#### **Art. 9 Rapporti e Comunicazioni**

I rapporti di audit devono essere comunicati al management dell'unità sottoposta a revisione, al Team di Audit, al Direttore Generale nonché al CCCi. Le raccomandazioni e i relativi piani di miglioramento, scaturiti dal rapporto di audit, devono essere seguiti e monitorati dall'I.A. fino alla loro completa attuazione. La pianificazione annuale delle attività di audit (Piano I.A.), le azioni di miglioramento ancora da implementare, e gli aggiornamenti di quelle implementate (follow-up), devono essere trasmessi alla Struttura Audit di Regione Lombardia secondo le modalità e le tempistiche stabilite dalla normativa vigente.

#### **Art. 10 Obbligo di denuncia**

Qualora dall'attività di audit emergano fatti di rilevanza penale, o che possano integrare responsabilità amministrativo-contabile, il Responsabile I.A. trasmette la relativa comunicazione all'Autorità Giudiziaria competente, informando contestualmente la Direzione Generale. Nel caso in cui si rilevino fatti che non integrino le tipologie illecite di cui sopra, ma che presentino potenziali rischi per la Fondazione, il Responsabile I.A. ne dà tempestiva notizia al Direttore Generale, per i provvedimenti del caso.

#### **Art. 11 Formazione e aggiornamento**

Il personale assegnato alla Funzione di I.A., per svolgere il suo compito con la dovuta competenza, deve seguire un percorso formativo adeguato, che garantisca il potenziamento e il mantenimento delle competenze delle professionalità impiegate.

Il Responsabile della Funzione di I.A. definisce i contenuti formativi, comunicandoli al Responsabile della Formazione, per il loro inserimento nel relativo Piano aziendale.

#### **Art. 12 Codice di Condotta**

Il personale dell'Internal Audit deve aderire ai principi etici di integrità, obiettività, riservatezza e competenza (secondo i principi e standard etici dello I.I.A.). Eventuali conflitti di interesse devono essere dichiarati e gestiti in modo appropriato.

#### **Art. 13 Confidenzialità delle Informazioni**

Il personale dell'Internal Audit è tenuto a rispettare la confidenzialità delle informazioni raccolte durante le attività di audit, con l'impegno a non divulgarle a terzi non autorizzati. Le informazioni devono essere utilizzate solo per finalità strettamente legate alle attività di audit e gestite secondo i principi di necessità e proporzionalità.

#### **Art. 14 Protezione dei Dati Personali**

L'Internal Audit deve operare nel rispetto delle normative sulla protezione dei dati personali (GDPR 2016/679 e decreto legislativo N. 196 del 2003) assicurando che i dati personali siano trattati solo se strettamente necessari e con il massimo livello di tutela.

#### **Art. 15 Norma di rinvio**

Per tutto quanto non previsto dal presente Regolamento, si rinvia al Manuale di Internal Auditing di Regione Lombardia (Decreto DDUO Sistema dei Controlli e Coordinamento Organismi Indipendenti n. 2822 del 3.4.2013).