Regolamento

di

Internal Auditing

(Reg. n. 41/2015)

Approvato con deliberazione n. 3/C.d.A./0286 del 14 dicembre 2015
Modificato con deliberazione n. 4/C.d.A./0056 del 20 luglio 2017
Modificato con deliberazione n. 5/C.d.A./11 del 14 febbraio 2022

Istituto di Ricerca e Cura a Carattere Scientifico di diritto pubblico
C.F. 00303490189 - P. IVA 00580590180
V.le Golgi, 19 - 27100 PAVIA
Tel. 0382 5011

SOMMARIO

CAPO I – DISPOSIZIONI GENERALI

ART. 1 – INTRODUZIONE

Con le "Regole di sistema 2015 - ambito sanitario" (Allegato B della D.G.R. 23 dicembre 2014, n. X/2989), Regione Lombardia ha stabilito di inserire nella Rete di Internal Auditing tutti gli Enti Sanitari che, pertanto, devono dotarsi di un proprio Regolamento in materia.

L'Internal Auditing (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".

L'attività di Internal Auditing è regolata a livello internazionale dai relativi Standard professionali emanati dall'I.I.A. (Institute of Internal Auditors) che, tra l'altro, ha redatto un Codice Etico con i Principi e le Regole di condotta (Integrità, Obiettività, Riservatezza, Competenza) cui gli auditor devono conformarsi.

A tali principi si ispira anche il presente Regolamento (vedi allegato 1).

Gli obiettivi strategici della Funzione di I.A. consistono nel verificare la funzionalità del sistema di controllo interno, che mira a migliorare l'efficacia/efficienza dell'attività di controllo, razionalizzandola in funzione dei rischi, individuare i punti di debolezza dei processi aziendali, ridurre gli impatti economici dei rischi e validare modelli interni.

ART. 2 – SCOPO E CAMPO DI APPLICAZIONE

Il presente Regolamento descrive i principi, le procedure, le metodologie e gli strumenti di lavoro utilizzati per l'attività di auditing.

I destinatari del Regolamento sono la Direzione Strategica, i Responsabili della funzione di *Internal Auditing* (di seguito in breve "Responsabile I.A."), il *Team* di *Auditor* (di seguito in breve "*Team* I.A."), tutte le Strutture e i Servizi a qualunque titolo interessati all'attività di auditing.

L'obiettivo che si intende perseguire attraverso il Regolamento è quello di definire la metodologia per assistere il management nell'identificazione, mitigazione e monitoraggio dei rischi e dei relativi controlli.

Il Regolamento potrà essere soggetto a revisioni nel caso di mutamento del contesto organizzativo e sulla base dei risultati annuali dell'attività di auditing. Le revisioni del Regolamento dovranno essere approvate seguendo l'iter procedurale previsto per l'adozione dello stesso.

ART. 3 – RIFERIMENTI NORMATIVI

- Decreti Legislativi 286/1999 e 165/2001, nelle rispettive versioni vigenti, per quanto attiene alle disposizioni sui controlli interni alle Pubbliche Amministrazioni;
- Legge Regionale n. 30 del 27 dicembre 2006 che, in attuazione dello Statuto di Regione Lombardia, ha istituito il Sistema Regionale costituito dalla Regione e dagli Enti individuati negli allegati 1 e 2 della stessa Legge;
- Legge Regionale n. 14 del 6 agosto 2010 che, secondo quanto stabilito dalla Legge di cui al capoverso precedente, ha differenziato la forma di partecipazione degli Enti al Sistema Regionale sulla base della loro tipologia;
- DGR n. 2524 del 24 novembre 2011 con la quale la Regione ha stabilito le modalità di esercizio dell'attività di vigilanza e controllo sugli Enti appartenenti al Sistema Regionale finalizzati al perseguimento di obiettivi di efficacia, efficienza ed economicità;
- Legge regionale n. 17 del 4 giugno 2014 in cui si stabilisce che il controllo regionale non sostituisce e non duplica i controlli interni posti in essere dagli Enti ma si aggiunge e si avvale degli stessi nell'ottica di cooperazione al miglioramento dei sistemi di gestione e controllo;
- DGR n. 1292/2014 del 30 gennaio 2014 con la quale Regione Lombardia ha definito le direttive agli Enti e alle Società del sistema regionale in merito alla tipologia dei controlli con particolare riguardo alla funzione di *Internal Auditing*;
- Nota prot. 30876 del 20.3.2014 con la quale la Direzione Centrale Legale, Legislativo, Istituzionale e Controlli Sistema dei Controlli e Coordinamento Organismi Indipendenti SIREG ha chiesto ad ogni Azienda Sanitaria l'individuazione del responsabile della funzione di *Internal Auditing*;

- DGR n. 2989 del 23 dicembre 2014 c.d. “Regole 2015” in cui si prevede che ogni Azienda approvi un proprio regolamento di *Internal Auditing* e rediga la Pianificazione annuale dell’attività di *audit* per il 2016, da trasmettere entro il 15 dicembre 2015 alla Direzione Generale Salute, utilizzando l’area del portale PIMO (Piano Integrato Informativo per il miglioramento dell’Organizzazione);
- DGR n. 1046 del 17 dicembre 2018 disciplinante le “Regole di gestione del Servizio Sociosanitario 2019” in cui:
    - si indica che la Funzione di I.A. venga collocata organizzativamente presso la Direzione Generale o che comunque riporti in ultima istanza a quest’ultima;
    - e si prevede quale adempimento la trasmissione della Pianificazione annuale di audit entro il 28 febbraio 2019 alla Struttura di Audit regionale;
- Nota mail della Struttura Audit Giunta Regionale del 07 gennaio 2020 avente oggetto “*RETE IA – Adempimenti 2020 relativi alla funzione Internal Auditing ex DGR 1046/2018 - DETERMINAZIONI IN ORDINE ALLA GESTIONE DEL SERVIZIO SOCIOSANITARIO PER L’ESERCIZIO 2019*” in cui si informa che in relazione agli adempimenti per l’anno 2020 relativi alla Funzione I.A. rimarranno in vigore le date e le modalità di trasmissione stabilite ex DGR 1046/2018, e precisamente:
    - il termine di trasmissione viene definito nella data del 28 febbraio 2020;
    - per la modalità di trasmissione si potrà utilizzare, come di consueto, la casella email (audit@regione.lombardia.it);
- Nota mail della Struttura Audit Giunta Regionale del 12 gennaio 2021 (prot. n. 0107458/21) avente oggetto “*RETE IA – Adempimenti 2021 relativi alla funzione Internal Auditing ex DGR 1046/2018 - DETERMINAZIONI IN ORDINE ALLA GESTIONE DEL SERVIZIO SOCIOSANITARIO PER L’ESERCIZIO 2019*”, in cui si informa che in relazione agli adempimenti per l’anno 2021 relativi alla Funzione I.A. rimarranno in vigore le date e le modalità di trasmissione stabilite ex DGR 1046/2018, e precisamente:
    - il termine di trasmissione viene definito nella data del 28 febbraio 2021;
    - per la modalità di trasmissione si potrà utilizzare, come di consueto, la casella email (audit@regione.lombardia.it).

ART. 4 – FUNZIONE E ATTIVITÀ

L'attività di I.A. è una funzione di verifica indipendente, operante all'interno della Fondazione e al suo servizio, con la finalità di esaminarne e valutarne i processi. Il suo obiettivo è fornire un supporto al vertice aziendale per un costante miglioramento di efficacia ed efficienza di gestione, e a tutti i componenti dell'organizzazione per un corretto adempimento alle loro responsabilità (ruolo consultivo/propositivo, rivolto a favorire l'individuazione di opportunità di miglioramento, in coerenza con gli obiettivi istituzionali).

In particolare, la Funzione di I.A., adottando la metodologia di lavoro basata sull'analisi dei processi, dei relativi rischi e dei controlli previsti per ridurne l'impatto, assiste la Direzione nel valutare l'adeguatezza del sistema dei controlli interni e la rispondenza ai requisiti minimi definiti dalle normative, verifica la conformità dei comportamenti alle procedure operative definite, identifica e valuta le aree operative maggiormente esposte a rischi e implementa misure idonee per ridurli. Grazie all'analisi sui processi, la Funzione contribuisce a individuare al loro interno eventuali aree e opportunità di miglioramento.

Secondo tali premesse, la Funzione di I.A. fornisce suggerimenti volti a migliorare il processo di *governance* con lo scopo di:

- favorire lo sviluppo di valori e principi etici nell'organizzazione;
- migliorare l'efficace gestione dell'organizzazione e l'*accountability*;
- comunicare informazioni su rischi e controlli ai responsabili interessati delle strutture interne;
- coordinare le attività e il processo di scambio di informazioni su rischi e controlli tra il Direttore, l'organismo di certificazione, gli *internal auditor* e il *management*.

Premesso che l'attività della Pubblica Amministrazione si palesa necessariamente attraverso atti scritti, il compito del Responsabile I.A. e del *Team* I.A. è quello di:

- identificare e valutare i fattori di rischio, tramite analisi dei processi basata sul rischio (*risk based*)
- verificare e monitorare la regolarità degli atti adottati dalla Fondazione, nonché la regolarità dei processi che hanno portato all'adozione dei suddetti atti e gli eventuali scostamenti rispetto alle leggi, alle norme, alle regole e alle disposizioni interne;
- verificare l'affidabilità dei sistemi di controllo;

- avanzare proposte di modifica regolamentari o altri suggerimenti volti a superare le difficoltà riscontrate.

In quest'ottica, il controllo di auditing si ispira al principio di autotutela della amministrazione che, nell'ipotesi in cui ravvisi in propri atti elementi di irregolarità o di illegittimità, può procedere a rettificarli, integrarli o annullarli.

Il Responsabile I.A. e il *Team* I.A. hanno una funzione di verifica indipendente operante all'interno dell'IRCCS auditato e al servizio delle strutture auditate con la finalità di analizzarne e valutarne le attività e hanno come obiettivo quello di prestare assistenza a tutti i componenti dell'organizzazione, nonché di fornire supporto al vertice aziendale.

CAPO II – FUNZIONAMENTO DEGLI AUDIT

ART. 5 – ORGANIZZAZIONE, RUOLI, COMPITI E RESPONSABILITÀ

L'I.A. è un'attività indipendente, pertanto la relativa Funzione aziendale, per svolgere il suo compito in modo obiettivo, dovrà godere della necessaria autonomia, libera da condizionamenti, quali potrebbero essere conflitti di interesse individuali, limitazioni del campo di azione, restrizioni nell'accesso a informazioni, rapporto di dipendenza gerarchica nei confronti di coloro che verifica o difficoltà analoghe.

La responsabilità della Funzione di I.A. è assegnata ad un Dirigente/Funzionario, posizionato nell'organizzazione in staff al Direttore Generale e solo a quest'ultimo dovrà relazionare e rispondere per tutte le proprie attività.

In attuazione di quanto precede, la Direzione Generale attribuisce alla Funzione I.A. le risorse ritenute necessarie per adempiere al suo mandato e ne supporta l'attività per consentirle di conseguire i relativi obiettivi.

Nell'ambito degli IRCCS pubblici, si è costituito un Gruppo *ad hoc*, prevalentemente per l'attività formativa, composto dai Responsabili I.A. dei seguenti IRCCS:

- Fondazione IRCCS Policlinico San Matteo di Pavia
  con sede legale in Pavia, Viale Golgi n. 19
- Fondazione IRCCS Istituto Nazionale dei Tumori
  con sede legale a Milano, Via Venezian n. 1
- Fondazione IRCCS Istituto Neurologico Carlo Besta

con sede legale a Milano, Via Celoria n. 11

- Fondazione IRCCS Cà Granda Ospedale Maggiore Policlinico
  con sede legale a Milano, Via Francesco Sforza n. 28

All'interno di ogni IRCCS si costituisce un Team I.A., i cui componenti sono nominati dal Direttore Generale, che deve contemplare le seguenti competenze:

- Legali (Laurea in Giurispudenza)
- Economiche (Laurea in Economia e Commercio, ovvero esperienza contabile)
- Qualità (Laurea in Medicina e Chirurgia, nelle Professioni Sanitarie, Lauree non Mediche ovvero esperienza nelle valutazioni di parte terza)
- Informatiche (Laurea in Ingegneria, Ingegneria gestionale, ovvero esperienza in progettazione e sicurezza informatica).

Al *Team* I.A. afferiranno anche altre competenze a cui il Responsabile I.A. potrà attingere di volta in volta al bisogno, in occasione di valutazioni di processi specifici e complessi e che richiedano competenze differenti da quelle proprie del *Team* I.A.

Al Responsabile I.A. compete:

- assistere la Direzione Strategica nel valutare il funzionamento del sistema dei controlli e delle procedure operative;
- redigere il Piano di *Audit*;
- regolare lo svolgimento delle attività programmate all'interno del Piano di Audit adottato;
- approvare i rapporti finali di *audit*;
- individuare e proporre le azioni migliorative;
- attivare consulenze interne, qualora ve ne sia il bisogno per carenza di competenze adeguate necessarie al Team I.A., per la pianificazione ed esecuzione degli interventi di *audit*;
- partecipare agli specifici corsi di formazione e/o aggiornamento.

Al *Team* I.A. compete:

- partecipare alle attività di *audit*;
- raccogliere, ordinare ed archiviare tutta la documentazione e le evidenze necessarie ad effettuare gli *audit* e a supportare le conclusioni tratte nel corso degli stessi;
- redigere le bozze dei verbali degli *audit* e dei rapporti preliminari e finali;
- individuare e proporre le azioni migliorative;

- aggiornare le tavole di *follow up* al termine di ciascun intervento di *audit*;
- collaborare alla revisione del Regolamento;
- partecipare agli specifici corsi di formazione e/o aggiornamento.

ART. 6 – TIPOLOGIA DEI CONTROLLI

L'attività di I.A., riferita ai principali obiettivi del controllo interno nelle organizzazioni, assume particolari caratteristiche, evidenziando le seguenti tipologie:

- 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: ***audit* di conformità (*compliance audit*)**
- l'efficacia ed efficienza delle attività operative e dei processi per monitorare il rispetto degli obiettivi*:* ***audit* operativo (*operational audit*)**
- l'attendibilità delle informazioni di bilancio (e salvaguardia del patrimonio): ***audit* finanziario - contabile (*financial audit*)**.

Ulteriori tipologie di audit sono:

- **IT *audit***: per verificare la conformità dei sistemi informativi alle necessità aziendali (coerenza logica delle informazioni trattate, etc.), alle normative vigenti (livelli di sicurezza e di affidabilità, etc.), etc.

- ***audit* direzionale**: per analizzare definizione e condivisione aziendale degli obiettivi strategici, e rischi correlati, e verificare nel tempo la coerenza dei comportamenti gestionali rispetto a tali obiettivi

- ***follow up***: per rilevare l'effettiva realizzazione delle azioni concordate a seguito di osservazioni formulate durante interventi precedenti.

ART. 7 – METODOLOGIA

7.1. Identificazione e valutazione del rischio *(Risk Assessment)*

La prima fase dell'attività di I.A. è costituita dal *Risk Assessment*, ossia da un processo sistematico di identificazione e valutazione dei rischi per individuare le aree maggiormente esposte a rischio, che potrebbero pregiudicare il raggiungimento degli obiettivi posti dal management.

Il *Risk Assessment* rappresenta l'analisi preliminare utile per la stesura del Piano di *Audit* e può essere definito dai Responsabili I.A., o costituito dai Modelli Organizzativi contenenti le mappature dei processi sensibili già presenti a vario titolo in Fondazione.

7.2. Pianificazione

La seconda fase consiste nella individuazione, sulla base del *risk assessment*, dei processi da sottoporre ad auditing nell'ambito di un Piano (di seguito in breve "Piano I.A.") predisposto con periodicità almeno annuale.

Il Piano I.A. viene approvato con provvedimento del Direttore Generale nel rispetto della tempistica prevista da Regione Lombardia per la sua trasmissione alle strutture regionali competenti e gli interventi in esso previsti fanno riferimento all'anno solare successivo. Per esigenze contingenti il Piano può subire variazioni; eventuali modifiche significative apportate in corso d'anno dovranno essere approvate con le stesse modalità.

Il Piano I.A. viene redatto secondo le proposte del Responsabile I.A. ed individua le attività da svolgere e le relative strutture interessate, senza escludere eventuali azioni autonome di altro livello, come tipologie di operazioni specifiche, nel caso queste presentino criticità particolari.

Il Piano prevede anche le risorse da destinarsi alle attività comprese al suo interno, in termini quantitativi e di competenza.

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

- processo e/o procedura oggetto di *audit*
- tipo e obiettivo dell'*audit*
- criteri di valutazione
- strumenti di supporto e di rilevazione
- modalità di comunicazione agli interessati del calendario e delle specifiche del singolo *audit*
- responsabile e/o referente interno alle strutture interessate per la fase di istruttoria e verifica sul campo
- modalità di comunicazione dei risultati agli interessati e alla Direzione Generale.

7.3. Rapporto

A chiusura dei lavori il Responsabile I.A e il *Team* I.A. predispongono un Rapporto Preliminare dove saranno esplicitate le Non Conformità/Raccomandazioni rilevate e sarà discusso durante la riunione di chiusura con il personale della struttura coinvolta definendo la Azioni Correttive e/o Preventive da mettere in atto. Il *Team* I.A. quindi stilerà il Rapporto Finale dove saranno esplicitate le eventuali osservazione della Struttura auditata qualora non condividesse le Non Conformità rilevate. In questo documento saranno definiti i responsabili delle Azioni da intraprendere e la data limite previste per la loro applicazione.

L'attività del Responsabile I.A. e del *Team* I.A. prosegue con il *follow-up*, ossia con il monitoraggio/verifica della Azioni Correttive da parte della struttura. Il tutto sarà verbalizzato e comunicato per iscritto al Direttore Generale dell'IRCCS auditato.

7.4. Archiviazione

Per ciascun intervento di *audit* viene creato un fascicolo contenente tutte le evidenze atte a documentare l'attività di *audit*.

La Funzione I.A. dell'IRCCS auditato conserva presso lo stesso IRCCS tutta la documentazione relativa all'attività di *audit*. Il materiale viene fascicolato e custodito all'interno di apposito armadio che consenta di mantenere la segretezza degli atti.

ART. 8 – OBBLIGO DI DENUNCIA

8.1. Denuncia di danno erariale

Qualora dall'attività di *audit* emergano fatti che possano dar luogo a responsabilità per danni causati alla finanza pubblica (responsabilità erariale), la denuncia va redatta sulla base delle rilevazioni del Responsabile e del Team I.A. e deve contenere tutti gli elementi raccolti per l'accertamento della responsabilità e la determinazione del danno.

L'obbligo di denuncia sussiste qualora il danno sia concreto e attuale e non quando i fatti abbiano solo una mera potenzialità lesiva. In quest'ultima ipotesi, il Responsabile IA e il *Team* I.A. informeranno per iscritto il Direttore Generale dell'obbligo di operare affinché il danno sia evitato e, nel caso si verifichi, dell'obbligo di denunciare il fatto alla Procura erariale.

8.2. Denuncia penale

Qualora nel corso dell'attività di *audit* venga acquisita notizia di un reato perseguibile d'ufficio, il Responsabile I.A. ed il *Team* IA devono farne denuncia senza ritardo. La denuncia, redatta dal Responsabile I.A. e dal *Team* I.A. che hanno preso notizia del reato, è inviata al Pubblico ministero o a un Ufficiale di polizia giudiziaria, con contestuale informativa per iscritto al Direttore Generale dell'IRCCS auditato.

Qualora gli elementi emersi, pur non integrando una notizia di reato, possano comunque ritenersi rilevanti per l'applicazione della legge penale, il Responsabile I.A. ed il *Team I.A.* invieranno una segnalazione al Pubblico Ministero o a un Ufficiale di Polizia giudiziaria.

ART. 9 – FORMAZIONE

Il personale assegnato alla Funzione di I.A., infine, per svolgere il suo compito con la dovuta competenza, altro principio costitutivo nell'attività degli *internal auditor*, deve seguire un percorso formativo adeguato, migliorando continuamente la propria preparazione professionale in materia.

Il Responsabile della Funzione di I.A. individua l'istruzione da fornire al personale mediante formazione interna, esterna, tirocini, etc.; le esigenze formative vengono inserite nel relativo piano annuale a seguito della rilevazione del fabbisogno formativo aziendale.

La formazione del *Team* I.A. deve svilupparsi su due direttrici: quella professionale (linee guida, normativa specifica, etc.) e quella generale di conoscenza dell'Ente e dei suoi processi, con particolare riguardo all'organizzazione, alle sue regole, alle attività e ai controlli interni. Il fabbisogno per la formazione professionale sarà gestito in modo interaziendale, tramite progettazione ed erogazione congiunta degli IRCCS citati all'articolo 5.

La formazione comprenderà anche l'esigenza di presentare l'I.A. a tutte le funzioni della Fondazione, per acquisire una partecipazione informata, e condivisa, sull'attività, affinché l'intervento di I.A. sia efficace e costituisca un interesse comune dell'organizzazione.

CAPO III - DISPOSIZIONI FINALI

ART. 10 – NORME TRANSITORIE E FINALI

Per tutto ciò che risultasse necessario rispetto all'attività di IA, non compreso nel presente documento, si potrà fare riferimento al Manuale di *Internal Auditing* di Regione Lombardia (Decreto DDUO Sistema dei Controlli e Coordinamento Organismi Indipendenti n. 2822 del 3.4.2013).

ART. 11 – ALLEGATI E MODULISTICA

- ALLEGATO 1 ALL RA C.d.A 21.1 CODICE ETICO I.I.A.
- ALLEGATO 2 ALL RA C.d.A 21.2 TERMINOLOGIA IN USO NELLA MATERIA

ART. 12 – ENTRATA IN VIGORE

Il presente regolamento entra in vigore dalla pubblicazione della deliberazione di approvazione del Consiglio di Amministrazione della Fondazione.

ALL RA C.d.A. 21.1 CODICE ETICO I.I.A.

Il Codice Etico enuncia i principi di integrità, obiettività, riservatezza e competenza che caratterizzano l'esercizio della funzione di IA, fornendo altresì le Regole di Condotta.

Introduzione. Lo scopo del Codice Etico dell'*Institute of Internal Auditors* è di promuovere la cultura etica nell'esercizio della professione di *internal auditing*.
L'*internal auditing* è un'attività indipendente ed 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 codice etico è uno strumento necessario ed appropriato per l'esercizio dell'attività professionale di *internal audit*, che è fondata sulla fiducia indiscussa nell'obiettività dei suoi servizi di assurance riguardanti la *governance*, la gestione dei rischi e il controllo.
Il Codice Etico dell'*Institute of Internal Auditors* si estende oltre la Definizione di *Internal Auditing* per includere due componenti essenziali:
1. i **Principi** fondamentali per la professione e la pratica dell'*Internal Auditing*;
2. le **Regole di Condotta** che descrivono le norme comportamentali che gli *internal auditor* sono tenuti ad osservare. Queste regole sono un aiuto per orientare l'applicazione pratica dei Principi e intendono fornire agli *internal auditor* una guida di comportamento professionale.

Il termine *internal auditor* si riferisce ai membri dell'*Institute of Internal Auditors*, ai detentori delle certificazioni professionali rilasciate dall'*Institute*, a coloro che si candidano a riceverle e a tutti coloro che svolgono attività di *internal audit* secondo la Definizione di *Internal Auditing*.

Applicabilità ed attuazione. Il Codice Etico si applica sia ai singoli individui sia alle strutture che forniscono servizi di *internal auditing*.
Il mancato rispetto del Codice Etico da parte dei membri dell'*Institute*, dei detentori delle certificazioni professionali e di coloro che si candidano a riceverle, sarà valutato e

sanzionato secondo le norme previste nello Statuto e nelle "*Administrative Directives*" dell'*Institute*.

Il fatto che non siano esplicitamente menzionati nel Codice non toglie che certi comportamenti siano inaccettabili o inducano discredito e quindi che possano essere passibili di azione disciplinare.

Principi. L'*internal auditor* è tenuto ad applicare e sostenere i seguenti principi:

1. Integrità

L'integrità dell'*internal auditor* permette lo stabilirsi di un rapporto fiduciario e quindi costituisce il fondamento dell'affidabilità del suo giudizio professionale.

2. Obiettività

Nel raccogliere, valutare e comunicare le informazioni attinenti l'attività o il processo in esame, l'*internal* auditor deve manifestare il massimo livello di obiettività professionale. L'*internal auditor* deve valutare in modo equilibrato tutti i fatti rilevanti, senza venire indebitamente influenzato da altre persone o da interessi personali nella formulazione dei propri giudizi.

3. Riservatezza

L'*internal auditor* deve rispettare il valore e la proprietà delle informazioni che riceve ed è tenuto a non divulgarle senza autorizzazione, salvo che lo impongano motivi di ordine legale o deontologico.

4. Competenza

Nell'esercizio dei propri servizi professionali, l'*internal auditor* utilizza il bagaglio più appropriato di conoscenze, competenze ed esperienze.

Regole di Condotta

1. Integrità

L'*internal auditor*:

1.1 Deve operare con onestà, diligenza e senso di responsabilità.

1.2 Deve rispettare la legge e divulgare all'esterno solo se richiesto dalla legge e dai principi della professione.

1.3 Non deve essere consapevolmente coinvolto in nessuna attività illegale, né intraprendere azioni che possano indurre discredito per la professione o per l'organizzazione per cui opera.

1.4 Deve rispettare e favorire il conseguimento degli obiettivi dell'organizzazione per cui opera, quando etici e legittimi.

2. Obiettività

L'*internal auditor*:

2.1 Non deve partecipare ad alcuna attività o avere relazioni che pregiudichino o appaiano pregiudicare l'imparzialità della sua valutazione. In tale novero vanno incluse quelle attività o relazioni che possano essere in conflitto con gli interessi dell'organizzazione.

2.2 Non deve accettare nulla che pregiudichi o appaia pregiudicare l'imparzialità della sua valutazione.

2.3 Deve riferire tutti i fatti significativi a lui noti, la cui omissione possa fornire un quadro alterato delle attività analizzate.

3. Riservatezza

L'*internal auditor*:

3.1 Deve acquisire la dovuta cautela nell'uso e nella protezione delle informazioni acquisite nel corso dell'incarico.

3.2 Non deve usare le informazioni ottenute né per vantaggio personale, né secondo modalità che siano contrarie alla legge o di nocumento agli obiettivi etici e legittimi dell'organizzazione.

4. Competenza

L'*internal auditor*:

4.1 Deve effettuare solo prestazioni per le quali abbia la necessaria conoscenza, competenza ed esperienza.

4.2 Deve prestare i propri servizi in pieno accordo con gli Standard internazionali per la Pratica Professionale dell'*Internal Auditing*

4.3 Deve continuamente migliorare la propria preparazione professionale nonché l'efficacia e la qualità dei propri servizi.

Le caratteristiche fondamentali dell'attività, ispirate ai principi e agli standard dell'IA, sono:

- **Indipendenza del sistema di controllo**. Il responsabile e gli addetti al controllo devono essere indipendenti dalle attività oggetto della verifica per consentire valutazioni imparziali e

obiettive; si ottiene con un'adeguata collocazione organizzativa. L'indipendenza si consolida se il responsabile della funzione di IA è designata dal Vertice aziendale (standard n.1100) ed è più garantita quando il servizio viene affidato a una struttura collegiale composta da membri interni e esterni.

- **Imparzialità**. Le finalità, i poteri e le responsabilità della funzione di IA sono definiti in una formale assegnazione di incarico, cui fa seguito la presentazione, da parte del responsabile incaricato, di un piano annuale di auditing (dove sono esplicitati gli strumenti di rilevazione) che, una volta approvato, viene divulgato all'interno della Fondazione e vincola l'ambito di azione; la standardizzazione degli strumenti di controllo garantisce una valutazione omogenea nella rilevazione delle informazioni.

– **Contestualità/utilità**. Peculiare dei controlli di regolarità contabile e amministrativa è il principio generale che non consente verifiche preventive se non nei casi previsti da espresse disposizioni di legge.

- **Procedure di controllo selezionate e indipendenti**. Non essendo realisticamente possibile sottoporre a controllo tutti i processi o i provvedimenti e le procedure adottati dall'organizzazione, occorre far ricorso alla individuazione di un campione significativo (coerente con le priorità indicate dal vertice aziendale).

- **Standardizzazione degli strumenti di controllo**. Gli standard predefiniti di riferimento, rispetto ai quali si verifica la rispondenza di un atto, di una procedura o di un processo, essendo la Fondazione una P.A., sono costituiti da leggi, regolamenti, linee guida, direttive interne, etc. Può essere utile definire delle griglie che richiamino i rispettivi elementi indispensabili e gli adempimenti necessari.

- **Trasparenza e coinvolgimento dei responsabili nell'organizzazione**. L'adozione del piano annuale di auditing deve produrre un confronto preliminare tra i soggetti interessati per evidenziare la funzione di assistenza, propria della funzione di IA, ed evitare che questa sia confusa con i controlli di carattere ispettivo.

- **Separazione** tra la funzione di IA da un lato e il controllo di gestione, il controllo strategico e la valutazione della dirigenza dall'altro, sono il cardine del nuovo sistema del controllo interno, introdotto dal d.lgs. 286/99. Tutte le tipologie di controllo, infatti, sono articolate in un unico sistema integrato, nel quale le varie funzioni interagiscono, costituendo elementi di garanzia per l'organizzazione e per il cittadino.

ALL RA C.d.A. 21.2 TERMINOLOGIA IN USO NELLA MATERIA

Adeguato controllo

Un controllo è adeguato se viene pianificato e organizzato (progettato) dal management in modo da dare ragionevole sicurezza che i rischi dell'organizzazione siano stati gestiti efficacemente e che le finalità e gli obiettivi dell'organizzazione saranno raggiunti in modo efficiente ed economico.

Ambiente di controllo

È costituito dagli atteggiamenti e dalle azioni del *board* e del management rispetto all'importanza del controllo all'interno dell'organizzazione. Esso fornisce la disciplina e l'organizzazione per il raggiungimento degli obiettivi primari del sistema di controllo interno. Gli elementi costitutivi dell'ambiente di controllo sono i seguenti:

• integrità e valori etici;
• filosofia e stile di direzione;
• Struttura organizzativa;
• attribuzione di poteri e responsabilità;
• politiche e prassi di gestione del personale;
• competenze del personale.

Attività di *internal audit*

Reparto, divisione, team di consulenti o di altri professionisti che forniscono servizi indipendenti e obiettivi di *assurance* e di consulenza, concepiti per aggiungere valore e migliorare l'operatività di un'organizzazione. L'attività di *internal audit* assiste un'organizzazione nel perseguimento dei propri obiettivi, tramite un approccio professionale sistematico finalizzato a valutare e migliorare l'efficacia dei processi di *governance*, di gestione dei rischi e di controllo.

Board

Per *board* si intende il massimo organo di governo, che ha la responsabilità di indirizzare e/o di sorvegliare le attività e la gestione dell'organizzazione. In genere, il *board* è costituito da un gruppo indipendente di amministratori (per esempio, consiglio di amministrazione, consiglio di sorveglianza, consiglio dei governatori o dei *trustee*). Nei casi in cui questo

gruppo non è presente, per "*board*" si può intendere la persona a capo dell'organizzazione. Il termine "*board*" può anche designare un *Audit Committee* al quale l'organo di governo abbia delegato determinate funzioni.

Codice Etico (o Codice Deontologico)

Il Codice Etico dell'*Institute of Internal Auditors* (IIA) è composto da Principi, fondamentali per la professione e la pratica dell'attività di *internal audit*, e da Regole di Condotta, che descrivono le norme comportamentali che gli auditor sono tenuti a osservare. Esso si applica sia alle singole persone sia agli enti che forniscono servizi di *internal audit*. Scopo del Codice Etico è quello di promuovere una cultura etica in tutti gli ambiti della professione di *internal auditor*.

Condizionamenti

Condizionamenti all'indipendenza organizzativa e all'obiettività individuale possono comprendere conflitti di interesse personali, limitazioni del campo di azione, restrizioni dell'accesso a dati, persone e beni aziendali e vincoli sulle risorse (come quelle finanziarie).

Conflitto di interessi

Qualsiasi relazione tra persone e/o organizzazioni che sia o appaia essere contraria agli interessi dell'organizzazione. Il conflitto di interessi pregiudica la capacità individuale di svolgere i propri compiti e responsabilità con obiettività.

Conformità

L'aderenza a direttive, piani, procedure, leggi, regolamenti, contratti o altri requisiti.

Controlli IT (*Information Technology*)

Controlli che supportano la gestione del business e la *governance* prevedendo controlli generali e specifici sulle infrastrutture informatiche quali sistemi applicativi, informazioni, infrastrutture e persone.

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. Il management pianifica, organizza e dirige l'esecuzione di iniziative in grado di fornire una ragionevole sicurezza sul raggiungimento di obiettivi e traguardi.

Deve (devono)

Gli Standard utilizzano la dizione "deve (devono)" per indicare un requisito la cui conformità è vincolante.

Dovrebbe (dovrebbero)

Gli Standard utilizzano la dizione "dovrebbe (dovrebbero)" per indicare un requisito la cui conformità è vincolante a meno di circostanze ed eventi che, sottoposti a un giudizio professionale, ne giustifichino l'inosservanza.

Frode

Qualsiasi atto illegale caratterizzato da falsità, dissimulazione e abuso di fiducia. Tali atti non sono legati a minacce di ricorso alla violenza o alla forza fisica. Le frodi sono perpetrate da persone e organizzazioni per ottenere denaro, beni o servizi, per evitare il pagamento o la perdita di servizi o per procurarsi vantaggi personali o commerciali.

Gestione del rischio

Processo teso a identificare, valutare, gestire e controllare possibili eventi o situazioni negativi, al fine di fornire una ragionevole assicurazione in merito al raggiungimento degli obiettivi dell'organizzazione.

Giudizio complessivo

Valutazione, conclusione e/o altra descrizione dei risultati presentata dal responsabile *internal auditing*; essa verte, in termini generali, sui processi di *governance*, di gestione dei rischi e/o di controllo dell'organizzazione. Per giudizio complessivo si intende il giudizio professionale del responsabile *internal auditing*, basato sui risultati di una serie di incarichi individuali e di altre attività per un determinato periodo di tempo.

Giudizio dell'incarico

Valutazione, conclusione e/o altra descrizione dei risultati di un incarico di *internal audit*, con

riferimento agli obiettivi e all'ambito di copertura dell'incarico.

Governance

Insieme dei procedimenti e delle strutture messi in atto dall'organo di governo dell'organizzazione per informare, indirizzare, gestire e controllare le attività dell'organizzazione nel raggiungimento dei suoi obiettivi.

***Governance* dei sistemi informativi**

Consiste nella guida, nelle strutture organizzative e nei processi finalizzati ad assicurare che la tecnologia informatica dell'azienda (IT) supporti le strategie e gli obiettivi dell'organizzazione.

Incarico

È la specifica assegnazione di un *audit*, compito o attività di verifica, siano essi un incarico di *internal audit*, una verifica di *control self-assessment*, una investigazione per frode o una consulenza. Un incarico può includere più compiti o attività, concepiti per raggiungere un insieme specifico di obiettivi interrelati.

Indipendenza

Libertà dai condizionamenti che minacciano la capacità dell'attività di *internal audit* di assolvere alle responsabilità di *internal audit* senza pregiudizi.

***International Professional Practices Framework* (IPPF)**

Schema concettuale che definisce come deve essere Struttura e l'insieme delle disposizioni normative (*authoritative guidance*) emanate dall'IIA (*The Institute of Internal Auditors*) che si suddividono in due categorie: (1) disposizioni vincolanti e (2) disposizioni fortemente raccomandate.

Livello di accettazione del rischio *(risk appetite*)

Il livello di rischio che un'organizzazione è disposta a sostenere.

Mandato di *internal audit*

Il Mandato di *internal audit* è un documento formale che definisce finalità, poteri e

responsabilità dell'attività di *internal audit*. Il Mandato deve determinare la posizione dell'*internal auditing* nell'organizzazione, autorizzare l'accesso ai dati, alle persone e ai beni aziendali necessari per lo svolgimento degli incarichi di *audit*, nonché definire l'ambito di copertura delle attività di *audit*.

Obiettivi dell'incarico

Enunciazioni di carattere generale che definiscono gli obiettivi attesi dell'incarico.

Prestatore esterno di servizi

Persona o società esterna all'organizzazione, munita di particolari conoscenze, competenze ed esperienze in una disciplina specifica.

Processi di controllo

Le politiche, le procedure (manuali e automatizzate) e le attività che fanno parte di un modello di controllo, progettato e gestito per assicurare che i rischi siano contenuti entro il livello che l'organizzazione è disposta a sostenere.

Programma di lavoro dell'incarico

Documento che precisa le procedure da seguire durante un incarico, elaborato per attuare quanto indicato dal piano dell'incarico stesso.

Responsabile *internal auditing* (CAE – *Chief Audit Executive*)

Il responsabile *internal auditing* è la persona con ruolo direttivo che ha la responsabilità di gestire in modo efficace l'attività di *internal audit*, in conformità al Mandato di *internal audit* e alla Definizione di *Internal Auditing*, al Codice Etico e agli Standard. Il responsabile *internal auditing* o i collaboratori che riferiscono a lui sono in possesso delle opportune qualifiche e certificazioni professionali. La designazione specifica del responsabile *internal auditing* può variare nelle diverse organizzazioni.

Rischio

Possibilità che si verifichi un evento che possa avere un effetto negativo sul raggiungimento degli obiettivi o delle finalità istituzionali. Il rischio si misura in termini di impatto e di probabilità.

Servizi di *assurance*

Consistono in un esame obiettivo delle evidenze, allo scopo di ottenere una valutazione indipendente dei processi di *governance*, di gestione del rischio e di controllo dell'organizzazione. Tra gli esempi si possono citare incarichi di tipo finanziario, di tipo operativo, di conformità, di sicurezza informatica e di due *diligence*.

Servizi di consulenza

Servizi di supporto e assistenza al cliente, la cui natura ed estensione vengano concordate con il cliente, tesi a fornire valore aggiunto e a migliorare i processi di *governance*, gestione del rischio e controllo di un'organizzazione, senza che l'*internal auditor* assuma responsabilità manageriali a riguardo. Tra i possibili esempi figurano consulenza, assistenza specialistica, facilitazione e formazione.

Significatività

Importanza relativa di un fatto, nell'ambito del contesto nel quale è considerato. Include fattori quantitativi e qualitativi quali la grandezza, la natura, le conseguenze, la rilevanza e l'impatto. Agli *internal auditor* è richiesto un giudizio professionale quando valutano la significatività dei fatti collocati nell'ambito degli obiettivi considerati.

Standard

Un enunciato professionale emanato dall'*Internal Audit Standards Board* che definisce le condizioni richieste per svolgere una vasta gamma di attività di *internal audit* e per la valutazione delle prestazioni dell'*internal audit*.

Strumenti informatici di supporto all'*audit*

Strumenti di *audit* automatizzati, quali *software* generici di *audit*, generatori dati di test, programmi informatici di *audit* e *computer-assisted audit techniques* (CAAT).

Valore aggiunto

L'attività di *internal audit* aggiunge valore all'organizzazione (e ai suoi *stakeholder*) quando fornisce un'*assurance* obiettiva e pertinente e quando contribuisce all'efficacia e all'efficienza dei processi di *governance*, di gestione del rischio e di controllo.