REGOLAMENTO PER L'ATTIVITÀ

DI INTERNAL AUDIT

NELLA FONDAZIONE

IL DIRETTORE
SC. Sistema qualità, formazione
e protezioni dati
Dott.ssa Anna Roli

SOMMARIO

IL DIRETTORE
SC. Sistema qualità, formazione
e protezioni dati
Dott.ssa Anna Roli

Art. 1 Premessa

Il presente Regolamento è emanato 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 Auditing tutti gli Enti Sanitari.
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 Audit 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 (che ispirano il presente Regolamento) e le Regole di condotta (Integrità, Obiettività, Riservatezza, Competenza), nonché lo specifico glossario, cui gli auditor devono conformarsi (Allegati 1 e 2).
Gli obiettivi strategici dell'attività 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

Il presente Regolamento disciplina le procedure, le metodologie e gli strumenti di lavoro utilizzati per l'attività di internal audit .

Art. 3 Ruoli, Funzioni e Responsabilità

Il Consiglio di Amministrazione

a) Approva e autorizza il Piano annuale di Internal Audit, redatto dal Responsabile della Funzione I.A.

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 Internal Audit, nel rispetto delle scadenze indicate da Regione Lombardia;
b) ne affida la responsabilità a un Dirigente che, per esperienza, capacità e affidabilità, possieda i requisiti idonei ad assolvere i compiti propri della Funzione di I.A.;
c) garantisce alla Funzione di I.A. la necessaria autonomia e indipendenza, secondo i principi costitutivi dell'attività;
d) individua, e assegna al Responsabile I.A., le risorse necessarie per adempiere al mandato;
e) promuove, per il tramite della s.c. Sistema qualità, formazione e protezione dati, la formazione specifica in materia di Internal Audit alle professionalità assegnate alla Funzione di I.A.

Il Responsabile I.A.

a) assiste il Consiglio di Amministrazione e la Direzione Strategica nel valutare il funzionamento del sistema dei controlli e delle procedure operative;
b) identifica e valuta i fattori di rischio, tramite analisi dei processi basata sul rischio (risk based);
c) redige il Piano di Audit;

IL DIRETTORE
SC. Sistema qualità, formazione e protezione dati
Dott.ssa Anna Roli

d) regola lo svolgimento delle attività programmate all'interno del Piano di Audit adottato, garantendone l'esecuzione e coordinando le iniziative di *follow-up*;
e) approva i programmi degli interventi e i rapporti finali di audit;
f) valuta le proposte di azioni migliorative;
g) attiva consulenze interne, qualora ve ne sia il bisogno per carenza di competenze adeguate necessarie ai Team I.A., per la pianificazione ed esecuzione degli interventi di audit;
h) avanza proposte di modifiche regolamentari o altri suggerimenti volti a superare le difficoltà riscontrate;
i) partecipa agli specifici corsi di formazione e/o aggiornamento;
j) relaziona e risponde al Consiglio di Amministrazione della Fondazione per tutte le proprie attività.

Il Team I.A., che svolge l'attività di audit
a) verifica 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;
b) raccoglie, ordina e archivia tutta la documentazione e le evidenze necessarie a effettuare gli audit e a supportare le conclusioni tratte nel corso degli stessi;
c) redige le bozze dei verbali degli audit e dei rapporti preliminari e finali;
d) individua e propone le azioni migliorative;
e) al termine di ciascun intervento di audit aggiorna la documentazione per eventuali successivi follow up (art. 6, lett. f);
f) collabora con il Responsabile I.A. alla revisione del Regolamento;
g) contribuisce all'aggiornamento e alla valutazione del modello di "Risk Assesment", secondo i risultati degli interventi di audit;
h) partecipa agli specifici corsi di formazione e/o aggiornamento.

Art. 4 Organizzazione

L'I.A. è un'attività indipendente.
Con il Piano di organizzazione aziendale strategico (breviter: POAS) approvato con D.G.R. 20 febbraio 2017, n. X/6251 – attuazione e prime determinazioni", è stato stabilito che il Responsabile della Funzione di Internal Audit risponde per tutte le proprie attività al Consiglio di Amministrazione.
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.
All'interno della Fondazione è costituito un Team I.A., i cui componenti sono nominati dal Direttore Generale, il Team contempla le seguenti competenze:
a) Legali
b) Economiche
c) Miglioramento Continuo della Qualità
d) Informatiche.

Il Team I.A. può essere integrato, per esigenze contingenti, con professionalità ulteriori, se necessarie in relazione alle specifiche attività di controllo.

Art. 5 Collaborazione 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.

IL DIRETTORE
SC. Sistema qualita', formazione
e protezione dati
Dott.ssa Anna Roli

Art. 6 Tipologia dei controlli

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

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).

Ulteriori tipologie di audit sono:

d) **IT audit**: verifica della conformità dei sistemi informativi alle necessità aziendali (coerenza logica delle informazioni trattate), alle normative vigenti (livelli di sicurezza e di affidabilità);
e) **audit direzionale**: analisi della definizione e della condivisione aziendale degli obiettivi strategici, e verifica della coerenza dei comportamenti gestionali rispetto a tali obiettivi;
f) **follow up**: rilevazione dell'effettiva, realizzazione delle azioni concordate a seguito di osservazioni formulate durante interventi precedenti.

Art. 7 Metodologia

L'attività di I.A. segue alcune fasi programmate, validate dall'Institute of Internal Auditors.
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 auditing 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 dal Consiglio di Amministrazione

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 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.

A chiusura dei lavori il Team IA redige un rapporto di 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. A seguito della valutazione del Responsabile, in merito alle considerazioni di parte, viene redatto il rapporto definitivo di audit, trasmesso anche al Direttore Generale. Il rapporto può determinare un follow up per il monitoraggio/verifica della 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.
Al termine dell'attività annuale di internal audit, il Responsabile I.A. trasmette al Consiglio di Amministrazione e al Direttore Generale una relazione sull'attività svolta e relativi esiti.

IL DIRETTORE
SC. Sistema qualità, formazione e protezione dati
Dott.ssa Anna Roli

Art. 8 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 Presidente, al Consiglio di Amministrazione e al Direttore Generale, per i provvedimenti del caso.

Art. 9 Formazione

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. 10 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).

IL DIRETTORE
SC. Sistema qualità, formazione
e protezione dati
Dott.ssa Anna Roli

APPENDICE 1

CODICE ETICO dell'Institute of Internal Auditors (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 audit.
L'Internal Audit 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 audit per includere due componenti essenziali:

1. i **Principi** fondamentali per la professione e la pratica dell' Internal Audit;
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 Audit.

Applicabilità ed attuazione. Il Codice Etico si applica sia ai singoli individui sia alle strutture che forniscono servizi di internal audit.
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.

IL DIRETTORE
SC. Sistema qualità, formazione e protezioni dati
Dott.ssa Anna Roli

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 audit

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,

IL DIRETTORE
SC. Sistema qualità, formazione
e protezione dati
Dott.ssa Anna Roli

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.

IL DIRETTORE
SC. Sistema qualita', formazione
e protezioni dati
Dott.ssa Anna Ros

APPENDICE 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).

IL DIRETTORE
SC. Sistema qualita', formazione
e protezione dati
Dott.ssa Anna Roli

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 dell'internal audit; 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 dell'internal audit, 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.

IL DIRETTORE
SC. Sistema qualita', formazione
e protezione dati
Dott.ssa Anna Rita

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 to 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 audit 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.

IL DIRETTORE
SC. Sistema qualità, formazione e protezione dati
Dott.ssa Anna Roli

Responsabile dell'Internal Audit (RIA)
Il responsabile dell'internal audit 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 audit, al Codice Etico e agli Standard. Il responsabile dell'internal audit o i collaboratori che riferiscono a lui sono in possesso delle opportune qualifiche e certificazioni professionali. La designazione specifica del responsabile dell'internal audit 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.

IL DIRETTORE
SC. Sistema qualità, formazione e protezione dati
Dott.ssa Anna Roli