Sistema Socio Sanitario
Regione Lombardia
ASST Santi Paolo e Carlo

Via A. di Rudinì,n.8 – 20142 MILANO
Tel. 02.8184.1 – Fax 02.8910875

Deliberazione n. 0000377 del 21/03/2018 - Atti U.O. S.C. Affari Generali

Oggetto: ADOZIONE MANUALE DI INTERNAL AUDIT DELLA ASST SANTI PAOLO E CARLO.

IL DIRETTORE S.C. "AFFARI GENERALI"

Premesso che, con DGR n. X/4473 del 10.12.2015, è stata costituita l' "Azienda Socio – Sanitaria Territoriale (ASST) Santi Paolo e Carlo" e che, pertanto, quest'ultima, ai sensi dell'art. 2, comma 8, lettera c), della Legge Regionale n. 23 dell'11.8.2015, a decorrere dall'1.1.2016. è subentrata nei rapporti giuridici attivi e passivi facenti capo alle A.O. San Paolo e A.O. San Carlo.

Vista la Deliberazione n. 1 dell'1.1.2016, esecutiva ai sensi di legge, avente ad oggetto "*Presa d'atto della DGR n. X/4473 del 10.12.2015 "Attuazione L.R. 23/2015: Costituzione Azienda Socio – Sanitaria Territoriale (ASST) Santi Paolo e Carlo*";

Richiamata la D.G.R. n. X/7600 del 20/12/2017 " *Determinazioni in ordine alla gestione del Servizio Sociosanitario per l'esercizio 2018"* che nel paragrafo 4.6.8. definisce la funzione di Internal Audit ed i relativi adempimenti;

Richiamate:
- la delibera n. 1766 del 18/10/2017 – POAS Aziendale – che prevede la funzione di Internal Audit;
- la delibera n. 12 del 10/01/2018 della ASST Santi Paolo Carlo con la quale veniva nominato il Direttore della S.C. Affari Generali D.ssa Donatella Peraldo, Responsabile della funzione di Internal Audit;

Dato atto che il presente provvedimento, non comporta oneri a carico del Bilancio Aziendale;

Preso atto della deliberazione del Direttore Generale n°187 del 14 febbraio 2018 avente ad oggetto "Approvazione proposta di Bilancio Preventivo Economico esercizio 2018. Versione V1".

Tutto ciò premesso, propone l'adozione della seguente deliberazione

IL DIRETTORE GENERALE

Acquisiti i pareri favorevoli del Direttore Amministrativo, del Direttore Sanitario e del Direttore Socio-Sanitario;

DELIBERA

Per i motivi di cui in premessa che qui si intendono integralmente trascritti:

1. di procedere all'adozione del Manuale Operativo delle Procedure di Internal Audit dell'ASST Santi Paolo e Carlo;

2. di dare atto che dall'adozione del presente provvedimento non derivano oneri aggiuntivi a carico di questa ASST;

3. di dare atto che il presente provvedimento è assunto su proposta del Direttore S.C. Affari Generali dott.ssa Donatella Peraldo in qualità di Responsabile della Funzione di Internal Audit e Responsabile del Procedimento, che provvederà a darne massima diffusione;

4. di dare atto che il presente provvedimento deliberativo è immediatamente esecutivo, in quanto non soggetto a controllo di Giunta Regionale, verrà pubblicato sul sito internet Aziendale, ai sensi dell'art. 17 comma 6 L. R. n. 33/2009 e ss.mm.ii.

Documento firmato digitalmente da: Direttore Amministrativo Dott.ssa Maria Grazia Colombo, Direttore Sanitario Dott. Mauro Moreno, Direttore Socio Sanitario Dott.ssa Daniela Malnis, Direttore Generale Dott. Marco Salmoiraghi ai sensi delle norme vigenti D.P.R. n.513 del 10/11/1997, D.C.P.M. del 08/02/1999, D.P.R. n. 445 del 08/12/2000, D.L.G. Del 23/01/2002

Pratica trattata da: Cinzia De Siati

Responsabile dell'istruttoria: Cinzia De Siati

Dirigente/Responsabile proponente: PERALDO DONATELLA

Il presente atto si compone di n. 63 pagine, di cui n. 60 pagine di allegati che costituiscono parte integrante e sostanziale.

Sistema Socio Sanitario
Regione Lombardia
ASST Santi Paolo e Carlo

Manuale operativo delle procedure di

Internal Audit 2018

INDICE

INTRODUZIONE

Il manuale di Internal Audit (Manuale) definisce le procedure e le modalità operative che devono essere seguite dagli auditors per l'esercizio dell'attività di Internal Audit (I.A.) nell'ambito dell' ASST Santi Paolo e Carlo.

Il contenuto del Manuale e dei suoi allegati potrà essere soggetto a periodiche valutazioni e, se del caso, revisioni in funzione delle variazioni:

- della normativa e delle procedure di riferimento;
- delle funzioni per cui l'Internal Audit è riconosciuto a svolgere l'attività;
- della strategia e dei risultati dell'attività di auditing.

L'attività di Internal Audit si riferisce ai tre obiettivi generali delle organizzazioni per i quali il controllo interno dovrebbe fornire, in base alla relativa definizione, una ragionevole sicurezza di realizzazione, ovvero:

- la conformità alle leggi e ai regolamenti in vigore;
- l'efficacia ed efficienza delle attività operative;
- l'attendibilità delle informazioni di bilancio.

L'audit di conformità può essere riferito alle normative esterne all'organizzazione o a quelle interne, o ad entrambe, come pure solo ad una parte delle suddette normative.

L'audit operativo può essere riferito agli ambiti di azione o alle attività delle funzioni, così come l'audit finanziario contabile può avere una componente di conformità, riferita alle norme di legge e ai principi contabili generalmente accettati, e una componente operativa riferita alla efficacia ed efficienza dei processi contabili.

Il Manuale viene aggiornato dalla funzione Internal Audit, e pubblicato sul sito istituzionale web: www.asst-santipaolocarlo.it.

1 LA FUNZIONE DI INTERNAL AUDIT

1.1 La funzione di Audit

La funzione di Internal Audit è qualificabile come indipendente e assiste il Direttore Generale e più ampiamente la Direzione Strategica, nelle attività di verifica e valutazione periodica dei sistemi di controllo interno. L'obiettivo primario dell'I.A. è quello di promuovere il continuo miglioramento del sistema complessivo di valutazione del rischio e di controllo interno attraverso la valutazione della sua funzionalità, la verifica della regolarità delle attività operative e l'andamento dei rischi, al fine di portare all'attenzione del management i possibili miglioramenti alle politiche, alle procedure di gestione dei rischi e ai mezzi di monitoraggio e di controllo.

In particolare, la funzione di I.A. valuta e fornisce appropriati suggerimenti volti a migliorare il processo di governance allo scopo di:

- favorire lo sviluppo di valori e principi etici nell'organizzazione;
- garantire l'efficace gestione dell'organizzazione e l'accountability;
- comunicare informazioni sui rischi e controlli alle relative funzioni dell'organizzazione.

Il controllo della funzione di I.A. viene realizzato mediante analisi, valutazioni e raccomandazioni in merito all'effettivo funzionamento dei processi di controllo interno avendo quale riferimento la legislazione vigente e le migliori prassi nazionali ed internazionali in materia di controllo interno e di Audit.

Alla funzione di I.A. compete lo svolgimento delle attività in materia di:

- impostazione dell'attività di Audit ed elaborazione di proposte di regolamentazione e programmi di controllo;

- controlli, in raccordo con le direzioni delle diverse Unità operative e/o funzioni aziendali inerenti l'adeguatezza e l'aderenza degli ambiti di azione e dell'organizzazione alle norme ed alle direttive impartite;
- coordinamento dei sistemi dei controlli interni operati dalle Unità operative e/o funzioni aziendali, in raccordo con le stesse e loro assistenza nella redazione di programmi di controllo e conseguente attività di monitoraggio;
- supporto alle Unità operative e/o funzioni aziendali nella pianificazione degli audit interni e nella mappatura dei rischi.

Nell'ambito delle proprie funzioni, il Dirigente responsabile della funzione Audit pianifica la propria attività tenendo conto delle esigenze e priorità di audit e delle risorse disponibili.

Le Unità operative e/o le funzioni auditate sono chiamate a collaborare con le attività della funzione di audit attraverso:

- messa a disposizione nei tempi concordati dei dati e delle informazioni richieste, su supporto cartaceo e/o informatico, anche in occasione di interviste;
- elaborazione tempestiva di commenti e di azioni migliorative in risposta ai rilievi e suggerimenti elaborati dalla funzione di I.A.;
- informativa in merito a riorganizzazioni e progetti speciali che comportino un cambiamento nel profilo dei rischi e del sistema di controllo interno a livello di intera organizzazione e/o di Unità operative e/o funzioni aziendali.

Il Dirigente responsabile della funzione I.A. e i suoi collaboratori sono tenuti agli obblighi di riservatezza in merito alle informazioni delle quali vengono a conoscenza. La funzione di Audit esamina il sistema di controllo interno in essere presso le Unità operative e/o funzioni dell'Azienda ed eventuali altri ambiti di attività individuati con apposita deliberazione o mandato formale dalla Direzione Generale.

A tali fini, la funzione di I.A. dispone:

- delle procedure nazionali e regionali, dei dati contabili e gestionali, degli atti e, più in generale, di ogni documento od informazione nazionale e regionale non riservata ai fini di legge;
- delle informazioni ottenibili tramite interviste al personale, fatto salvo quanto diversamente stabilito dalla legge o contrario all'etica professionale;
- di risorse quantitativamente adeguate e professionalmente capaci, anche per il tramite di collaborazione e di consulenze esterne.

L'attività di Audit svolta non solleva i responsabili delle Unità operative e/o funzioni dell'Azienda dalle proprie responsabilità in merito al mantenimento di un sistema di controllo interno efficace ed adeguato ai rischi della gestione.

1.2 Principi di riferimento

La funzione di I.A. e gli auditors fanno riferimento, per l'esplicazione della proprie attività, alle linee guida e ai principi generali espressi nel presente Manuale, al mandato formale conferitogli e ad eventuali altre normative interne specifiche. Tali normative sono emesse dal Dirigente responsabile della funzione Audit per regolamentare la produzione e archiviazione delle carte di lavoro, la protezione dei dati personali trattati, le presentazioni standard della funzione, il reporting delle attività ed eventuali altre attività tecnico-operative.

Gli auditors, nello svolgimento della funzione di I.A., fanno riferimento per l'esplicazione della proprie attività:

- alla normativa nazionale e regionale in materia di audit, nonché ai principi di revisione aziendale ed alle norme che disciplinano il sistema dei controlli interni nella pubblica amministrazione;

- agli “Standard per la pratica professionale dell’I.A.”, alle relative “Guide interpretative” ed al “Codice etico” emanati dall’Associazione Italiana Internal Auditors (A.I.I.A.) laddove non in contrasto con le normative che disciplinano l’attività amministrativa regionale.

La definizione dell’attività di Audit validata dall’organizzazione mondiale che fa capo all’A.I.I.A. americano è la seguente:

“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 controllo, di gestione dei rischi e di corporate governance”.

Il nuovo codice etico dell’associazione professionale enuncia i principi di integrità, obiettività, riservatezza e competenza che caratterizzano l’esercizio della funzione di Audit fornendo altresì le regole di condotta.

L’associazione professionale ha altresì riorganizzato e rinnovato, con validità dal 2002, gli “Standard per la pratica professionale dell’Audit Interno”, distinguendoli in Standard di 7 Connotazione (serie 1000), che riguardano le caratteristiche delle organizzazioni e degli individui che svolgono l’attività di Audit Interno, Standard di Prestazione (serie 2000), che riguardano la natura e le modalità di svolgimento di tale attività e Standard Applicativi, specifici per ciascuna tipologia di attività di Audit Interno e riferibili a ciascuna delle prime due categorie di standard generali sopra indicate.

Gli standard di connotazione riguardano:

- 1000 – Finalità, Autorità e Responsabilità
- 1100 – Indipendenza e Obiettività;

- 1200 – Competenza e Diligenza Professionale;
- 1300 – Programma di Assicurazione e Miglioramento Qualità.

Gli standard di prestazione riguardano:

- 2000 – Gestione dell'Attività di Audit Interno;
- 2100 – Natura dell'Attività;
- 2200 – Pianificazione dell'Incarico;
- 2300 – Svolgimento dell'Incarico;
- 2400 – Comunicazione dei Risultati;
- 2500 – Processo di Monitoraggio;
- 2600 – Assunzione del Rischio da parte del Management.

Mentre il codice etico e gli standard hanno carattere obbligatorio per gli auditors, le guide interpretative sono costituite da prassi di audit consolidate che, anche se facoltative, sono "altamente raccomandate" dall'associazione professionale.

Ai fini di una migliore interpretazione nell'ambito della pubblica amministrazione dei principi che caratterizzano l'attività di Audit Interno si fa riferimento anche a quanto indicato dai seguenti principi nazionali ed internazionali in materia di audit interno:

- standard I.I.A. (Institute of Internal Auditors);
- il ruolo dell'auditing nella governance del settore pubblico – Associazione Italiana Internal Auditors (A.I.I.A.);
- A.I.C.P.A. (American Institution of Certified Pubblic Accountants);
- norme INT.O.S.A.I. (International Organisation of Supreme Audit Institutions);
- principiinternazionali di revisione: ISA/ISAE/ISRE (International Standards on Auditing/Internationally Standards on Attestation Engagements/International Standard On Review Engagements);

- indirizzi, direttive e linee guida della Corte dei Conti con riferimento alla tematica dell'audit interno.

1.3 Struttura organizzativa

La funzione di Internal Audit viene collocata in staff della Direzione Generale e dipende direttamente ed esclusivamente dal Direttore Generale.

In caso di condizionamenti nell'indipendenza organizzativa o nell'obiettività individuale, devono essere tempestivamente comunicate al Direttore Generale le circostanze di tali avvenimenti.

Tra i fattori che possono condizionare l'indipendenza o l'obiettività si possono annoverare conflitti di interesse individuali, limitazione del campo di azione, restrizioni dell'accesso a dati, persone e vincoli di risorse tra cui quelle finanziarie e organizzative.

L'Internal auditor per poter svolgere correttamente le proprie funzioni deve poter avere accesso:

- alla documentazione relativa alle singole pratiche presenti presso qualsiasi Unità operativa e/o funzione dell'Azienda;
- a tutti i dati contenuti nelle banche dati utilizzate;
- alle registrazioni contabili (cartacee e informatiche);
- a ogni altra informazione che ritenga utile.

L'Internal auditor per poter mantenere l'indipendenza e l'oggettività di giudizio:

- non deve avere responsabilità diretta nei processi oggetto del controllo;
- non deve occuparsi direttamente del disegno, dell'installazione e dell'esecuzione dei processi operativi, né della definizione delle procedure.

1.4 Ruoli e responsabilità

Il Dirigente responsabile della funzione di I.A. deve periodicamente verificare che le finalità, l'autorità e le responsabilità definite nel Mandato siano sempre adeguate a consentire il raggiungimento dei propri obiettivi.

Il Dirigente responsabile della funzione di I.A. ha il compito di presentare al Direttore Generale entro il 28 febbraio dell'anno successivo a quello di riferimento una relazione annuale sulle attività di audit interno svolte, proporre entro il 31 Gennaio il nuovo piano annuale di audit, il piano triennale e le relative proposte di variazione e, da ultimo, approvarlo a seguito della validazione del Direttore Generale.

Il Dirigente responsabile I.A. ha, inoltre, la funzione di:

- assistere il Direttore Generale e più ampiamente la Direzione Strategica nel valutare il funzionamento del sistema dei controlli e delle procedure operative;
- assistere i responsabili delle Unità operativa e/o funzioni dell'Azienda nell'identificazione e nella valutazione delle aree maggiormente esposte ai rischi, nonché nella predisposizione di nuovi sistemi gestionali, per ottenere la garanzia che gli stessi siano conformi alle discipline del sistema dei controlli;
- coordinare e supervisionare l'attività della funzione;
- regolare lo svolgimento delle attività programmate all'interno del piano di audit annuale e coordinare le iniziative di follow up;
- approvare i programmi degli interventi e i rapporti di audit;
- attivare le collaborazioni con soggetti esterni all'Azienda, per l'affidamento di incarichi mirati di auditing;
- gestire le risorse umane, strumentali e finanziarie assegnate alla struttura, assicurando un'idonea formazione del personale.

Gli auditors hanno il compito di:

- pianificare ed eseguire gli audit e gli interventi di consulenza programmati;
- raccogliere, ordinare ed archiviare tutta la documentazione e le evidenze necessarie a supportare le conclusioni tratte nel corso degli interventi di audit;
- individuare e proporre azioni migliorative;
- redigere i “Programmi di audit” e i “Rapporti di audit”;
- aggiornare le tavole di follow up al termine di ciascun intervento di audit;
- collaborare alla revisione del Manuale interno;
- partecipare agli specifici percorsi di formazione;
- raccogliere e aggiornare la normativa comunitaria, nazionale e regionale di riferimento;

Al fine di conferire oggettività ai giudizi di valutazione dei sistemi di controllo, gli auditors incaricati devono svolgere le loro funzioni secondo i principi di obiettività e indipendenza.
L’indipendenza degli auditors è assicurata, in primo luogo, dalla collocazione organizzativa della funzione di I.A. in staff alla Direzione Generale e, in secondo luogo, dall’assenza in capo agli auditors ed al Dirigente responsabile I.A. di responsabilità operative nell’ambito dei processi o delle attività esaminate.
In particolare gli auditors incaricati ed il Dirigente responsabile della funzione di Audit non devono aver avuto, almeno nell’anno precedente l’incarico, responsabilità operative nell’ambito dei processi o delle attività oggetto dell’incarico.

1.4.1 Denuncia di danno erariale

Qualora dall'attività di audit emergano fatti che possano dar luogo a responsabilità per danni causati alla finanza pubblica (responsabilità amministrativa) deve essere presentata denuncia alla Procura regionale presso la Sezione giurisdizionale della Corte dei Conti.

La valutazione della sussistenza dell'ipotesi di danno erariale viene condivisa con il Dirigente responsabile I.A., il quale dovrà effettuare una tempestiva segnalazione alla Direzione Generale ai fini delle eventuali comunicazioni alle autorità competenti. 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 Dirigente responsabile I.A. informerà il Direttore Generale e i vertici delle funzioni o Unità operative interessati dell'obbligo di operare affinché il danno sia evitato e, nel caso si verifichi, dell'obbligo di denunciare il fatto alla Procura erariale.

1.4.2 Denuncia penale

Qualora nel corso dell'attività di audit venga acquisita notizia di un reato perseguibile d'ufficio deve esserne fatta denuncia senza ritardo. La valutazione della sussistenza dell'ipotesi di reato viene condivisa con il Dirigente responsabile I.A., il quale dovrà effettuare una tempestiva segnalazione alla Direzione Generale ai fini delle eventuali comunicazioni alle autorità competenti.

La denuncia contiene l'esposizione degli elementi essenziali del fatto e indica il giorno dell'acquisizione della notizia nonché le fonti di prova già note. Contiene, quando è possibile, le generalità, il domicilio e quanto altro valga all'identificazione della persona alla quale il fatto è attribuito, della persona offesa e di coloro che siano in grado di riferire su circostanze rilevanti per la ricostruzione dei fatti.

2 GLI AUDITORS

2.1 Caratteristiche

L'Internal auditor deve possedere caratteristiche personali necessarie per un efficace espletamento degli incarichi d'audit. Deve avere una rapidità di comprensione delle diverse situazioni organizzative dell'Azienda, capacità di analisi e di sintesi, elevato senso dell'etica ed integrità morale, atteggiamento mentale di obiettività, attitudine ai rapporti interpersonali e capacità di comunicazione, conoscenza delle tecniche di "problemsolving" e creatività nella ricerca di soluzioni per i problemi rilevati, determinazione nel conseguimento degli obiettivi.

L'attività di I.A. si sviluppa per progetti d'audit realizzati da specifici team di lavoro costituiti da personale con caratteristiche professionali e di esperienza idonee al conseguimento degli obiettivi dei singoli progetti. Il lavoro di gruppo, salvo eccezioni, costituisce pertanto un presupposto di base per l'espletamento dell'attività di I.A..

2.2 Formazione

Il personale al momento del suo ingresso nella funzione di I.A deve essere adeguatamente formato. L'esigenza formativa si sviluppa lungo due direttrici separate: la formazione professionale di audit e la formazione generale di conoscenza dell'Azienda, con riguardo all'attività, all'organizzazione e alle regole interne.

La formazione professionale di I.A è indirizzata verso i corsi base di audit, nel caso di risorse prive di esperienza professionale, al fine di consentirne il raggiungimento dell'autonomia professionale nel più breve tempo possibile.

Per il personale già in servizio nella funzione di I.A con un determinato livello d'esperienza professionale, la formazione di audit è invece adattata a tale livello, sempre nell'ottica di una continua crescita professionale.

È utile, comunque, affermare che la formazione più efficace rimane sempre quella sul lavoro, per cui parallelamente alla formazione d'aula è sviluppato per ciascuna risorsa un adeguato programma di addestramento sul lavoro.

3 PIANIFICAZIONE DELLE ATTIVITÀ DI AUDIT

3.1 Pianificazione triennale delle attività

La pianificazione delle attività di I.A. avviene su base triennale ed è formalizzata in un Piano triennale di Audit adeguato alle risorse disponibili.

Il Piano triennale di Audit è soggetto all'approvazione da parte della Direzione Generale su proposta del Dirigente responsabile I.A..

Le priorità nell'ambito del piano sono attribuite in funzione del livello di rischio connesso ai diversi oggetti d'audit, per cui la prima fase dell'attività di pianificazione è costituita dalla mappatura dei possibili oggetti d'audit, seguita dalla valutazione dei relativi livelli di rischio.

L'attribuzione delle priorità d'audit ai vari oggetti mappati è connessa ai punteggi complessivi di valutazione dei rischi ad essi assegnati (a conclusione delle attività di "Riskassessment").

Nel Piano triennale di Audit i progetti sono inseriti con riferimento al livello di rischio attribuito agli oggetti di base e partendo, di norma, dai progetti a più alta priorità.

La collocazione temporale dei progetti è, in prima analisi, guidata dalle priorità corrispondenti ai diversi gradi di rischio connessi agli oggetti d'audit, ma può rispondere anche ad aspetti/esigenze diversi, quali ad esempio, l'attuazione di attività non di audit (stages, workshop, attività di sede), la necessità di evitare sovrapposizioni con altri team di auditors, la conciliabilità con le ferie degli auditors, ecc.Il Piano può subire variazioni per effetto dell'inserimento di progetti connessi a richieste d'interventi urgenti da parte della Direzione

Generale (interventi spot) o dell'annullamento/slittamento di audit programmati per motivazioni varie.

Le richieste di interventi d'audit da parte della Direzione Generale, se non considerati in fase di stesura del Piano fanno slittare a cascata, i progetti d'audit a più bassa priorità.

3.2 Piano annuale di Audit

Il Piano triennale di Audit viene attuato attraverso il piano annuale che definisce in dettaglio i programmi e gli obiettivi per l'anno in corso.

Il Piano Annuale di Audit fa riferimento all'anno solare, viene presentato al Direttore Generale entro il 31 gennaio di ogni anno e, una volta approvato da quest'ultimo, diviene operativo.

L'attività prevista nel piano annuale deve:

- essere coerente alle linee guida definite nel Piano triennale di Audit, soprattutto con riferimento alla rilevanza e rischiosità dei processi e alla disponibilità di risorse;
- dare risposte adeguate alle aspettative del Direttore Generale e più ampiamente della Direzione strategica , in termini di mitigazione dei rischi segnalati;
- allocare le risorse sugli interventi aventi la maggiore rilevanza;
- considerare eventuali ulteriori esigenze del Direttore Generale e più ampiamente della Direzione strategica per l'effettuazione di attività particolari (es. progetti speciali);
- verificare le aree non coperte dai precedenti piani.

Nel corso della predisposizione del Piano di Audit il Dirigente responsabile I.A. verifica il personale disponibile e il tempo che deve essere dedicato a ciascun intervento e, tenendo in considerazione le competenze specifiche e l'esperienza maturata dai diversi auditor,

assegna le attività. Per ogni intervento inserito nel Piano di audit devono infatti essere dettagliate almeno le seguenti informazioni:

- titolo;
- soggetti auditati;
- obiettivo;
- auditors incaricati;
- periodo indicativo di svolgimento dell'intervento;
- tipologia dell'intervento (es. assurance / consulenza).

3.3 Attività di riskassessment e valutazione dei rischi e dei controlli

Il rischio è definito come "la possibilità che si verifichi un qualsiasi evento che possa impattare negativamente sugli obiettivi fissati nella programmazione e/o connaturati alle finalità istituzionali".

Ai fini della rilevazione e valutazione dei rischi aziendali si utilizza un questionario di autovalutazione dei principali fattori di rischio, propedeutico all'attività di Internal Audit.

Il questionario di autovalutazione dei rischi può essere distribuito sotto forma di file di Microsoft Word tramite posta elettronica. Nel caso in cui questa forma di distribuzione non risultasse applicabile o opportuna, sarà distribuito in forma cartacea o compilato direttamente dall'auditor per formalizzare le indicazioni acquisite attraverso colloqui e/o interviste effettuate presso le Unità operative e/o funzioni aziendali.

Il questionario deve essere compilato inserendo la valutazione che si ritiene più adatta a rappresentare il rischio potenziale e residuoin considerazione sia della probabilità che l'evento abbia di manifestarsi che dell'entità del danno eventualmente provocato.

A fronte di ogni valutazione attribuita devono essere specificate, a cura del compilatore, le aree di impatto che si ritengono coinvolte in modo da consentire l'associazione dei rischi ai singoli ambiti.

I fattori di rischio che risultino non applicabili alla specifica realtà dell'amministrazione non dovranno essere valutati.

La valutazione dei rischi viene fatta sulla base dei parametri di probabilità e di impatto. La graduazione di questi parametri consente di costruire la griglia, usata per classificare i rischi individuati in ciascun processo e ai quali è stato attribuito un livello di probabilità e uno d'impatto. A fronte dei rischi identificati, sono individuati quei controlli che consentono la loro mitigazione entro livelli accettabili.

La funzione di Internal Audit valuta ciascun controllo in termini di efficacia nel mitigare il rischio e di implementazione del controllo stesso.

La definizione del livello di rischio di un processo è la sintesi della valutazione di tutti i rischi e dei relativi controlli. La valutazione della rischiosità complessiva a livello di processo deve essere condivisa con il responsabile del processo stesso.

Le analisi di rischio vengono aggiornate dagli auditors nel corso degli interventi di audit. I risultati delle analisi consentono, con riferimento agli ambiti di attività aziendale, di identificare i fattori di rischio da monitorare al fine di:

- tutelare gli obiettivi strategici attraverso il presidio delle variabili esogene (fattori di rischio esterni) ed endogene (fattori di rischio interni) che possono comprometterne il raggiungimento;
- supportare i processi decisionali della Direzione strategica e delle Unità operative e/o funzioni aziendali in una logica di riduzione dei fenomeni potenzialmente dannosi che identifichino qualitativamente e quantitativamente opportunità e minacce;

- migliorare l'efficienza e la qualità degli ambiti di attività regionale grazie ad una maggiore sensibilità ai fattori di origine dei rischi;
- migliorare la percezione dell'immagine dell'Azienda da parte degli interlocutori esterni (ad es. cittadini, utenti dei servizi, altre Istituzioni ecc.).

3.3.1 Identificazione dei fattori di rischio

Per una più agevole analisi i fattori di rischio possono essere raggruppati in funzione della loro origine in categorie di rischio omogenee al loro interno, distinguendo tra quelli che nascono all'esterno dell'Azienda (rischi esterni) e quelli connessi alle caratteristiche ed all'articolazione dell'organizzazione stessa (rischi interni).

Si riporta, di seguito un prospetto generale del modello dei rischi:

Rischi interni

- regole e modello organizzativo;
- incidenza fattore umano;
- processi e procedure;

Rischi esterni:

- contesto (politico, economico-finanziario, socio-culturale, tecnologico, legislativo, ambientale, competitività);
- terze parti;
- eventi eccezionali.

Rischi trasversali:

- rischio di reputazione.

Il questionario richiede una valutazione dei fattori di rischio sia a livello potenziale che residuo.

Per rischio potenziale si intende il rischio valutato a prescindere dai sistemi di controllo interno operanti e dagli strumenti di gestione che sono stati istituiti e messi in atto per ridurne la probabilità di accadimento e/o il relativo impatto.

Per rischio residuo si intende viceversa quel rischio che permane anche dopo l'applicazione dei sistemi di controllo. La presenza di tale rischio non è necessariamente un'indicazione di inefficacia dei sistemi di controllo interno, dal momento che non è possibile operare in un'ottica di eliminazione assoluta del rischio in quanto il rischio residuo può rappresentare un aspetto connaturato all'attività istituzionale.

3.3.2 Valutazione dei fattori di rischio

La valutazione deve essere effettuata secondo la scala di valutazione di seguito riportata.

Acronimo	Significato
A	Alto
MA	Medio Alto
M	Medio
MB	Medio Basso
B	Basso

Le valutazioni dovranno essere effettuate tenendo in considerazione la combinazione dei due seguenti fattori:

- Probabilitàdi accadimento: possibilità che un evento si verifichi.

- Impatto: effetto derivante dal verificarsi dell'evento in termini di maggiori spese o altri effetti non previsti a carico del bilancio aziendale (impatti finanziari) o in termini di deviazioni dal corretto procedimento amministrativo (impatto da non conformità senza ricadute finanziarie) o, ancora in termini di difficoltà operative, ritardi e/o anomalie nello svolgimento dell'attività e nell'erogazione dei servizi.

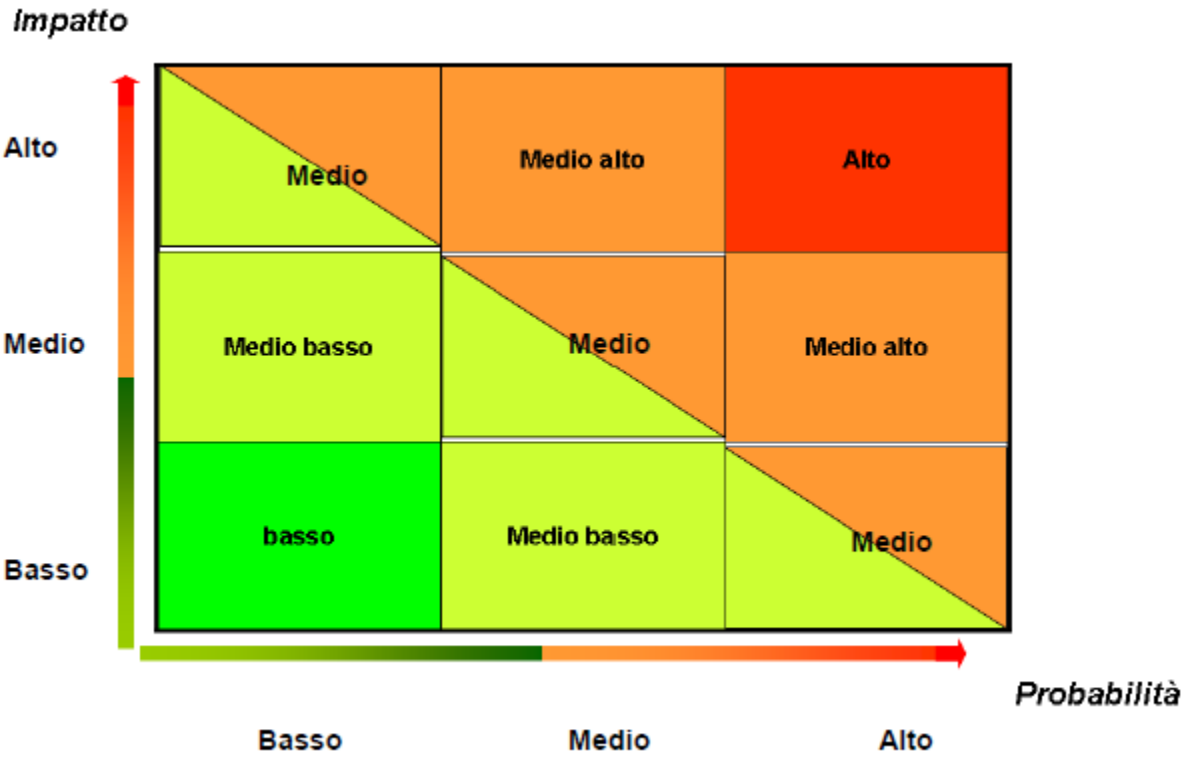
La probabilità può avere i seguenti valori:

ALTO	È presumibile che l'evento si manifesti sistematicamente o ripetutamente nell'arco di un periodo definito (es: anno).
MEDIO	L'evento ha probabilità di manifestarsi nel periodo anche se non con caratteristiche di sistematicità.
BASSO	La probabilità di accadimento dell'evento è da considerarsi remota.

Analogamente anche l'impatto può avere i seguenti valori:

ALTO	Gli effetti derivanti dal verificarsi dell'evento sono altamente negativi.
MEDIO	Gli effetti derivanti dal verificarsi dell'evento hanno un'incidenza media negativa.
BASSO	Gli effetti derivanti dal verificarsi dell'evento hanno una bassa incidenza negativa.

La valutazione complessiva del rischio in termini di probabilità e impatto viene effettuata utilizzando la seguente matrice:



3.3.3 Analisi preliminare dei rischi, risk scoring e definizione delle priorità

L'analisi preliminare dei rischi sarà articolata nelle seguenti fasi:

1) Analisi della documentazione disponibile e ottenimento di informazioni su:

- risultanze delle attività di controllo effettuate negli anni precedenti, ove applicabile;
- eventuali relazioni su altri controlli svolti;
- altro (manuali, procedure ecc.).

2) Elaborazione del modello di misurazione dei rischi.

L'analisi preliminare dei rischi individua i principali fattori di rischio tenendo conto delle caratteristiche delle operazioni.

L'analisi preliminare dei rischi individua i principali fattori di rischio tenendo conto delle caratteristiche delle operazioni.

3) Riunioni per la valutazione dei rischi

Per condividere l'analisi preliminare dei rischi con i responsabili delle Unità operative e/o funzioni aziendali, potranno essere organizzate delle riunioni per la valutazione dei rischi (riskassessment) per raccogliere la valutazione dei responsabili relativamente ai rischi delle operazioni).

L'attività di valutazione dei rischi è articolata nelle seguenti fasi:

- Individuazione dei componenti del focus group;
- Somministrazione di questionari di autovalutazione;
- Discussione per l'identificazione e la misurazione dei rischi potenziali e residui.

Sulla base della valutazione dei rischi si procede al riskscoringper ordinare le Unità operative e/o funzioni aziendali a seconda dell'intensità dei rischi individuati.

I risultati del riskscoringconsentiranno alla funzione di I.A. di ordinare le Unità operative e/o funzioni aziendali da auditare per intensità di rischio e individuare le priorità secondo le quali procedere all'effettuazione dei controlli sulle stesse.

4 L'INTERVENTO DI AUDIT

4.1 Assegnazione dell'incarico

Il Dirigente responsabile dell'I.A. individua gli auditors incaricati di svolgere l'attività di controllo e provvede alla supervisione della stessa.

4.2 Preparazione, comunicazione avvio audit e richiesta di documentazione

In tale fase la funzione di I.A. provvede all'individuazione delle informazioni utili ai fini del controllo mediante la raccolta e l'esame di tutta la documentazione ritenuta rilevante ai fini della comprensione del funzionamento del sistema di controllo interno dell'Unità operativa e/o funzione dell'Azienda sottoposta ad audit.

In seguito, a firma del Dirigente responsabile I.A., viene trasmessa, con un anticipo non superiore ai dieci giorni lavorativi rispetto alla data dell'audit in loco, la comunicazione al responsabile dell'Unità operativa e/o funzione interessato dell'avvio dell'Audit con indicazione della data e luogo dell'incontro e degli aspetti da esaminare. Alla comunicazione può essere allegata una lista indicativa della documentazione da rendere disponibile nel corso dell'incontro.

4.3 Analisi preliminare del soggetto sottoposto a verifica

In tale fase funzione di I.A. provvede allo svolgimento, presso l'Unità operativa e/o funzione dell'Azienda sottoposta a controllo, di appositi incontri al fine di raccogliere elementi probatori sul funzionamento del sistema di controllo adottato, secondo le seguenti procedure di verifica:

• acquisizione ed esame della documentazione ritenuta rilevante ai fini della comprensione del funzionamento del sistema di controllo;

• acquisizione di informazioni in merito a specifici aspetti o situazioni attraverso l'organizzazione di appositi incontri e attraverso l'ottenimento di risposte, anche in forma scritta, a specifici quesiti.

La documentazione raccolta nel corso dell'incontro e integrata da eventuali ed ulteriori informazioni viene esaminata e opportunamente archiviata dalla funzione di I.A..

Si procede dunque attraverso l'analisi di tutta la documentazione alla valutazione del livello di rischio (o grado di funzionamento del sistema) con l'eventuale impiego di una check-list.

Relativamente a ciascun punto di controllo della check-list si associa un valore qualitativo del tipo:

Funziona bene, **sono necessari solo miglioramenti marginali**. Non ci sono punti deboli ovvero sono state trovate solo criticità marginali. Queste criticità non hanno alcun impatto significativo sul funzionamento dell'Unità operativa e/o funzione dell'Azienda.

Funziona, ma sono necessari dei miglioramenti. Sono stati riscontrati dei punti deboli. Queste debolezze hanno un moderato impatto sul funzionamento dell'Unità operativa e/o funzione dell'Azienda. Sono state fatte delle raccomandazioni che devono essere implementate da parte del soggetto verificato.

Funziona parzialmente, sono necessari miglioramenti sostanziali. Sono state riscontrate delle criticità che hanno portato o potrebbero portare ad irregolarità. L'impatto sull'efficace funzionamento dell'Unità operativa e/o funzione dell'Azienda è significativo. Sono state fatte raccomandazioni e/o piani di azioni.

Fondamentalmente non funziona. Sono state trovate numerose criticità che hanno portato o potrebbero portare ad irregolarità. L'impatto sull'efficace funzionamento dell'Unità operativa

e/o funzione dell'Azienda è significativo, funzionano male o non funzionano affatto. Le criticità sono sistemiche ed estese. In tal caso si valuterà l'opportunità di intraprendere un piano di azione formale per la risoluzione della problematica.

In relazione ai risultati ottenuti per ciascun punto di controllo viene individuato il livello di affidabilità complessiva del sistema di controllo interno.

Tale valutazione è da utilizzare nell'ambito dell'estrazione campionaria in base alle indicazioni contenute nella seguente tabella:

Livelli di attendibilità derivante dall'analisi preliminare del sistema di controllo per ciascun punto di controllo	**Criterio quantitativo di affidabilità complessiva**	**Livello di affidabilità del sistema di controllo**
Funzionamento buono, sono necessari solo dei miglioramenti di modesta entità (punteggio 4)	Media dei punteggi pari a 4	Alto
Funzionamento corretto, ma sono necessari dei miglioramenti (punteggio 3)	Media dei punteggi compresi tra 2.51 e 4	Medio Alto
Funzionamento parziale, sono necessari dei miglioramenti sostanziali (punteggio 2)	Media dei punteggi compresi tra 1 e 1.25	Medio Basso
Mancato funzionamento generale (punteggio 1)	Media dei punteggi pari a 1	Basso

4.4 Programma operativo e campionamento

A seguito dell'analisi del sistema dei controlli interni nel suo complesso, la funzione di I.A. elabora un programma operativo di audit, composto dalla sezione relativa al campionamento da utilizzare e da una check list di dettaglio dei controlli da svolgere.

Per gli audit delle operazioni la funzione di I.A. deve dotarsi di una metodologia di campionamento. La metodologia campionaria si basa sull'utilizzo, ove applicabile, del campionamento statistico casuale o sulla base della valutazione professionale dell'auditor.

4.5 Gestione del contraddittorio ed emissione del rapporto finale di controllo

La funzione di I.A. registra gli esiti del controllo e nel caso non emergano criticità emette il rapporto finale di controllo.

Nel caso emergano criticità dall'esame della check list, l'Unità operativa e/o funzione dell'Azienda auditata dovrà fornire utili integrazioni e informazioni orientativamente entro 30 giorni lavorativi. A seguito dell'esame delle informazioni ricevute dal soggetto sottoposto ad audit la funzione di I.A. registra gli esiti del controllo ed emette il rapporto finale di controllo.

Il rapporto finale di controllo è trasmesso al soggetto auditato.

Nel caso in cui il rapporto finale preveda delle ipotesi di miglioramento il soggetto auditato dovrà procedere, orientativamente entro il termine di sessanta giorni lavorativi, alla correzione delle eventuali osservazioni rilevate.

4.6 Follow up e misure correttive

Il follow up è l'intervento per la verifica dell'effettiva implementazione dei piani di azione concordati con i responsabili delle Unità operative e/o funzioni aziendali, a fronte delle osservazioni rilevate nel corso dell'intervento di audit.

Una volta completato l'intervento, ciascun auditor raccoglie le osservazioni e il piano di azione riportato nel rapporto di audit e implementa la "tavola di follow up".

La "tavola di follow up", gestita su formato elettronico, è mantenuta e archiviata dalla funzione I.A. ed utilizzata nella pianificazione degli interventi di follow up.

L'intervento di follow up può avere modalità differenti a seconda della complessità dei piani di azione concordati.

Qualora le raccomandazioni da implementare siano di bassa rilevanza e/o riguardino problematiche che possono essere sanate in tempi brevi e con facilità per il responsabile del processo di audit (es. irregolarità documentali, errori materiali, ecc.) la verifica del recepimento delle raccomandazioni può avvenire tramite l'analisi delle evidenze trasmesse all' I.A.

Nel caso in cui i piani di azione proposti siano complessi, la verifica del loro accoglimento si effettua con interventi di follow up che prevedono una nuova visita presso il responsabile dell'Unità operative e/o funzione aziendale e l'analisi delle evidenze raccolte.

In quest'ultimo caso, al termine dell'intervento di follow up, viene redatto un apposito documento che riporta la descrizione di quanto verificato.

Successivamente alla verifica del recepimento dei piani di azione, l'auditor aggiorna la tavola di follow up. In particolare, si possono verificare le seguenti situazioni:

- il piano di azione è stato implementato correttamente. In tal caso l'auditor indica la data di completamento, se disponibile, e le valutazioni conclusive;
- il piano di azione è stato parzialmente eseguito e necessita di un tempo supplementare o di una revisione dell'originario piano di azione. In tal caso l'auditor aggiorna la tavola di follow up specificando le attività che devono essere ancora

implementate o che necessitano di una modifica. Inoltre indica la nuova data prevista di completamento;

- il piano di azione non è stato implementato. Si possono presentare diversi casi:
  - il piano di azione non risulta applicabile (ad esempio in seguito ad un cambiamento della legislazione di riferimento) e necessita di una modifica. In questo caso, una volta concordate le attività fra il responsabile del processo e la funzione di I.A., occorre rivedere il piano e aggiornare la tavola;
  - i responsabili preposti all'implementazione risultano inadempienti. Occorre rilevare nella tavola che il piano risulta ancora aperto, indicare una nuova data di scadenza e informare il Dirigente responsabile I.A.

5 LA VERIFICA DELLA STRATEGIA DI AUDIT

5.1 La relazione annuale

Al termine di ogni annualità il Dirigente responsabile della funzione di I.A. redige un rapporto sull'attività svolta, destinato al Direttore Generale. Questa rendicontazione a consuntivo è tra l'altro propedeutica alla definizione del Piano di audit dell'annualità successiva.

Il Rapporto annuale viene presentato dal Dirigente responsabile I.A. al Direttore Generale entro il 28 febbraio di ogni anno e fa riferimento all'anno solare.

Il rapporto presenta i risultati dell'attività, articolandoli come segue:

- copertura del piano di audit, cioè quanto effettivamente svolto nel corso del periodo, in comparazione con quanto era stato previsto; vengono giustificate tutte le variazioni rispetto alla programmazione iniziale e definiti i tempi e le modalità di effettuazione degli interventi non svolti nell'anno;
- sintesi delle principali osservazioni, rilevate nel corso degli interventi effettuati, accompagnate da una valutazione e pesatura;

- sintesi dell'attività di follow up, inerente al grado di implementazione dei piani di azione concordati nel corso dei periodi precedenti e oggetto di specifiche verifiche nel corso dell'annualità appena conclusa;
- valutazione sintetica del sistema di gestione e controllo dell'Azienda, sulla base dei test condotti direttamente e delle risultanze dei controlli che gli uffici interni hanno effettuato;
- sintesi delle altre attività extra Piano, cioè quelle di eventuali audit / interventi consulenziali non programmati; vengono inoltre riassunte le attività non di controllo svolte, quali progetti speciali a supporto della Direzione, ecc.;
- analisi e valutazione dell'attività di audit, che consiste in una disamina dell'operato, delle prestazioni e delle eventuali difficoltà emerse, delle possibilità di intervento per incrementare qualità ed efficacia dell'azione di audit, sia a livello di organizzazione interna dell'ufficio che di sviluppo delle professionalità e delle competenze degli auditors.

5.2 Procedura di adeguamento della strategia e dei piani di Audit

Ogni revisione e/o cambiamento della strategia di audit che comporti un cambiamento o una modifica dei suoi contenuti nonché del Piano annuale di Audit sarà:

- sottoposta all'approvazione del Dirigente responsabile I.A.;
- approvata dal Direttore Generale.

5.3 Il sistema di monitoraggio dei controlli

Le attività di controllo pianificate sono inserite all'interno del sistema di monitoraggio dei controlli ai fini del monitoraggio delle stesse. La registrazione degli esiti di ogni audit permette

l'elaborazione periodica e la verifica della presenza di eventuali anomalie riscontrate nel corso dello svolgimento delle attività di controllo. L'analisi di dette informazioni, nell'ambito dell'attività di pianificazione e controllo, consente di formulare adeguati interventi correttivi e migliorativi alla strategia di audit.

6 ARCHIVIAZIONE DELLA DOCUMENTAZIONE DI AUDIT

6.1. Archivio degli interventi di audit

Per ciascun intervento di audit viene creato un fascicolo allo scopo di raccogliere e ordinare le evidenze che documentano le attività di pianificazione e di controllo, le informazioni raccolte e le conclusioni cui si è pervenuti.

L'archiviazione cartacea della documentazione può seguire le seguenti specifiche:

A - Normativa

B - Documentazione specifica

B 1 - Comunicazione avvio audit

B 2 - Corrispondenza

B 3 - Foglio presenze

B 4 - Check list

B 5 - Rapporto finale di audit

B 6- Rapporto follow-up

C – Documentazione sul campionamento

6.1.1 Archivio cartaceo

Il Dirigente responsabile dell'I.A. raccoglie e conserva le comunicazioni e la documentazione da e verso l'esterno e la documentazione ad uso interno (Mandato di Audit Interno, Manuale di Audit Interno, Piano triennale di audit, fascicoli degli audit, ecc.). Il materiale viene fascicolato e custodito all'interno di appositi armadi.

La documentazione è custodita per i 5 anni successivi all'anno di riferimento.

6.2 L'archivio informatico e il Sistema Informativo di Audit

L'archivio informatico è organizzato in sezioni o cartelle, indicativamente secondo la seguente architettura:

• **Mandato di Audit Interno;**

• **Manuale di Audit Interno;**

• **Modulistica** contenente i modelli della documentazione operativa necessaria a supportare lo svolgimento dell'attività di audit;

• **Normativa** contenente un archivio delle principali normative di riferimento;

• **Piano Triennale di Audit Interno**;

• **Interventi** (per anno di attività), contenente tutta la documentazione prodotta nel corso degli audit effettuati;

• **Follow-up** (per anno di attività), con le osservazioni effettuate.

APPENDICE 1

Definizione 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.

Codice Etico

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 auditors sono tenuti ad osservare. Queste regole sono un aiuto per orientare l'applicazione pratica dei Principi e intendono fornire agli internal auditors 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 "AdministrativeDirectives" 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.

Standard Internazionali

Standard di Connotazione

1000 – Finalità, poteri e responsabilità

Le finalità, i poteri e le responsabilità dell'attività di internal audit devono essere formalmente definiti in un Mandato di internal audit, coerente con la Definizione di Internal Auditing, il Codice Etico e gli Standard. Il responsabile internal auditing deve verificare periodicamente il Mandato e sottoporlo all'approvazione del senior management e del board.

Interpretazione:

Il Mandato dell'internal audit è un documento formale che definisce finalità, poteri e responsabilità dell'attività di internal audit. Il Mandato stabilisce la posizione dell'attività di internal audit nell'organizzazione, precisando la natura del riporto funzionale del responsabile internal auditing al board; autorizza l'accesso ai dati, alle persone e ai beni aziendali che sono necessari per lo svolgimento degli incarichi di audit e definisce l'ambito di copertura delle attività di internal audit. L'approvazione finale del Mandato di internal audit è una responsabilità del board.

1000.A1 – La natura dei servizi di assurance forniti all'organizzazione deve essere definita nel Mandato di internal audit. Anche nel caso in cui i servizi di assurance sono forniti a soggetti esterni all'organizzazione, la natura di tali servizi deve essere dichiarata nel Mandato di internal audit.

1000.C1 – La natura dei servizi di consulenza deve essere definita nel Mandato di internal audit.

1010 – Riconoscimento della Definizione di Internal Auditing, del Codice Etico e degli Standard nel Mandato di internal audit

Il carattere vincolante della Definizione di Internal Auditing, del Codice Etico e degli Standard deve essere rispecchiato nel Mandato di internal audit. Il responsabile internal auditing dovrebbe discutere la Definizione di Internal Auditing, il Codice Etico e gli Standard con il senior management e il board.

1100 – Indipendenza e obiettività

L'attività di internal audit deve essere indipendente e gli internal auditors devono essere obiettivi nell'esecuzione del loro lavoro.

Interpretazione:

Indipendenza è la libertà da condizionamenti che minaccino la capacità dell'attività di internal audit di adempiere senza pregiudizio alle proprie responsabilità. Per raggiungere il livello di indipendenza necessario per esercitare in modo efficace le responsabilità dell'attività di internal audit, il responsabile internal auditing ha diretto e libero accesso al senior management e al board. Ciò può essere conseguito tramite un duplice riporto organizzativo. Casi di limitazione all'indipendenza devono essere gestiti a livello di singolo auditor, di incarico, funzionale e organizzativo.

Obiettività è l'attitudine mentale di imparzialità che consente agli internal auditors di svolgere i propri incarichi in un modo che consenta loro di credere nella validità del lavoro svolto e nell'assenza di compromessi sulla qualità. In materia di audit, l'obiettività richiede che gli internal auditors non subordinino il proprio giudizio professionale a quello di altri. Eventuali ostacoli all'obiettività devono essere gestiti a livello di singolo auditor, di incarico, funzionale e organizzativo.

1110 – Indipendenza organizzativa

Il responsabile internal auditing deve riportare ad un livello dell'organizzazione che consenta all'attività di internal audit il pieno adempimento delle proprie responsabilità. Il responsabile internal auditing deve confermare al board, almeno una volta l'anno, lo stato di indipendenza organizzativa dell'attività di internal audit.

Interpretazione:

Si realizza un'indipendenza organizzativa efficace quando il responsabile internal auditing riferisce funzionalmente al board. Esempi di riporto funzionale al board comportano che il board:

• approvi il Mandato di internal audit;

• approvi il piano di attività basato sulla valutazione dei rischi;

• approvi il budget e il piano delle risorse dell'attività di internal audit;

• riceva comunicazioni dal responsabile internal auditing in merito ai risultati dell'attività di internal audit rispetto al piano e ad altre questioni;

• approvi le decisioni relative alla nomina e all'esonero del responsabile internal auditing;

• approvi il compenso spettante al responsabile internal auditing;

• effettui opportune verifiche con il management e il responsabile internal auditing per stabilire se sono presenti limitazioni non appropriate dell'ambito di copertura e delle risorse.

1110.A1 – L'attività di internal audit deve essere libera da interferenze nella definizione dell'ambito di copertura, nell'esecuzione del lavoro e nella comunicazione dei risultati.

1111 – Comunicazione con il board

Il responsabile internal auditing deve poter comunicare e interagire direttamente con il board.

1120 – Obiettività individuale

Gli internal auditors devono avere un atteggiamento imparziale e senza pregiudizi; devono inoltre evitare qualsiasi conflitto di interesse.

Interpretazione:

Conflitto di interessi è una situazione nella quale gli internal auditors, che godono di una posizione di fiducia, si trovano ad avere un interesse personale o professionale contrario agli interessi dell'organizzazione. Un simile contrasto con l'organizzazione rende difficile l'adempimento dei compiti dell'internal auditor con imparzialità. Un conflitto di interessi può sussistere anche quando non dà luogo a comportamenti non etici o comunque impropri. L'esistenza di un conflitto di interessi può dare l'impressione che vi siano comportamenti scorretti, con il risultato di compromettere la fiducia verso gli internal auditors, l'attività di internal audit e la professione. Il conflitto di interessi può pregiudicare la capacità individuale di svolgere con obiettività i propri compiti e responsabilità.

1130 – Condizionamenti dell'indipendenza o dell'obiettività

Se indipendenza od obiettività sono compromesse o appaiono tali, le circostanze dei condizionamenti devono essere riferite a un livello appropriato. La natura dell'informativa dipende dal tipo di condizionamento.

Interpretazione:

Tra i fattori che possono condizionare l'indipendenza organizzativa e l'obiettività individuale si possono annoverare conflitti di interesse individuali, limitazioni del campo di azione, restrizioni dell'accesso a dati, persone e beni aziendali e vincoli di risorse, tra cui quelle finanziarie.

La determinazione del livello più appropriato al quale dovrebbero essere riferite le circostanze di pregiudizio all'indipendenza o all'obiettività dipende dalle aspettative dell'attività di internal audit, dai doveri del responsabile internal auditing verso il senior management e il board, definiti nel Mandato di internal audit, e dalla natura dei condizionamenti stessi.

1130.A1 – Gli internal auditors devono evitare di effettuare attività di audit in ambiti in cui ricoprivano una precedente responsabilità. Si presume che l'obiettività sia condizionata se un internal auditor effettua un servizio di assurance sulle attività di cui è stato responsabile nell'anno precedente.

1130.A2 – Gli incarichi di assurance per attività che rientrano nella gestione del responsabile internal auditing devono essere supervisionati da soggetti esterni alla Struttura di internal audit.

1130.C1 – Gli internal auditors possono fornire servizi di consulenza anche per quelle attività operative delle quali siano stati precedentemente responsabili.

1130.C2 – Se gli internal auditors, a fronte di prospettati servizi di consulenza, si trovano in una situazione di potenziale condizionamento della propria indipendenza od obiettività, devono segnalarlo al cliente prima di accettare l'incarico.

1200 – Competenza e diligenza professionale

Gli incarichi devono essere effettuati con la dovuta competenza e diligenza professionale.

1210 – Competenza

Gli internal auditors devono possedere le conoscenze, capacità e altre competenze necessarie all'adempimento delle loro responsabilità individuali. L'attività di internal audit nel suo insieme deve possedere o dotarsi delle conoscenze, capacità e altre competenze necessarie all'esercizio delle proprie responsabilità.

Interpretazione:

I termini conoscenze, capacità e altre competenze si riferiscono nel loro complesso alla competenza professionale richiesta agli internal auditors per adempiere efficacemente alle proprie responsabilità professionali. Gli internal auditors sono incoraggiati a dimostrare la propria competenza conseguendo le opportune certificazioni e qualifiche professionali, come quella di "CertifiedInternal Auditor" e altre certificazioni rilasciate dal "The Institute of Internal Auditors" e da altri organismi professionali riconosciuti.

1210.A1 – Il responsabile internal auditing deve dotarsi di opportuna assistenza e consulenza se gli internal auditors non possiedono le conoscenze, le capacità o altre competenze necessarie per lo svolgimento di tutto o di parte dell'incarico.

1210.A2 – Gli internal auditors devono possedere conoscenze sufficienti per valutare i rischi di frode e il modo in cui l'organizzazione li gestisce, senza aspettarsi che essi abbiano le competenze proprie di chi ha come responsabilità primaria quella di individuare e investigare frodi.

1210.A3 – Gli internal auditors devono possedere una sufficiente conoscenza dei rischi e dei controlli chiave dell'Information Technology, nonché degli strumenti informatici di supporto all'attività di audit per svolgere gli incarichi assegnati. Tuttavia, non è richiesto che tutti gli internal auditors posseggano le competenze di chi ha come responsabilità primaria quella dell'Information Technology auditing.

1210.C1 – Il responsabile internal auditing deve rifiutare l'incarico di consulenza, oppure dotarsi di valido supporto e assistenza nel caso in cui gli internal auditors non posseggano le conoscenze, le capacità o le altre competenze necessarie per lo svolgimento di tutto o di parte dell'incarico.

1220 – Diligenza professionale

Gli internal auditors devono applicare la diligenza e le capacità che ci si attende da un internal auditor ragionevolmente prudente e competente. Diligenza professionale non implica infallibilità.

1220.A1 – L'internal auditor deve esercitare la diligenza professionale tenendo in considerazione:

• l'ampiezza del lavoro necessario per raggiungere gli obiettivi dell'incarico;

• la complessità, importanza o la significatività delle attività oggetto di assurance;

• l'adeguatezza e l'efficacia dei processi di governance, di gestione del rischio e di controllo;

• la probabilità della presenza di errori, frodi o non conformità significativi;

• il costo dell'assurance in relazione ai suoi potenziali benefici.

1220.A2 – Per svolgere l'attività di audit con diligenza professionale, gli internal auditors devono considerare l'utilizzo di strumenti informatici di supporto e di altre tecniche di analisi dei dati**.**

1220.A3 – Gli internal auditors devono prestare attenzione ai rischi significativi che possono incidere su obiettivi, attività o risorse. Comunque, le sole procedure di assurance, anche quando effettuate con la dovuta diligenza professionale, non garantiscono che tutti i rischi significativi vengano individuati.

1220.C1 – Nel corso di un incarico di consulenza, gli internal auditors devono esercitare la dovuta diligenza professionale, tenendo in considerazione:

• le esigenze e le aspettative dei clienti, inclusa la natura, i tempi e le forme di comunicazione dei risultati dell'incarico;

• la complessità e l'ampiezza del lavoro necessario per raggiungere gli obiettivi dell'incarico;

• il costo dell'incarico di consulenza in relazione ai suoi potenziali benefici.

1230 – Aggiornamento professionale continuo

Gli internal auditors devono migliorare le proprie conoscenze, capacità e altre competenze attraverso un aggiornamento professionale continuo.

1300 – Programma di assurance e miglioramento della qualità

Il responsabile internal auditing deve sviluppare e sostenere un programma di assurance e miglioramento della qualità che copra tutti gli aspetti dell'attività di internal audit.

Interpretazione:

L'elaborazione di un programma di assurance e miglioramento della qualità permette una valutazione di conformità dell'attività di internal audit alla Definizione di Internal Auditing e agli Standard e consente di verificare se gli internal auditors rispettano il Codice Etico. Il programma valuta inoltre l'efficienza e l'efficacia dell'attività di internal audit e identifica opportunità per il suo miglioramento.

1310 – Requisiti del programma di assurance e miglioramento della qualità

Il programma di assurance e miglioramento della qualità deve includere valutazioni sia interne che esterne.

1311 – Valutazioni interne

Le valutazioni interne devono includere:

• il monitoraggio continuo della prestazione dell'attività di internal auditing;

• periodiche auto-valutazioni o valutazioni condotte da altre persone interne all'organizzazione che abbiano conoscenze adeguate delle metodologie di internal audit.

Interpretazione: Il monitoraggio continuo costituisce parte integrante dell'attività quotidiana di supervisione, verifica e misurazione dell'attività di internal audit. Il monitoraggio continuo è incorporato nelle procedure utilizzate di norma per gestire l'attività di internal audit e viene svolto utilizzando processi, strumenti e informazioni necessari per valutare la conformità alla Definizione di Internal Auditing, al Codice Etico e agli Standard.

Le valutazioni periodiche sono effettuate con l'obiettivo specifico di valutare la conformità alla Definizione di Internal Auditing, al Codice Etico e agli Standard.

La comprensione di tutti gli elementi dell'International Professional Practices Framework è necessaria per una adeguata conoscenza della metodologia di internal audit.

1312 – Valutazioni esterne

Le valutazioni esterne devono essere effettuate almeno una volta ogni cinque anni da parte di un valutatore, o di un team di valutatori, qualificato e indipendente, esterno all'organizzazione. Il responsabile internal auditing deve discutere con il board:

• la modalità e la frequenza della valutazione esterna;

• le qualifiche e l'indipendenza del valutatore o del team di valutatori esterni, inclusa l'esistenza di qualsiasi possibile situazione di conflitto di interessi.

Interpretazione:

Le valutazioni esterne possono essere costituite da valutazioni esterne complete oppure essere condotte sotto forma di autovalutazione con convalida esterna indipendente.

Un valutatore o un team di valutatori qualificati devono dimostrare di essere competenti in due ambiti: la pratica professionale dell'internal auditing e il processo di valutazione esterna. La competenza può essere dimostrata attraverso una combinazione di esperienza e conoscenze teoriche. L'esperienza acquisita presso organizzazioni analoghe per dimensioni, complessità, settore o comparto e specializzazione tecnica è più significativa di un'esperienza meno specifica. Nei team di valutatori, non è necessario che tutti i componenti del team posseggano tutte le competenze, in quanto è il team nel suo insieme a risultare idoneo. Nel determinare

se un valutatore o un team di valutatori dimostrino competenza sufficiente per essere ritenuti idonei, il responsabile internal auditing applica un giudizio professionale.

Il valutatore o il team di valutatori sono indipendenti quando non hanno alcun reale o apparente conflitto di interessi e non fanno parte né sono sotto il controllo dell'organizzazione alla quale appartiene l'attività di internal audit oggetto di valutazione esterna.

1320 – Comunicazione del programma di assurance e miglioramento della qualità

Il responsabile internal auditing deve comunicare i risultati del programma di assurance e miglioramento della qualità al senior management e al board.

Interpretazione:

La forma, il contenuto e la periodicità della comunicazione dei risultati del programma di assurance e miglioramento della qualità vanno concordati con il senior management e il board, considerando le responsabilità dell'attività di internal audit e del responsabile internal auditing definite nel Mandato. Per dimostrare la conformità alla Definizione di Internal Auditing, al Codice Etico e agli Standard, i risultati delle valutazioni periodiche esterne e interne vanno comunicati al termine del processo di valutazione, mentre i risultati del monitoraggio continuo vanno comunicati almeno una volta l'anno. I risultati devono includere la valutazione del valutatore o del team di valutatori sul livello di conformità**.**

1321 – Uso della dizione "Conforme agli Standard Internazionali per la Pratica Professionale dell'Attività di Internal Auditing"

Il responsabile internal auditing può dichiarare che l'attività di internal audit è conforme agli Standard Internazionali per la Pratica Professionale dell'Attività di Internal Auditing solo se le risultanze del programma di assurance e miglioramento della qualità avvalorano tale affermazione.

Interpretazione: L'attività di internal audit risulta conforme agli Standard quando raggiunge i risultati descritti nella Definizione di Internal Auditing, nel Codice Etico e negli Standard. I risultati del programma di assurance e miglioramento della qualità comprendono i risultati delle valutazioni interne ed esterne. Tutte le attività di internal audit devono essere oggetto di valutazioni interne, mentre le attività di internal audit che operano da almeno cinque anni devono essere oggetto anche di valutazioni esterne.

1322 – Comunicazione di non conformità

In presenza di non conformità alla Definizione di Internal Auditing, al Codice Etico o agli Standard che influiscano in modo significativo sull'ambito complessivo di copertura o sull'operatività dell'attività di internal

audit, il responsabile internal auditing deve comunicare le non conformità e il relativo impatto al senior management e al board.

Standard di Prestazione

2000 – Gestione dell'attività di internal audit

Il responsabile internal auditing deve gestire in modo efficace l'attività al fine di assicurare che essa apporti valore aggiunto all'organizzazione.

Interpretazione:

L'attività di internal audit è gestita efficacemente quando:

• i risultati del lavoro dell'attività di internal audit permettono di raggiungere le finalità e le responsabilità indicate nel Mandato di internal audit;

• l'attività di internal audit è conforme alla Definizione di Internal Auditing e agli Standard;

• coloro che svolgono l'attività di internal audit dimostrano di operare in conformità al Codice Etico e agli Standard.

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

2010 – Piano delle attività di internal audit

Il responsabile internal auditing deve predisporre un piano delle attività, basato sulla valutazione dei rischi, al fine di determinarne le priorità in linea con gli obiettivi dell'organizzazione.

Interpretazione:

Il responsabile internal auditing deve predisporre un piano, basato sulla valutazione dei rischi, tenendo conto dei processi aziendali di gestione del rischio e dei limiti di accettabilità dello stesso stabiliti dal management per le diverse attività o parti dell'organizzazione. Se non esiste un modello di riferimento, il responsabile internal auditing esprimerà un proprio giudizio sui rischi, sulla base delle indicazioni fornite dal senior management e dal board. Il responsabile internal auditing deve rivedere e adeguare opportunamente il piano, in risposta ai cambiamenti intervenuti a livello di attività, rischi, operatività, programmi, sistemi e controllo dell'organizzazione.

2010.A1 – Il piano delle attività di internal audit deve basarsi su una documentata valutazione del rischio, effettuata almeno una volta l'anno. Le indicazioni del senior management e del board devono essere tenute in debita considerazione nella formulazione del piano.

2010.A2 – Il responsabile internal auditing deve individuare e considerare le aspettative del senior management, del board e degli altri stakeholder verso i giudizi dell'internal audit e le altre conclusioni.

2010.C1 – Il responsabile internal auditing deve decidere se accettare un incarico di consulenza, sulla base delle possibilità di miglioramento della gestione dei rischi, delle possibilità di aggiungere valore e di migliorare l'operatività dell'organizzazione. Gli incarichi accettati devono essere inclusi nel piano di audit.

2020 – Comunicazione e approvazione del piano

Il responsabile internal auditing deve sottoporre il piano delle attività di internal audit e delle risorse necessarie, incluse eventuali variazioni significative intervenute, al senior management e al board per il relativo esame e approvazione. Il responsabile internal auditing deve, inoltre, segnalare l'impatto di un'eventuale carenza di risorse.

2030 – Gestione delle risorse

Il responsabile internal auditing deve assicurare che le risorse disponibili siano adeguate, sufficienti ed efficacemente impiegate per l'esecuzione del piano approvato.

Interpretazione:

Il termine "adeguate" è riferito all'insieme di conoscenze, capacità e altre competenze necessarie per dare esecuzione al piano. Il termine "sufficienti" è riferito alla quantità di risorse necessarie per portare a termine il piano. Le risorse sono efficacemente impiegate quando vengono utilizzate in modo da ottimizzare il raggiungimento del piano approvato.

2040 – Direttive e procedure

Il responsabile internal auditing deve definire direttive e procedure per lo svolgimento dell'attività.

Interpretazione:

La forma e il contenuto di direttive e procedure dipende dalla Struttura e dalle dimensioni dell'attività di internal audit, nonché dalla complessità dei suoi compiti.

2050 – Coordinamento delle attività

Il responsabile internal auditing dovrebbe condividere le informazioni e coordinare le diverse attività con i diversi prestatori, esterni e interni, di servizi di assurance e consulenza, al fine di assicurare un'adeguata copertura e di minimizzare le possibili duplicazioni.

2060 – Informazione periodica al senior management e al board

Il responsabile internal auditing deve informare periodicamente il senior management e il board in merito a finalità, poteri e responsabilità dell'attività di internal audit, nonché comunicare lo stato di avanzamento del

piano. Tale comunicazione deve comprendere inoltre i rischi significativi, inclusi quelli di frode, i problemi di controllo, i problemi di governance e ogni altra informazione necessaria o richiesta dal senior management e dal board.

Interpretazione:

Frequenza e contenuto dell'attività di comunicazione sono definiti di concerto con il senior management e il board e variano a seconda della rilevanza delle informazioni che devono essere comunicate e dell'urgenza dei relativi provvedimenti che competono al senior management e al board.

2070 – Prestatore esterno di servizi e responsabilità organizzativa sull'internal auditing

Quando l'attività di internal audit è affidata a un prestatore esterno di servizi, quest'ultimo deve fare in modo che l'organizzazione sia consapevole di avere la responsabilità di mantenere un'attività di internal audit efficace.

Interpretazione

Questa responsabilità si dimostra attraverso il programma di assurance e miglioramento della qualità, che valuta la conformità alla Definizione di Internal Auditing, al Codice Etico e agli Standard.

2100 – Natura dell'attività

L'attività di internal audit deve valutare e contribuire al miglioramento dei processi di governance, gestione del rischio e di controllo, tramite un approccio professionale e sistematico.

2110 – Governance

L'attività di internal audit deve valutare e fornire appropriati suggerimenti volti a migliorare il processo di governance nel raggiungimento dei seguenti obiettivi:

• favorire lo sviluppo di appropriati valori e principi etici nell'organizzazione;

• garantire l'efficace gestione dell'organizzazione e l'accountability;

• comunicare informazioni su rischi e controllo alle relative funzioni dell'organizzazione;

• coordinare le attività e il processo di scambio di informazioni tra il board, i revisori esterni, gli internal auditors e il management.

2110.A1 – L'attività di internal audit deve valutare l'architettura, l'attuazione e l'efficacia degli obiettivi, dei programmi e delle attività dell'organizzazione in materia di etica.

2110.A2 – L'attività di internal audit deve valutare se il processo di governance dei sistemi informativi aziendali aiuta le strategie e gli obiettivi dell'organizzazione stessa.

2120 – Gestione del rischio

L'attività di internal audit deve valutare l'efficacia e contribuire al miglioramento dei processi di gestione del rischio. **Interpretazione:** Determinare se i processi di gestione del rischio siano efficaci è un giudizio che l'internal auditor esprime in base alla propria valutazione dei seguenti aspetti:

• che gli obiettivi aziendali supportino e siano coerenti con la "mission" aziendale;

• che i rischi significativi siano identificati e valutati;

• che vengano individuate opportune azioni di risposta ai rischi, al fine di ricondurli entro i limiti di accettabilità per l'azienda;

• che le informazioni sui rischi vengano raccolte e diffuse tempestivamente all'interno dell'organizzazione, consentendo al personale, al management e al boarddi adempiere alle rispettive responsabilità.

L'attività di internal audit può raccogliere le informazioni necessarie per questa valutazione attraverso molteplici incarichi. I risultati di questi incarichi, visti nel complesso, permettono di capire i processi di gestione del rischio dell'organizzazione e la loro efficacia.

I processi di gestione del rischio sono monitorati attraverso la gestione manageriale continua, specifiche valutazioni, o entrambi.

2120.A1 – L'attività di internal audit deve valutare l'esposizione al rischio che attiene alla governance, all'operatività e ai sistemi informativi dell'organizzazione, in termini di:

• raggiungimento degli obiettivi strategici dell'organizzazione;

• affidabilità e integrità delle informazioni contabili, finanziarie e operative;

• efficacia ed efficienza delle operazioni e dei programmi;

• salvaguardia del patrimonio;

• conformità a leggi, regolamenti, direttive, procedure e contratti.

2120.A2 – L'attività di internal audit deve valutare la potenziale presenza di casi di frode e come l'organizzazione gestisce tali rischi.

2120.C1 – Nello svolgimento di incarichi di consulenza, gli internal auditors devono tenere conto degli eventi di rischio attinenti agli obiettivi dell'incarico e prestare attenzione a qualsiasi altro rischio significativo.

2120.C2 – Nella valutazione dei processi di gestione del rischio, gli internal auditors devono tenere conto anche delle conoscenze dei rischi dell'organizzazione, acquisite nel corso di incarichi di consulenza.

2120.C3 – Quando assistono il management nella implementazione o nel miglioramento dei processi di gestione del rischio, gli internal auditors devono evitare di gestire direttamente i rischi, perché verrebbero così ad assumere responsabilità manageriali.

2130 – Controllo

L'attività di internal audit deve assistere l'organizzazione nel garantire la validità dei controlli attraverso la valutazione della loro efficacia ed efficienza e attraverso la promozione di un continuo miglioramento.

2130.A1 – L'attività di internal audit deve valutare l'adeguatezza e l'efficacia dei controlli introdotti in risposta ai rischi riguardanti la governance, le operazioni e i sistemi informativi dell'organizzazione, relativamente a:

• raggiungimento degli obiettivi strategici dell'organizzazione;

• affidabilità e integrità delle informazioni contabili, finanziarie e operative;

• efficacia ed efficienza delle operazioni e dei programmi;

• salvaguardia del patrimonio;

• conformità a leggi, regolamenti, direttive, procedure e contratti.

2130.C1 – Nella valutazione dei processi di controllo dell'organizzazione, gli internal auditors devono tenere conto anche delle conoscenze in materia di controllo acquisite nel corso di incarichi di consulenza.

2200 – Pianificazione dell'incarico

Per ciascun incarico gli internal auditors devono predisporre e documentare un piano che comprenda gli obiettivi dell'incarico, l'ambito di copertura, la tempistica e l'assegnazione delle risorse.

2201 – Elementi della pianificazione

Nel pianificare l'incarico, gli internal auditors devono considerare:

• gli obiettivi e le modalità di controllo dell'andamento dell'attività oggetto di audit;

• i rischi significativi dell'attività, i propri obiettivi, risorse e operazioni, nonché le modalità di contenimento dei rischi entro i livelli di accettabilità;

• l'adeguatezza e l'efficacia dei processi di governance, di gestione dei rischi e di controllo dell'attività oggetto di audit, in riferimento a un quadro o modello di riferimento riconosciuto;

• le possibilità di apportare significativi miglioramenti ai processi di governance, di gestione dei rischi e di controllo dell'attività oggetto di audit.

2201.A1 – Nel pianificare un incarico per conto di terze parti esterne all'organizzazione, gli internal auditors devono definire con queste un accordo scritto che chiarisca obiettivi, ambito di copertura, rispettive responsabilità ed eventuali aspettative e che stabilisca restrizioni alla diffusione dei risultati dell'incarico e all'accesso alla relativa documentazione.

2201.C1 – Gli internal auditors devono concordare con i clienti di un incarico di consulenza gli obiettivi, l'ambito di copertura, le rispettive responsabilità e ciò che di ulteriore ci si attende. Per gli incarichi di maggiore rilevanza, tale accordo deve essere formalizzato in un documento scritto.

2210 – Obiettivi dell'incarico

Per ciascun incarico devono essere fissati obiettivi specifici.

2210.A1 – Gli internal auditors devono effettuare una valutazione preliminare dei rischi afferenti l'attività oggetto di audit. Gli obiettivi dell'incarico devono rispecchiare i risultati di tale valutazione.

2210.A2 – Al momento della definizione degli obiettivi dell'incarico, gli internal auditors devono considerare il grado di probabilità che esistano errori significativi, frodi, non conformità e altre situazioni pregiudizievoli.

2210.A3 – Per valutare la governance, la gestione dei rischi e dei controlli, sono necessari criteri adeguati. Gli internal auditors devono accertare che il management e/o il board abbiano stabilito criteri adeguati per valutare il raggiungimento di obiettivi e traguardi. Se tali criteri sono adeguati, gli internal auditors devono utilizzarli nell'effettuare la propria valutazione. In caso contrario, devono collaborare con il management e/o il board allo sviluppo di opportuni criteri di valutazione.

2210.C1 – Gli obiettivi degli incarichi di consulenza devono riguardare processi di governance, di gestione dei rischi e di controllo, nella misura concordata con il cliente.

2210.C2 – Gli obiettivi degli incarichi di consulenza devono essere coerenti con i valori, le strategie e gli obiettivi dell'organizzazione.

2220 – Ambito di copertura dell'incarico

L'ambito di copertura definito, deve essere sufficiente per consentire il raggiungimento degli obiettivi dell'incarico.

2220.A1 – L'ambito di copertura dell'incarico deve tenere conto dei sistemi informativi, delle registrazioni, del personale e dei beni patrimoniali, compresi quelli sotto il controllo di terze parti esterne.

2220.A2 – Qualora, nel corso di un incarico di assurance, emergano opportunità significative di incarichi di consulenza, si dovrebbe stipulare uno specifico accordo scritto su obiettivi, ambito di copertura, rispettive

responsabilità e su ciò che di ulteriore ci si attenda. I risultati raggiunti vanno comunicati secondo gli standard vigenti per gli incarichi di consulenza.

2220.C1 – Nello svolgimento di un incarico di consulenza, gli internal auditors devono assicurarsi che l'ambito di copertura dell'incarico sia sufficientemente ampio per conseguire gli obiettivi concordati. Se, nel corso dell'incarico, gli internal auditors ritengono di ridefinire l'ambito di copertura, ne devono discutere con il cliente, per decidere se sia opportuno proseguire.

2220.C2 – Nel corso degli incarichi di consulenza, gli internal auditors devono analizzare i controlli in coerenza con gli obiettivi dell'incarico ed essere attenti all'eventuale presenza di problematiche di controllo significative.

2230 – Assegnazione delle risorse

Gli internal auditors devono determinare le risorse necessarie e sufficienti per conseguire gli obiettivi dell'incarico in base alla valutazione della natura e complessità dello stesso, dei vincoli temporali e delle risorse a disposizione.

2240 – Programma di lavoro

Gli internal auditors devono sviluppare e documentare programmi di lavoro che permettano di conseguire gli obiettivi dell'incarico.

2240.A1 – I programmi di lavoro devono includere le procedure per raccogliere, analizzare, valutare e documentare le informazioni durante lo svolgimento dell'incarico. I programmi di lavoro devono essere approvati prima della loro utilizzazione e ogni successiva modifica deve essere prontamente approvata.

2240.C1 – I programmi di lavoro per gli incarichi di consulenza possono variare nella forma e nel contenuto, secondo la natura dell'incarico.

2300 – Svolgimento dell'incarico

Gli internal auditors devono raccogliere, analizzare, valutare e documentare informazioni sufficienti al raggiungimento degli obiettivi dell'incarico.

2310 – Raccolta delle informazioni

Gli internal auditors devono raccogliere informazioni sufficienti, affidabili, pertinenti e utili per conseguire gli obiettivi dell'incarico.

Interpretazione:

Le informazioni sono sufficienti quando sono concrete, adeguate e convincenti, così che, in base a esse, qualunque persona prudente e informata giungerebbe alle stesse conclusioni dell'auditor. Le informazioni sono affidabili quando sono fondate e sono le migliori ottenibili attraverso l'uso di tecniche adeguate all'incarico. Le

informazioni sono pertinenti quando sono coerenti con gli obiettivi dell'incarico e danno fondamento ai rilievi e alle raccomandazioni. Le informazioni sono utili quando possono aiutare l'organizzazione a raggiungere le proprie finalità.

2320 – Analisi e valutazione

Gli internal auditors devono pervenire alle conclusioni e ai risultati dell'incarico sulla base di analisi e valutazioni appropriate.

2330 – Documentazione delle informazioni

Gli internal auditors devono documentare le informazioni atte a supportare le conclusioni e i risultati dell'incarico.

2330.A1 – Il responsabile internal auditing deve controllare l'accesso alla documentazione dell'incarico. Prima di distribuire tale documentazione a parti terze, il responsabile internal auditing deve ottenere l'approvazione del senior management e/o, secondo le circostanze, il parere dell'ufficio legale.

2330.A2 – Il responsabile internal auditing deve definire i criteri di conservazione delle carte di lavoro, indipendentemente dalle modalità di archiviazione. Tali criteri devono essere conformi alle linee guida dell'organizzazione, alla regolamentazione vigente in materia o a disposizioni di altro genere.

2330.C1 – Il responsabile internal auditing deve definire le direttive concernenti la custodia e l'archiviazione della documentazione relativa agli incarichi di consulenza, nonché la sua distribuzione all'interno e all'esterno dell'organizzazione. Tali direttive devono essere conformi alle linee guida dell'organizzazione, alla regolamentazione vigente in materia o a disposizioni di altro genere.

2340 – Supervisione dell'incarico

Gli incarichi devono essere sottoposti a opportuna supervisione al fine di garantire che gli obiettivi vengano raggiunti, che la qualità sia assicurata e che il personale possa crescere professionalmente.

Interpretazione:

Il grado di supervisione richiesta dipende dalla professionalità e dall'esperienza degli internal auditors, nonché dalla complessità dell'incarico. Il responsabile internal auditing ha la completa responsabilità della supervisione dell'incarico, anche nel caso in cui questo sia svolto per conto dell'internal audit. Il responsabile internal auditing può delegare tale supervisione a internal auditors di provata esperienza. Evidenza dell'avvenuta supervisione deve essere documentata e opportunamente conservata.

2400 – Comunicazione dei risultati

Gli internal auditors devono comunicare i risultati degli incarichi.

2410 – Modalità di comunicazione

La comunicazione deve includere gli obiettivi e l'estensione dell'incarico, così come le pertinenti conclusioni, raccomandazioni e piani d'azione.

2410.A1 – Laddove appropriato, la comunicazione finale dei risultati deve contenere il giudizio o le conclusioni degli internal auditors. Quando espressi, il giudizio o la conclusione devono tenere in considerazione le aspettative del senior management, del board e degli altri stakeholder e devono essere corroborati da informazioni sufficienti, affidabili, pertinenti e utili.

Interpretazione:

I giudizi espressi a livello di incarico possono essere valutazioni, conclusioni o altre descrizioni dei risultati. In questi casi, l'incarico può riguardare il controllo su un processo, un rischio o una business unit specifici. Per formulare questi giudizi è necessario considerare i risultati dell'incarico e il loro significato.

2410.A2 – Nelle comunicazioni relative all'incarico, gli internal auditors sono incoraggiati a dare atto delle operazioni svolte in modo adeguato dall'organizzazione.

2410.A3 – In caso di invio a terze parti esterne all'organizzazione, la comunicazione dei risultati deve prevedere espressamente limiti di utilizzo e di distribuzione.

2410.C1 – Le comunicazioni relative allo stato di avanzamento e ai risultati finali degli incarichi di consulenza possono variare, nella forma e nei contenuti, in funzione della natura dell'incarico e delle esigenze del cliente.

2420 – Qualità della comunicazione

La comunicazione deve essere accurata, obiettiva, chiara, concisa, costruttiva, completa e tempestiva.

Interpretazione:

Una comunicazione accurata non presenta errori né distorsioni ed è fedele ai fatti rilevati. Una comunicazione obiettiva è corretta, imparziale e scevra da pregiudizi ed è il risultato di una valutazione imparziale ed equilibrata di tutti i fatti e le circostanze rilevanti. Una comunicazione chiara ha senso logico ed è facilmente comprensibile. La chiarezza può essere migliorata limitando l'uso di termini tecnici e fornendo sufficienti informazioni di supporto. Una comunicazione concisa è essenziale, evita formulazioni non necessarie, dettagli superflui, ridondanze e prolissità. Una comunicazione costruttiva è utile al committente dell'incarico e all'organizzazione e induce miglioramenti laddove necessari. Una comunicazione completa contiene tutti gli elementi informativi essenziali per i destinatari, nonché tutte le informazioni e le osservazioni significative atte a corroborare raccomandazioni e conclusioni. Una comunicazione tempestiva è puntuale e opportuna nei tempi, in funzione della portata del problema, consentendo al management di intraprendere appropriate azioni correttive.

2421 – Errori e omissioni nella comunicazione

Se la comunicazione finale dei risultati contiene significativi errori od omissioni, il responsabile internal auditing deve inviare rettifiche e correzioni a tutti coloro che hanno ricevuto la comunicazione originale.

2430 – Uso della dizione "Effettuato in accordo con gli Standard Internazionali per la Pratica Professionale dell'Internal Auditing"

Gli internal auditors possono indicare che i loro incarichi sono "effettuati in conformità agli Standard Internazionali per la Pratica Professionale dell'Internal Auditing" solo se le risultanze del programma di assurance e miglioramento della qualità avvalorano tale affermazione.

2431 – Comunicazione di non conformità di uno specifico incarico

Nel caso di non conformità al Codice Etico o agli Standard che incidano negativamente su uno specifico incarico, la comunicazione dei risultati dell'incarico deve riportare:

• il principio o la regola di condotta del Codice Etico oppure lo Standard che non è stato pienamente rispettato;

• le ragioni della non conformità;

• le conseguenze della non conformità sull'incarico e sulla comunicazione dei relativi risultati.

2440 – Divulgazione dei risultati

Il responsabile internal auditing deve comunicare i risultati agli opportuni destinatari.

Interpretazione:

Il responsabile internal auditing, è tenuto a verificare ed approvare sia la comunicazione finale dei risultati dell'incarico prima dell'emissione degli stessi, sia la lista di distribuzione che la modalità di divulgazione. Laddove il responsabile internal auditing deleghi queste funzioni, egli ne rimane comunque totalmente responsabile.

2440.A1 – Il responsabile internal auditing ha la responsabilità di comunicare i risultati finali dell'incarico ai soggetti dell'organizzazione in grado di assicurarne un seguito adeguato.

2440.A2 – Se non diversamente prescritto da leggi, normative o regolamenti, prima di comunicare i risultati a terze parti esterne all'organizzazione, il responsabile internal auditing deve:

• valutare i potenziali rischi per l'organizzazione;

• consultare il senior management e/o l'ufficio legale a seconda delle circostanze;

• controllare la divulgazione, disponendo limitazioni sull'utilizzo dei risultati.

2440.C1 – Il responsabile internal auditing è responsabile della comunicazione ai clienti dei risultati finali dell'incarico di consulenza.

2440.C2 – Nel corso di incarichi di consulenza è possibile che vengano rilevate criticità concernenti la governance, la gestione dei rischi e il controllo. Se tali criticità sono significative per l'organizzazione, esse devono essere segnalate al senior management e al board.

2450 – Giudizi complessivi

Quando si esprime un giudizio complessivo, questo deve tenere in considerazione le aspettative del senior management, del board e degli altri stakeholder e deve essere corroborato da informazioni sufficienti, affidabili, pertinenti e utili.

Interpretazione: La comunicazione deve precisare:

• l'ambito di copertura, specificando il periodo di tempo cui si riferisce il giudizio;

• le limitazioni dell'ambito di copertura;

• tutti i progetti connessi che sono stati presi in considerazione, indicando l'eventuale ricorso ad altri fornitori di assurance;

• il modello di rischio o di controllo o gli altri criteri usati come fondamento per esprimere il giudizio complessivo;

• il parere, il giudizio o la conclusione complessivi formulati.

È necessario specificare i motivi dell'eventuale giudizio complessivo sfavorevole.

2500 – Monitoraggio delle azioni correttive

Il responsabile internal auditing deve stabilire e mantenere un sistema di monitoraggio delle azioni intraprese a seguito dei risultati segnalati al management.

2500.A1 – Il responsabile internal auditing deve impostare un processo di follow up per monitorare e assicurare che le azioni correttive siano state effettivamente attuate dal management oppure che il senior management abbia accettato il rischio di non intraprendere alcuna azione.

2500.C1 – L'attività di internal audit deve monitorare le azioni intraprese a seguito di incarichi di consulenza nella misura concordata con il cliente.

2600 – Comunicazione dell'accettazione del rischio

Qualora il responsabile internal auditing concluda che il management abbia accettato un livello di rischio che potrebbe essere inaccettabile per l'organizzazione, ne deve discutere con il senior management. Se il responsabile internal auditing ritiene che la problematica non sia stata risolta, deve informarne il board.

Interpretazione:

È possibile identificare il rischio accettato dal management o attraverso un incarico di assurance o di consulenza che permetta di monitorare lo stato di implementazione delle azioni intraprese dal management in risposta a incarichi precedenti, oppure in altri modi. Il responsabile internal auditing non è responsabile per la gestione del rischio.

APPENDICE 2

GLOSSARIO

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 auditors 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.

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.

International Professional Practices Framework (IPPF)

Schema concettuale che definisce come deve essere strutturato l'insieme delle disposizioni normative (authoritativeguidance) 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 sul raggiungimento degli obiettivi. 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 auditors 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.