MANUALE *INTERNAL AUDIT*

P.A.C. *COMPLIANT*

(approvato con deliberazione n. 297 del 6/2/2018)

Indice

1. PREMESSA

Lo scopo di questo Manuale è quello di delineare l'autorità e la portata operativa della funzione di *Internal audit* (di seguito anche "IA") all'interno della Azienda Sanitaria Provinciale di Trapani ("ASP TP" o "Ente") e di fornire ai membri delle funzioni preposte a vario titolo al controllo dell'ASP TP indicazioni pratiche, strumenti e informazioni per gestire l'attività di *internal audit* nella fase di pianificazione, conduzione e *reporting*, affinché possa essere di supporto ai diversi attori interessati alla funzione IA. Come espressamente previsto dall'Azione A.1.7 del Percorso Attuativo di Certificabilità ("PAC") adottato dalla Regione Siciliana, gli Enti del Servizio Sanitario della Regione sono obbligati alla "*Istituzione di una funzione d'internal audit indipendente ed obiettiva, finalizzata al miglioramento dell'efficacia e dell'efficienza dell'organizzazione amministrativo-contabile aziendale*".

Con nota protocollo n. 65013 del 2 agosto 2016 il Dipartimento Regionale per la Pianificazione Strategica (Servizio 2) dell'Assessorato della Salute della Regione Siciliana ha definito che la funzione IA deve:

- **svolgere attività di verifica indipendente**, con la finalità di esaminare e valutare i processi amministrativo-contabili e gestionali;
- **fornire supporto consultivo e propositivo** alla Direzione, e a tutti i componenti dell'organizzazione, per il costante miglioramento di gestione e il corretto adempimento delle loro responsabilità in coerenza con obiettivi e azioni previste dal Percorso Attuativo di Certificabilità della Regione;
- **analizzare i processi ed i relativi rischi e fissare i controlli** previsti per ridurne l'impatto;
- **assistere la Direzione nel valutare l'adeguatezza del sistema dei controlli interni** e la risposta ai requisiti minimi definiti dalle normative;
- **verificare la conformità dei comportamenti alle procedure operative definite** ed identificare e valutare le aree operative maggiormente esposte a rischi e implementare misure idonee per ridurli. Pertanto, la funzione IA contribuisce ad individuare aree ed opportunità di miglioramento fornendo suggerimenti volti a migliorare il processo di *Governance* con lo scopo di: favorire lo sviluppo di valori e principi etici all'interno delle Azienda; migliorare l'efficace gestione dell'organizzazione e l'*accountability*; comunicare informazioni sui rischi e controlli ai responsabili interessati delle strutture interne; coordinare le attività e il processo di scambio di informazioni su rischi e controlli tra la Direzione, gli Organismi di Controllo Esterno ed Interno e la Dirigenza.

La richiamata nota precisa inoltre che, *tenuto conto che l'attività della Pubblica Amministrazione si palesa necessariamente attraverso atti scritti, il compito della funzione I.A. è quello di:*

- *identificare e valutare i fattori di rischio, tramite analisi dei processi basata sul rischio (risk based);*
- *verificare e monitorare la regolarità degli atti adottati dall'Azienda, nonché la regolarità dei processi che hanno portato all'adozione dei suddetti atti e gli eventuali scostamenti rispetto alle leggi, alle norme, alle regole e alle disposizioni interne;*
- *verificare l'affidabilità dei sistemi di controllo;*
- *avanzare proposte di modifica di procedure e regolamenti o altri suggerimenti volti a superare le difficoltà riscontrate.*

Pertanto, il controllo interno svolto dalla funzione IA si ispira al principio di autotutela dell'Amministrazione che, nell'ipotesi in cui ravvisi in propri atti e comportamenti elementi di irregolarità o di illegittimità, può procedere a rettificarli, integrarli o annullarli. La funzione IA è un'attività esclusiva e indipendente, pertanto la relativa funzione aziendale, per svolgere il proprio compito in modo obiettivo, dovrà godere della necessaria autonomia, libera da condizionamenti, quali potrebbero essere conflitti d'interesse individuali, limitazione del campo d'azione, restrizioni nell'accesso a informazioni, rapporto di dipendenza gerarchica nei confronti di coloro che verifica o difficoltà analoghe.

La responsabilità della funzione IA è assegnata ad un Dirigente/Funzionario con adeguate competenze (in materia di *internal audit*, indicatori di frode, sistemi di prevenzione della corruzione; sistemi informativi aziendali), posizionato nell'organizzazione in *staff* al Direttore Generale e solo a quest'ultimo dovrà relazionare e rispondere per le proprie attività.

Titolo del documento	Manuale *Internal audit*
Data di creazione	29 Gennaio 2018 V1
Adottato da:	Direzione Generale (deliberazione n. 297 del 6/2/2018)
Responsabile di funzione	
Distribuzione	Gruppo *Internal audit*

2. IL SISTEMA DI CONTROLLO INTERNO E DI GESTIONE DEI RISCHI

Il sistema di controllo interno e di gestione dei rischi (in breve "sistema di controllo interno" o "SCI") è costituito dall'insieme delle regole, delle procedure e delle strutture organizzative adottate dall'ASP TP per il raggiungimento degli obiettivi aziendali, quali l'attendibilità dell'informativa economico-finanziaria, l'efficacia e l'efficienza della gestione ed il rispetto della normativa applicabile al settore in cui opera l'Ente.

Il sistema di controllo interno e gestione dei rischi è strutturato per consentire l'identificazione, la misurazione, la gestione e il monitoraggio dei principali rischi. Tale sistema è integrato nei più generali assetti organizzativi e di governo adottati dall'Ente e tiene in adeguata considerazione i modelli di riferimento previsti dal PAC (Percorso attuativo di Certificabilità).

Il sistema di controllo interno e di gestione dei rischi consente la conduzione dell'Ente in modo coerente con gli obiettivi aziendali definiti dalla Direzione Generale in risposta alle richieste del SSR e del SSN. Esso concorre ad assicurare la salvaguardia del patrimonio sociale, l'efficienza e l'efficacia dei processi aziendali, l'affidabilità delle informazioni fornite ai diversi operatori del sistema ed ai vari soggetti che hanno interesse nelle attività dell'Ente, il rispetto di leggi e regolamenti nonché delle procedure interne.

I pilastri su cui si fonda il SCI dell'ASP TP sono cosi schematizzati:

Obiettivi	Principi	Componenti
▪ Salvaguardia del patrimonio aziendale; ▪ conformità a leggi e regolamenti; ▪ attendibilità informazioni; ▪ efficacia ed efficienza operazioni gestionali.	▪ Separazione dei ruoli; ▪ *accountability*; ▪ oggettivazione delle scelte; ▪ tracciabilità delle informazioni;	▪ Ambiente di controllo; ▪ valutazione del rischio; ▪ attività di controllo; ▪ informazione e comunicazione; ▪ monitoraggio;

Nei paragrafi successivi si descrivono i significati degli Obiettivi, Principi e Componenti del sistema di controllo.

2.1. Gli obiettivi del sistema di controllo interno

Nella tabella che segue sono riepilogati gli obiettivi del SCI dell'ASP TP

Salvaguardia del patrimonio aziendale	Il sistema di controllo interno dell'ASP TP è strutturato per raggiungere l'obiettivo di salvaguardare il patrimonio aziendale nelle sue diverse configurazioni, ovvero: ▪ patrimonio tangibile: beni materiali (es. immobilizzazioni, disponibilità finanziaria, ecc.); ▪ patrimonio intangibile: beni immateriali (es. *know-how*, reputazione aziendale, ecc.).

Conformità a leggi e regolamenti	Il sistema di controllo interno è strutturato per raggiungere l'obiettivo di garantire che le azioni svolte siano conformi alle leggi e regolamenti, ovvero: ▪ conformità esterna a leggi, normative e regolamenti; ▪ conformità interna a politiche, procedure e istruzioni aziendali.
Attendibilità informazioni	Il sistema di controllo interno è strutturato per raggiungere l'obiettivo di garantire che le informazioni siano attendibili quando esse si riferiscono a: ▪ informazioni economico patrimoniale (annuali e/o periodiche) verso l'esterno; ▪ informazioni gestionali e operative verso l'interno.
Efficacia ed efficienza delle operazioni aziendali	Il sistema di controllo interno è strutturato per raggiungere l'obiettivo di garantire che le operazioni aziendali siano improntate in maniera **Efficace** (raggiungimento degli obiettivi aziendali nello svolgimento delle operazioni) ed **Efficiente** (miglior rapporto costi / benefici nell'impiego delle risorse aziendali).

2.2. I principi del sistema di controllo interno

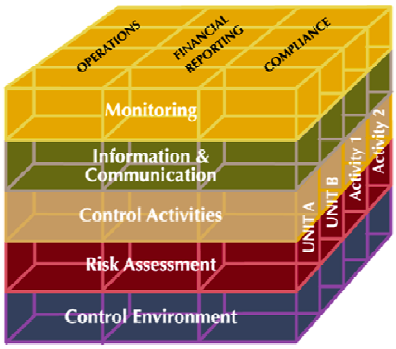
Nella tabella che segue sono riepilogati i principi del SCI dell'ASP TP

Separazione dei ruoli	ASP TP, attraverso le procedure e prassi adottate, garantisce che un intero processo non è mai gestito in autonomia da una sola persona. Le procedure prevedono sempre che esecuzione e controllo siano adeguatamente separate. Nei casi in cui la separazione non è possibile si alza il livello di supervisione e di monitoraggio delle operazioni ad opera della funzione IA.
Accountability	Le procedure aziendali e le prassi adottate garantiscono che l'attività e le decisioni sono riconducibili alla responsabilità di un determinato soggetto individuato in modo specifico.
Oggettivazione delle scelte	Le procedure aziendali e le prassi adottate garantiscono che le decisioni derivanti da valutazioni siano il più possibile razionali e oggettive. Il processo decisionale è sempre motivato e condiviso con i soggetti interessati nel rispetto delle norme, regolamenti e procedure interne formalizzate.
Tracciabilità delle informazioni	Le procedure aziendali e le prassi adottate garantiscono che le scelte siano sempre formalizzate e quindi tracciabili. Tutte le operazioni aziendali sono adeguatamente documentate. Il sistema informatico garantisce anche la tracciabilità delle operazioni e la relativa archiviazione.

2.3. Le componenti del sistema di controllo interno

Le componenti del sistema di controllo interno sono identificati nel documento *Internal Control-Integrated Framework* (COSO *Report*) pubblicato nel 1992 ed aggiornato periodicamente dal *Committee on Sponsoring Organization* (COSO). Il modello è richiamato da numerose disposizioni quali i principi di revisione internazionali e nazionali.

Il sistema di controllo interno aziendale è rappresentato (figura a lato) su 5 componenti. Ognuna di queste componenti ha delle implicazioni funzionali sulle unità e sulle attività della organizzazione aziendale, sulle attività di *business* (*Operations*), sui documenti che sintetizzano le *performance* (*Financial Reporting*) e sulle strutture aziendali dedicate al rispetto delle norme di legge, regolamenti esterni ed interni (*Compliance*).



Nella tabella che segue si identificano gli elementi che formano il sistema di controllo interno dell'ASP TP.

Ambiente di Controllo	L'ambiente di controllo, inteso quale l'insieme di valori, competenze, stile di direzione, assegnazione di autorità, risorse in campo, ecc. Si realizza attraverso i principi, le linee guida e l'organizzazione dell'ASP TP, che costituiscono le fondamenta di tutti gli altri componenti del controllo interno e determina il livello di sensibilità del personale alla necessità di controllo.
Valutazione del Rischio	La valutazione del rischio è una attività volta a garantire la realizzazione di obiettivi e procedure attuative aziendali attraverso l'individuazione e l'analisi dei fattori che possono pregiudicare il raggiungimento degli stessi obiettivi. La valutazione del rischio ha il fine di determinare come questi rischi dovranno essere gestiti.
Attività di Controllo	Le attività di controllo sono quelle attività volte ad individuare ed analizzare i fattori che possono pregiudicare il raggiungimento degli obiettivi. L'ASP TP svolge le attività di controllo attraverso l'applicazione di politiche e delle procedure per i principali processi, oppure prassi, che garantiscono al *management* che le sue direttive siano attuate.

Monitoraggio	Il monitoraggio è una attività volta ad assicurare che il sistema di controllo interno sia sempre aggiornato e adatto alle dimensioni della azienda. Il monitoraggio è svolto attraverso l'attività di supervisione continua, in valutazioni periodiche oppure combinazione dei due metodi ed attraverso la valutazione delle *performance* dei sistemi di controllo.
Informazione e comunicazione	L'informazione e comunicazione è un'attività di diffusione delle informazioni di natura contabile, sull'attività operativa e sull'ambiente in cui opera l'Azienda. Tale attività è svolta attraverso la predisposizione di canali informativi aziendali che consentano l'adempimento delle proprie responsabilità e che producano rapporti contenenti dati operativi, contabili e relativi al rispetto degli obblighi legali e regolamentari, che permettono di gestire e controllare l'attività aziendale.

2.4. Ruoli e responsabilità dei principali attori della *Governance* del SCI.

Nell'ambito della sua struttura organizzativa, l'ASP TP assicura la funzionalità del sistema di controllo interno attraverso la definizione di ruoli e responsabilità. I principali ruoli e responsabilità nell'ambito del SCI sono i seguenti:

Direzione Strategica	Alla Direzione Strategica spetta il ruolo di indirizzo e di valutazione dell'adeguatezza del sistema di controllo interno. Spetta alla Direzione Strategica la funzione di monitoraggio ed il controllo sul mantenimento di un efficace sistema di controllo interno e di gestione dei rischi.
***Internal audit* ("IA")**	Al responsabile della funzione di *Internal audit* è attribuito il compito di verificare che il sistema di controllo interno e di gestione dei rischi sia funzionante ed adeguato alla struttura dell'Ente. La funzione di *Internal audit* deve essere dotata di risorse adeguate al lavoro da svolgere sulla base degli obiettivi definiti dalla Direzione Strategica.
Dirigenti e titolari di posizioni organizzative	Ai vari dirigenti e titolari di posizioni organizzative dell'Ente, sulla base delle procedure interne previste dal PAC, dalle prassi operative e dai vari regolamenti adottati, sono assegnati specifici compiti, ruoli e responsabilità in tema di controllo interno e gestione dei rischi. Gli atti amministrativi interni individuano gli specifici ruoli e responsabilità.
Controllo di Gestione	Nell'ambito della pianificazione strategica sono assegnate al Controllo di Gestione specifiche funzioni finalizzate alla verifica dell'appropriato utilizzo delle risorse in relazione agli obiettivi prefissati. Il processo di controllo della gestione si articola in: esplicitazione degli obiettivi aziendali; rilevazione dei risultati ottenuti; confronto tra obiettivi e risultati per l'analisi degli scostamenti; esame delle possibili cause degli scostamenti più rilevanti; correzione dei risultati (*feed-back* correttivo). Più in particolare, il Controllo di Gestione può essere: controllo antecedente

	(consiste in una autorizzazione preventiva a compiere una o più operazioni); controllo concomitante (monitoraggio della gestione); controllo susseguente (raccolta di informazioni per rendere efficace la programmazione dell'esercizio successivo).
Collegio Sindacale	Al Collegio Sindacale, oltre agli altri adempimenti attribuiti per legge, è affidato il compito di vigilare sull'efficacia ed efficienza del sistema di controllo interno e di gestione dei rischi.
Responsabile della Prevenzione della Corruzione ("RPC")	Al RPC è affidata la funzione di prevenzione del rischio di corruzione. La normativa assegna al RPC alcuni importanti compiti il cui corretto assolvimento permette di rafforzare l'efficacia del sistema di controllo preventivo e, quindi, di rafforzamento del SCI.
Responsabile per la Trasparenza	Al Responsabile per la Trasparenza sono affidate le funzioni previste dal d.lgs. n. 33/2013. In particolare, elabora la proposta di Programma triennale per la trasparenza e l'integrità, in rapporto con il Piano triennale di prevenzione della corruzione; svolge stabilmente un'attività di controllo sull'attuazione da parte dell'ASP TP degli obblighi di pubblicazione previsti dalla normativa vigente; segnala i casi di inadempimento, ritardato adempimento o di adempimento parziale degli obblighi di pubblicazione all'organo di indirizzo politico amministrativo e all'OIV.
L'Organismo Indipendente di Valutazione della *Performance* (OIV)	All'OIV sono attribuite specifiche funzioni di controllo, nell'ambito del sistema di controllo interno, previste dalla legge istitutiva dell'organismo.

2.5. Ambiente di Controllo

L'ambiente di controllo, inteso quale insieme di valori, competenze, stile di direzione, assegnazione di autorità, risorse in campo, ecc. è realizzato dall'Ente attraverso i principi, le linee guida e l'organizzazione, che costituiscono le fondamenta di tutti gli altri componenti del controllo interno. Più in particolare, l'ambiente di controllo si realizza attraverso le seguenti azioni.

Integrità, valori etici e stile	Nell'ambito dello sviluppo ed adozione del modello organizzativo, l'Ente ha messo a punto i seguenti documenti applicativi: ▪ codice Etico; ▪ protocolli di Legalità. Tali documenti racchiudono i principi di Etica, Valori, Stile ed integrità cui si ispira la gestione dell'ASP TP.
Altri sistemi di controllo	▪ Anticorruzione; ▪ trasparenza; ▪ procedure amministrative PAC *Compliant*.
Struttura Organizzativa	▪ Funzionigramma con descrizione di funzioni e compiti.

Poteri e responsabilità	▪ Struttura formalizzata delle Deleghe; ▪ responsabilità attribuite nei regolamenti interni; ▪ responsabilità attribuite nelle procedure PAC.
Competenze e professionalità	▪ Regolamenti per l'assegnazione ed attribuzione degli incarichi di consulenza; ▪ formazione del personale.
Risorse Umane	▪ Sistema di incentivazione su progetti obiettivo; ▪ sistema sanzionatorio su base contrattuale e funzionale.

L'*Internal audit*, nell'ambito delle proprie funzioni, analizza, utilizzando il suo giudizio professionale, l'ambiente di controllo per identificare i rischi, anche di natura fraudolenta, e per definire le attività di controllo formalizzate nel piano di *Audit*. Nel piano delle azioni correttive, IA potrà fornire indicazioni e suggerimenti finalizzati al miglioramento e/o implementazione di tematiche che impattano sull'ambiente di controllo.

2.6. Valutazione del Rischio

La valutazione del rischio è l'attività volta a garantire la realizzazione di obiettivi stabiliti dall'Ente. Le procedure PAC rappresentano lo strumento operativo adottato dall'Ente per il raggiungimento degli obiettivi prefissati. La valutazione del rischio si concretizza in modo continuativo e sistematico durante le attività svolte dai diversi attori della *Governance* dell'ASP TP, a tal fine lo scambio di informazione tra i diversi attori della *Governance* rappresenta un punto dirimente per la valutazione del rischio.

L'ASP TP struttura la valutazione del rischio attraverso le seguenti azioni.

Obiettivi strategici dell'Ente	▪ Piano della *Performance* (Piano strategico); ▪ obiettivi della Direzione Generale (SODG); ▪ piano degli investimenti; ▪ *budget* annuale; ▪ bilancio Previsionale annuale; ▪ programma biennale di acquisto beni e servizi; ▪ programmazione triennale del fabbisogno del personale.
Individuazione e valutazione dei rischi	L'individuazione e la valutazione dei rischi a livello di Direzione Strategica viene desunta dai documenti sopradetti, redatti per la formalizzazione degli obiettivi.

Gestione del cambiamento	▪ Sviluppo infrastrutturale; ▪ relazioni con il territorio; ▪ Livelli Essenziali di Assistenza (LEA).

L'*Internal audit*, nell'ambito delle proprie funzioni, analizza, utilizzando il suo giudizio professionale, la documentazione relativa agli obiettivi dell'Ente con la finalità ultima di definire le attività di controllo e, quindi, il piano di *audit*. Nel piano delle azioni correttive, IA potrà fornire indicazioni e suggerimenti finalizzati al miglioramento e/o implementazione di tematiche che impattano sulla capacità del raggiungimento degli obiettivi e relativa valutazione del rischio.

2.7. Attività di Controllo

La attività di controllo consistono nell'applicazione di politiche, procedure, processi e prassi operative, che garantiscono il raggiungimento degli obiettivi prefissati dall'Ente anche in presenza di rischi impliciti negli obiettivi aziendali. L'ASP TP struttura le attività di controllo attraverso le seguenti azioni.

Politiche e procedure	▪ Comunicazioni interne, *policy* e regolamenti operativi; ▪ procedure amministrativo contabili formalizzate conformi al PAC; ▪ moduli *standard*.
Prassi e sistemi di controllo	▪ Autorizzazioni, approvazioni e verifiche; ▪ sistema informativo aziendale (inclusi i *software* di contabilità, controllo di gestione, ecc); ▪ *password* e blocchi informatici; ▪ protocollazione documenti; ▪ classificazione e archiviazione documenti; ▪ *Check list*.
Esame delle *performance*	▪ Consuntivazione costi/obiettivi (es. spese legali / buon esito contenzioso, ecc.); ▪ *Reporting* finanziario e indici di *performance*; ▪ Analisi del Controllo di Gestione.

L'*Internal audit*, nell'ambito delle proprie funzioni, analizza, utilizzando il suo giudizio professionale, la documentazione relativa alle attività di controllo con la finalità ultima di definire le proprie attività di controllo e, quindi, il piano di *audit*, ovvero per identificare l'esistenza di ulteriori attività di controllo da svolgere per ridurre l'impatto dei rischi identificati. Nel piano delle azioni correttive, IA potrà fornire indicazioni e suggerimenti finalizzati al miglioramento e/o implementazione di tematiche che

impattano sulla capacità del raggiungimento degli obiettivi e relativa valutazione del rischio e connesse attività di controllo.

2.8. Monitoraggio

L'attività di monitoraggio consente di assicurare che il sistema di controllo interno sia sempre aggiornato e adatto alle dimensioni della azienda. L'ASP TP esegue l'attività di monitoraggio attraverso la supervisione continua, attraverso valutazioni periodiche, oppure combinazione dei due metodi ed attraverso la valutazione delle *performance* dei sistemi di controllo. L'ASP TP struttura l'attività di monitoraggio attraverso le seguenti azioni.

Monitoraggio delle prestazioni	▪ Attività di supervisione continua da parte della Direzione Strategica; ▪ analisi di indicatori di *performance* e *report* periodici.
Valutazioni specifiche	▪ Attività di *audit* (*Internal audit*, Qualità e Ambiente, esterni); ▪ attività di *audit* di *follow-up*.

L'*Internal audit*, nell'ambito delle proprie funzioni, utilizzando il suo giudizio professionale e tenuto conto che il monitoraggio fornisce regolarmente informazioni sull'efficienza e l'efficacia dei controlli, analizza la documentazione e le azioni relative alle attività svolte con la finalità ultima di identificare le proprie attività di monitoraggio e, quindi, il piano di *audit*. Nel piano delle azioni correttive, IA potrà fornire indicazioni e suggerimenti finalizzati al miglioramento e/o implementazione di tematiche che impattano sulla capacità del raggiungimento degli obiettivi e relativa valutazione del rischio e le connesse attività di monitoraggio.

2.9. Informazione e Comunicazione

L'ASP TP, attraverso l'azione di informazione e comunicazione, diffonde le informazioni di natura contabile sull'attività operativa e sull'ambiente in cui opera l'Azienda. Il sistema informativo dell'ASP TP è costituito da un'infrastruttura composta da *hardware*, *software*, persone, procedure e dati e tratta i dati in modo che gli stessi, interni o esterni, siano adeguati per la gestione dei rischi e per prendere le dovute decisioni. Le informazioni pertinenti sono identificate, raccolte e diffuse in modo tempestivo accertandone preventivamente la qualità ossia l'appropriatezza, l'attualità e l'accuratezza dei contenuti.

Tale attività è svolta attraverso la predisposizione di canali informativi aziendali che consentano l'adempimento delle proprie responsabilità e che producano rapporti contenenti dati operativi e contabili, relativi al rispetto degli obblighi legali e regolamentari, che permettono di gestire e controllare l'attività aziendale nel suo complesso. L'ASP TP struttura l'attività di circolazione delle

informazioni attraverso: *report* periodici, riunioni esecutive ed informative, comunicazioni interne, circolari, ordini di servizio, attività formativa specifica.

L'*Internal audit*, nell'ambito delle proprie funzioni e a suo giudizio professionale, tenuto conto che il flusso delle informazioni rappresenta il veicolo attraverso il quale l'azienda diffonde le regole applicative ed informative del proprio sistema di controllo, analizza la documentazione e le azioni relative alle attività svolte per la diffusione delle informazioni con la finalità ultima di identificare eventuali azioni migliorative da apportare al sistema di informazione e comunicazione adottato.

3. I FLUSSI INFORMATIVI TRA I DIVERSI ATTORI DELLA *GOVERNANCE*

La struttura operativa del sistema di controllo interno prevede che l'IA riporti direttamente al Direttore Generale. Inoltre scambia informazioni, almeno una volta l'anno, con i seguenti attori:

- Dirigenti di Funzione e/ funzionari incaricati;
- Responsabile Controllo di Gestione;
- Collegio Sindacale;
- Responsabile prevenzione della corruzione;
- Responsabile per la trasparenza;
- OIV.

I diversi attori della *Governance*, fatta eccezione per la Direzione Generale, non possono chiedere pareri alla funzione di *Internal audit*; allo stesso modo la funzione di IA non può chiedere pareri ai diversi attori della *Governance*. Tutti gli attori devono operare con "*indipendenza di giudizio*" e non possono attribuire agli altri attori le proprie responsabilità, né le proprie attività da svolgere.

Segnalazione di eventuale danno erariale

Qualora nel corso dell'attività di *audit* emergano fatti che possano dar luogo ad un'ipotesi di responsabilità per danni causati alla finanza pubblica o nel caso di potenzialità lesiva, il Responsabile *Internal audit* informa il Direttore Generale che, disposta l'istruttoria agli uffici competenti, se del caso provvede all'inoltro degli atti alla Procura Regionale presso la Sezione Giurisdizionale della Corte dei Conti.

Segnalazione di eventuale denuncia penale

Qualora nel corso dell'attività di *audit*, venga acquista notizia di un reato perquisibile d'ufficio, il Responsabile *Internal audit* ed il *team* di lavoro, che sono venuti a conoscenza dei fatti, predispongono

una relazione indirizzata al Direttore Generale nella quale si dà evidenza delle circostanze riscontrate, i dati circa il giorno di acquisizione della notizia e le fonti di prova già note. Il Direttore Generale, disposta l'istruttoria agli uffici competenti, provvede a trasmettere gli atti alla Procura della Repubblica.

4. LA FUNZIONE DI *INTERNAL AUDIT* ED I PRINCIPI DI RIFERIMENO

4.1. Definizione di *Internal audit*

L'Associazione Italiana degli *Internal auditors* definisce l'*Internal auditing* come *«un'attività indipendente e obiettiva di assurance e consulenza, finalizzata al miglioramento dell'efficacia ed 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».*

L'ASP TP fa propria questa definizione e sviluppa la propria funzione di IA tenendo conto delle indicazioni fornite dall'Assessorato Salute con la nota protocollo n. 65013 del 2 agosto 2016.

4.2. Il ruolo dell'*Internal Audit*

L'*Internal Audit* assiste la Direzione Generale nel processo di gestione del sistema di controllo interno nell'ambito di un processo strutturato. Lo scopo di questa funzione è quello di assistere 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*. Più in particolare, alla funzione IA sono affidati i seguenti compiti:

- identificare e valutare i fattori di rischio, tramite analisi dei processi basata sul rischio (*risk based*);
- verificare e monitorare la regolarità degli atti adottati dall'Azienda, nonché la regolarità dei processi che hanno portato all'adozione dei suddetti atti e gli eventuali scostamenti rispetto alle leggi, alle norme, alle regole e alle disposizioni interne;
- verificare l'affidabilità delle procedure emesse in applicazione della normativa PAC;
- avanzare proposte di modifica di procedure e regolamenti o altri suggerimenti volti a superare le difficoltà riscontrate.

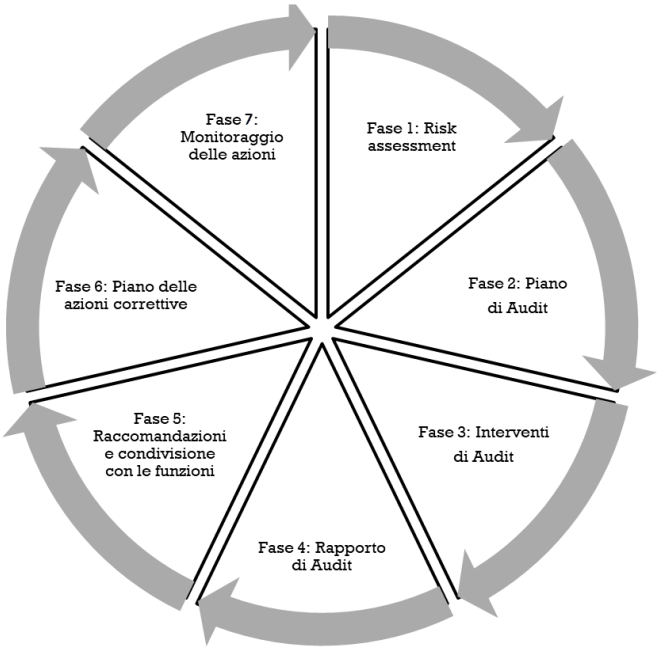
4.3. I principi etici e le regole di condotta dell'*Internal audit*

L'attività svolta dalla Funzione di *Internal audit* si conforma ai principi contenuti nel Codice Etico proprio della funzione di IA come riportato in **Allegato 1**.

5. IL CICLO DI *AUDIT* E LA VALUTAZIONE DEL RISCHIO

5.1. Il ciclo di *Audit* dell'ASP TP

Il ciclo di *Audit* opera mediante una funzionalità circolare. Lo stesso prende avvio dalla analisi dei rischi e termina con il monitoraggio della azioni. Lo schema tipo del processo funzionale del ciclo di *Audit* si può così rappresentare:



5.2. Il *Risk Assessment*

Il *Risk Assessment* è il processo sistematico di identificazione e valutazione dei rischi, svolto dalla funzione di *Internal audit* che individua le aree maggiormente esposte a rischio, che potrebbero pregiudicare il raggiungimento degli obiettivi posti dalla Direzione Generale. Il *Risk Assessment* rappresenta l'attività preliminare alla formazione dei piani annuali e pluriennali di *audit*. Le principali fasi in cui si articola il *Risk Assessment* della Ente sono le seguenti:

a) la definizione dell'Universo di *Audit*;
b) l'identificazione dei rischi dei processi aziendali e la loro valutazione;
c) l'identificazione dei controlli operativi e la loro valutazione;
d) la definizione del piano di *audit* sulla base del *risk scoring*;
e) formalizzazione in una relazione del processo seguito.

5.2.1. Universo di *Audit*

L'Universo di *Audit* è costituito da tutti gli obiettivi e le relative azioni attuative identificate dalla Ente. In relazione all'analisi delle operazioni, l'universo di *audit* è invece costituito dall'insieme delle procedure PAC e prassi poste in essere dalle diverse funzioni aziendali.

5.2.2. Identificazione dei Rischi

La funzione di *Internal audit* procede alla definizione dell'elenco dei rischi principali con la relativa valutazione. Generalmente la valutazione dei rischi è effettuata al "**lordo**" del controllo ovvero si valuta il rischio inerente e, quindi, non si tiene conto dell'effetto del controllo di linea realizzato dal responsabile di processo per presidiare quel rischio e ridurne gli impatti negativi sul raggiungimento degli obiettivi. Nell'ambito della propria azione l'IA dell'ASP TP si troverà ad analizzare le seguenti macro tipologie di rischio:

Tipologia di Rischio	Descrizione
Rischi Strategici	Rischi derivanti dal manifestarsi di eventi che possono condizionare e/o modificare in modo rilevante le strategie e il raggiungimento degli obiettivi dell'ASP TP. Possono avere origine esterna ma anche interna.
Rischi di Processo	Rischi connessi alla normale operatività dei processi dell'Ente, che possono pregiudicare il raggiungimento di obiettivi di efficienza/efficacia, di salvaguardia del patrimonio e di conformità normativa.
Rischi di informativa	Rischi connessi alla possibile inadeguatezza dei flussi informativi interni e verso l'esterno, che possono impedire una adeguata analisi e valutazione delle diverse problematiche e pregiudicare la correttezza dell'informativa prodotta nonché l'efficacia delle decisioni strategiche e operative.
Rischio di *Compliance*	Rischi derivanti dalla applicazione della normativa di riferimento e/o procedure PAC in termini di errata applicazione o di mancata conoscenza delle stesse, che, ove emergenti, pregiudicano il raggiungimento degli obiettivi dell'ASP TP.

La funzione di IA analizza e condivide con la Direzione Generale il "catalogo dei rischi" applicabili all'ASP TP.

5.2.3. Metodologia di valutazione dei Rischi

Come richiesto dalla nota protocollo n. 65013 del 2 agosto 2016 richiamata in premessa, la funzione IA adotta un modello di valutazione dei rischi in termini di probabilità di accadimento e di impatto. Lo strumento metodologico adottato dall'ASP TP, per valutare il rischio, è la matrice **RACM (*Risk Assessment Criteria Matrix*)** che permette di valutare il rischio in termini di probabilità e di impatto, con una valutazione quindi di tipo qualitativo.

(P) PROBABILITÀ (*) DI ACCADIMENTO		
RATING	**PROBABILITÀ**	**DESCRIZIONE**
1	**Impossibile**	Evento negativo mai o raramente verificatosi o verificabile (≤ 5 %)
2	**Improbabile**	Evento negativo che si può generare solo in particolari circostanze ad oggi inesistenti per la tipologia di attività svolta (≤ 25%)
3	**Possibile**	Evento che si è verificato in realtà analoghe e che potrebbe presentarsi anche nell'ASP TP come conseguenza di particolari circostanze (≤ 60%)
4	**Probabile**	Evento negativo che si è verificato nell'ASP TP, seppur raramente, e tale da influenzarne lo svolgimento delle attività (≤ 80%)
5	**Molto Probabile**	Evento negativo quasi certo generato anche da circostanze routinarie e già verificatosi nell'Ente (> 80%)

(*) Probabilità: è la frequenza del manifestarsi del rischio (significativa è l'esperienza e la capacità di giudizio del responsabile di processo e dell'*audit*or).

IMPATTO (**)		
RATING	**IMPATTO**	**DESCRIZIONE**
1	**Immateriale**	Conseguenze praticamente nulle sull'attività e sugli obiettivi
2	**Basso**	Conseguenze minime che non generano una priorità di intervento
3	**Medio**	Conseguenze che influenzano l'efficiente conduzione dell'attività e in quanto tali meritevoli di considerazione
4	**Alto**	Conseguenze rilevanti sull'efficienza e adeguatezza dell'attività e che potrebbero comportare modifiche anche di strategie aziendali
5	**Elevato - Significativo**	Conseguenze pericolose per la continuità dell'attività e in quanto tali il presidio deve essere prioritario e costante

(**) Impatto: livello in cui il manifestarsi del rischio potrebbe influenzare il raggiungimento delle strategie e degli obiettivi.

La valutazione complessiva del rischio in termini di probabilità e impatto viene effettuata utilizzando la seguente matrice, moltiplicano il *rating* assegnato all'impatto per quello assegnato alla probabilità.

RACM (*Risk Assessment Criteria Matrix*)			**IMPATTO**				
			1	**2**	**3**	**4**	**5**
			Immateriale	**Basso**	**Medio**	**Alto**	**Pericoloso**
PROBABILITÀ	**5**	**Molto Probabile**	**5**	**10**	**15**	**20**	**25**
	4	**Probabile**	**4**	**8**	**12**	**16**	**20**
	3	**Possibile**	**3**	**6**	**9**	**12**	**15**
	2	**Improbabile**	**2**	**4**	**6**	**8**	**10**
	1	**Impossibile**	**1**	**2**	**3**	**4**	**5**

Definendo i dati di probabilità ed impatto si ottiene la misurazione del **RISCHIO INERENTE**, ovvero del rischio che non tiene conto delle azioni di controllo.

MISURAZIONE DEL LIVELLO DI RISCHIO INERENTE		
RATING	**RISCHIO**	**DESCRIZIONE**

	INERENTE	
1	**Remoto**	Rischio inerente non rilevante
2 ≤ 5	**Basso**	Rischio inerente esiguo per il quale le azioni di mitigazione non sono una priorità
5,01 ≤ 11	**Medio**	Rischio inerente meritevole di considerazione per il quale è opportuno attivare una risposta al rischio stesso
11,01 ≤ 18	**Alto**	Rischio inerente elevato per il quale è necessario attivare un costante presidio e una efficiente risposta
≥18,01	**Elevato**	Rischio inerente massimo per il quale è indispensabile una risposta efficiente, tempestiva, costante e immediata

5.2.4. Identificazione dei controlli operativi e loro valutazione

Prima di definire il piano di *Audit* e completare l'*iter* previsto del *Risk Assessment* la funzione *Internal audit* deve valutare i controlli esistenti a presidio dei rischi inerenti identificati. La valutazione delle attività di controllo esistenti a presidio dei rischi devono anche tenere conto delle propensioni al rischio dei referenti. La valutazione è espressa in termini di assorbimento del rischio inerente ossia quanto l'attività/azioni di controllo in essere e la propensione al rischio riescono a mitigare/coprire i rischi stessi.

VALUTAZIONE DEL CONTROLLO ESISTENTE			
RATING	**CONTROLLO**	**RISCHIO RESIDUO**	**DESCRIZIONE**
1	**Adeguato**	10%	Attività di controllo efficiente e adeguata (% di assorbimento del rischio 90%)
2	**Parzialmente Adeguato**	30%	Attività di controllo efficiente ma ottimizzabile (% di assorbimento del rischio 70%)
3	**Debole**	60%	Attività di controllo non sufficiente (% di assorbimento del rischio 40%)
4	**Critico**	80%	Attività di controllo non efficace (% di assorbimento del rischio 20%)
5	**Non adeguato**	100%	Attività di controllo inesistente (% di assorbimento del rischio 0%)

La tabella che segue sintetizza la fase finale di valutazione del rischio inerente dopo la valutazione dei controlli. Il rischio residuo è calcolato attraverso la media delle valutazioni ponderate dei rischi inerenti con i relativi controlli esistenti che mitigano (assorbono) il rischio. Nella valutazione del rischio è considerata anche la percezione dello stesso (propensione al rischio) definita per ciascun *owner* di processo individuato nelle procedure PAC.

MISURAZIONE DEL LIVELLO DI RISCHIO INERENTE RESIDUO		
RATING	**RISCHIO INERENTE**	**DESCRIZIONE**
0 ≤ 1,5	**Remoto**	Rischio residuo trascurabile grazie ad un sistema di controllo efficace e a una irrilevante percezione dello stesso
1,51 ≤ 5	**Basso**	Rischio residuo esiguo grazie alle attività di controllo poste in essere. La percezione del rischio è irrilevante
5,01 ≤ 11	**Medio**	Rischio residuo meritevole di considerazione e percepito come un pericolo per il business. Le attività di controllo non riescono a ridurne

		l'impatto
11,01 ≤ 18,99	**Alto**	Rischio residuo elevato e percepito in modo significativo e per il quale le attività di controllo non risultano essere sufficienti
≥19	**Elevato (Significativo)**	Rischio residuo massimo percepito come una minaccia per il business e per il quale le attività di controllo risultano essere insufficienti

5.2.5. Definizione delle priorità di *Audit* sulla base del *risk scoring*

La funzione IA opera sulla base delle risorse di cui dispone, con la finalità di presidiare i rischi elevati, ovvero quei rischi che rappresentano una minaccia al raggiungimento degli obiettivi. Verranno anche presidiate le attività ed i processi PAC che presentano dapprima i rischi elevanti, poi quelli alti, medi e così via, sempre nel rispetto delle esigenze di tempo e risorse disponibili.

5.2.6. Elaborazione della relazione di *Risk Assessment* e condivisione con il *management*

La relazione di *Risk Assessment* precede l'elaborazione del piano di *Audit*, quest'ultimo verrà elaborato in risposta al *Risk Assessment*. La relazione di *Risk Assessment* verrà condivisa con la Direzione Generale che l'approva prima del piano di *audit*.

5.2.7. Documentazione dell'attività svolta

La funzione di IA per lo svolgimento della sua attività utilizza strumenti di formalizzazione anche Informatici (*Software*). Nelle more dello sviluppo di apposito *Software* la formalizzazione del lavoro potrà avvenire tramite l'utilizzo di fogli elettronici e documentazione cartacea appositamente acquisita o prodotta ed opportunamente archiviata.

5.2.8. Formazione della funzione di IA

La funzione di IA, per lo svolgimento della sua attività, deve essere sempre formata ed aggiornata, a tal fine partecipa a corsi di formazione professionale e si avvale di consulenti che la possono guidare nello sviluppo della funzione stessa.

6. PIANIFICAZIONE DELLA ATTIVITÀ DELL'*INTERNAL AUDIT*

La fase di pianificazione rappresenta la risposta ai rischi identificati nella fase del "*Risk Assessment*". Il piano di *Audit* viene quindi strutturato nella fase di pianificazione, dove si analizza l'insieme delle possibili alternative di attività di *audit* realizzabili. Esistono, infatti, vari raggruppamenti di attività operative aziendali che si prestano a divenire oggetto delle attività di verifica, e per questo sono denominati "**oggetti di *Audit***". A titolo di esempio, le verifiche di *Audit* possono essere indirizzate sui seguenti oggetti:

- verifica della funzionalità operativa dei processi aziendali PAC e relative prassi applicate dalla diverse funzioni aziendali;
- verifica di particolari progetti e commesse (sia interne che esterne) che richiedono un intervento specifico di *Audit* interno;
- verifica della struttura organizzativa aziendale e relativa funzionalità;
- verifica su particolari saldi di bilancio che possano rappresentare un rischio per la Direzione Generale.

La scelta della tipologia di oggetti di *Audit* da impiegare per la definizione del piano di *Audit* deve tenere conto dall'aspetto dimensionale per ottenere un piano di *Audit*, che possa essere coperto dalle risorse disponibili in un orizzonte temporale ragionevole rispetto alle esigenze di *Governance* dell'organizzazione.

Gli orizzonti temporali previsti dall'ASP TP per la pianificazione degli interventi di *Audit* sono riassumibili in due piani, uno annuale ed uno triennale. Il piano annuale rappresenta la struttura degli interventi da svolgere nel corso di un anno e coincide con il periodo amministrativo di chiusura del bilancio. Il piano triennale deve essere ispirato agli obiettivi generali dell'Ente. Il piano triennale non ha l'obiettivo di qualificare i rischi ma riassume gli interventi di massima.

Il Piano di *Audit* consente di identificare gli obiettivi di *audit* a livello di ciclo aziendale PAC e di definire la portata dell'intervento, ovvero di identificare la natura, l'estensione e la tempistica delle procedure riferite agli obiettivi di verifica, al fine di svolgere il lavoro in maniera efficace ed efficiente.

6.1. Obiettivi del piano di *audit*

Nell'identificazione e valutazione dei rischi, l'*Internal audit* valuta l'adeguatezza del sistema di controllo interno adottato dall'Ente in relazione alla normativa PAC. Tale attività è stata descritta in precedenza al paragrafo "Il *Risk Assessment*".

La valutazione dei controlli esistenti e delle procedure operative applicate consente alla funzione di *Internal audit* di esprimere un giudizio professionale sul livello di adeguamento dei controlli PAC e, quindi, della qualità procedure PAC applicate.

Il Piano di *Audit* sarà impostato per acquisire ogni elemento necessario per ottenere una ragionevole certezza che le procedure PAC messe in atto dalla diverse funzioni aziendali ed adottate dalla Direzione Generale, siano in grado di garantire tutte le asserzioni di bilancio e, quindi, consentano agli uffici preposti alla redazione dello stesso, di addivenire ad una rappresentazione veritiera e corretta della situazione patrimoniale, finanziaria e del risultato economico dell'ASP TP.

L'azione dell'*Internal audit* sarà, quindi, improntata alla raccolta delle evidenze documentali che consentano di mostrare che gli obiettivi dei controlli implementati siano raggiunti. I principali obiettivi che dovranno essere presidiati dalle procedure aziendali in termini di Asserzioni sono riepilogati nella tabella seguente.

Asserzione	**Definizione**	**Applicazione**	
		SP	**CE**
Esistenza	Le rilevazioni contabili devono avvenire secondo appropriate procedure e strumenti in modo da consentire che una attività o passività esposta in bilancio ad una certa data è esistente.	**X**	
Manifestazione	Le rilevazioni contabili devono avvenire secondo appropriate procedure e strumenti in modo da consentire che una transazione od evento relativa alla Ente e riflessa in bilancio è avvenuta.		**X**
Valutazione	Le rilevazioni contabili devono avvenire secondo appropriate procedure e strumenti in modo da consentire che una attività o passività sia registrata per un appropriato valore.	**X**	
Competenza	Le rilevazioni contabili devono avvenire secondo appropriate procedure e strumenti in modo da consentire che una transazione o evento sia registrata per un ammontare appropriato e il ricavo o la spesa siano allocati nell'appropriato periodo.		**X**
Completezza	Le rilevazioni contabili devono avvenire secondo appropriate procedure e strumenti in modo da consentire che non vi siano significative attività/passività e transazioni o eventi che non siano registrati o elementi di cui tenere evidenza.	**X**	**X**
Diritti ed obblighi	Le rilevazioni contabili devono avvenire secondo appropriate procedure e strumenti in modo che le attività e le passività iscritte in bilancio ad una certa data rappresentino, rispettivamente, diritti ed obbligazioni della Ente.	**X**	
Presentazione e Informativa	Le poste di bilancio sono correttamente denominate, classificate e illustrate.	**X**	**X**

Nel piano di *Audit*, pertanto, dovranno essere previste le seguenti attività:

- verifica della esistenza ed aggiornamento della procedure PAC;
- verifica operativa della loro applicazione operativa;
- verifica dell'adeguata pubblicazione e comunicazione delle procedure PAC;

- attivazione dei flussi informativi verso i soggetti in precedenza individuati;
- azioni di monitoraggio sulla informativa annuale;
- verifica sullo stato di avanzamento delle attività implementate per il rimedio dei *gap* di disegno individuati;
- *Follow Up* della azioni suggerite.

6.2. Attività di *audit* operativo

L'attività di *audit* operativo viene definita ed implementata laddove sono state ravvisate esigenze di verificare e/o controllare processi o attività dell'Ente, le quali sono state considerate sensibili rispetto all'operatività e possono essere fonte di rischi e/o punti di miglioramento. Tali processi possono essere individuati dalle attività di *Compliance* precedenti o dall'analisi dei rischi effettuata sulla realtà dell'Ente.

6.3. Campionamento

L'applicazione delle procedure di *audit* descritte nei precedenti paragrafi richiede una selezione del campione da testare. In particolare, l'*Internal audit* ha a disposizione tre alternative, la cui scelta dipende dagli elementi probativi che devono essere raccolti, dagli obiettivi che si vogliono raggiungere e dalle valutazioni del rischio. In particolare, l'IA può:

1) decidere che sia più appropriato esaminare l'intera popolazione, cioè l'insieme delle unità da cui è selezionato il campione in riferimento al quale intende trarre le proprie conclusioni. Per esempio, nel caso di popolazioni con un ridotto numero di "*items*" o di classi di valori composte da poche operazioni, l'*Internal audit* può ritenere che sia più efficiente ed efficace ricorrere all'esame dell'intera popolazione;
2) selezionare controlli specifici, individuati in base alla conoscenza acquisita, all'esperienza maturata, alle caratteristiche della popolazione e alla valutazione del rischio intrinseco e del rischio di controllo. Il criterio di selezione delle voci può fare riferimento:

    - al loro valore o alla loro criticità (valori inusuali o per i quali in passato sono stati rilevati errori);
    - alla necessità di ottenere informazioni specifiche;
    - all'opportunità di valutare il funzionamento di una procedura.

3) l'*Internal audit* può anche decidere di non sottoporre a verifica voci il cui importo non è significativo e per le quali il rischio di errori significativi è considerato basso (per esempio crediti e debiti diversi di importo non significativo).

La necessità di svolgere verifiche a campione è motivata dall'impossibilità di effettuare una verifica integrale per le classi di valori composte da un elevato numero di operazioni. Al contrario, nel caso di classi di valori composte da un numero ridotto di operazioni, è evidentemente più efficiente effettuare una verifica integrale delle medesime.

Qualora l'*Internal audit* scelga di procedere con il metodo del campione deve dare evidenza nelle proprie carte di lavoro della metodologia di campionamento adottato.

7. *REPORTING* E RELAZIONE ANNUALE DELL'*INTERNAL AUDIT*

La comunicazione dei risultati costituisce la garanzia della trasparenza e della completezza del processo di *audit*. I risultati dell'incarico con le relative conclusioni, raccomandazioni e piani d'azione devono essere comunicati dall'*Internal audit* alla Direzione Generale.

8. IL PIANO DELLE AZIONI CORRETTIVE

È il piano dettagliato delle azioni previste per la mitigazione dei *gap*. Il piano prodotto dall'*Internal audit* deve riportare un contenuto minimo, ovvero:

- l'elenco dei *gap* da mitigare con l'indicazione dei relativi Responsabili di processo e controllo;
- le azioni previste;
- le date di implementazione delle singole azioni;
- la valutazione sul rischio relativo al *gap* individuato e sul rischio rimanente dopo l'implementazione.

Il rispetto del *Risk Remediation Plan* da parte dei singoli referenti deve essere verificato costantemente dall'*Internal audit*.

9. I CONTROLLI DI *FOLLOW UP* SULLE AZIONI CORRETTIVE PREVISTE

Lo svolgimento del *Follow Up* consiste nell'accertamento relativo all'attuazione e all'effettiva funzionalità delle soluzioni proposte. Attraverso questo strumento si dà continuità a quanto implementato nel *Remediation Plan* nell'intento di conseguire una risoluzione definitiva dei *gap* identificati.

* * *

Allegati 1 e 2 – Codice Etico e *Standards* Internazionali Professionali.

CODICE ETICO

Introduzione

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 e appropriato per l'esercizio dell'attività professionale di Internal Audit, che è fondata sulla fiducia indiscussa nell'obiettività dei suoi servizi di *assurance* riguardanti la *governance*, la gestione dei rischi e il controllo.

Il Codice Etico dell'*Institute of Internal Auditors* si estende oltre la Definizione di *Internal Auditing* per includere due componenti essenziali.

1) I Principi, fondamentali per la professione e la pratica dell'*internal auditing*.

2) Le Regole di Condotta, che descrivono le norme comportamentali che gli *internal auditor* sono tenuti a osservare. Queste regole sono un aiuto per orientare l'applicazione pratica dei Principi e intendono fornire agli internal auditor una guida di comportamento professionale.

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

Applicabilità e attuazione

Il Codice Etico si applica sia ai singoli individui, sia alle strutture che forniscono servizi di *internal auditing*.

Il mancato rispetto del Codice Etico da parte dei membri dell'*Institute*, dei detentori delle certificazioni professionali e di coloro che si candidano a riceverle, sarà valutato e sanzionato secondo le norme previste nello Statuto e nelle "*Administrative Directives*" dell'*Institute*.

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

Principi

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

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

2) Obiettività - Nel raccogliere, valutare e comunicare le informazioni attinenti l'attività o il processo in esame, l'*internal auditor* deve manifestare il massimo livello di obiettività professionale. L'*internal auditor*

deve valutare in modo equilibrato tutti i fatti rilevanti, senza venire indebitamente influenzato da altre persone o da interessi personali nella formulazione dei propri giudizi.

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

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

Regole di condotta

1) Integrità - L'*internal auditor*:

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

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

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

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

2) Obiettività - L'*internal auditor*:

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

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

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

3) Riservatezza - L'*internal auditor*:

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

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

4) Competenza - L'*internal auditor*:

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

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

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

STANDARD INTERNAZIONALI PER LA PRATICA PROFESSIONALE DELL'INTERNAL AUDITING (STANDARD)

Introduzione agli *Standard*

L'internal auditing viene svolto in contesti giuridici e culturali diversi, all'interno di organizzazioni che variano per finalità, dimensioni, complessità e struttura, e da persone interne o esterne all'organizzazione. Anche se le differenze nei vari contesti possono influire sullo svolgimento dell'internal auditing, la conformità agli *Standard internazionali per la pratica professionale dell'internal auditing (Standard*) dell'IIA è essenziale per l'espletamento delle responsabilità degli internal auditor e dell'attività di internal audit.

Gli *Standard* hanno lo scopo di:

1. Promuovere l'aderenza agli elementi vincolanti dell'International Professional Practices Framework.
2. Fornire un quadro di riferimento per lo svolgimento e lo sviluppo di una vasta gamma di servizi di internal audit a valore aggiunto.
3. Definire i parametri per la valutazione della prestazione dell'internal audit.
4. Promuovere il miglioramento dei processi e delle attività dell'organizzazione.

Gli *Standard* sono un insieme di requisiti vincolanti, basati su principi, che consistono in:

- Definizioni dei requisiti fondamentali per la pratica professionale dell'internal auditing e per la valutazione dell'efficacia della prestazione, applicabili su scala internazionale a livello di organizzazione e di singoli individui.
- Interpretazioni che chiariscono termini e concetti contenuti negli *Standard*.

Gli *Standard*, insieme al Codice Etico, trattano tutti gli elementi vincolanti dell'International Professional Practices Framework; pertanto la conformità al Codice Etico e agli *Standard* costituisce prova del rispetto di tutti gli elementi vincolanti dell'International Professional Practices Framework.

Gli *Standard* utilizzano termini che sono stati definiti specificatamente nel Glossario. Per comprendere e applicare correttamente gli *Standard*, è necessario considerare i significati specifici riportati nel Glossario. Inoltre, gli *Standard* usano la parola "deve" per specificare un requisito vincolante e la parola "dovrebbe" per indicare un requisito al quale si presuppone la conformità a meno di circostanze che, sottoposte a un giudizio professionale, ne giustifichino l'inosservanza.

Gli *Standard* comprendono due categorie principali: gli Standard di Connotazione e gli Standard di Prestazione. Gli Standard di Connotazione precisano le caratteristiche che le organizzazioni e gli individui che effettuano attività di internal audit devono possedere. Gli Standard di Prestazione descrivono la natura dell'internal auditing e forniscono criteri qualitativi in base ai quali è possibile valutarne la prestazione. Gli Standard di Connotazione e gli Standard di Prestazione si applicano a tutti i servizi di internal audit.

Sono inoltre previsti gli Standard Applicativi che dettagliano i contenuti degli Standard di Connotazione e degli Standard di Prestazione definendo i requisiti da applicare ai servizi di assurance (.A) o di consulenza (.C).

I servizi di assurance comportano un'obiettiva valutazione delle evidenze da parte degli internal auditor finalizzata alla formulazione di giudizi o conclusioni riferiti a un'organizzazione, attività, funzione, processo, sistema o altro. L'internal auditor definisce la natura e l'ampiezza dell'incarico di assurance. Tre sono le parti generalmente coinvolte nei servizi di assurance: (1) il process owner, cioè la persona o il gruppo direttamente coinvolti nell'organizzazione, attività, funzione, processo, sistema o altro, (2) l'internal auditor, cioè la persona o il gruppo che effettua la valutazione e (3) l'utente, cioè la persona o il gruppo che utilizzerà tale valutazione.

I servizi di consulenza sono attività di advisory e sono generalmente effettuati dietro specifica richiesta di un cliente committente. Natura e ampiezza dell'incarico di consulenza sono definiti in accordo con il cliente. Due sono, in genere, le parti coinvolte nei servizi di consulenza: (1) l'internal auditor, cioè la persona o il gruppo che offre il servizio, e (2) il cliente, cioè la persona o il gruppo che lo richiede e ne beneficia. Nello svolgimento dei servizi di consulenza, gli internal auditor dovrebbero mantenere l'obiettività e non assumere responsabilità di tipo manageriale.

Gli *Standard* si applicano ai singoli internal auditor e all'attività di internal audit nel complesso. Tutti gli internal auditor sono tenuti a rispettare gli *Standard* riferiti all'obiettività, alla competenza e alla diligenza professionale, nonché gli *Standard* correlati all'assolvimento delle proprie responsabilità professionali. Oltre a ciò i responsabili delle funzioni di internal auditing sono responsabili della complessiva conformità agli Standard dell'attività di internal audit.

Qualora leggi o regolamenti vietino agli internal auditor o all'attività di internal audit di operare in conformità con alcune parti degli *Standard*, essi dovranno tuttavia rispettarne tutte le altre parti e dare adeguata informativa.

Se gli *Standard* sono utilizzati congiuntamente con requisiti rilasciati da altri organismi riconosciuti, gli internal auditor possono comunicare nel modo più opportuno anche l'uso di altri requisiti. In tal caso, se l'attività di internal audit indica la conformità con gli *Standard* ed esistono differenze tra gli *Standard* e altri requisiti eventualmente adottati, gli internal auditor e l'attività di internal audit devono rispettare gli *Standard* e possono conformarsi ad altri requisiti solo se questi sono più restrittivi.

La revisione e lo sviluppo degli *Standard* è un processo in continua evoluzione. Prima di emanare gli *Standard*, l'International Internal Auditing Standards Board (IASB) intraprende una vasta attività di consultazione e discussione, che comprende la diffusione di exposure draft a livello internazionale per raccogliere commenti dalla comunità degli auditor. Tutti gli exposure draft sono disponibili nel sito Web dell'IIA e vengono distribuiti a tutti gli istituti IIA.

Suggerimenti e commenti in merito agli *Standard* possono essere inviati a:

The Institute of Internal Auditors
Standards and Guidance
1035 Greenwood Blvd, Suite 401
Lake Mary, FL 32746 USA
E-mail: guidance@theiia.org
Web: www.globaliia.org

***

STANDARD INTERNAZIONALI PER LA PRATICA PROFESSIONALE DELL'INTERNAL AUDITING (STANDARD)

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 Mission dell'Internal Auditing e con gli elementi vincolanti dell'International Professional Practices Framework (i Principi fondamentali per la pratica professionale dell'internal auditing, il Codice Etico, gli *Standard* e la Definizione di Internal Auditing). Il responsabile internal auditing deve verificare periodicamente il Mandato di internal audit e sottoporlo all'approvazione del senior management e del board.

Interpretazione:

Il Mandato di 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 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 siano 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 delle guidance vincolanti nel Mandato di internal audit

Il carattere vincolante dei Principi fondamentali per la pratica professionale dell'internal auditing, del Codice Etico, degli *Standard* e della Definizione di Internal Auditing deve essere specificato nel Mandato di internal audit. Il responsabile internal auditing dovrebbe discutere la Mission dell'internal auditing e gli elementi vincolanti dell'International Professional Practices Framework con il senior management e il board.

1100 – Indipendenza e obiettività

L'attività di internal audit deve essere indipendente e gli internal auditor 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 alle proprie responsabilità senza pregiudizi. Per raggiungere il livello di indipendenza necessario per adempiere efficacemente alle 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. I casi di limitazione all'indipendenza devono essere gestiti a livello di singolo auditor, di incarico, funzione e organizzazione

Obiettività è l'attitudine mentale di imparzialità che consente agli internal auditor di svolgere gli 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 auditor non subordinino il loro giudizio 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 a 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:

L'indipendenza organizzativa si realizza con efficacia quando il responsabile internal auditing riferisce funzionalmente al board. Ad esempio, il riporto funzionale al board comporta che il board:

- *approvi il Mandato di internal audit;*
- *approvi il piano di internal audit 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 alla revoca del responsabile internal auditing;*
- *approvi il compenso spettante al responsabile internal auditing;*
- *effettui opportune verifiche con il management e con 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 delle attività di internal auditing, nell'esecuzione del lavoro e nella comunicazione dei risultati. Il responsabile internal auditing deve comunicare eventuali interferenze al board e discuterne le implicazioni.

1111 – Interazione diretta con il board

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

1112 – Ruoli addizionali del responsabile internal auditing

Laddove il responsabile internal auditing abbia, o si prevede abbia, ruoli e/o responsabilità che esulano dall'internal auditing, devono essere poste in essere opportune misure di tutela atte a limitare i condizionamenti all'indipendenza o all'obiettività.

Interpretazione:

Al responsabile internal auditing possono essere richiesti ruoli e responsabilità addizionali che esulano dall'internal auditing, come ad esempio la responsabilità per attività di Compliance o Risk Management. Tali ruoli e responsabilità possono condizionare, anche solo apparentemente, l'indipendenza organizzativa dell'attività di internal audit o l'obiettività individuale dell'internal auditor. Le misure di tutela sono quelle attività di supervisione, spesso intraprese dal board, atte a indirizzare questi potenziali condizionamenti e possono comprendere attività come la valutazione periodica delle linee di riporto e delle responsabilità e lo sviluppo di processi alternativi per ottenere l'assurance sulle aree di responsabilità addizionali.

1120 – Obiettività individuale

Gli internal auditor devono avere un atteggiamento imparziale e senza pregiudizi ed evitare qualsiasi conflitto di interessi.

Interpretazione:

Il conflitto di interessi è una situazione nella quale un internal auditor, che gode di una posizione di fiducia, si trova ad avere un interesse personale o professionale contrario agli interessi dell'organizzazione. Un simile interesse contrario rende difficile per l'internal auditor assolvere ai propri compiti con imparzialità. Un conflitto di interessi sussiste anche quando non dà luogo a comportamenti non etici o 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 l'internal auditor, l'attività di internal audit e la professione. Il conflitto di interessi può pregiudicare la capacità individuale di assolvere 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 rese note ad appropriati interlocutori. 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 a titolo unicamente esemplificativo conflitti di interessi personali, limitazioni del campo di azione, restrizioni dell'accesso a dati, persone e beni e vincoli di risorse, tra cui quelle finanziarie.

L'individuazione degli interlocutori più appropriati al quale devono essere rese note le circostanze del condizionamento all'indipendenza o all'obiettività dipende dalle aspettative relative all'attività di internal audit e dalle responsabilità del responsabile internal auditing nei confronti del senior management e del board definite nel Mandato di internal audit, nonché dalla natura del condizionamento stesso.

1130.A1 – Gli internal auditor devono astenersi dal valutare specifiche attività per le quali sono stati in precedenza responsabili. Si presume che l'obiettività sia condizionata se un internal auditor effettua un servizio di assurance per un'attività di cui è stato responsabile nell'anno precedente.

1130.A2 – Gli incarichi di assurance per funzioni che ricadono sotto la responsabilità del responsabile internal auditing devono essere supervisionati da soggetti esterni all'attività di internal audit.

1130.A3 – L'attività di internal audit può fornire servizi di assurance anche per quelle aree dove ha in precedenza svolto servizi di consulenza, a patto che la natura della consulenza non condizioni l'obiettività e che, nell'assegnazione delle risorse all'incarico, l'obiettività individuale sia salvaguardata.

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

1130.C2 – Se gli internal auditor, 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 auditor 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:

Il termine competenza si riferisce complessivamente alle conoscenze, capacità e altre caratteristiche *richieste agli internal auditor per adempiere efficacemente alle proprie responsabilità professionali. Questo include la valutazione della situazione attuale, dei trend e delle tematiche emergenti, allo scopo di consentire la formulazione di pareri e raccomandazioni pertinenti. Gli internal auditor sono incoraggiati a dimostrare la propria competenza conseguendo le opportune certificazioni e qualifiche professionali, come quella di "Certified Internal Auditor" e altre certificazioni rilasciate da "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 auditor non possiedono le conoscenze, le capacità o altre competenze necessarie per lo svolgimento di tutto o di parte dell'incarico.

1210.A2 – Gli internal auditor devono possedere conoscenze sufficienti per valutare i rischi di frode e le modalità con cui l'organizzazione li gestisce; tuttavia non è richiesto che essi abbiano le competenze proprie di chi ha come responsabilità primaria quella di individuare e investigare frodi.

1210.A3 – Gli internal auditor devono possedere una sufficiente conoscenza dei rischi e dei controlli chiave a livello di Information Technology, nonché avere a disposizione degli

strumenti informatici di supporto all'audit per svolgere gli incarichi assegnati. Tuttavia, non è richiesto che tutti gli internal auditor 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 auditor 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 auditor 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 dovuta diligenza professionale tenendo in considerazione:

- l'ampiezza del lavoro necessario per raggiungere gli obiettivi dell'incarico;
- la complessità, importanza o 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 di eventi di non conformità significativi;
- il costo dell'assurance in relazione ai suoi potenziali benefici.

1220.A2 – Nell'esercizio dell'opportuna diligenza professionale, gli internal auditor devono considerare l'utilizzo di strumenti informatici di supporto all'audit e di altre tecniche di analisi dei dati**.**

1220.A3 – Gli internal auditor devono prestare attenzione ai rischi significativi che possono incidere su obiettivi, attività o risorse. In ogni caso, 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 auditor devono esercitare la dovuta diligenza professionale tenendo in considerazione:

- le esigenze e le aspettative dei clienti, inclusa la natura, i tempi e la 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 auditor 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:

Il programma di assurance e miglioramento della qualità è disegnato per permettere una valutazione di conformità dell'attività di internal audit agli Standard *e per consentire di verificare se gli internal auditor 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. Il responsabile internal auditing dovrebbe incoraggiare il board a supervisionare il programma di assurance e miglioramento della qualità.*

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 audit;
- periodiche auto-valutazioni o valutazioni condotte da altre persone interne all'organizzazione che abbiano conoscenze adeguate della pratica professionale 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 considerati necessari per valutare la conformità al Codice Etico e agli Standard*.*

Le valutazioni periodiche sono effettuate con l'obiettivo di valutare la conformità al Codice Etico e agli Standard*.*

L'adeguata conoscenza delle metodologie di internal audit presuppone perlomeno l'adeguata comprensione di tutti gli elementi dell'International Professional Practices Framework.

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 potenziali conflitti di interessi.

Interpretazione:

Le valutazioni esterne possono essere effettuate con una valutazione interamente esterna oppure tramite un'autovalutazione con convalida esterna indipendente. Il valutatore esterno deve esprimere le proprie conclusioni in merito alla conformità al Codice Etico e agli Standard*; la valutazione esterna può altresì comprendere osservazioni operative o strategiche.*

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. Per quanto attiene ai 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 il proprio 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. Il responsabile internal auditing dovrebbe adoperarsi affinché il board supervisioni la valutazione esterna allo scopo di ridurre i conflitti di interessi percepiti o potenziali.

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. La comunicazione dovrebbero comprendere:

- l'ambito e la frequenza delle valutazioni interne ed esterne;
- le qualifiche e l'indipendenza del(i) valutatore(i) o del team di valutatori, inclusa l'esistenza di potenziali conflitti di interessi;
- le conclusioni dei valutatori;
- le azioni correttive.

Interpretazione:

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

È consentito indicare che l'attività di internal audit risulta conforme agli *Standard internazionali per la pratica professionale dell'internal auditing* unicamente se i risultati del programma di assurance e miglioramento della qualità avvalorano tale affermazione.

Interpretazione:

L'attività di internal audit risulta conforme al Codice Etico e agli Standard *quando raggiunge i risultati in essi descritti. 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. Le strutture 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 al Codice Etico o agli *Standard* che influiscano 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 efficacemente l'attività al fine di assicurare che essa aggiunga valore all'organizzazione.

Interpretazione:

L'attività di internal audit è gestita efficacemente quando:

- *raggiunge le finalità e le responsabilità indicate nel Mandato di internal audit;*
- *è conforme agli* Standard*;*
- *i suoi singoli membri rispettano il Codice Etico e gli* Standard*;*
- *tiene in considerazione i trend e le tematiche emergenti che potrebbero influire sull'organizzazione.*

L'attività di internal audit aggiunge valore all'organizzazione e ai suoi stakeholder quando tiene in considerazione le strategie, gli obiettivi e i rischi; si adopera per fornire soluzioni per migliorare i processi di governance, di gestione del rischio e di controllo; fornisce in via oggettiva assurance rilevante.

2010 – Pianificazione

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

Interpretazione:

Per predisporre il piano risk based, il responsabile internal auditing si consulta con il senior management e il board per comprendere le strategie, i principali obiettivi di business, i rischi associati e i processi di gestione del rischio dell'organizzazione. Il responsabile internal auditing deve rivedere e adeguare opportunamente il piano, in risposta ad eventuali cambiamenti intervenuti a livello di attività, rischi, operatività, programmi, sistemi e controlli dell'organizzazione.

2010.A1 – Il piano degli incarichi dell'attività di internal audit deve basarsi su una documentata valutazione del rischio, effettuata almeno una volta l'anno. Tale processo deve tenere in considerazione le indicazioni del senior management e del board.

2010.A2 – Il responsabile internal auditing deve individuare e considerare le aspettative del senior management, del board e degli altri stakeholder per quanto attiene ai giudizi e alle conclusioni dell'internal audit.

2010.C1 – Il responsabile internal auditing dovrebbe 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.

2020 – Comunicazione e approvazione

Il responsabile internal auditing deve sottoporre il piano dell'attività di internal audit e delle risorse necessarie, incluse eventuali significative variazioni intervenute, all'esame e all'approvazione del senior management e del board. 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 temine "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 volte a guidare l'attività di internal audit.

Interpretazione:

La forma e il contenuto delle direttive e delle procedure dipende dall'entità e dalla struttura dell'attività di internal audit, nonché dalla complessità dei suoi compiti.

2050 – Coordinamento e affidamento

Il responsabile internal auditing dovrebbe condividere le informazioni, coordinare le attività e considerare la possibilità di affidarsi all'operato di altri prestatori, esterni e interni, di servizi di assurance e consulenza, al fine di assicurare un'adeguata copertura e minimizzare le possibili duplicazioni.

Interpretazione:

Nel coordinare le attività, il responsabile internal auditing può fare affidamento sull'operato di altri prestatori di servizi di assurance e consulenza. A tal fine andrebbe definito un processo strutturato e il responsabile internal auditing dovrebbe valutare la competenza, l'obiettività e la diligenza professionale dei prestatori di servizi di assurance e consulenza. Il responsabile internal auditing dovrebbe altresì avere una visione chiara dell'ambito, degli obiettivi e dei risultati dell'operato degli altri prestatori di servizi di assurance e consulenza. Quando viene fatto affidamento sull'operato di terzi, il responsabile internal auditing ha comunque la responsabilità di garantire che le conclusioni e i giudizi formulati nell'ambito dell'attività di internal audit siano opportunamente supportati.

2060 – Comunicazione al senior management e al board

Il responsabile internal auditing deve periodicamente informare il senior management e il board in merito a finalità, poteri e responsabilità dell'attività d'internal audit nonché comunicare lo stato di avanzamento del piano e la conformità dell'attività d'internal audit al Codice Etico e agli *Standard*. Tale comunicazione deve comprendere inoltre i rischi significativi, inclusi quelli di frode, i problemi di controllo e governance e ogni altra questione che necessita di essere sottoposta all'attenzione del senior management e/o del board.

Interpretazione:

Frequenza e tipologia di contenuti delle comunicazioni sono definiti in maniera condivisa dal responsabile internal auditing, dal senior management e dal board e variano a seconda della rilevanza delle informazioni che devono essere comunicate e dall'urgenza delle azioni correlate che competono al senior management e/o al board.

I report e le comunicazioni del responsabile internal auditing al senior management e al board devono includere informazioni riferite a:

- *il Mandato di internal audit;*
- *l'indipendenza dell'attività di internal audit;*
- *il piano di audit e il suo stato di avanzamento;*
- *i requisiti in termini di risorse;*
- *i risultati delle attività di audit;*
- *la conformità al Codice Etico e agli* Standard *e i piani d'azione volti a gestire eventuali non conformità significativ*e;
- *la risposta del management in merito a eventuali rischi che a giudizio del responsabile internal auditing potrebbero essere inaccettabili per l'organizzazione.*

Questi e altri requisiti riferiti alle comunicazioni del responsabile internal auditing sono illustrati all'interno degli Standard*.*

2070 – Prestatore esterno di servizi e responsabilità organizzativa per l'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 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 controllo dell'organizzazione, tramite un approccio sistematico, rigoroso e risk based. La credibilità e il valore dell'internal auditing sono rafforzati quando gli auditor agiscono in maniera proattiva e le loro valutazioni offrono nuove riflessioni e tengono in considerazione gli impatti futuri.

2110 – Governance

L'attività di internal audit deve valutare e fornire appropriati suggerimenti volti a migliorare il processo di governance dell'organizzazione con riferimento a:

- prendere decisioni di natura strategica e operativa;
- supervisionare i processi di gestione e controllo dei rischi;
- promuovere adeguati valori e principi etici nell'organizzazione;
- garantire l'efficace gestione dell'organizzazione e l'accountability;
- comunicare informazioni su rischi e controlli alle opportune funzioni dell'organizzazione;
- coordinare le attività e il processo di scambio di informazioni tra il board, i revisori esterni, gli internal auditor, gli altri prestatori di servizi di assurance 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 dell'organizzazione supporta 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 dell'organizzazione;*
- *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 dell'organizzazione;*
- *che le informazioni sui rischi vengano raccolte e diffuse tempestivamente all'interno dell'organizzazione, consentendo al personale, al management e al board di adempiere alle rispettive responsabilità.*

L'attività di internal audit può raccogliere le informazioni utili ai fini di questa valutazione nel corso di 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 attività di gestione continua, specifiche valutazioni, o entrambi.

2120.A1 – L'attività di internal audit deve valutare l'esposizione ai rischi relativi alla governance, alle attività e ai sistemi informativi dell'organizzazione, in termini di:

- raggiungimento degli obiettivi strategici dell'organizzazione;
- affidabilità e integrità delle informazioni 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 le modalità con cui l'organizzazione gestisce i rischi di frode.

2120.C1 – Nello svolgimento di incarichi di consulenza, gli internal auditor devono valutare i rischi attinenti agli obiettivi dell'incarico e prestare attenzione a qualsiasi altro rischio significativo.

2120.C2 – Nella valutazione dei processi di gestione del rischio dell'organizzazione, gli internal auditor devono tenere conto delle conoscenze dei rischi acquisite in occasione di incarichi di consulenza.

2120.C3 – Quando assistono il management nella definizione o nel miglioramento dei processi di gestione del rischio, gli internal auditor devono evitare di assumere responsabilità manageriali tramite una gestione diretta dei rischi.

2130 – Controllo

L'attività di internal audit deve assistere l'organizzazione nel mantenere controlli efficaci attraverso la valutazione della loro efficacia ed efficienza e promuovendo il miglioramento continuo.

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 attività e i sistemi informativi dell'organizzazione, relativamente a:

- raggiungimento degli obiettivi strategici dell'organizzazione;
- affidabilità e integrità delle informazioni 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 auditor devono tenere conto delle conoscenze in materia di controllo acquisite in occasione di incarichi di consulenza.

2200 – Pianificazione dell'incarico

Per ciascun incarico gli internal auditor devono predisporre e documentare un piano che comprenda gli obiettivi dell'incarico, l'ambito di copertura, la tempistica e l'assegnazione delle risorse. Il piano deve tenere in considerazione le strategie e gli obiettivi dell'organizzazione nonché i rischi attinenti l'incarico.

2201 – Elementi della pianificazione

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

- le strategie e gli obiettivi dell'attività oggetto di revisione e le modalità con cui l'attività controlla la propria prestazione;
- i rischi significativi per gli obiettivi, risorse e operazioni dell'attività 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 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.

2201.A1 – Nel pianificare un incarico per conto di terze parti esterne all'organizzazione, gli internal auditor 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 auditor devono concordare con i clienti di un incarico di consulenza gli obiettivi, l'ambito di copertura, le rispettive responsabilità e le altre eventuali aspettative. 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 auditor devono effettuare una valutazione preliminare dei rischi afferenti l'attività oggetto di revisione. Gli obiettivi dell'incarico devono rispecchiare i risultati di tale valutazione.

2210.A2 – Al momento della definizione degli obiettivi dell'incarico, gli internal auditor 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 i controlli sono necessari criteri adeguati. Gli internal auditor 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 auditor devono utilizzarli nell'effettuare la propria valutazione. In caso contrario, gli internal auditor devono individuare dei criteri di valutazione adeguati di concerto con il management e/o il board.

Interpretazione:

Le tipologie di criteri possono comprendere:

- *criteri interni (es. direttive e procedure dell'organizzazione);*
- *criteri esterni (es. leggi e regolamenti imposti dagli organismi competenti);*
- *prassi esistenti (es. linee guida di settore e professionali).*

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 includere i sistemi, i documenti, il personale e i beni patrimoniali rilevanti, compresi quelli sotto il controllo di terzi.

2220.A2 – Qualora nel corso di un incarico di assurance emergano opportunità significative di consulenza, si dovrebbe stipulare uno specifico accordo scritto su obiettivi, ambito di copertura, rispettive responsabilità e altre aspettative e i risultati dell'incarico di consulenza dovrebbero essere comunicati secondo gli standard vigenti per gli incarichi di consulenza.

2220.C1 – Nello svolgimento di un incarico di consulenza, gli internal auditor devono assicurarsi che l'ambito di copertura dell'incarico sia sufficientemente ampio per conseguire gli obiettivi concordati. Se, nel corso dell'incarico, gli internal auditor maturano delle riserve in merito all'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 auditor 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 per l'incarico

Gli internal auditor devono determinare le risorse adeguate 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.

Interpretazione:

Il termine "adeguate" è riferito all'insieme di conoscenze, capacità e altre competenze necessarie per dare esecuzione all'incarico. Il temine "sufficienti" è riferito alla quantità di risorse necessarie per portare a termine l'incarico con la dovuta diligenza professionale.

2240 – Programma di lavoro dell'incarico

Gli internal auditor 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 individuare, analizzare, valutare e documentare le informazioni durante lo svolgimento dell'incarico. I programmi di lavoro devono essere approvati prima della loro attuazione e ogni successiva modifica deve essere tempestivamente approvata.

2240.C1 – I programmi di lavoro per gli incarichi di consulenza possono variare nella forma e nel contenuto in funzione della natura dell'incarico.

2300 – Svolgimento dell'incarico

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

2310 – Raccolta delle informazioni

Gli internal auditor 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 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 aiutano l'organizzazione a raggiungere le proprie finalità.

2320 – Analisi e valutazioni

Gli internal auditor devono basare le conclusioni e i risultati dell'incarico su opportune analisi e valutazioni.

2330 – Documentazione delle informazioni

Gli internal auditor devono documentare informazioni sufficienti, affidabili, pertinenti e utili per supportare i risultati e le conclusioni dell'incarico.

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

2330.A2 – Il responsabile internal auditing deve definire i criteri di conservazione della documentazione dell'incarico, indipendentemente dalle modalità di archiviazione. Tali criteri devono essere conformi alle linee guida dell'organizzazione e ai requisiti normativi o di altra natura in materia.

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 e ai requisiti normativi o di altra natura in materia.

2340 – Supervisione dell'incarico

Gli incarichi devono essere opportunamente supervisionati al fine di garantire che gli obiettivi siano 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 auditor e dalla complessità dell'incarico. Il responsabile internal auditing ha la responsabilità generale di supervisionare l'incarico, sia esso svolto da o per conto dell'internal audit. Il responsabile internal auditing può delegare tale supervisione a membri dell'attività di internal audit di provata esperienza. Evidenza dell'avvenuta supervisione deve essere documentata e conservata.

2400 – Comunicazione dei risultati

Gli internal auditor devono comunicare i risultati degli incarichi.

2410 – Modalità di comunicazione

La comunicazione deve includere gli obiettivi, l'ambito di copertura e i risultati dell'incarico.

2410.A1 – La comunicazione finale dei risultati dell'incarico deve contenere le relative conclusioni e raccomandazioni e/o piani d'azione. Laddove appropriato, dovrebbe essere fornito il giudizio dell'internal auditor. Il giudizio deve tenere in considerazione le aspettative del senior management, del board e degli altri stakeholder e deve essere avvalorato da informazioni sufficienti, affidabili, pertinenti e utili.

Interpretazione:

I giudizi espressi a livello di incarico possono consistere in 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 la loro rilevanza.

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

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

2410.C1 – Le comunicazioni relative allo stato di avanzamento e ai risultati 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 e distorsioni ed è fedele ai fatti rilevati. Una comunicazione obiettiva è corretta, imparziale e scevra da pregiudizi ed è il risultato di una valutazione bilanciata ed equilibrata di tutti i fatti e le circostanze rilevanti. Una comunicazione chiara ha senso logico ed è facilmente comprensibile, evita l'uso di termini tecnici non necessari e fornisce tutte le informazioni significative e pertinenti. 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 essenziali per i destinatari, nonché tutte le informazioni e le osservazioni significative atte ad avvalorare raccomandazioni e conclusioni. Una comunicazione tempestiva è puntuale e opportuna nei tempi, in funzione della significatività del problema, e consente al management di intraprendere opportune azioni correttive.

2421 – Errori e omissioni

Se la comunicazione finale contiene significativi errori od omissioni, il responsabile internal auditing deve inviare le informazioni corrette 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*"

Indicare che gli incarichi sono "effettuati in accordo con gli *Standard internazionali per la pratica professionale dell'internal auditing*" è appropriato solo se i risultati del programma di assurance e miglioramento della qualità avvalorano tale affermazione.

2431 – Comunicazione di non conformità dell'incarico

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

- il(i) principio(i) o la(e) regola(e) di condotta del Codice Etico oppure lo(gli) Standard non completamente rispettato(i);
- la(e) motivazione(i) della non conformità;
- l'impatto della non conformità sull'incarico e sui relativi risultati comunicati.

2440 – Divulgazione dei risultati

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

Interpretazione:

Il responsabile internal auditing è tenuto a verificare e approvare la comunicazione finale dei risultati dell'incarico prima dell'emissione degli stessi e a determinare la lista dei destinatari e le modalità della divulgazione. Laddove il responsabile internal auditing deleghi queste funzioni, ne rimarrà in ogni caso pienamente responsabile.

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

2440.A2 – Se non diversamente prescritto da requisiti di legge o normativi, 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 ha la responsabilità di comunicare i risultati finali degli incarichi di consulenza ai clienti.

2440.C2 – Nel corso degli 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 strategie, gli obiettivi e i rischi dell'organizzazione, nonché le aspettative del senior management, del board e degli altri stakeholder e deve essere avvalorato da informazioni sufficienti, affidabili, pertinenti e utili.

Interpretazione:

La comunicazione deve includere:

- *l'ambito di copertura dell'incarico, compreso il periodo di tempo cui si riferisce il giudizio;*
- *le limitazioni all'ambito di copertura;*
- *considerazioni in merito a progetti correlati, indicando l'eventuale ricorso ad altri fornitori di assurance;*
- *una sintesi delle informazioni che supportano il giudizio;*
- *il modello di rischio o di controllo o gli altri criteri usati come fondamento del giudizio complessivo;*
- *il parere, il giudizio o la conclusione complessivi espressi.*

È necessario specificare le motivazioni di un 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 segnalarlo al board.

Interpretazione:

È possibile identificare il rischio accettato dal management attraverso un incarico di assurance o di consulenza, attraverso il monitoraggio dello 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.

Glossario

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.

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 sono stati gestiti efficacemente e che le finalità e gli obiettivi dell'organizzazione saranno raggiunti in modo efficiente ed economico.

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.

Board
Il massimo organo di governo (per esempio consiglio di amministrazione, consiglio di sorveglianza, consiglio dei governatori o dei trustee) che ha la responsabilità di indirizzare e/o di supervisionare le attività dell'organizzazione e di chiederne conto al senior management. Sebbene le regole di governance possano variare tra le diverse giurisdizioni e i vari settori, generalmente il board comprende membri che non fanno parte del management. Laddove non esista un board, il termine "board" negli *Standard* fa riferimento ad un gruppo di soggetti o alla persona incaricata della governance dell'organizzazione. Inoltre, il termine "board" negli *Standard* può riferirsi a un comitato o altro organo al quale l'organo di governo ha delegato determinate funzioni (ad esempio, un comitato di audit, un comitato controllo e rischi…)

Mandato
Il Mandato di internal audit è un documento formale che definisce finalità, poteri e responsabilità dell'attività di internal audit. Il Mandato di internal audit stabilisce la posizione dell'attività di internal audit nell'organizzazione, autorizza l'accesso ai dati, al personale e ai beni aziendali necessari per lo svolgimento degli incarichi e definisce l'ambito di copertura delle attività di internal audit.

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 agli elementi vincolanti dell'International Professional Practices Framework. Il responsabile internal auditing o i collaboratori che riportano al responsabile internal auditing sono in possesso delle opportune qualifiche e certificazioni professionali. La designazione specifica della posizione (Job Title) e/o le responsabilità specifiche del responsabile internal auditing possono variare nelle diverse organizzazioni.

Codice Etico
Il Codice Etico dell'Institute of Internal Auditors (IIA) è composto dai Principi fondamentali per la professione e la pratica dell'internal auditing e dalle Regole di condotta che descrivono le norme comportamentali che gli auditor sono tenuti a osservare. Il Codice Etico si applica sia ai singoli

individui 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.

Conformità
Aderenza a direttive, piani, procedure, leggi, regolamenti, contratti o altri requisiti.

Conflitto di interessi
Qualsiasi relazione che sia o appaia essere contraria agli interessi dell'organizzazione. Il conflitto di interessi pregiudica la capacità di un individuo di adempiere ai propri obblighi e alle proprie responsabilità in maniera obiettiva.

Servizi di consulenza
Servizi di supporto e assistenza al cliente, la cui natura ed estensione vengono 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.

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.

Ambiente di controllo
Atteggiamento e azioni del board e del management rispetto all'importanza del controllo all'interno dell'organizzazione. L'ambiente di controllo 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 operativo del management;
- struttura organizzativa;
- attribuzione di poteri e responsabilità;
- politiche e prassi di gestione del personale;
- competenza del personale.

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.

Principi fondamentali per la pratica professionale dell'internal auditing
I Principi fondamentali per la pratica professionale dell'internal auditing sono il fondamento dell'International Professional Practices Framework e supportano l'efficacia dell'internal audit.

Incarico
La specifica assegnazione di un audit, compito o attività di verifica, siano essi un incarico di internal audit, un'autovalutazione dei controlli, un'investigazione per frode o una

consulenza. Un incarico può includere più compiti o attività, concepiti per raggiungere un insieme specifico di obiettivi interrelati.

Obiettivi dell'incarico
Enunciazioni di carattere generale sviluppate dagli internal auditor che definiscono gli obiettivi attesi dell'incarico.

Giudizio dell'incarico
Valutazione, conclusione e/o altra descrizione dei risultati di un singolo incarico di internal audit, riferita agli aspetti che rientrano negli obiettivi e nell'ambito di copertura dell'incarico.

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.

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

Frode
Qualsiasi atto illegale caratterizzato da falsità, dissimulazione o 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.

Governance
Insieme dei procedimenti e delle strutture messi in atto dal board per informare, indirizzare, gestire e controllare le attività dell'organizzazione nel raggiungimento dei suoi obiettivi.

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).

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

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.

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

Attività di internal audit
Reparto, divisione, team di consulenti o 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 suoi obiettivi, tramite un approccio professionale sistematico finalizzato a valutare e migliorare l'efficacia dei processi di governance, di gestione dei rischi e di controllo.

International Professional Practices Framework
Schema concettuale che organizza l'insieme delle disposizioni normative (authoritative guidance) emanate dall'IIA (The Institute of Internal Auditors) che si suddividono in due categorie: (1) guidance vincolanti e (2) guidance raccomandate.

Deve (devono)
Gli *Standard* utilizzano la dizione "deve (devono)" per indicare un requisito vincolante.

Obiettività
L'attitudine mentale di imparzialità che consente agli internal auditor di svolgere gli 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 auditor non subordinino il loro giudizio a quello di altri.

Giudizio complessivo
Valutazione, conclusione e/o altra descrizione dei risultati presentata dal responsabile internal auditing che 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.

Rischio
Possibilità che si verifichi un evento che può influire sul raggiungimento degli obiettivi. Il rischio si misura in termini di impatto e di probabilità.

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

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.

Dovrebbe (dovrebbero)
Gli *Standard* utilizzano la dizione "dovrebbe (dovrebbero)" per indicare un requisito al quale si presuppone la conformità a meno di circostanze che, sottoposte a un giudizio professionale, ne giustifichino l'inosservanza.

Significatività
Importanza relativa di un fatto, nel contesto nel quale è considerato. Include elementi quantitativi e qualitativi quali la grandezza, la natura, le conseguenze, la rilevanza e l'impatto. Agli internal auditor è richiesto un giudizio professionale quando valutano la significatività dei fatti nel contesto degli obiettivi specifici.

Standard
Enunciato professionale emanato dall'International Internal Audit Standards Board che definisce

i requisiti per lo svolgimento di 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 di dati di test, programmi informatici di audit e computer-assisted audit techniques (CAAT).

***