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).

***