

STANDARD DI CONNOTAZIONE

1000 – Finalità, Poteri e Responsabilità

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

Interpretazione:

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

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

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

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

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

1100 – Indipendenza e Obiettività

L'attività di internal audit deve essere indipendente e gli internal 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, o del suo responsabile, di adempiere senza pregiudizio alle proprie responsabilità. Per raggiungere il livello di indipendenza necessario per esercitare in modo efficace le responsabilità dell'attività di internal audit, il responsabile internal auditing ha diretto e libero accesso al senior management e al board. Ciò può essere conseguito tramite un duplice rapporto organizzativo. Casi di limitazione all'indipendenza devono essere gestiti a livello di singolo auditor, di incarico, funzionale ed organizzativo.

Obiettività è l'attitudine mentale di imparzialità che consente agli internal auditor di svolgere i propri incarichi in un modo che consenta loro di credere nella validità del lavoro svolto e nell'assenza di compromessi sulla qualità. In materia di audit, l'obiettività richiede che gli internal 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 ed organizzativo.

1110 – Indipendenza Organizzativa

Il responsabile internal auditing deve riportare ad un livello dell'organizzazione che consenta 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.

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

1111 – Comunicazione con il board

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

1120 – Obiettività Individuale

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

Interpretazione:

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

1130 – Condizionamenti dell'Indipendenza o dell'Obiettività

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

Interpretazione:

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

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

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

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

1130.C1 – Gli internal 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 o 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:

I termini conoscenze, capacità e altre competenze si riferiscono nel loro complesso alla competenza professionale richiesta agli internal auditor per adempiere efficacemente alle proprie responsabilità professionali. 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 fornite dal “The Institute of Internal Auditors” e da altri organismi professionali riconosciuti.

1210.A1 – Il responsabile internal auditing deve dotarsi di opportuna assistenza e consulenza se gli internal 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 ed il modo con cui l’organizzazione li gestisce, senza aspettarsi che abbiano le competenze proprie di chi ha come responsabilità primaria quella di individuare ed investigare frodi.

1210.A3 – Gli internal auditor devono possedere una sufficiente conoscenza dei rischi e dei controlli chiave dell’information technology, nonché degli strumenti informatici di supporto all’attività di audit per svolgere gli incarichi assegnati. Tuttavia, non è richiesto che tutti gli internal 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 diligenza professionale tenendo in considerazione:

- l’ampiezza del lavoro necessario per raggiungere gli obiettivi dell’incarico;
- la complessità, importanza o la significatività delle attività oggetto di assurance;
- l’adeguatezza e l’efficacia dei processi di governance, risk management e di controllo;
- la probabilità della presenza di significativi errori, frodi o non conformità;
- il costo dell’assurance in relazione ai suoi potenziali benefici.

1220.A2 – Per svolgere l’attività di audit con diligenza professionale, gli internal auditor devono considerare l’utilizzo di strumenti informatici di supporto 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. Comunque, le sole procedure

di assurance, anche quando effettuate con la dovuta diligenza professionale, non garantiscono che tutti i rischi significativi vengano individuati.

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

- le esigenze e le aspettative dei clienti, inclusa la natura, i tempi e le forme di comunicazione dei risultati dell'incarico;
- la complessità e l'ampiezza del lavoro necessario per raggiungere gli obiettivi dell'incarico;
- il costo dell'incarico di consulenza in relazione ai suoi potenziali benefici.

1230 – Aggiornamento Professionale Continuo

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

1300 – Programma di assurance e miglioramento della qualità

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

Interpretazione:

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

1310 – Requisiti del programma di assurance e miglioramento della qualità

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

1311 – Valutazioni interne

Le valutazioni interne devono includere:

- il monitoraggio continuo della prestazione dell'attività di internal auditing;
- verifiche periodiche, effettuate per mezzo di processi di auto-valutazione o da parte di chi all'interno dell'organizzazione abbia adeguate conoscenze delle metodologie di internal audit.

Interpretazione:

Il monitoraggio continuo costituisce parte integrante dell'attività quotidiana di supervisione, verifica e misurazione dell'attività di internal audit. Il monitoraggio continuo è incorporato nelle procedure utilizzate di norma per gestire l'attività di internal

audit, ed è svolto utilizzando processi, strumenti e informazioni necessari per valutare la conformità alla Definizione di Internal Auditing , al Codice Etico ed agli Standard. Le verifiche periodiche sono effettuate con l'obiettivo specifico di valutare la conformità alla Definizione di Internal Auditing, al Codice Etico ed agli Standard. La comprensione di tutti gli elementi dell' International Professional Practices Framework è necessaria per una adeguata conoscenza della metodologia di internal audit.

1312 – Valutazioni Esterne

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

- la necessità di valutazioni esterne più frequenti;
- le qualifiche e l'indipendenza del valutatore o del team di valutatori esterni, inclusa l'esistenza di qualsiasi possibile situazione di conflitto di interessi.

Interpretazione:

Il valutatore o il team di valutatori sono qualificati quando hanno competenze nella pratica professionale dell'attività di internal audit e nei processi di verifica e valutazione esterna. La valutazione di tali competenze deve tener conto dell'esperienza professionale di internal audit e delle credenziali professionali degli individui selezionati per svolgere questo tipo di verifica. La valutazione delle specifiche competenze deve anche tener conto della dimensione e della complessità delle organizzazioni in cui i valutatori hanno prestato la propria opera, nonché della necessità di specifiche conoscenze tecniche, di settore o di attività.

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

1320 – Comunicazione del programma di assurance e miglioramento della qualità

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

Interpretazione:

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

1321 – Uso della dizione “Conforme agli Standard Internazionali per la Pratica Professionale dell’attività di internal audit”

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

1322 – Comunicazione di Non Conformità

In presenza di non conformità alla Definizione di Internal Auditing, al Codice Etico o agli *Standard* che influiscano in modo significativo sull’ambito complessivo di copertura o sull’operatività dell’attività di internal audit, il responsabile internal auditing deve comunicare le non conformità e il relativo impatto al senior management e al board.

STANDARD DI PRESTAZIONE

2000 - Gestione dell'Attività di Internal Audit

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

Interpretazione:

L'attività di internal audit è gestita efficacemente quando:

- *i risultati del lavoro dell'attività di internal audit permettono di raggiungere le finalità e le responsabilità indicate nel Mandato di internal audit;*
- *l'attività di internal audit è conforme alla Definizione di Internal Auditing e agli Standard;*
- *coloro che svolgono l'attività di internal audit dimostrano di conoscere e applicare il Codice Etico e gli Standard.*

2010 – Piano delle Attività di Internal Audit

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

Interpretazione:

Il responsabile internal auditing deve predisporre un piano, basato sulla valutazione dei rischi, tenendo conto dei processi aziendali di gestione del rischio e dei limiti di accettabilità dello stesso stabiliti dal management per le diverse attività o parti dell'organizzazione. Se non esiste un modello di riferimento, il responsabile internal auditing esprimerà un proprio giudizio sui rischi previa consultazione con il senior management e il board.

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

2010.C1 – Il responsabile internal auditing deve decidere se accettare un incarico di consulenza, sulla base delle possibilità di miglioramento della gestione dei rischi, e delle possibilità di aggiungere valore e di migliorare l'operatività dell'organizzazione.

Gli incarichi accettati devono essere inclusi nel piano di audit.

2020 – Comunicazione e Approvazione del Piano

Il responsabile internal auditing deve sottoporre il piano delle attività di internal audit e delle risorse necessarie, incluse eventuali significative variazioni intervenute, al senior management e al board per il relativo esame ed approvazione.

Il responsabile internal auditing deve, inoltre, segnalare l'impatto di un'eventuale carenza di risorse.

2030 – Gestione delle Risorse

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

Interpretazione:

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

2040 – Direttive e Procedure

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

Interpretazione:

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

2050 – Coordinamento delle attività

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

2060 – Informazione periodica al senior management e al board

Il responsabile internal auditing deve 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.

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

Interpretazione:

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

2100 – Natura dell'Attività

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

2110 – Governance

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

- favorire lo sviluppo di appropriati valori e principi etici nell'organizzazione;
- garantire l'efficace gestione dell'organizzazione e l'accountability;
- comunicare informazioni su rischi e controlli alle relative funzioni dell'organizzazione;
- coordinare le attività e il processo di scambio di informazioni tra il board, i revisori esterni, gli internal auditor e il management.

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

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

2110.C1 – Gli obiettivi degli incarichi di consulenza devono essere coerenti con valori ed obiettivi dell'organizzazione.

2120 – Gestione del rischio

L'attività di internal audit deve valutare l'efficacia e contribuire al miglioramento dei processi di gestione del rischio.

Interpretazione:

Determinare se i processi di gestione del rischio siano efficaci è un giudizio che l'internal auditor esprime in base alla propria valutazione dei seguenti aspetti:

- *che gli obiettivi aziendali supportino e siano coerenti con la "mission" aziendale;*
- *che i rischi significativi siano identificati e valutati;*
- *che vengano individuate opportune azioni di risposta ai rischi, al fine di ricondurli entro i limiti di accettabilità per l'azienda;*
- *che le informazioni sui rischi vengano tempestivamente raccolte e diffuse all'interno dell'organizzazione, consentendo al personale, al management e al board di adempiere alle rispettive responsabilità.*

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

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

- affidabilità e integrità delle informazioni contabili, finanziarie e operative;
- efficacia ed efficienza delle operazioni;
- salvaguardia del patrimonio;
- conformità a leggi, regolamenti e contratti.

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

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

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

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

2130 – Controllo

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

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

sistemi informativi dell'organizzazione, relativamente a:

- affidabilità e integrità delle informazioni contabili, finanziarie e operative;
- efficacia ed efficienza delle operazioni;
- salvaguardia del patrimonio;
- conformità a leggi, regolamenti e contratti.

2130.A2 – Gli internal auditor dovrebbero accertare che siano definiti traguardi e obiettivi operativi e di programma, e che questi siano coerenti con quelli dell'organizzazione.

2130.A3 – Gli internal auditor dovrebbero verificare operazioni e programmi dell'organizzazione al fine di valutarne la coerenza con i traguardi e gli obiettivi stabiliti, e per stabilire se operazioni e programmi sono attuati o eseguiti come previsto.

2210.A3 – Per valutare i controlli sono necessari adeguati criteri. Gli internal auditor devono accertare che il management abbia stabilito adeguati criteri 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, devono collaborare con il management nello sviluppo di opportuni criteri di valutazione.

2130.C1 – 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 significative problematiche di controllo.

2130.C2 – Nella valutazione dei processi di controllo dell'organizzazione, gli internal auditor devono tener conto anche delle conoscenze in materia di controllo acquisite nel corso 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.

2201 – Elementi della Pianificazione

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

- gli obiettivi e le modalità di controllo dell'andamento dell'attività oggetto di audit;
- i rischi significativi dell'attività, i propri obiettivi, risorse e operazioni, nonché le modalità di contenimento dei rischi entro i livelli di accettabilità;
- l'adeguatezza e l'efficacia dei processi di gestione dei rischi e di controllo, in riferimento ad un riconosciuto modello di controllo;
- le possibilità di apportare significativi miglioramenti ai processi di gestione dei rischi e di controllo dell'attività oggetto di audit.

2201.A1 – Nel pianificare un incarico per conto di terze parti esterne all'organizzazione, gli internal 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 ciò che di ulteriore ci si attende. Per gli incarichi di maggiore rilevanza tale accordo deve risultare in un documento scritto.

2210 – Obiettivi dell'incarico

Per ciascun incarico devono essere fissati specifici obiettivi.

2210.A1 – Gli internal auditor devono effettuare una valutazione preliminare dei rischi afferenti l'attività oggetto di audit. Gli obiettivi dell'incarico devono riflettere 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 i controlli sono necessari criteri adeguati. Gli internal auditor devono accertare che il management abbia stabilito adeguati criteri 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, devono collaborare con il management nello sviluppo di opportuni criteri di valutazione.

2210.C1 – L'obiettivo degli incarichi di consulenza deve riguardare processi di governance, di gestione dei rischi e di controllo, nella misura concordata con il cliente.

2220 – Ambito di copertura dell'incarico

L'ambito di copertura che viene definito deve essere sufficiente a soddisfare gli obiettivi dell'incarico.

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

2220.A2 – Qualora nel corso di un incarico di assurance, emergano significative opportunità di incarichi di consulenza, si dovrebbe stipulare uno specifico accordo scritto su obiettivi, ambito di copertura, rispettive responsabilità e su ciò che di ulteriore ci si attenda. I risultati raggiunti vanno comunicati secondo gli standard sugli 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 che sono stati concordati. Se nel corso dell'incarico gli internal auditor ritengono di ridefinire l'ambito di copertura, ne devono discutere con il cliente, per decidere se sia opportuno proseguire.

2230 – Assegnazione delle risorse

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

2240 – Programma di Lavoro

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

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

2300 – Svolgimento dell'incarico

Gli internal 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, rilevanti e utili per conseguire gli obiettivi dell'incarico.

Interpretazione:

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

Le informazioni sono utili quando possono aiutare l'organizzazione a raggiungere le proprie finalità.

2320 – Analisi e Valutazioni

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

2330 – Documentazione delle informazioni

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

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

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

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

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 completa responsabilità della supervisione dell'incarico, anche nel caso in cui questo sia svolto per conto dell'internal audit. Il responsabile internal auditing può delegare tale supervisione a internal auditor di provata esperienza. Evidenza dell'avvenuta supervisione deve essere documentata e opportunamente conservata.

2400 – Comunicazione dei risultati

Gli internal auditor devono comunicare i risultati dell'incarico.

2410 – Modalità di Comunicazione

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

2410.A1 – Laddove appropriato, la comunicazione finale dei risultati deve contenere il giudizio complessivo o le conclusioni dell'internal auditor.

2410.A2 – Nelle comunicazioni relative all'incarico gli internal auditor sono incoraggiati a dare riconoscimento alle operazioni dell'organizzazione 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 finali degli incarichi di consulenza possono variare, nella forma e nei contenuti, in funzione della natura dell'incarico e delle esigenze del cliente.

2420 – Qualità della Comunicazione

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

Interpretazione:

Una comunicazione accurata non presenta errori 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. La chiarezza può essere migliorata limitando l'uso di termini tecnici e fornendo sufficienti informazioni di supporto.

Una comunicazione concisa è essenziale, evita formulazioni non necessarie, dettagli superflui e ridondanze. Una comunicazione costruttiva è utile al committente

dell'incarico e all'organizzazione e induce miglioramenti laddove necessari. Una comunicazione completa contiene tutti gli elementi informativi essenziali per i destinatari, tutte le informazioni e le osservazioni significative adatte a supportare raccomandazioni e conclusioni. Una comunicazione tempestiva è puntuale e opportuna nei tempi, in funzione della significatività del problema, consentendo al management di intraprendere appropriate azioni correttive.

2421 – Errori e omissioni nella comunicazione

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

2430 – Uso della dizione “Effettuato in accordo con gli Standard Internazionali per la Pratica Professionale dell’Internal Auditing”

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

2431 Comunicazione di Non Conformità

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

- il principio o la regola di condotta del Codice Etico oppure lo *Standard* che non è stato completamente rispettato;
- le ragioni della non conformità;
- le conseguenze della non conformità sull'incarico e sulla comunicazione dei relativi risultati.

2440 – Divulgazione dei Risultati

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

Interpretazione:

Il responsabile internal auditing, o un suo delegato, deve verificare ed approvare la comunicazione finale dei risultati dell'incarico e decide la lista di distribuzione e le modalità di divulgazione.

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

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

- valutare i potenziali rischi per l'organizzazione;
- consultare il senior management e/o l'ufficio legale a seconda delle circostanze;
- controllare la divulgazione disponendo limitazioni all'utilizzo dei risultati.

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

2440.C2 – Nel corso di incarichi di consulenza è possibile che siano identificate 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.

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 – Risoluzione dei contrasti in merito all'Accettazione del Rischio da parte del Senior Management

Qualora il responsabile internal auditing ritenga che il senior management abbia accettato un livello di rischio residuo inaccettabile per l'organizzazione, ne deve discutere con il senior management.

Se il disaccordo permane, il responsabile internal auditing deve riportare il problema al board per l'opportuna risoluzione.

GLOSSARIO

Adeguato controllo

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

Ambiente di controllo

È costituito dagli atteggiamenti e dalle azioni del board e del management rispetto all'importanza del controllo all'interno.

Esso fornisce la disciplina e l'organizzazione per il raggiungimento degli obiettivi primari del sistema di controllo interno. Gli elementi dell'ambiente di controllo sono i seguenti:

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

Attività di Internal Auditing

Un reparto, una divisione, un team di consulenti o di altri professionisti che forniscono servizi indipendenti ed obiettivi di assurance e di consulenza, concepiti per aggiungere valore e migliorare l'operatività di un'organizzazione.

L'attività di internal audit assiste un'organizzazione nel perseguimento dei propri obiettivi, tramite un approccio professionale sistematico finalizzato a valutare e migliorare l'efficacia dei processi di governance, di gestione dei rischi e di controllo.

Board

Per board si intende l'organo di governo dell'organizzazione; rientrano in tale definizione il consiglio di amministrazione, un organo di supervisione, il vertice di una istituzione pubblica o di un ente legislativo, il consiglio direttivo di un'organizzazione senza fini di lucro o qualsiasi altra entità designata dell'organizzazione compreso il comitato per il controllo interno, cui il responsabile internal auditing può funzionalmente riportare.

Codice Etico (o Codice Deontologico)

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

Condizionamenti

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

Conflitto di interessi

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

Conformità

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

Controllo

Qualsiasi azione intrapresa dal management, dal board o da altri soggetti per gestire i rischi ed 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.

Controlli IT (Information Technology)

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

Deve (devono)

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

Dovrebbe (dovrebbero)

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

Frode

Qualsiasi atto illegale caratterizzato da raggirio, occultamento e abuso di fiducia. Tali atti non fanno ricorso a minacce di violenza o all'uso della forza fisica. Le frodi sono perpetrate da individui e organizzazioni per ottenere denaro, beni o servizi; per evitare il pagamento o la perdita di servizi; o per procurarsi vantaggi personali o aziendali.

Gestione del Rischio

Un processo per 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.

Governance

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

Governance dei sistemi informativi

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

Incarico

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

Indipendenza

L'assenza di condizioni che minacciano l'obiettività, o che ne possano apparire pregiudizievoli. Eventuali situazioni di pregiudizio all'obiettività devono essere gestiti a livello funzionale, organizzativo, di singolo auditor e di incarico.

International Professional Practices Framework

Fornisce uno schema sul "come" deve essere strutturato l'insieme delle *authoritative guidance* emesse dal "The Institute of Internal Auditors", e che comprendono due categorie – (1) vincolanti e (2) fortemente raccomandate.

Livello di accettazione del rischio (*risk appetite*)

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

Mandato di internal audit

Il Mandato di internal audit è un documento formale che definisce finalità, poteri e responsabilità dell'attività di internal audit. Il Mandato deve determinare la posizione dell' internal auditing nell'organizzazione; autorizzare l'accesso ai dati, alle persone e ai beni aziendali necessari per lo svolgimento degli incarichi di audit; definire l'ambito di copertura delle attività di audit.

Obiettivi dell'incarico

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

Obiettività

E' l'attitudine mentale di imparzialità che consente agli internal auditor di eseguire i propri incarichi in modo tale sostenere la validità del risultato finale del proprio lavoro senza pregiudizio sulla qualità. L'obiettività richiede che, in materia di audit, gli internal auditor non subordinino il loro giudizio a quello di altri.

Prestatore esterno di servizi

Una persona o una società esterna all'organizzazione, dotata di particolari conoscenze, competenze ed esperienze in una specifica disciplina.

Processi di controllo

Le politiche, le procedure e le attività che fanno parte di un modello di controllo, progettato per assicurare che i rischi siano contenuti entro il livello di rischio accettabile definito dal processo di gestione del rischio.

Programma di lavoro dell'incarico

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

Responsabile internal auditing (CAE – Chief Audit Executive)

All'interno dell'organizzazione, il responsabile internal auditing è la persona con ruolo direttivo che ha la responsabilità dell'attività di internal audit. Di solito assume la qualifica di "Direttore Internal Auditing". Nel caso in cui le attività di audit siano fornite da prestatori esterni, il responsabile internal auditing è la persona responsabile della supervisione del contratto di servizio e della qualità complessiva di tali attività, e riferisce al senior management e al board in merito alle attività di internal audit e ai follow-up sui risultati degli incarichi di audit. Vengono talvolta usati anche termini come "capo dell'internal audit", "capo dell'ispettorato", eccetera.

Rischio

La possibilità che si verifichi un evento che possa avere un impatto sul raggiungimento degli obiettivi. Il rischio si misura in termini di probabilità e di impatto.

Rischio residuo

Il livello di rischio che rimane dopo le misure introdotte dal management per ridurre l'impatto e la probabilità di accadimento di un evento negativo, comprese le attività di controllo in risposta al rischio.

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 includere incarichi di tipo finanziario, di tipo operativo, di conformità, di sicurezza informatica e di *due diligence*.

Servizi di Consulenza

Servizi di supporto e assistenza al cliente, la cui natura ed estensione vengano concordate con il cliente, intesi 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 in materia. Tra i possibili esempi figurano consulenza, assistenza specialistica, facilitazione e formazione.

Significatività

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

Standard

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

Strumenti informatici di supporto all'audit

Sono strumenti di audit automatizzati, quali software generici di audit, generatori dati di test, programmi computerizzati di audit e computer-assisted audit techniques (CAATs).

Valore aggiunto

Si conferisce valore aggiunto quando, tramite servizi di assurance e di consulenza, vengono migliorate le prospettive di raggiungimento degli obiettivi dell'organizzazione, sono identificati miglioramenti operativi e/o vengono ridotte le esposizioni al rischio.