Global Internal Audit Standards™

The Institute of Internal Auditors

Pubblicato il 9 gennaio 2024

Sommario

Ringraziamenti

L'**Institute of Internal Auditors** è grato agli stakeholder che hanno fornito indirizzo e supporto nello sviluppo dei Global Internal Audit Standards™. L'IIA ringrazia in particolare i membri dell'International Internal Audit Standards Board, un gruppo di Internal Auditor provenienti da tutto il mondo che hanno generosamente offerto il loro tempo e le loro competenze affinché gli Standard elevino la pratica professionale dell'Internal Auditing. L'IIA ringrazia l'International Professional Practices Framework Oversight Council per il suo ruolo essenziale nel garantire che il processo di definizione degli Standard serva l'interesse pubblico, il Professional Certification Board per la sua attività di consulenza e il personale e i consulenti tecnici dell'IIA che hanno permesso il successo dell'implementazione e della gestione di tutti gli aspetti del progetto.

International Professional Practices Framework

In generale, un **framework** fornisce uno schema che facilita lo sviluppo, l'interpretazione e l'applicazione coerenti di un insieme di conoscenze utili a una disciplina o a una professione. L'International Professional Practices Framework (IPPF)® ha lo scopo di organizzare quell'insieme di conoscenze, promulgate dall'Institute of Internal Auditors, per la pratica dell'attività di Internal Auditing e include i Global Internal Audit Standards, i Requisiti Tematici e le Global Guidance.

L'IPPF supporta l'Internal Auditor e i suoi stakeholder, a livello mondiale, nel rispondere attivamente alle sempre maggiori richieste di attività di Internal Auditing di elevata qualità in contesti ambientali e organizzativi che possono variare per scopo, dimensioni e struttura.

Obbligatorio	I **Global Internal Audit Standards** intendono guidare la professione di Internal Auditing a livello mondiale e rappresentano la base per valutare e migliorare la qualità della funzione Internal Audit. Il cuore degli Standard è costituito da 15 principi guida che consentono un Internal Auditing efficace. Ogni principio è supportato da Standard che contengono requisiti, indicazioni per l'implementazione ed esempi di conformità. L'insieme di questi elementi aiuta gli Internal Auditor a rispettare i propri principi e a realizzare il Purpose dell'Internal Auditing.
	I **Requisiti Tematici** sono concepiti per migliorare la coerenza e la qualità delle attività di Internal Auditing relative a specifici rischi oggetto di audit e per supportare gli Internal Auditor che svolgono incarichi in tali aree. Gli Internal Auditor devono conformarsi ai requisiti pertinenti quando l'ambito di un incarico include una delle tematiche identificate. I Requisiti Tematici rafforzano la sempre crescente rilevanza dell'Internal Auditing nell'affrontare l'evoluzione del panorama dei rischi in ogni settore.

Supplementare	Le **Global Guidance** completano gli Standard fornendo informazioni non obbligatorie, consigli e best practice per l'esecuzione delle attività di Internal Auditing. Sono promosse dall'IIA attraverso processi formali di revisione e approvazione. Le Global Practice Guides forniscono esempi di approcci, processi step-by-step ed esempi su argomenti quali: • servizi di assurance e advisory; • pianificazione, svolgimento e comunicazione dell'incarico; • servizi finanziari; • frodi e altri rischi pervasivi; • strategia e gestione della funzione Internal Audit; • settore pubblico; • sostenibilità. Le Global Technology Audit Guides (GTAG)® forniscono agli Auditor le conoscenze necessarie per svolgere servizi di assurance o advisory su rischi e controlli di Information Technology e Information Security di un'organizzazione.

I pilastri dei Global Internal Audit Standards

I **Global Internal Audit Standards** intendono guidare la professione di Internal Auditing a livello mondiale e rappresentano la base per valutare e migliorare la qualità dell'operato della funzione Internal Audit. Il cuore degli Standard è costituito da 15 principi guida che consentono un Internal Auditing efficace. Ogni principio è supportato da Standard che contengono requisiti, indicazioni per l'implementazione ed esempi di conformità. L'insieme di questi elementi aiuta gli Internal Auditor a rispettare i propri principi e a realizzare il Purpose dell'Internal Auditing.

L'Internal Auditing e il pubblico interesse

Per pubblico interesse si intende l'insieme degli interessi sociali ed economici e il benessere complessivo di una società e delle organizzazioni che operano all'interno della stessa (compresi gli interessi dei datori di lavoro, dei dipendenti, degli investitori, della comunità imprenditoriale e finanziaria, dei clienti, dei regulator e del governo). Le questioni di pubblico interesse sono legate al contesto e dovrebbero considerare l'etica, l'uguaglianza, le norme, i valori culturali e i potenziali diversi impatti su determinati individui e sottogruppi della società.

L'Internal Auditing svolge un ruolo fondamentale nel migliorare la capacità di un'organizzazione di servire il pubblico interesse. Sebbene la funzione principale dell'Internal Auditing sia quella di rafforzare la governance, il risk management e i processi di controllo, i suoi effetti si estendono ben oltre. L'Internal Auditing contribuisce infatti alla stabilità e alla sostenibilità complessive di un'organizzazione fornendo assurance sulla sua efficienza operativa, sull'affidabilità del reporting, sulla conformità a leggi e/o regolamenti, sulla salvaguardia delle risorse e sulle questioni etiche. Questo, a sua volta, favorisce la fiducia del pubblico nell'organizzazione e nei sistemi più ampi di cui fa parte.

L'IIA si impegna a stabilire gli Standard con il contributo del pubblico e a beneficio del pubblico. L'International Internal Audit Standards Board è responsabile della definizione e dell'aggiornamento degli Standard nel pubblico interesse. Tutto questo grazie alla supervisione continua di un organismo indipendente, l'IPPF Oversight Council. Il processo include la richiesta di input e la valutazione degli interessi di vari stakeholder, tra cui professionisti di Internal Audit, esperti, enti governativi, regulator, rappresentanti pubblici e altri, in modo che gli Standard riflettano le diverse esigenze e priorità della società.

Applicabilità ed elementi degli Standard

I Global Internal Audit Standards stabiliscono principi, requisiti, indicazioni ed esempi per la pratica dell'Internal Auditing a livello globale. Gli Standard si applicano a qualsiasi individuo o funzione che svolge attività di Internal Auditing, indipendentemente dal fatto che un'organizzazione impieghi auditor interni, si avvalga di un fornitore esterno di servizi o entrambi. Le organizzazioni che ricevono i servizi di Internal Auditing possono variare per settore, scopo, dimensioni, complessità e struttura.

Gli Standard si applicano alla funzione Internal Audit e ai singoli Internal Auditor, incluso il Chief Audit Executive. Sebbene il Chief Audit Executive sia responsabile dell'operato della funzione Internal Audit nel suo complesso e della conformità della stessa a tutti i Principi e agli Standard, ogni Internal Auditor è responsabile della propria conformità ai Principi e agli Standard rilevanti per lo svolgimento delle attività di cui è incaricato, presentate principalmente nella Sezione "II: Etica e professionalità" e nella Sezione "V: Svolgimento delle attività di Internal Auditing".

Gli Standard sono organizzati in cinque Sezioni:

- Sezione I: Purpose dell'Internal Auditing;
- Sezione II: Etica e professionalità;
- Sezione III: Governo della funzione Internal Audit;
- Sezione IV: Gestione della funzione Internal Audit;
- Sezione V: Svolgimento delle attività di Internal Auditing.

Le Sezioni dalla II alla V contengono i seguenti elementi:

- Principi: insieme di requisiti e indicazioni tra loro correlati.
- Standard, che includono:
  - requisiti: pratiche obbligatorie per l'Internal Auditing;
  - indicazioni per l'implementazione: pratiche comuni e raccomandate di cui tenere conto per l'implementazione dei requisiti;
  - esempi di conformità: modi per dimostrare l'implementazione dei requisiti degli Standard.

Gli Standard utilizzano la parola "deve" nei requisiti e le parole "dovrebbe" e "può" per specificare pratiche comuni e raccomandate nelle indicazioni per l'implementazione. Ogni Standard termina con un elenco di esempi di conformità. Gli esempi non devono essere considerati né requisiti, né come gli unici modi per dimostrare la conformità; piuttosto, vengono forniti per supportare le funzioni Internal Audit a prepararsi per i quality assessment, che si basano sulle dimostrazioni di conformità. Gli Standard utilizzano termini specifici, definiti nel glossario, che è necessario comprendere e adottare al fine di implementarli correttamente.

Dimostrazione di conformità agli Standard

I requisiti, le indicazioni per l'implementazione e gli esempi di conformità sono definiti per aiutare gli Internal Auditor a essere conformi agli Standard. Sebbene ci si aspetti la conformità ai requisiti, gli Internal Auditor occasionalmente potrebbero non essere in grado di conformarsi, pur raggiungendo l'intento dello Standard. Le circostanze suscettibili di adeguamenti sono spesso legate a limitazioni delle risorse o a particolarità specifiche di un settore, di un mercato e/o di un'area geografica. In queste circostanze eccezionali, dovrebbero essere implementate azioni idonee a soddisfare la finalità dello Standard in oggetto. Il Chief Audit Executive ha la responsabilità di documentare e trasmettere alle parti interessate le cause dell'impedimento e le azioni adottate. I requisiti e le informazioni correlate sono riportati nello Standard "4.1 Conformità ai Global Internal Audit Standards" e nella Sezione "III: Governo della funzione di Internal Audit", insieme ai relativi Principi e Standard. Sebbene le circostanze che richiedono adeguamenti siano troppo varie per essere elencate, la sezione seguente riconosce due aspetti che suscitano costantemente considerazioni: l'applicazione nelle funzioni Internal Audit di piccole dimensioni e nel settore pubblico.

Applicazione nelle funzioni Internal Audit di piccole dimensioni

La capacità della funzione Internal Audit di conformarsi pienamente agli Standard può essere influenzata dalle sue dimensioni o dalle dimensioni dell'organizzazione in cui opera. In presenza di risorse limitate, portare a termine alcuni compiti può risultare difficile. Inoltre, se la funzione Internal Audit comprende una sola persona, un adeguato programma di assurance e miglioramento della qualità richiederà un supporto esterno alla funzione di Internal Audit (si vedano gli Standard "10.1 Risorse finanziarie", "12.1 Quality assessment interno" e "12.3 Supervisione e miglioramento delle prestazioni dell'incarico").

Applicazione nel Settore Pubblico

Sebbene i Global Internal Audit Standards si applichino a tutte le funzioni Internal Audit, gli Internal Auditor nel settore pubblico operano in un ambiente politico, con strutture di governance, organizzative e di finanziamento che possono differire da quelle del settore privato. La natura di tali strutture e le relative condizioni possono essere influenzate dalla giurisdizione e dal governo in cui opera la funzione Internal Audit. Inoltre, alcuni termini utilizzati nel settore pubblico differiscono da quelli del settore privato e queste differenze possono influenzare il modo in cui gli Standard vengono applicati. Il capitolo "Applicazione dei Global Internal Audit Standards nel Settore Pubblico", che segue la Sezione "V: Svolgimento delle attività di Internal Auditing" descrive le strategie utili per raggiungere la conformità anche in presenza di circostanze e condizioni peculiari come quelle in cui opera l'Internal Audit del settore pubblico.

Glossario

Attività oggetto di Audit – L'oggetto di un incarico di Internal Audit. Alcuni esempi: un'area o una funzione, un'operazione, un processo o un sistema.

Assurance – Attestazione volta ad aumentare il livello di fiducia degli stakeholder nei processi di governance, risk management e controllo di un'organizzazione riguardo ad un'attività, un tema, una situazione oggetto di audit, rispetto ai criteri stabiliti.

Board – Il massimo organo di governo, quale:

- un Consiglio di Amministrazione;
- un Audit Committee;
- un Consiglio Direttivo o di fiduciari;
- un gruppo di funzionari eletti o nominati politicamente;
- un altro organo che abbia autorità sulle funzioni di governance rilevanti.

In un'organizzazione che prevede più di un organo di governo, il termine "Board" si riferisce all'organo o agli organi autorizzati a conferire alla funzione Internal Audit autorità, ruolo e responsabilità appropriate.

Laddove non esista nessuno dei precedenti, "Board" dovrebbe essere riferito a un gruppo di soggetti o alla persona che agisce come massimo organo di governo dell'organizzazione, ad esempio il CEO.

Carte di lavoro – L'insieme della documentazione prodotta dall'Internal Audit durante la pianificazione e lo svolgimento degli incarichi. La documentazione fornisce le informazioni di supporto per la formulazione dei rilievi e delle valutazioni dell'incarico.

Chief Audit Executive (di seguito CAE) – La persona che ha la responsabilità di gestire effettivamente le attività della funzione Internal Audit e di garantirne la qualità dei servizi in conformità con i Global Internal Audit Standards. Job title e/o responsabilità specifiche possono variare da un'organizzazione all'altra.

Competenza – Insieme delle conoscenze e delle capacità sia tecniche che comportamentali.

Compliance – Conformità a leggi, regolamenti, contratti, policy, procedure e altri requisiti.

Conflitto di interessi – Qualsiasi situazione, attività o relazione che possa influenzare, o che sembri influenzare, la capacità di un Internal Auditor di formulare giudizi professionali o di adempiere alle proprie responsabilità in modo obiettivo.

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.

Criteri – Detti anche "criteri di valutazione", definiscono, nell'ambito di un incarico, le caratteristiche attese ("to-be") delle attività oggetto di audit.

Deve – Nei Global Internal Audit Standards viene utilizzato il termine "deve" per specificare un requisito vincolante.

Dovrebbe – Nei Global Internal Audit Standards viene utilizzato il termine "dovrebbe" nelle indicazioni per l'implementazione per descrivere le pratiche raccomandate, ma non vincolanti.

Fornitore di servizi – Risorsa interna o esterna all'organizzazione che fornisce conoscenze, competenze, esperienza e/o strumenti a supporto dei servizi di Internal Auditing.

Frode – Qualsiasi atto intenzionale caratterizzato da inganno, occultamento, disonestà, appropriazione indebita di beni o informazioni, falsificazione o violazione della fiducia perpetrato da individui o organizzazioni per procurarsi un vantaggio personale o commerciale ingiusto o illegale.

Funzione Internal Audit – Un singolo individuo o un gruppo di individui responsabili di fornire servizi di assurance e advisory a un'organizzazione.

Governance – L'insieme dei processi e delle strutture implementate dal Board per produrre informazioni, indirizzare, gestire e monitorare le attività dell'organizzazione nel raggiungimento degli obiettivi.

Impatto – Il risultato o l'effetto di un evento. Un evento può avere un impatto positivo o negativo sulla strategia o sugli obiettivi di business di un'organizzazione.

Incarico – Uno specifico intervento di assurance o di advisory, che include più compiti o attività, concepiti per raggiungere un insieme specifico di obiettivi correlati. Si vedano anche le definizioni di "Servizi di assurance" e "Servizi di advisory".

Indipendenza – Libertà da condizionamenti che possono minacciare la capacità della funzione Internal Audit di assolvere alle proprie responsabilità senza pregiudizi o distorsioni.

Integrità – Atteggiamento caratterizzato dall'adesione a principi morali ed etici, come l'onestà e il coraggio professionale di agire basandosi su fatti rilevanti.

Internal Auditing – L'Internal Auditing è un'attività indipendente e obiettiva di assurance e advisory, finalizzata al miglioramento dell'efficacia e dell'efficienza dell'organizzazione. Assiste l'organizzazione nel perseguimento dei propri obiettivi tramite un approccio professionale sistematico, che genera valore aggiunto in quanto finalizzato a valutare e migliorare i processi di governance, di risk management e di controllo.

Internal Audit Charter – Un documento formale, che include il Mandato della funzione di Internal Audit e il suo posizionamento all'interno dell'organizzazione, i flussi informativi, l'ambito di copertura, le tipologie di attività e altre specifiche.

Mandato di Internal Audit – L'insieme di poteri, ruoli e responsabilità che possono essere conferiti dal Board e/o da leggi e regolamenti alla funzione di Internal Audit.

Manuale di Internal Audit – Documentazione a cura del Chief Audit Executive che definisce le metodologie (policy, processi e procedure) per guidare e gestire gli Internal Auditor della funzione.

Matrice di rischio e controllo – Strumento che facilita lo svolgimento delle attività di Internal Auditing, permettendo la correlazione tra obiettivi aziendali, rischi, processi di controllo e informazioni chiave.

Metodologie – L'insieme di policy, processi e procedure definito dal Chief Audit Executive per guidare la funzione di Internal Audit e migliorarne l'efficacia.

Obiettività – L'attitudine di imparzialità che consente agli Internal Auditor di formulare giudizi professionali, adempiere alle proprie responsabilità e realizzare il Purpose dell'Internal Auditing senza compromessi.

Obiettivi dell'incarico – Dichiarazioni che definiscono il purpose di un incarico e gli specifici risultati attesi.

Outsourcing – Contratto di esternalizzazione dei servizi di Internal Auditing a un fornitore indipendente. L'esternalizzazione può essere completa o parziale (detta anche "cosourcing").

Periodicamente – A intervalli regolari, in base alle esigenze dell'organizzazione e della funzione Internal Audit.

Pianificazione dell'incarico – Processo nel corso del quale gli Internal Auditor raccolgono informazioni, valutano e assegnano le priorità ai rischi rilevanti dell'attività oggetto di audit, stabiliscono gli obiettivi e l'ambito dell'incarico, identificano i criteri di valutazione e definiscono un programma di lavoro.

Piano di Audit – Un documento, sviluppato dal Chief Audit Executive, che identifica gli incarichi e gli altri servizi di Internal Auditing che si prevede di svolgere durante un determinato periodo. Il piano dovrebbe essere risk-based e dinamico e riflettere adeguamenti tempestivi in risposta ai cambiamenti che interessano l'organizzazione.

Probabilità – La possibilità che si verifichi un determinato evento.

Processi di controllo – Le policy, le procedure e le attività disegnate e attuate per assicurare che i rischi siano contenuti entro il livello di risk tolerance di un'organizzazione.

Programma di assurance e miglioramento della qualità – Un programma sviluppato dal Chief Audit Executive per valutare e assicurare la conformità ai Global Internal Audit Standards, il raggiungimento degli obiettivi di performance e il miglioramento continuo della funzione Internal Audit. Il programma prevede valutazioni sia interne che esterne.

Programma di lavoro – Un documento che definisce i compiti da svolgere, la metodologia, gli strumenti necessari per raggiungere gli obiettivi dell'incarico e identifica gli Internal Auditor assegnati allo svolgimento dei compiti previsti. Il programma di lavoro si basa sulle informazioni raccolte durante la pianificazione dell'incarico.

Può – Nei Global Internal Audit Standards viene utilizzato il termine "può" nelle indicazioni per l'implementazione per descrivere le pratiche opzionali per l'implementazione dei requisiti.

Rilievo – L'identificazione, nell'ambito di un incarico, dell'esistenza di una differenza ("gap") tra i criteri ("to-be") e la condition (situazione reale, "as-is") dell'attività oggetto di audit. Possono essere usati anche altri termini, come ad es. "osservazioni".

Rischio – Un evento incerto che può influire positivamente o negativamente sul raggiungimento degli obiettivi.

Rischio inerente – L'insieme dei fattori di rischio interni ed esterni in assenza di attività di controllo.

Rischio residuo – La parte di rischio inerente che permane dopo aver attuato le azioni di prevenzione, mitigazione e controllo.

Risk appetite – Indicatore del livello e del tipo di rischio che una società è disposta ad assumere nel perseguimento degli obiettivi strategici.

Risk assessment – L'insieme delle azioni volte a individuare e analizzare i rischi rilevanti per capirne gli impatti sul raggiungimento degli obiettivi di un'organizzazione. La significatività dei rischi viene generalmente valutata in termini di impatto e probabilità.

Risk management – L'insieme delle azioni volte a identificare, valutare, gestire e controllare potenziali eventi o situazioni, al fine di fornire una reasonable assurance sul raggiungimento degli obiettivi dell'organizzazione.

Risk tolerance – Devianza massima dal risk appetite consentita nel perseguimento degli obiettivi strategici.

Risultati delle attività di Internal Auditing – Esiti, come le valutazioni dell'incarico, le tematiche di rilievo (ad es. le prassi in atto o le root cause) e le conclusioni a livello di business unit o organizzazione.

Risultati dell'incarico – I rilievi e la valutazione di un incarico. I risultati dell'incarico possono anche includere le raccomandazioni e/o i piani d'azione concordati.

Root cause – Il problema principale o il motivo sottostante alla differenza tra i criteri e la condition rispetto a un'attività oggetto di Audit.

Scetticismo professionale – Atteggiamento caratterizzato da una valutazione critica dell'affidabilità delle informazioni.

Servizi di advisory – Servizi la cui natura e ambito vengono concordati con gli stakeholder dell'organizzazione, attraverso i quali gli Internal Auditor possono dare supporto senza fornire assurance, né assumersi responsabilità manageriali. Tra gli esempi troviamo la consulenza sulla progettazione e implementazione di nuove policy, processi, sistemi e prodotti; indagini investigative; formazione; facilitazione di confronti e discussioni su rischi e controlli.

Servizi di assurance – Servizi attraverso i quali gli Internal Auditor svolgono esami obiettivi allo scopo di fornire assurance (sopra definita). Alcuni esempi: incarichi di compliance, financial, operational e tecnologici. Gli Internal Auditor possono fornire una limited o una reasonable assurance a seconda della natura, della tempistica e dell'estensione delle procedure eseguite.

Settore pubblico – Enti governativi, agenzie, istituzioni, imprese e altri enti controllati o finanziati con fondi pubblici, che erogano programmi e servizi o forniscono beni al pubblico.

Significatività – Importanza relativa di un fatto rispetto al contesto in cui è considerato. Include elementi quantitativi e qualitativi quali la grandezza, la natura, le conseguenze, la rilevanza e l'impatto. Agli Internal Auditor è richiesta l'applicazione del giudizio professionale per la valutazione della significatività dei fatti rispetto al contesto e agli obiettivi di riferimento.

Stakeholder – Ciascuno dei soggetti aventi un interesse diretto o indiretto rispetto ai risultati o alle attività di un'organizzazione. Gli stakeholder possono includere il Board, il management, i dipendenti, i clienti, i fornitori, gli azionisti, gli enti regolatori, le istituzioni finanziarie, gli Auditor esterni, il pubblico e altri.

Supervisore dell'incarico – Un Internal Auditor responsabile della supervisione di un incarico di Audit; la supervisione può comprendere la revisione e approvazione di programma di lavoro, carte di lavoro, comunicazione finale e prestazioni dell'incarico, così come la formazione e l'assistenza agli Internal Auditor. Il Chief Audit Executive può essere il supervisore dell'incarico o può delegare tale responsabilità.

Top Management – Il più alto livello di dirigenza di un'organizzazione che è in ultima analisi responsabile nei confronti del Board per l'esecuzione delle decisioni strategiche dell'organizzazione; in genere è un gruppo di persone che include il Chief Executive Officer.

Valutazione dell'incarico – Giudizio professionale complessivo degli Internal Auditor sui rilievi dell'incarico. La valutazione dovrebbe indicare se l'esito è stato soddisfacente o insoddisfacente.

Sezione I: Purpose dell'Internal Auditing

Il Purpose ha l'obiettivo di supportare gli Internal Auditor e gli stakeholder nel comprendere e divulgare il valore dell'Internal Auditing.

Purpose

L'Internal Auditing rafforza la capacità dell'organizzazione di creare valore e di mantenerlo nel tempo, fornendo al Board e al management assurance, advisory, approfondimenti e previsioni, in modo indipendente, obiettivo e risk-based.

L'Internal Auditing supporta l'organizzazione:

- nel raggiungimento dei propri obiettivi;
- nella governance, nel risk management e nei processi di controllo;
- nei processi decisionali e di supervisione;
- nella costruzione della reputazione e della credibilità nei confronti degli stakeholder;
- nella capacità di servire l'interesse pubblico.

L'Internal Auditing è maggiormente efficace quando:

- le attività sono svolte da professionisti competenti, in conformità con i Global Internal Audit Standards, che sono definiti nell'interesse pubblico;
- la funzione Internal Audit è indipendente e risponde direttamente al Board;
- gli Internal Auditor sono liberi da qualsiasi condizionamento e si impegnano a effettuare valutazioni obiettive.

Sezione II: Etica e professionalità

I **Principi** e gli **Standard** contenuti nella Sezione II "Etica e professionalità" dei Global Internal Audit Standards sostituiscono il precedente Codice Etico dell'IIA e delineano i comportamenti attesi da parte dei professionisti di Internal Audit, compresi i CAE e qualsiasi altro individuo o entità che fornisca servizi di Internal Auditing. La conformità a questi Principi e questi Standard consolida la fiducia nei confronti dell'Internal Auditing, sviluppa una cultura etica all'interno della funzione Internal Audit e rafforza l'affidabilità del lavoro dell'Internal Audit e del suo giudizio.

Tutti gli Internal Auditor sono tenuti alla conformità agli Standard contenuti nella Sezione II "Etica e professionalità" anche quando sono chiamati a rispettare altri codici etici, di comportamento o di condotta, come ad esempio quelli dell'organizzazione in cui operano. Il fatto che un particolare comportamento non sia menzionato all'interno di questa sezione non esclude che possa essere considerato inaccettabile o inappropriato.

Sebbene ogni Internal Auditor ne sia personalmente responsabile, il CAE deve favorire e promuovere la conformità ai Principi e agli Standard contenuti nella Sezione II "Etica e professionalità", attraverso attività di formazione e orientamento. Il CAE può scegliere di delegare alcune responsabilità legate al raggiungimento della conformità, ma rimane comunque responsabile dell'etica e della professionalità dimostrate dalla funzione Internal Audit.

Principio 1 Dimostrare integrità

Gli Internal Auditor dimostrano integrità attraverso il proprio lavoro e il proprio comportamento.

Per integrità si intende quell'atteggiamento caratterizzato dall'adesione a principi morali ed etici, come l'onestà e il coraggio di agire basandosi su fatti rilevanti, anche in caso di eventuali pressioni esterne o quando ciò rischiasse di creare potenziali conseguenze personali o professionali. Ci si aspetta, in altri termini, che gli Internal Auditor dicano la verità e facciano la cosa giusta, anche quando ciò risulta scomodo o difficile.

L'integrità è alla base degli altri principi dell'etica e della professionalità, ad esempio l'obiettività, la competenza, la diligenza professionale e la riservatezza ed è essenziale per stabilire relazioni di fiducia e ottenere rispetto.

Standard 1.1 Onestà e coraggio professionale

Requisiti

Gli Internal Auditor devono svolgere il proprio lavoro con onestà e coraggio professionale. Devono essere attendibili, precisi, chiari, aperti e rispettosi in tutte le relazioni e comunicazioni professionali, anche quando esprimono scetticismo o punti di vista differenti. Non devono rilasciare dichiarazioni false, fuorvianti o ingannevoli, né nascondere o omettere dalle comunicazioni alcun rilievo o altre informazioni pertinenti. Gli Internal Auditor devono, inoltre, divulgare tutti i fatti rilevanti a loro noti che, se non divulgati, potrebbero influire sui processi decisionali dell'organizzazione.

Gli Internal Auditor devono dimostrare coraggio professionale, comunicare in modo veritiero e adottare le misure appropriate, anche quando si trovano di fronte a dilemmi o situazioni difficili.

Il CAE deve garantire un ambiente di lavoro in cui gli Internal Auditor si sentano liberi di esprimere i risultati di un incarico, legittimi e supportati da evidenze, che siano positivi o meno.

Indicazioni per l'implementazione

Gli Internal Auditor dovrebbero migliorare la propria consapevolezza e comprensione dell'onestà e del coraggio professionale attraverso formazione continua in materia di etica. Mentre la formazione aiuta a creare consapevolezza in situazioni ipotetiche, il tutoring, la supervisione e l'esperienza sul campo consentono agli Internal Auditor di apprendere e mettere in pratica abilità come il tatto e la comunicazione rispettosa, necessarie per agire con coraggio professionale nelle situazioni reali. Quando gli Internal Auditor si trovano in situazioni che mettono alla prova la loro onestà o il loro coraggio professionale, dovrebbero condividere queste circostanze con un supervisore al fine di delineare la migliore linea d'azione.

Per supportare gli Internal Auditor, il CAE dovrebbe organizzare momenti formativi, nonché di confronto su situazioni ipotetiche e reali che richiedono scelte etiche. Una gestione efficace della funzione Internal Audit necessita di un'adeguata supervisione degli incarichi e di revisioni periodiche delle performance degli Internal Auditor. Ad esempio, quando approva i programmi o esamina le carte di lavoro di un incarico, un supervisore può fornire agli Internal Auditor indicazioni per aiutarli ad affrontare situazioni che potrebbero rappresentare una minaccia per la loro onestà e integrità. Nell'ambito della valutazione delle performance degli Internal Auditor, il CAE può anche richiedere un parere sulla loro onestà e coraggio professionale agli stakeholder con cui interagiscono.

Esempi di conformità

- Un piano formativo che includa interventi in materia di etica.
- Documenti che attestano la partecipazione degli Internal Auditor alle attività formative in materia di etica.
- Valutazioni delle performance che comprendono tra gli obiettivi l'onestà e il coraggio professionale.
- Feedback da parte dei principali stakeholder in merito all'onestà e al coraggio professionale degli Internal Auditor.

Standard 1.2 Aspettative etiche dell'organizzazione

Requisiti

Gli Internal Auditor devono comprendere, rispettare e soddisfare le aspettative legittime ed etiche dell'organizzazione e devono essere in grado di riconoscere i comportamenti che vanno contro queste aspettative.

Gli Internal Auditor devono incoraggiare e promuovere all'interno dell'organizzazione una cultura basata sull'etica. Se individuano un comportamento non coerente con le aspettative etiche dell'organizzazione, devono segnalare il problema secondo quanto previsto dalle policy e dalle procedure applicabili.

Indicazioni per l'implementazione

Le aspettative etiche di un'organizzazione sono generalmente raccolte in un codice etico, in un codice di condotta e/o all'interno di policy relative al comportamento professionale e alla condotta etica. Tali policy, unitamente agli obiettivi e ai processi dell'organizzazione orientati alla promozione dell'etica e dei valori aziendali, forniscono la base per una cultura etica.

Il piano di Audit può includere valutazioni dei rischi legati all'etica dell'organizzazione per determinare se le policy e i processi di controllo esistenti tengono nella dovuta considerazione questi rischi. Ad esempio, le policy dell'organizzazione possono specificare: i criteri e il processo per la gestione e la comunicazione delle questioni etiche, quali attori debbano ricevere le comunicazioni e il protocollo per l'escalation in caso di problemi irrisolti. Il CAE dovrebbe anche determinare una metodologia per affrontare le questioni etiche e condividerla con il Board e il Top Management per garantire allineamento nella strategia.

Gli Internal Auditor dovrebbero considerare i rischi e i controlli relativi all'etica durante i singoli incarichi e se identificano, all'interno dell'organizzazione, un comportamento non coerente con le aspettative etiche, dovrebbero comunicare i propri dubbi secondo la metodologia stabilita dal CAE, che tiene conto di policy e processi dell'organizzazione, nonché di leggi e/o regolamenti.

Se gli Internal Auditor stabiliscono che un Top Manager si è comportato in modo non coerente con le aspettative etiche dell'organizzazione, siano esse documentate in un codice di condotta, in un codice etico o in altro documento, il CAE dovrebbe segnalare la violazione al Board. Se un problema relativo all'etica riguarda il Presidente del Board, il CAE dovrebbe segnalarlo all'intero Board. Gli Internal Auditor dovrebbero poi dare seguito alle questioni etiche che coinvolgono il Board o il Top Management e verificare che siano state intraprese le appropriate azioni correttive.

Esempi di conformità

- Registri o altre evidenze della partecipazione degli Internal Auditor a workshop, corsi di formazione o incontri in cui siano state condivise le aspettative e le questioni etiche.
- Moduli firmati dai singoli Internal Auditor che attestano la loro conoscenza delle policy e delle procedure etiche e il loro impegno a rispettarle.
- Il piano di Audit, il programma di lavoro o le carte di lavoro che mettano in evidenza che obiettivi, rischi e processi di controllo relativi all'etica sono stati presi in considerazione.
- Documentazione che dimostri che le questioni etiche sono state comunicate al Board, al Top Management e agli Organismi preposti in conformità con le policy dell'organizzazione e le relative leggi e/o regolamenti.

Standard 1.3 Comportamento legale ed etico

Requisiti

Gli Internal Auditor non devono essere coinvolti in alcuna attività che possa essere considerata illegale o poco onorevole o che possa danneggiare l'organizzazione, i suoi dipendenti o la professione di Internal Audit.

Gli Internal Auditor devono comprendere e rispettare le leggi e/o i regolamenti specifici del settore e dell'area in cui opera l'organizzazione, inclusi quelli relativi alla divulgazione delle informazioni.

Se gli Internal Auditor individuano delle violazioni, devono segnalarlo alle persone fisiche o giuridiche che hanno l'autorità di intraprendere le azioni correttive adeguate, come specificato nelle leggi, nei regolamenti, nelle policy e nelle procedure di riferimento.

Indicazioni per l'implementazione

Se le policy aziendali non sono sufficientemente specifiche per regolamentare le situazioni che la funzione Internal Audit incontra, il CAE potrebbe sviluppare e implementare una metodologia per indicare quali azioni intraprendere in risposta alle violazioni di cui vengono a conoscenza. Tale metodologia può includere anche la definizione delle azioni correttive necessarie per affrontare la violazione.

Il CAE dovrebbe stabilire una metodologia per garantire che gli Internal Auditor siano sottoposti ad adeguata supervisione, conformemente ai Global Internal Audit Standards e tengano comportamenti allineati ai valori etici e professionali.

Alcuni esempi di comportamenti disdicevoli:

- attuare prevaricazioni, molestie o discriminazioni;
- mentire o ingannare intenzionalmente gli altri, falsificare le proprie competenze o qualifiche professionali (affermando, ad esempio, di essere in possesso di una certificazione anche nel caso in cui essa sia scaduta o inattiva, sia stata revocata o addirittura mai conseguita);
- pubblicare intenzionalmente false informazioni o comunicazioni o consentire o ancora incoraggiare altri a farlo, favorire la minimizzazione, l'occultamento o l'omissione di rilievi, conclusioni o valutazioni dell'incarico di Internal Audit;
- sottovalutare attività illegali, anche se tollerate dall'organizzazione;
- divulgare informazioni riservate senza un'adeguata autorizzazione;
- svolgere servizi di Internal Auditing in presenza di limitazioni non dichiarate all'obiettività o all'indipendenza;
- dichiarare che la funzione Internal Audit opera in conformità con i Global Internal Audit Standards senza averne prove a supporto;
- non assumersi la responsabilità degli errori.

Esempi di conformità

- Registri o altre evidenze della partecipazione degli Internal Auditor alla formazione su leggi, regolamenti e comportamenti etici e professionali.
- Evidenze dell'impegno degli Internal Auditor ad agire in conformità con le aspettative legali e professionali.
- Definizione di metodologie per documentare la gestione di comportamenti illegali o disdicevoli da parte di Internal Auditor ed eventuali violazioni di norme e regolamenti da parte di altri soggetti interni all'organizzazione.
- Comunicazioni documentate tra gli Internal Auditor e i loro supervisori e/o consulenti legali che affrontano problemi relativi ad azioni illegali o non professionali.
- Evidenza della revisione delle carte di lavoro.
- Comunicazione finale dell'incarico, ove prevista.

Principio 2 Mantenere l'obiettività

Gli Internal Auditor adottano comportamenti imparziali e obiettivi, sia durante l'esecuzione dei servizi di Internal Auditing, sia nel prendere decisioni.

Per obiettività si intende l'attitudine di imparzialità che consente agli Internal Auditor di formulare giudizi professionali, adempiere alle proprie responsabilità e realizzare il Purpose dell'Internal Auditing senza compromessi.

Una funzione Internal Audit indipendente mette gli Internal Auditor nelle condizioni di riuscire a garantire l'obiettività.

Standard 2.1 Obiettività individuale

Requisiti

Gli Internal Auditor devono garantire l'obiettività professionale in tutti gli aspetti dell'esecuzione dei servizi di Internal Auditing. L'obiettività richiede che gli Internal Auditor adottino un approccio mentale imparziale e che esprimano giudizi basati su valutazioni ponderate di tutti gli aspetti rilevanti.

Gli Internal Auditor devono essere consapevoli dei loro potenziali pregiudizi e devono saperli gestire in modo opportuno.

Indicazioni per l'implementazione

Obiettività significa che gli Internal Auditor svolgono la propria attività senza compromessi o influenze di altri. I Global Internal Audit Standards, le policy e le attività formative organizzate dal CAE, sostengono l'obiettività fornendo requisiti, procedure e linee guida che stabiliscono un approccio sistematico e disciplinato per la raccolta e la valutazione delle informazioni, al fine di fornire un giudizio obiettivo dell'attività oggetto di audit. La formazione può aiutare gli Internal Auditor a comprendere meglio gli scenari che compromettono l'obiettività e fornisce loro gli strumenti necessari per affrontarli nel migliore dei modi.

Un approccio mentale imparziale e libero da qualsiasi influenza è essenziale per effettuare valutazioni obiettive e fornire assurance e advisory al Board e al Top Management. Gli Internal Auditor dovrebbero quindi sviluppare consapevolezza nei confronti di quelle situazioni, attività e relazioni che possono influenzare la loro capacità di essere obiettivi.

Gli Internal Auditor dovrebbero tenere in considerazione la propensione dell'essere umano a interpretare erroneamente le informazioni o a fare supposizioni, che compromettono la capacità di valutare obiettivamente le informazioni e le evidenze.

Alcuni esempi di distorsioni includono:

- la mancanza di giudizio critico quando si esamina il proprio lavoro, che può portare a trascurare errori o carenze (self-review bias);
- i condizionamenti dell'abitudine, ovvero fare supposizioni basate su esperienze passate, che possono compromettere lo scetticismo professionale (familiarity bias);
- i pregiudizi che possono condurre ad una errata interpretazione delle informazioni, basata su preconcetti su cultura, etnia, genere, ideologia, razza o altro (unconscious bias).

Esempi di conformità

- I riferimenti alla responsabilità degli Internal Auditor di mantenere l'obiettività contenuti nell'Internal Audit Charter.
- Policy e procedure relative all'obiettività.
- Registri o altre evidenze della formazione pianificata e completata in materia di obiettività.
- Dichiarazioni che attestano la consapevolezza da parte degli Internal Auditor dell'importanza dell'obiettività e l'obbligo di comunicare eventuali limitazioni.
- Disclosure formale di potenziali conflitti di interesse o altre limitazioni all'obiettività.
- Note dei supervisori e dei tutor degli Internal Auditor.

Standard 2.2 Protezione dell'obiettività

Requisiti

Gli Internal Auditor devono riconoscere ed evitare o mitigare le limitazioni effettive, potenziali e percepite all'obiettività.

Gli Internal Auditor non devono accettare alcun elemento tangibile o intangibile, come un regalo, una ricompensa o un favore, che possa compromettere o si presume che possa compromettere l'obiettività.

Gli Internal Auditor devono evitare conflitti di interesse e non devono farsi influenzare né dai propri interessi, né da quelli di altri, Top Management incluso, né tantomeno dal contesto politico o da altri aspetti dell'ambiente circostante.

Quando vengono svolte attività di Internal Audit:

- gli Internal Auditor devono astenersi dal valutare attività specifiche di cui sono stati precedentemente responsabili. Si presume infatti che, se un Internal Auditor fornisce servizi di assurance per un'attività di cui è stato responsabile nei 12 mesi precedenti, l'obiettività possa essere compromessa;
- se la funzione Internal Audit deve fornire servizi di assurance laddove in precedenza aveva svolto servizi di advisory, il CAE deve confermare che la natura dei servizi di advisory non pregiudica l'obiettività e deve assegnare le risorse in modo tale da poter garantire l'obiettività individuale. Gli incarichi di assurance per le funzioni di cui è responsabile il CAE devono essere supervisionati da un soggetto indipendente esterno alla funzione Internal Audit;
- se gli Internal Auditor devono fornire servizi di advisory relativi ad attività di cui sono stati precedentemente responsabili, devono comunicare le potenziali limitazioni all'obiettività alla parte che richiede i servizi prima di accettare l'incarico.

Il CAE deve definire delle metodologie per gestire le limitazioni all'obiettività e gli Internal Auditor devono condividerle e intraprendere le azioni correttive più appropriate.

Indicazioni per l'implementazione

L'obiettività è compromessa quando situazioni, attività o relazioni possono influenzare i giudizi e le decisioni degli Internal Auditor in modo tale da modificare i rilievi e le conclusioni dell'incarico di Internal Audit. Le limitazioni all'obiettività possono esistere, di fatto o in apparenza, anche quando non sono intenzionali. L'obiettività può essere percepita da altri come limitata anche in assenza di fatti specifici. Gli Internal Auditor dovrebbero quindi esprimere un giudizio sia sulle circostanze che possono compromettere l'obiettività, sia su quelle che si presume possano comprometterla.

I conflitti di interesse sono situazioni in cui un Internal Auditor ha un interesse professionale o personale che può rendere difficile lo svolgimento obiettivo delle attività di Internal Auditing. I conflitti di interesse possono dare un'impressione di inappropriatezza che potrebbe minare la fiducia in un Internal Auditor, nella funzione Internal Audit e nella professione di Internal Audit in generale, anche se non ne derivano veri e propri atti che possono essere considerati poco etici o impropri.

Esempi di conflitti di interesse includono situazioni, attività e relazioni che possono, di fatto o in apparenza:

- essere contrarie o in conflitto con gli interessi dell'organizzazione;
- dare luogo a un potenziale indebito guadagno personale finanziario o di altra natura;
- essere intraprese esclusivamente allo scopo di proteggersi da perdite o danni potenziali o effettivi;
- avere finalità di nepotismo o favoritismi individuali.

Le metodologie della funzione Internal Audit dovrebbero specificare aspettative e requisiti in merito a:

- accettazione di omaggi, favori e ricompense;
- identificazione delle situazioni che possono compromettere l'obiettività;
- reazioni appropriate a fronte di casi di limitazione all'obiettività.

Molte organizzazioni hanno una policy relativa all'accettazione di regali, ricompense e favori, ad esempio una policy che limita il valore degli omaggi che possono essere accettati. Dal momento che garantire l'obiettività è fondamentale nello svolgimento delle attività di Internal Auditing, il CAE potrebbe essere sottoposto a policy più stringenti rispetto a quelle in essere nell'organizzazione. Anche gli Internal Auditor dovrebbero seguire delle policy più restrittive e valutare attentamente se l'accettazione di un omaggio, di una ricompensa o di un favore possa essere percepita come un condizionamento del loro giudizio o un ringraziamento per rilievi, valutazioni o risultati favorevoli.

Le policy dell'organizzazione e/o della funzione Internal Audit possono vietare specifiche attività o relazioni che potrebbero creare conflitti di interesse. Gli Internal Auditor dovrebbero essere consapevoli del fatto che le relazioni personali e/o che implicano legami finanziari, come gli investimenti, al di fuori del lavoro, possono essere o sembrare conflitti di interesse.

Il CAE dovrebbe prendere precauzioni per ridurre le potenziali limitazioni all'obiettività che possono derivare dalla definizione dei sistemi di valutazione delle performance e degli accordi di remunerazione e incentivanti. Esempi di accordi retributivi che possono compromettere l'obiettività includono:

- basare le valutazioni delle performance e gli accordi di remunerazione principalmente su indagini o input provenienti dal management dell'area oggetto di audit;
- misurare le performance rispetto al numero di rilievi identificati durante l'incarico, alla crescita dei ricavi dell'attività in esame o ai risparmi o alla riduzione di posti di lavoro imposti all'area oggetto di audit;
- consentire al management di elargire compensi indiretti sotto forma di regali e omaggi.

Gli Internal Auditor dovrebbero basarsi sulla loro cognizione di obiettività e conoscenza di policy e procedure per valutare se situazioni, attività o relazioni possano compromettere, o si possa presumere che compromettano, la loro obiettività. Dovrebbe essere considerato anche il percepito delle altre persone.

I requisiti per l'assegnazione delle risorse e della supervisione nell'ambito degli incarichi hanno lo scopo di garantire che gli Internal Auditor assegnati non siano stati recentemente responsabili di alcuna attività all'interno dell'area oggetto di audit che possa influenzare il loro punto di vista, conferire loro un interesse personale o favorire la percezione che la loro obiettività possa essere compromessa. Per ogni incarico, gli Internal Auditor che svolgono le attività o le supervisionano, dovrebbero essere indipendenti e non avere nessun legame con l'area oggetto di audit.

Al momento di assegnare le risorse a un incarico, il CAE, o un supervisore designato, dovrebbe condividere i dettagli dell'incarico con gli Internal Auditor, per identificare eventuali limitazioni all'obiettività, siano esse reali o potenziali.

Il confronto dovrebbe includere l'esame di eventuali limitazioni precedentemente comunicate. Nell'ambito del processo di supervisione degli incarichi, le carte di lavoro vengono esaminate per garantire che rilievi e valutazioni siano adeguatamente supportati. La supervisione dell'incarico offre inoltre l'opportunità agli Internal Auditor più esperti di fornire feedback e mentoring in merito a potenziali problemi di obiettività (si vedano gli Standard "12.3 Supervisione e miglioramento delle performance dell'incarico" e "13.5 Assegnazione delle risorse"). Quando una limitazione è inevitabile, essa dovrebbe essere indicata e mitigata, come descritto nello Standard "2.3 Comunicazione di limitazioni all'obiettività".

Esempi di conformità

- Policy e procedure per l'identificazione di potenziali limitazioni all'obiettività e delle necessarie misure di protezione.
- Registri o altre evidenze di attività di formazione sull'obiettività.
- Documentazione attraverso la quale gli Internal Auditor attestano di non avere limitazioni note o di aver comunicato quelle potenziali.
- Feedback sulla percezione dell'obiettività degli Internal Auditor, come ad esempio sondaggi presso gli stakeholder.
- Note sulla supervisione.
- Piano di remunerazione.
- Verbali delle riunioni del Board in cui sono state discusse le limitazioni all'obiettività.
- Piani che mostrano le misure alternative adottate per realizzare le attività del piano di Audit nei casi di limitazioni inevitabili all'obiettività.
- Risultati del quality assessment esterno effettuato da un valutatore indipendente.

Standard 2.3 Comunicazione di limitazioni all'obiettività

Requisiti

Se l'obiettività è compromessa, o appare come tale, i dettagli delle limitazioni devono essere comunicati tempestivamente alle parti interessate.

Se gli Internal Auditor vengono a conoscenza di limitazioni che possono influire sulla loro obiettività, devono comunicarlo al CAE o al supervisore designato. Se il CAE stabilisce la presenza di limitazioni che influenzano la capacità di un Internal Auditor di svolgere i propri compiti in modo obiettivo, deve discuterne con il management responsabile dell'area oggetto di audit, con il Board e/o con il Top Management e definire le azioni più appropriate per risolvere la situazione.

Se dopo il completamento di un incarico vengono riscontrate limitazioni che influiscono sull'affidabilità, reale o percepita dei rilievi, delle raccomandazioni e/o delle valutazioni dell'incarico, il CAE deve discutere il problema con il management dell'area oggetto di audit, con il Board, con il Top Management e/o altri stakeholder interessati e definire le azioni più appropriate per risolvere la situazione (si veda lo Standard "11.4 Errori e omissioni").

Se l'obiettività del CAE è compromessa, o appare come tale, egli deve informare il Board delle limitazioni esistenti (si veda lo Standard "7.1 Indipendenza organizzativa").

Indicazioni per l'implementazione

Le caratteristiche della comunicazione relativa alla presenza di limitazioni all'obiettività sono generalmente definite nelle metodologie della funzione Internal Audit e descrivono le azioni da intraprendere per affrontare ciascuna tipologia di limitazione. L'approccio da tenere per la comunicazione delle limitazioni e le conseguenti azioni correttive, viene generalmente definito dal CAE in accordo con il Board e il Top Management.

Se non è possibile evitare una limitazione all'obiettività, il CAE può prendere in considerazione diverse opzioni per gestirla, ad esempio:

- rivedere l'assegnazione degli Internal Auditor al fine di rimuovere dall'incarico chi è interessato dalla limitazione;
- riprogrammare un incarico per garantire l'impiego di personale adeguato;
- rivedere l'ambito di un incarico;
- esternalizzare l'esecuzione o la supervisione dell'incarico.

Qualora durante la pianificazione dell'incarico sorgesse una preoccupazione in merito alla percezione di limitazioni all'obiettività, il CAE può scegliere di condividerla con il management dell'area oggetto di audit e/o con il Top Management, spiegare perché l'esposizione al rischio è minima e come sarà gestita e documentare la discussione e la decisione finale su come procedere.

Lo Standard "7.1 Indipendenza organizzativa" fornisce ulteriori requisiti e informazioni relative all'assunzione da parte del CAE di ruoli o responsabilità che vanno oltre l'Internal Auditing.

Esempi di conformità

- Metodologie di Internal Audit per la comunicazione di limitazioni all'obiettività.
- Documentazione che riveli la presenza o affermi l'assenza di limitazioni all'obiettività.
- Registrazioni della comunicazione delle limitazioni all'obiettività e della risposta e/o dell'approvazione della strategia di mitigazione del rischio da parte dei soggetti interessati.

Principio 3 Dimostrare la competenza

Gli Internal Auditor applicano le conoscenze, le competenze e le abilità per adempiere con successo al loro ruolo e alle loro responsabilità.

Dimostrare la competenza richiede lo sviluppo e l'applicazione di conoscenze, capacità e abilità nel fornire servizi di Internal Auditing. Poiché gli Internal Auditor forniscono una vasta gamma di servizi, le competenze necessarie a ciascun Internal Auditor variano. Oltre a possedere o ottenere le competenze necessarie per svolgere i servizi, gli Internal Auditor migliorano l'efficacia e la qualità delle stesse perseguendo lo sviluppo professionale.

Standard 3.1 Competenza

Requisiti

Gli Internal Auditor devono possedere o ottenere le competenze necessarie ad adempiere con successo alle loro responsabilità. Le competenze richieste comprendono le conoscenze, le capacità e le abilità in linea con la propria posizione e le proprie responsabilità, secondo il livello di esperienza. Gli Internal Auditor devono possedere o sviluppare la conoscenza dei Global Internal Audit Standards.

Gli Internal Auditor devono impegnarsi solo in quelle attività per le quali hanno o possono raggiungere le competenze necessarie.

Ogni Internal Auditor è responsabile dello sviluppo continuo e dell'applicazione delle competenze necessarie per adempiere alle proprie responsabilità professionali. Inoltre, il CAE deve garantire che la funzione Internal Audit possieda collettivamente le competenze per svolgere i servizi di Internal Auditing descritti nell'Internal Audit Charter; in caso contrario, le deve ottenere (si vedano anche gli Standard "7.2 Qualifiche del Chief Audit Executive" e "10.2 Risorse umane").

Indicazioni per l'implementazione

Gli Internal Auditor dovrebbero sviluppare competenze relative a:

- comunicazione e collaborazione;
- governance, risk management e processi di controllo;
- attività aziendali, come i servizi finanziari e i sistemi informativi;
- rischi pervasivi, come le frodi;
- strumenti e tecniche per la raccolta, l'analisi e la valutazione dei dati;
- rischi e potenziali impatti di diverse situazioni economiche, ambientali, legali, politiche e sociali;
- leggi, regolamenti e pratiche rilevanti per l'organizzazione, il settore e l'industria;
- tendenze e problematiche emergenti rilevanti per l'organizzazione e per l'Internal Auditing;
- supervisione e leadership.

Per sviluppare e dimostrare le proprie competenze, gli Internal Auditor possono:

- ottenere credenziali professionali adeguate, come la qualifica di Certified Internal Auditor® e altre certificazioni;
- identificare le opportunità di miglioramento e le competenze che necessitano di sviluppo, sulla base dei feedback forniti da stakeholder, colleghi e supervisori;
- perseguire una formazione adeguata non solo sulle metodologie di Internal Audit, ma anche sulle attività di business rilevanti per l'organizzazione. Le opportunità di formazione possono includere l'iscrizione a corsi, la collaborazione con un mentore o l'assegnazione di nuovi compiti, sotto supervisione, durante un incarico.

Mentre gli Internal Auditor sono responsabili di garantire il proprio sviluppo professionale e possono valutare le proprie competenze e opportunità di sviluppo, il CAE dovrebbe supportarne lo sviluppo professionale. Il CAE può stabilire aspettative minime per lo sviluppo professionale e dovrebbe incoraggiare il perseguimento di qualifiche professionali. Egli dovrebbe prevedere l'inclusione di risorse nel budget dell'Internal Audit per la formazione e lo sviluppo professionale e fornire opportunità, sia internamente, sia esternamente all'organizzazione, attraverso l'istruzione professionale continua, la formazione e le conferenze (si vedano anche gli Standard "10.1 Risorse finanziarie" e "10.2 Risorse umane").

Per garantire che la funzione Internal Audit possieda nel suo complesso le competenze per svolgere i servizi di Internal Auditing, il CAE dovrebbe:

- conoscere le competenze da utilizzare negli incarichi, identificando le necessità di formazione e selezionando gli Internal Auditor;
- partecipare alle valutazioni delle performance individuali degli Internal Auditor;
- identificare le aree in cui le competenze della funzione Internal Audit dovrebbero essere migliorate;
- incoraggiare la curiosità intellettuale degli Internal Auditor e investire nella formazione e in altre opportunità per migliorare le perfomance dell'Internal Audit;
- comprendere le competenze di altre funzioni di servizi di assurance e di advisory e considerare la possibilità di fare affidamento su tali funzioni come fonte di competenze aggiuntive o specialistiche non disponibili nell'ambito della funzione Internal Audit;
- prendere in considerazione la possibilità di stipulare contratti con fornitori esterni nei casi in cui la funzione Internal Audit non possieda al suo interno le competenze necessarie a eseguire i servizi richiesti;
- implementare effettivamente un programma di assurance e miglioramento della qualità.

Esempi di conformità

- Documentazione che elenca le certificazioni, l'istruzione, l'esperienza, la storia lavorativa e altre qualifiche degli Internal Auditor.
- Autovalutazione delle competenze e dei piani di sviluppo professionale da parte degli Internal Auditor.
- Documentazione del completamento della formazione professionale continua da parte degli Internal Auditor, come corsi, conferenze, workshop e seminari.
- Revisioni documentate delle performance degli Internal Auditor.
- Review documentate degli incarichi, indagini post-incarico completate dagli stakeholder dell'Internal Audit e altre forme di feedback che indicano le competenze dimostrate dai singoli Internal Auditor e dalla funzione Internal Audit.
- I risultati dei processi di quality assessment interni ed esterni.
- Documentazione a supporto delle principali competenze necessarie per eseguire il piano di Audit, analisi delle risorse mancanti e conseguente identificazione delle necessità formative e di budget per colmare le carenze.
- Documentazione (per esempio una mappa) della rilevazione delle competenze delle altre funzioni di assurance e advisory sulle quali la funzione Internal Audit possa fare affidamento.

Standard 3.2 Aggiornamento professionale continuo

Requisiti

Gli Internal Auditor devono mantenere e sviluppare continuamente le proprie competenze per migliorare l'efficacia e la qualità dei servizi di Internal Auditing. Gli Internal Auditor devono perseguire lo sviluppo professionale continuo, compresa l'istruzione e la formazione. Gli Internal Auditor che hanno conseguito le certificazioni professionali di Internal Audit devono seguire le regole di formazione professionale continua e adempiere ai requisiti applicabili alle loro certificazioni.

Indicazioni per l'implementazione

Lo sviluppo professionale continuo può includere lo studio autonomo, il training on-the-job, l'opportunità di apprendere nuove competenze in incarichi speciali (ad esempio attraverso programmi di rotazione), il tutoring, l'ottenimento di feedback dell'attività di supervisione e la formazione gratuita e a pagamento. Per migliorare la qualità nell'esecuzione dei servizi di Internal Auditing, gli Internal Auditor dovrebbero perseguire le opportunità di conoscere i trend e le best practice, nonché i temi, i rischi, le tendenze e i cambiamenti emergenti che possono interessare le organizzazioni per le quali lavorano e la professione di Internal Audit.

Gli Internal Auditor sono responsabili dello sviluppo delle loro competenze e dovrebbero cercare opportunità di apprendimento. Tuttavia, il CAE è responsabile delle competenze della funzione Internal Audit e dovrebbe inserire nel budget e nel piano delle attività le opportunità di formazione del personale della funzione Internal Audit. Ad esempio, gli Internal Auditor possono sviluppare nuove competenze quando adeguatamente supervisionati e assegnati a incarichi che coinvolgono processi o aree in cui hanno una limitata esperienza. Gli Internal Auditor dovrebbero ricercare e accogliere favorevolmente la supervisione e l'insegnamento mediante i quali possono ottenere validi feedback, consigli e approfondimenti.

Molte certificazioni professionali richiedono un numero minimo di ore di formazione professionale continua in periodi determinati, ad esempio annualmente. Il CAE dovrebbe prendere in considerazione l'implementazione di un piano che permetta agli Internal Auditor di usufruire di un adeguato programma di formazione professionale continua.

Gli Internal Auditor in possesso di certificazioni, come ad esempio il Certified Internal Auditor®, dovrebbero essere a conoscenza dei requisiti specifici per il mantenimento della certificazione previsti dall'organismo preposto. Il mancato rispetto di tali requisiti può comportare conseguenze, tra cui la sospensione dell'autorizzazione a utilizzare le credenziali. Tutti gli Internal Auditor dovrebbero sviluppare obiettivi e programmi di formazione e istruzione continua. Nell'ambito della formazione professionale continua prevista, l'IIA richiede ai titolari delle certificazioni di completare la formazione etica. Sebbene questo requisito sia specificamente legato alle certificazioni IIA, tutti i professionisti dell'Internal Audit dovrebbero ottenere regolarmente una formazione professionale continua incentrata sull'etica.

I servizi di rassegna stampa, i webinar e gli eventi professionali offrono agli Internal Auditor l'opportunità di rimanere aggiornati sugli sviluppi della professione di Internal Audit e dei settori rilevanti per le organizzazioni per cui lavorano. La formazione può essere utilizzata per introdurre nuove tecnologie o cambiamenti nelle pratiche di Internal Audit.

Le iniziative di sviluppo professionale dovrebbero includere un riesame e una valutazione periodica dei percorsi di carriera e delle esigenze di sviluppo professionale degli Internal Auditor. Il CAE dovrebbe garantire che il piano delle attività e il budget per la formazione riflettano un equilibrio tra l'investimento nello sviluppo delle competenze della funzione Internal Audit nel suo complesso e l'offerta agli Internal Auditor di opportunità per il raggiungimento dei loro obiettivi individuali di crescita professionale.

Esempi di conformità

- Piani documentati di partecipazione a corsi di formazione, conferenze e altre occasioni di formazione professionale continua.
- Registri o altre evidenze della formazione professionale continua completata dagli Internal Auditor e delle certificazioni ottenute.
- Valutazioni delle performance degli Internal Auditor e/o piani di sviluppo professionale.
- Evidenza del coinvolgimento attivo nelle attività dell'IIA e altre organizzazioni professionali pertinenti, per esempio come volontari.

Principio 4 Esercitare la diligenza professionale

Gli Internal Auditor applicano la diligenza professionale nella pianificazione e nell'esecuzione dei servizi di Internal Auditing.

Per l'esercizio di un'adeguata diligenza professionale si richiede:

- la conformità ai Global Internal Audit Standards;
- di tenere in considerazione la natura, le circostanze e i requisiti del lavoro da eseguire;
- l'applicazione dello scetticismo professionale per valutare criticamente le informazioni.

La diligenza professionale richiede la pianificazione e l'esecuzione dei servizi di Internal Auditing con attenzione, discernimento e scetticismo. Con l'esercizio dell'adeguata diligenza professionale, gli Internal Auditor operano al meglio nell'interesse di coloro i quali ricevono servizi di Internal Auditing, ma non ci si aspetta che siano infallibili.

Standard 4.1 Conformità ai Global Internal Audit Standards

Requisiti

Gli Internal Auditor devono pianificare ed eseguire i servizi di Internal Auditing in conformità con i Global Internal Audit Standards.

Le metodologie della funzione Internal Audit devono essere stabilite, documentate e mantenute in linea con gli Standard. Gli Internal Auditor devono seguire gli Standard e le metodologie della funzione Internal Audit nella pianificazione e nell'esecuzione dei servizi di Internal Auditing e nella comunicazione dei risultati.

Se gli Standard sono utilizzati in combinazione con i requisiti emessi da altri organismi, le comunicazioni dell'Internal Audit devono citare il riferimento anche agli altri requisiti, laddove appropriato.

Se le leggi o i regolamenti impediscono agli Internal Auditor o alla funzione Internal Audit di conformarsi ad alcune parti degli Standard, è richiesta la conformità a tutte le altre parti degli Standard e deve essere fornita adeguata disclosure.

Quando gli Internal Auditor non sono in grado di conformarsi a un requisito, il CAE deve documentare e comunicare la circostanza, le azioni alternative intraprese, l'impatto delle azioni e la motivazione. I requisiti relativi alla disclosure della non conformità agli Standard sono descritti negli Standard "8.3 Qualità", "12.1 Quality assessment interno" e "15.1 Comunicazione finale dell'incarico".

Indicazioni per l'implementazione

Il CAE dovrebbe esaminare gli Standard quando sono oggetto di modifiche e allineare di conseguenza le metodologie della funzione Internal Audit. In caso di incongruenze tra Standard e requisiti emessi da altri organismi, gli Internal Auditor e la funzione Internal Audit possono essere tenuti o a conformarsi ai requisiti più rigorosi o scegliere di farlo.

Il CAE, o un supervisore designato, dovrebbe garantire che i programmi di lavoro dell'incarico siano in linea con i requisiti degli Standard e che gli incarichi di Internal Audit siano condotti in conformità con i requisiti degli Standard.

Sebbene ci si aspetti la conformità ai requisiti, gli Internal Auditor o la funzione Internal Audit possono occasionalmente non essere in grado di conformarsi a un requisito, ma possono adottare azioni alternative per conseguire il relativo principio. Queste circostanze sono solitamente legate a settori, business e paesi specifici. Documentando la circostanza, le azioni alternative intraprese, l'impatto e la motivazione, il CAE fornisce informazioni a supporto del quality assessment esterno in modo tale che la funzione Internal Audit possa essere in grado di raggiungere la conformità a un principio, anche quando la conformità a uno Standard non è possibile.

Se non sono in grado di conformarsi a uno Standard quando svolgono un incarico di Internal Audit, gli Internal Auditor dovrebbero discutere con il CAE o con un supervisore designato il motivo della non conformità e l'effetto sull'incarico. Questi, dovrebbero fornire indicazioni su destinatari e modalità della comunicazione di non conformità (si veda lo Standard "15.1 Comunicazione finale dell'incarico").

Inoltre, leggi, regolamenti, metodologie di Internal Audit e procedure organizzative possono fornire indicazioni per determinare quando e come la non conformità debba essere divulgata.

Esempi di conformità

- Evidenza documentale delle metodologie della funzione Internal Audit e indicazione della data dell'ultimo aggiornamento.
- Evidenza delle comunicazioni finali dell'incarico e delle comunicazioni al Board e al Top Management in caso di disclosure di non conformità.
- Documentazione che fa riferimento alle leggi e/o ai regolamenti a cui gli Internal Auditor sono stati tenuti a conformarsi e che hanno pregiudicato la loro conformità agli Standard.
- Documentazione che fa riferimento a requisiti di altri organismi ai quali la funzione Internal Audit aderisce in aggiunta agli Standard.
- Risultati del programma di assurance e miglioramento della qualità.

Standard 4.2 Diligenza professionale

Requisiti

Gli Internal Auditor devono esercitare la diligenza professionale valutando la natura, le circostanze e i requisiti dei servizi da fornire, tra cui:

- la strategia e gli obiettivi dell'organizzazione;
- gli interessi di coloro ai quali sono forniti i servizi di Internal Auditing e gli interessi degli altri stakeholder;
- l'adeguatezza ed efficacia dei processi di governance, risk management e controllo;
- il costo dei servizi di Internal Auditing da svolgere rispetto ai potenziali benefici;
- l'entità e le esigenze temporali del lavoro necessario per raggiungere gli obiettivi dell'incarico;
- la complessità, rilevanza o significatività dei rischi relativi all'attività oggetto di audit;
- la probabilità di errori significativi, frodi, non conformità e altri rischi che potrebbero influire su obiettivi, operazioni o risorse;
- l'uso di tecniche, strumenti e tecnologie appropriate.

Indicazioni per l'implementazione

Per svolgere i servizi con diligenza professionale è necessario che gli Internal Auditor considerino e comprendano il Purpose e la natura dei servizi di Internal Auditing da fornire. Gli Internal Auditor dovrebbero iniziare dalla comprensione dell'Internal Audit Charter, del piano di Audit e dei fattori che aiutano a determinare quali incarichi siano inclusi nel piano. Durante la pianificazione e l'esecuzione dei servizi di Internal Auditing, gli Internal Auditor considerano anche gli interessi dei clienti interni e di altri stakeholder (incluso il pubblico) impattati dalle azioni dell'organizzazione. Tali interessi includono le aspettative degli stakeholder (come le pratiche commerciali corrette e oneste), le esigenze (come la sicurezza) e la potenziale esposizione a rischi sottostanti che potrebbero non essere esplicitamente correlati alla strategia e agli obiettivi dell'organizzazione.

Le considerazioni relative alla diligenza professionale comprendono gli aspetti che il CAE deve considerare nell'eseguire la valutazione dei rischi su cui si basa il piano di Audit. Quelli rilevanti includono la strategia e gli obiettivi dell'organizzazione, l'adeguatezza e l'efficacia dei processi di governance, risk management e controllo dell'organizzazione.

Inoltre, gli Internal Auditor considerano queste circostanze in relazione a un'attività oggetto di audit durante la pianificazione dell'incarico, come descritto nella Sezione "V: Svolgimento delle attività di Internal Auditing". La complessità, la materialità e la significatività dei rischi valutati sono relative. Un rischio può non essere rilevante o significativo per l'organizzazione, ma può esserlo nell'ambito di un incarico di audit.

Pertanto, comprendere la complessità, la materialità e il significato nel contesto è necessario per valutare correttamente i rischi rilevanti e determinare quali rischi dovrebbero essere prioritari per una successiva valutazione.

La diligenza professionale richiede anche di soppesare i costi (come il fabbisogno di risorse) dei servizi di Internal Auditing rispetto ai benefici che possono derivarne. Ad esempio, se i controlli in un'attività oggetto di audit non sono adeguatamente definiti, è probabile che i benefici derivanti dall'efficacia di tali controlli non compensino i costi. Gli Internal Auditor cercano di fornire il massimo valore o ritorno dell'investimento dell'organizzazione nei servizi di Internal Auditing. Inoltre, una pianificazione accurata richiede che gli Internal Auditor considerino le tecniche, gli strumenti, la tecnologia, l'entità e le esigenze temporali del lavoro necessarie per raggiungere gli obiettivi dell'incarico nel modo più efficiente possibile. Gli Internal Auditor, in particolare il CAE, dovrebbero prendere in considerazione l'uso di software di analisi dei dati e altre tecnologie che supportino la verifica e la valutazione dei processi.

Un'adeguata supervisione dell'incarico e un programma di assurance e miglioramento della qualità promuovono la diligenza professionale (si vedano anche gli Standard "8.3 Qualità", "8.4 Quality assessment esterno" e il Principio "12 Migliorare la qualità" e i relativi Standard).

Esempi di conformità

- Documentazione di pianificazione (es. Planning Memo) che consideri la strategia e gli obiettivi dell'organizzazione e dell'attività oggetto di audit.
- Valutazioni documentate dei processi di governance, risk management e controllo.
- Note che documentino la valutazione dei rischi, inclusi errori, non conformità e frodi.
- Note tratte da riunioni o discussioni sui potenziali costi e benefici dei servizi di Internal Auditing e sull'entità e le esigenze temporali dell'incarico di audit.
- Carte di lavoro che attestino la review del supervisore dell'incarico.
- Valutazioni delle performance degli Internal Auditor.
- Note tratte da riunioni, corsi di formazione o altre discussioni sulla diligenza professionale.
- Feedback da parte degli stakeholder richiesti tramite sondaggi o altri strumenti.
- Valutazioni interne ed esterne effettuate nell'ambito del programma di assurance e miglioramento della qualità della funzione Internal Audit.

Standard 4.3 Scetticismo professionale

Requisiti

Gli Internal Auditor devono esercitare lo scetticismo professionale quando pianificano ed eseguono i servizi di Internal Audit.

Per esercitare lo scetticismo professionale, gli Internal Auditor devono:

- mantenere un atteggiamento che includa curiosità;
- valutare criticamente l'affidabilità delle informazioni;
- essere diretti e onesti in caso di dubbi e domande su informazioni incoerenti;
- cercare ulteriori evidenze per esprimere un giudizio su informazioni e dichiarazioni che potrebbero essere incomplete, incoerenti, false o fuorvianti.

Indicazioni per l'implementazione

Lo scetticismo professionale consente agli Internal Auditor di formulare giudizi oggettivi basati su fatti, informazioni e logica, piuttosto che sulla fiducia o sulle convinzioni. Lo scetticismo è l'atteggiamento di mettere sempre in discussione o alla prova la validità e la veridicità di affermazioni e di altre informazioni. Gli Internal Auditor applicano lo scetticismo professionale quando cercano prove a supporto e conferma delle dichiarazioni fatte dal management, piuttosto che fidarsi semplicemente delle informazioni presentate come vere o autentiche senza domande o dubbi. Lo scetticismo professionale richiede curiosità e volontà di esplorare oltre il livello superficiale un determinato argomento.

Durante la raccolta e l'analisi delle informazioni, gli Internal Auditor dovrebbero applicare lo scetticismo professionale per determinare se le informazioni sono pertinenti, affidabili e sufficienti. Se gli Internal Auditor stabiliscono che le informazioni sono incomplete, incoerenti, false o fuorvianti, dovrebbero eseguire ulteriori analisi per identificare le informazioni corrette e complete, necessarie per supportare i risultati dell'incarico. Un'ulteriore convalida è fornita dalla revisione e dall'approvazione delle carte di lavoro e/o delle comunicazioni relative all'incarico da parte del CAE o di un supervisore designato.

Il CAE dovrebbe aiutare gli Internal Auditor a sviluppare le loro competenze relative allo scetticismo professionale. I workshop e altre opportunità di formazione possono aiutare gli Internal Auditor a sviluppare e imparare ad applicare lo scetticismo professionale e a comprendere l'importanza di evitare i pregiudizi e mantenere una mentalità aperta e curiosa. Gli Internal Auditor possono imparare a riconoscere le informazioni incoerenti, incomplete, false e/o fuorvianti.

Esempi di conformità

- Registri o altre evidenze della formazione pianificata e completata, compreso l'elenco dei partecipanti.
- Carte di lavoro che identificano l'approccio di un Internal Auditor per valutare e convalidare le informazioni raccolte durante un incarico.
- Documentazione attestante che le informazioni false o fuorvianti sono state trattate come rilievo dell'incarico.
- Carte di lavoro e comunicazioni degli incarichi esaminate e firmate o siglate dal supervisore dell'incarico.

Principio 5 Mantenere la riservatezza

Gli Internal Auditor utilizzano e proteggono le informazioni in modo appropriato.

Poiché gli Internal Auditor hanno accesso illimitato ai dati, ai registri e ad altre informazioni necessarie per adempiere al Mandato di Internal Audit, spesso ricevono informazioni riservate, di proprietà e/o personali (vedere anche il Principio "6 Autorizzata dal Board" e i relativi Standard). Le informazioni possono essere in qualsiasi forma fisica o digitale, incluse quelle emerse da colloqui verbali, come ad esempio le riunioni formali o informali. Gli Internal Auditor devono rispettare il valore e la titolarità delle informazioni che ricevono utilizzandole solo per scopi professionali e proteggendole da accessi o divulgazioni non autorizzate, internamente ed esternamente.

Standard 5.1 Utilizzo delle informazioni

Requisiti

Gli Internal Auditor devono seguire adeguate policy, procedure, leggi e regolamenti quando utilizzano le informazioni. Queste non devono essere utilizzate per interesse personale o in un modo che possa contrastare o pregiudicare gli obiettivi legittimi ed etici dell'organizzazione.

Indicazioni per l'implementazione

Gli Internal Auditor hanno accesso illimitato alle informazioni per poter fornire servizi di Internal Auditing senza interferenze. Tuttavia, ogni Internal Auditor è responsabile dell'utilizzo e della gestione appropriata delle informazioni. L'utilizzo o la gestione inappropriata di informazioni riservate, di proprietà e/o personali possono avere conseguenze negative, come danni reputazionali e multe per violazione di leggi e/o regolamenti.

Le policy e le procedure dell'organizzazione e della funzione Internal Audit disciplinano generalmente la gestione e l'utilizzo delle informazioni da parte degli Internal Auditor durante tutto il ciclo di vita, dall'accesso alla raccolta, al trasferimento, all'archiviazione e/o alla distruzione. Inoltre, gli Internal Auditor dovrebbero essere a conoscenza e rispettare tutte le policy e le procedure relative alle informazioni di terze parti alle quali possono accedere.

Il CAE dovrebbe discutere con gli Internal Auditor le policy, le procedure e le aspettative relative all'utilizzo appropriato delle informazioni alle quali hanno accesso. Il CAE può richiedere agli Internal Auditor di confermarne l'accettazione tramite sottoscrizione di specifici moduli.

Nel trattamento di dati sensibili e/o personali, la funzione Internal Audit dovrebbe applicare adeguate misure di sicurezza informatica. A titolo di esempio si possono citare controlli automatici come password e crittografia.

Esempi di uso improprio delle informazioni includono l'utilizzo, la vendita o il rilascio di informazioni finanziarie, strategiche o operative dell'organizzazione per prendere decisioni informate sull'acquisto o la vendita di titoli o per creare un prodotto concorrente.

Esempi di conformità

- Controlli efficaci sull'accesso alle informazioni e sul loro utilizzo.
- Documentazione delle policy, delle procedure e della formazione in merito all'utilizzo corretto delle informazioni.
- Verbali delle riunioni durante le quali è stato discusso l'utilizzo appropriato delle informazioni.
- Registri delle presenze ai corsi di formazione sull'utilizzo delle informazioni.
- Documentazione con cui gli Internal Auditor riconoscono l'accettazione delle policy, delle procedure, delle leggi e dei regolamenti pertinenti.
- Review delle performance che dimostrano il rispetto di policy, procedure, leggi e regolamenti pertinenti.

Standard 5.2 Protezione delle informazioni

Requisiti

Gli Internal Auditor devono essere consapevoli delle loro responsabilità in materia di protezione delle informazioni e dimostrare rispetto per la confidenzialità, la privacy e la titolarità delle informazioni acquisite durante l'esecuzione di servizi di Internal Auditing o in virtù di relazioni professionali.

Gli Internal Auditor devono comprendere e rispettare le leggi, i regolamenti, le policy e le procedure che si applicano all'organizzazione e alla funzione Internal Audit in materia di confidenzialità, privacy e sicurezza delle informazioni.

Tra le indicazioni più importanti per la funzione Internal Audit rientrano:

- la custodia, la conservazione e l'eliminazione dei documenti dell'incarico;
- la consegna di documenti dell'incarico a soggetti interni o esterni;
- il trattamento, l'accesso o la conservazione di copie di informazioni riservate quando non sono più necessarie.

Gli Internal Auditor non devono divulgare informazioni riservate a soggetti non autorizzati, a meno che non vi sia un obbligo legale o professionale.

Gli Internal Auditor devono gestire il rischio di accesso o divulgazione non intenzionale di informazioni.

Il CAE deve garantire che la funzione Internal Audit e le persone che la supportano rispettino le stesse regole di protezione.

Indicazioni per l'implementazione

Le informazioni acquisite, utilizzate e prodotte dalla funzione Internal Audit sono protette da leggi, regolamenti e dalle policy e procedure dell'organizzazione e della funzione Internal Audit e riguardano generalmente la sicurezza fisica e informatica e l'accesso, la conservazione e l'eliminazione delle informazioni.

Il CAE dovrebbe consultare un legale per comprendere meglio l'impatto dei requisiti e delle tutele legali e/o normativi (ad esempio, il segreto professionale o il rapporto avvocato-cliente). Le policy e le procedure dell'organizzazione possono richiedere che organi competenti esaminino e approvino le informazioni aziendali prima del rilascio esterno.

L'accesso alle informazioni può essere monitorato per verificare l'aderenza alle metodologie. Le informazioni possono essere protette dalla divulgazione intenzionale o non intenzionale attraverso controlli quali la crittografia dei dati, la protezione con password, le regole di distribuzione delle e-mail, le restrizioni sull'utilizzo dei social media e le restrizioni all'accesso fisico. Quando gli Internal Auditor non hanno più bisogno di accedere ai dati, le autorizzazioni digitali dovrebbero essere revocate e le copie stampate dovrebbero essere trattate secondo le metodologie stabilite.

Esempi di informazioni riservate che possono essere protette dalla divulgazione includono gli stipendi del personale e la registrazione di problemi personali dei dipendenti.

Il CAE dovrebbe valutare e confermare periodicamente le esigenze degli Internal Auditor in termini di accesso alle informazioni e il funzionamento efficace dei relativi controlli.

Esempi di conformità

- Documentazione che dimostra l'applicazione delle metodologie pertinenti.
- Documentazione relativa all'implementazione di meccanismi che limitano l'accesso alle informazioni e mitigano il rischio di elusione dei controlli previsti.
- Registri delle presenze ai corsi di formazione sulla protezione delle informazioni.
- Documentazione con cui gli Internal Auditor attestano la loro comprensione di policy, procedure, leggi e regolamenti pertinenti.
- Evidenze delle restrizioni alla distribuzione delle carte di lavoro e della comunicazione finale.
- Documentazione delle divulgazioni e della distribuzione autorizzate.
- Registrazione delle divulgazioni di informazioni richieste dalla legge o approvate da parere legale, se applicabile, e/o dal Board e dal Top Management.
- Accordi firmati di riservatezza o non divulgazione delle informazioni.
- Review delle performance che dimostrino che sono state seguite le policy e le procedure relative alla protezione e alla divulgazione delle informazioni.

Sezione III: Governo della funzione Internal Audit

Un'**adeguata governance è essenziale** per l'efficacia della funzione Internal Audit. La presente sezione definisce i requisiti necessari per i CAE al fine di lavorare in stretta collaborazione con il Board che istituisce la funzione Internal Audit, le conferisce indipendenza e ne supervisiona le performance. La presente sezione definisce anche le responsabilità del Top Management a supporto del Board per una governance solida della funzione Internal Audit.

Sebbene il CAE sia responsabile dei requisiti della presente sezione, le attività del Board e del Top Management sono essenziali per realizzare il Purpose dell'Internal Auditing. Queste attività sono identificate come "condizioni essenziali" in ogni Standard e stabiliscono la base per il dialogo tra il Board, il Top Management e il CAE, consentendo la piena efficacia della funzione Internal Audit.

Incontri con il Board e il Top Management

Il CAE deve discutere il contenuto della presente sezione con il Board e il Top Management. La discussione dovrebbe riguardare i seguenti aspetti:

- il Purpose dell'Internal Auditing come descritto nella Sezione "I: Purpose dell'Internal Auditing";
- le condizioni essenziali evidenziate in ciascuno degli Standard della Sezione "III: Governo della funzione Internal Audit";
- il potenziale impatto sull'efficacia della funzione Internal Audit, nel caso in cui il Board o il Top Management non forniscano il supporto previsto nelle condizioni essenziali.

Il confronto con il Board e il Top Management è necessario per informarli dell'importanza delle condizioni essenziali e per un allineamento sulle rispettive responsabilità.

La natura e la frequenza di questi incontri dipendono dalle circostanze e dagli eventuali cambiamenti all'interno di un'organizzazione. Ad esempio, il CAE dovrebbe discutere queste condizioni essenziali con il Board e il Top Management se:

- gli Standard cambiano in modo significativo o viene costituita una nuova funzione Internal Audit;
- il CAE è nuovo nel ruolo o nell'organizzazione;
- vi sono cambiamenti significativi nella relazione tra il Board e il CAE, come ad esempio un nuovo Presidente a cui riferisce il CAE o un cambiamento nella struttura o nella composizione del Board che influisce sui flussi informativi;
- ci sono cambiamenti significativi nella struttura o nella composizione del Top Management che influenzano il posizionamento del CAE nell'organizzazione.

È importante che il CAE riceva input sia dal Board che dal Top Management. Sebbene sia il Board ad avere la responsabilità ultima di approvare il Mandato, l'Internal Audit Charter e gli altri requisiti descritti in questa sezione, il Top Management ha in genere un ruolo chiave nel fornire input al Board e al CAE. Il punto di vista del Top Management è prezioso e aiuta a sostenere il posizionamento e l'autorità della funzione Internal Audit nell'organizzazione.

Divergenze sulle condizioni essenziali

Se il Board o il Top Management non concordano con una o più di queste condizioni essenziali, il CAE deve evidenziare, con esempi, come l'assenza delle condizioni possa influire sulla capacità della funzione Internal Audit di realizzare il proprio purpose o di conformarsi a specifici Standard. Il CAE dovrebbe anche discutere le alternative alle condizioni essenziali che possono fornire analoghi risultati.

Il CAE può raggiungere un accordo con il Board e il Top Management sul fatto che una o più delle condizioni essenziali non siano necessarie per conformarsi agli Standard. In tali casi, il CAE deve documentare:

- le ragioni per cui una particolare condizione non è necessaria;
- condizioni alternative che compensino le condizioni assenti, a supporto dei giudizi del Board e del Top Management.

Se non è d'accordo con le ragioni del Board e/o del Top Management, il CAE può concludere che la funzione Internal Audit non può essere conforme agli Standard. In questi casi, il CAE dovrebbe documentare i motivi per cui il Board e/o il Top Management non adempiranno alle condizioni essenziali. Questa documentazione dovrebbe essere condivisa con il Board e il Top Management per garantire chiarezza in merito alle loro posizioni e messa a disposizione di un Quality Assessor esterno.

Quando, per qualsiasi motivo, la posizione di CAE risulta vacante, il Board dovrebbe nominare una o più persone ad interim.

Definizione di Board

Il glossario dei Global Internal Audit Standards definisce con il termine "Board" l'organo di più alto livello incaricato della governance, come ad esempio:

- un Consiglio di Amministrazione;
- un Audit Committee;
- un Consiglio Direttivo o di fiduciari;
- un gruppo di funzionari eletti o nominati politicamente;
- un altro organo che abbia autorità sulle funzioni di governance rilevanti.

In un'organizzazione che prevede più di un organo di governo, il termine "Board" si riferisce all'organo o agli organi autorizzati a conferire alla funzione Internal Audit autorità, ruolo e responsabilità appropriate.

Laddove non esista nessuno dei precedenti, "Board" dovrebbe essere riferito a un gruppo di soggetti o alla persona che agisce come massimo organo di governo dell'organizzazione, ad esempio il CEO.

Se la natura del Board differisse dalla definizione fornita nel glossario, il CAE dovrebbe identificare l'organo amministrativo cui fa capo la funzione Internal Audit ed esaminare in che modo tale struttura organizzativa è coerente con la definizione di Board. Ciò può accadere laddove coesistano diversi organi, come ad esempio in organizzazioni multinazionali o nel settore pubblico, o in una struttura a più livelli.

Applicazione di questa sezione

Gli Standard si applicano alle persone e alle funzioni che forniscono servizi di Internal Auditing. I servizi di Internal Auditing possono essere forniti da persone interne o esterne all'organizzazione, per organizzazioni che possono variare per scopo, dimensioni, complessità e struttura. Gli Standard si applicano sia alle organizzazioni che assumono direttamente gli Internal Auditor, sia a quelle che prevedono un contratto con un fornitore esterno di servizi o a situazioni ibride. Le responsabilità del CAE sono svolte da una o più persone nominate dal Board. Il CAE, che sia un dipendente dell'organizzazione o un fornitore esterno di servizi, è responsabile della conformità agli Standard, da comprovare attraverso il programma di assurance e miglioramento della qualità. In tutti i casi, il Board mantiene la responsabilità di supportare e supervisionare la funzione Internal Audit.

Principio 6 Autorizzata dal Board

Il Board stabilisce, approva e supporta il Mandato della funzione Internal Audit.

La funzione Internal Audit riceve il suo Mandato dal Board (o dalla legge applicabile in determinati contesti del settore pubblico). Il Mandato specifica l'autorità, il ruolo e le responsabilità della funzione Internal Audit ed è documentato nell'Internal Audit Charter. Il Mandato conferisce alla funzione Internal Audit il potere di fornire in modo oggettivo, al Board e al Top Management, assurance, advisory, approfondimenti e visione prospettica. La funzione Internal Audit svolge il Mandato tramite un approccio sistematico e rigoroso nella valutazione e nel miglioramento della governance, del risk management e nei processi di controllo in tutta l'organizzazione.

Standard 6.1 Mandato di Internal Audit

Requisiti

Il CAE deve fornire al Board e al Top Management le informazioni necessarie per definire il Mandato di Internal Audit. Nei paesi e nei settori in cui il Mandato della funzione Internal Audit è normato, in tutto o in parte, da leggi o regolamenti, l'Internal Audit Charter deve includere i requisiti legali del Mandato (si vedano lo Standard "6.2 Internal Audit Charter" e il capitolo "Applicazione dei Global Internal Audit Standards nel Settore Pubblico").

Per aiutare il Board e il Top Management a determinare l'ambito e i tipi di servizi di Internal Auditing, il CAE deve coordinarsi con gli altri fornitori di assurance interni ed esterni per comprendere i rispettivi ruoli e responsabilità (si veda anche lo Standard "9.5 Coordinamento e reliance").

Il CAE deve formalizzare il Mandato o farvi riferimento nell'Internal Audit Charter, approvato dal Board (si veda lo Standard "6.2 Internal Audit Charter").

Periodicamente, il CAE deve valutare se eventuali cambiamenti rendano necessario un confronto con il Board e il Top Management. In tal caso, il CAE deve rivedere il Mandato con il Board e il Top Management per valutare se l'autorità, il ruolo e le responsabilità permettono alla funzione Internal Audit di proseguire nella realizzazione della propria strategia e dei propri obiettivi.

Condizioni essenziali

Il Board

- Discute con il CAE e il Top Management l'autorità, il ruolo e le responsabilità della funzione Internal Audit.
- Approva l'Internal Audit Charter, che include il Mandato di Internal Audit, l'ambito e le tipologie di servizi di Internal Auditing.

Il Top Management

- Partecipa agli incontri con il Board e il CAE e fornisce indicazioni sulle aspettative nei confronti della funzione Internal Audit che il Board dovrebbe prendere in considerazione quando definisce il Mandato.
- Supporta, all'interno dell'organizzazione, il Mandato e promuove l'autorità conferita alla funzione Internal Audit.

Indicazioni per l'implementazione

Il CAE presenta al Board e al Top Management le caratteristiche di un'efficace funzione Internal Audit, attraverso la presentazione degli Standard, delle leggi e/o regolamenti pertinenti e degli studi sulle best practice delle funzioni di Internal Audit.

Il CAE dovrebbe discutere con il Board e il Top Management il Mandato e altri aspetti chiave dell'Internal Audit Charter, concentrandosi nell'aiutarli a comprendere:

- **autorità** – l'autorità della funzione Internal Audit è conferita dal riporto diretto al Board. Tale autorità permette alla funzione Internal Audit di avere accesso libero e illimitato al Board, nonché a tutte le attività e informazioni nell'organizzazione (ad esempio, registri, persone e spazi fisici);
- **ruolo/i** – il ruolo principale della funzione Internal Audit è quello di svolgere l'attività di Internal Auditing e fornire i servizi propri dell'Internal Audit. Ci possono essere casi in cui l'Internal Audit è solo una delle responsabilità di un CAE, che potrebbe avere responsabilità anche nel risk management o nella compliance. Questi casi sono ulteriormente approfonditi nello Standard "7.1 Indipendenza organizzativa";
- **responsabilità** – le responsabilità di una funzione Internal Audit comprendono gli obblighi di svolgere il proprio ruolo, nonché di soddisfare le aspettative dei propri stakeholder. Per esempio, tali responsabilità includono, generalmente, le aspettative nello svolgimento dei servizi di audit, nei flussi informativi, nel garantire conformità a leggi, regolamenti e procedure nonché ai Global Internal Audit Standards e altre attività inerenti al ruolo;
- **ambito** - l'ambito dei servizi di Internal Auditing ricomprende l'organizzazione nel suo complesso. Ciò può includere quindi tutte le attività, i beni e il personale dell'organizzazione o può essere limitato a un sottoinsieme in base all'area geografica o ad altro tipo di suddivisione. La definizione dell'ambito può specificare la natura dei servizi (ad esempio, solo di assurance o assurance e advisory oppure focus sulla rendicontazione finanziaria o sulla compliance a leggi e/o regolamenti) o può specificare altre limitazioni;
- **servizi di Internal Auditing** – i servizi di Internal Auditing possono essere definiti semplicemente come servizi di assurance e advisory o possono essere definiti in modo più specifico, ad esempio: operational audit, assurance sui controlli interni nell'ambito della rendicontazione finanziaria e investigazioni.

Alcune circostanze possono richiedere un successivo confronto con il Board e il Top Management sul Mandato di Internal Audit o su altri aspetti dell'Internal Audit Charter. Queste circostanze possono includere, a titolo esemplificativo:

- un cambiamento significativo nei Global Internal Audit Standards;
- un'acquisizione o una riorganizzazione significativa;
- cambiamenti significativi nel Board e/o nel Top Management;
- cambiamenti significativi nelle strategie, negli obiettivi, nel profilo di rischio o nell'ambiente in cui si opera;
- nuove leggi o regolamenti che possono influire sulla natura e/o sull'ambito dei servizi di Internal Auditing.

Queste condizioni possono verificarsi in qualsiasi momento dell'anno. Tuttavia, il CAE dovrebbe considerare esplicitamente l'eventuale occorrenza di queste condizioni almeno una volta all'anno.

Il CAE si coordina con le funzioni di assurance dell'organizzazione e comunica al Board come le altre funzioni possono contribuire al Mandato di Internal Audit. Aiutando il Board a comprendere i ruoli e le responsabilità degli altri fornitori di servizi di assurance interni ed esterni e degli enti di regolamentazione, il CAE può chiarire gli elementi utili a definire un Mandato di Internal Audit appropriato (si veda anche lo Standard "9.5 Coordinamento e reliance").

Esempi di conformità

- Verbali delle riunioni del Board in cui è stato discusso il Mandato, che possono far parte della più ampia approvazione dell'Internal Audit Charter.
- Verbali delle riunioni del Board durante le quali vengono discusse e approvate eventuali modifiche all'Internal Audit Charter.

Standard 6.2 Internal Audit Charter

Requisiti

Il CAE deve sviluppare e mantenere aggiornato l'Internal Audit Charter che deve specificare almeno i seguenti punti:

- il Purpose dell'Internal Auditing;
- l'impegno ad aderire ai Global Internal Audit Standards;
- il Mandato, comprensivo dell'ambito e delle tipologie di servizi di audit, nonché delle responsabilità del Board nel supportare la funzione Internal Audit (si veda anche lo Standard "6.1 Mandato di Internal Audit");
- posizione organizzativa e reporting (si veda anche lo Standard "7.1 Indipendenza organizzativa").

Il CAE deve condividere la proposta dell'Internal Audit Charter con il Board e il Top Management per confermare che esso rifletta accuratamente le loro aspettative in merito alla funzione Internal Audit.

Condizioni essenziali

Il Board

- Discute con il CAE e il Top Management altri argomenti che dovrebbero essere inclusi nell'Internal Audit Charter per consentire l'efficacia della funzione Internal Audit.
- Approva l'Internal Audit Charter.
- Rivede l'Internal Audit Charter con il CAE per prendere in considerazione i cambiamenti che riguardano l'organizzazione, come ad esempio l'assunzione di un nuovo CAE o cambiamenti che riguardano i rischi dell'organizzazione e la loro rilevanza.

Il Top Management

- Comunica con il Board e il CAE in merito alle aspettative del management che dovrebbero essere prese in considerazione nell'Internal Audit Charter.

Indicazioni per l'implementazione

I requisiti chiave dell'Internal Audit Charter sono definiti negli Standard "6.1 Mandato di Internal Audit" e "7.1 Indipendenza organizzativa".

L'Internal Audit Charter dovrebbe indicare a chi riporta gerarchicamente il CAE per gli aspetti amministrativi, ad esempio:

- approvazione del budget e della gestione amministrativa delle risorse umane della funzione Internal Audit;
- approvazione delle spese del CAE;
- revisione delle performance del CAE.

Laddove siano presenti leggi o regolamenti che specifichino queste responsabilità, i riferimenti a tali documenti dovrebbero essere inclusi nell'Internal Audit Charter. Se le leggi e/o i regolamenti coprono in modo completo i requisiti del Charter, possono essere sostituiti allo stesso.

La struttura di un Internal Audit Charter può variare da un'organizzazione all'altra. Sebbene esistano template per la costruzione di un Internal Audit Charter, il CAE dovrebbe personalizzare il documento per affrontare gli aspetti organizzativi specifici che possono influire sul Mandato, sull'ambito e sui servizi della funzione Internal Audit.

Il CAE in genere presenta una bozza finale dell'Internal Audit Charter in occasione di una seduta del Board affinché questa venga discussa e approvata.

Il CAE e il Board dovrebbero, inoltre, concordare la frequenza con cui rivedere le disposizioni dell'Internal Audit Charter per confermare se consentono alla funzione Internal Audit di continuare a raggiungere i suoi obiettivi. È prassi rivedere periodicamente l'Internal Audit Charter e aggiornarlo se necessario.

Tra gli altri temi da considerare nell'Internal Audit Charter troviamo:

- le modalità di tutela dell'obiettività e dell'indipendenza, che prevedano anche i casi di eventuali limitazioni, e la frequenza con cui tali tutele vengono riviste per garantirne sempre l'efficacia (si veda anche lo Standard "7.1 Indipendenza organizzativa");
- le modalità di esercizio del diritto di accesso illimitato, con cui la funzione Internal Audit ottiene l'accesso ai dati, alle registrazioni, alle informazioni, al personale e agli spazi fisici necessari per adempiere al Mandato;
- le comunicazioni, tra cui la natura e la tempistica del reporting al Board e al Top Management;
- il processo di audit, comprese le eventuali necessità di reporting al management coinvolto nell'attività di audit (prima, durante e dopo un incarico) e le modalità di gestione degli eventuali disaccordi;
- il processo di assurance e miglioramento della qualità, comprese le previsioni per lo sviluppo e lo svolgimento di valutazioni interne ed esterne della funzione Internal Audit e la comunicazione dei risultati delle valutazioni (si vedano anche gli Standard "8.3 Qualità" e "8.4 Quality assessment esterno", il Principio "12 Migliorare la qualità" e i relativi Standard);
- le approvazioni, compresi eventuali casi specificati dal Board e dal Top Management.

Esempi di conformità

- Verbali delle riunioni del Board durante le quali è stato discusso e approvato l'Internal audit Charter.
- L'Internal Audit Charter approvato, con relativa data di approvazione.
- Verbali delle riunioni tra il CAE, il Board e il Top Management quale evidenza della revisione periodica dell'Internal Audit Charter.

Standard 6.3 Supporto dal Board e dal Top Management

Requisiti

Il CAE deve fornire al Board e al Top Management le informazioni necessarie per supportare e promuovere il riconoscimento della funzione Internal Audit in tutta l'organizzazione.

Il CAE deve supportare il Board nelle sue comunicazioni con il Top Management relative alla funzione Internal Audit.

Condizioni essenziali

Il Board

- Sostiene la funzione Internal Audit per consentirle di realizzare il Purpose dell'Internal Auditing e perseguire la sua strategia e i suoi obiettivi.
- Collabora con il Top Management per consentire l'accesso illimitato della funzione Internal Audit ai dati, alle registrazioni, alle informazioni, al personale e agli spazi fisici necessari per adempiere al Mandato di Internal Audit.
- Supporta il CAE attraverso comunicazioni regolari e dirette.
- Dimostra il proprio supporto:
  - specificando che il CAE riferisce a un livello all'interno dell'organizzazione che consente alla funzione Internal Audit di adempiere al Mandato;
  - approvando l'Internal Audit Charter, il piano di Audit, il budget e il piano delle risorse;
  - effettuando le opportune verifiche con il Top Management e il CAE per determinare se eventuali restrizioni all'ambito, all'accesso, all'autorità o alle risorse della funzione Internal Audit ne limitino la capacità di attuare efficacemente le proprie responsabilità;
  - incontrando periodicamente il CAE in assenza del Top Management.

Il Top Management

- Supporta il riconoscimento della funzione Internal Audit in tutta l'organizzazione.
- Collabora con il Board e con il management per consentire alla funzione Internal Audit di avere accesso illimitato ai dati, ai registri, alle informazioni, al personale e agli spazi fisici necessari per adempiere al Mandato di Internal Audit.

Indicazioni per l'implementazione

Il Board e il CAE dovrebbero incontrarsi almeno una volta all'anno in assenza del management. Prevedere tali riunioni trimestralmente è considerata una best practice. Tali riunioni si svolgono spesso come sessioni private o chiuse a seguito di una riunione del Board.

Il CAE dovrebbe anche avere altri momenti di confronto con il Board negli intervalli tra le riunioni ufficiali, per tenerlo informato sui progressi della funzione Internal Audit. Le tipologie di informazioni che il CAE comunica al Board e il relativo livello di dettaglio dovrebbero essere concordati tra le parti.

Come previsto dallo Standard "7.1 Indipendenza organizzativa", è importante che il CAE riporti amministrativamente a una persona all'interno dell'organizzazione che possa supportare la funzione Internal Audit nel perseguimento del Mandato di Internal Audit. Una best practice è che il CAE riferisca all'Amministratore Delegato o equivalente.

Sebbene sia fondamentale che il CAE si incontri privatamente con il Board, egli dovrebbe informare il Top Management di tali incontri, a meno che ciò non sia inappropriato (ad esempio, se una conversazione privata riguarda una scorrettezza da parte di un soggetto appartenente al Top Management).

Il CAE dovrebbe collaborare con il Top Management per definire i rispettivi requisiti di reporting nei confronti del Board per contribuire a una rendicontazione tempestiva, chiara e trasparente, non ripetitiva o contrastante. Ciò aiuta il Board a esercitare le proprie responsabilità di supervisione e consente un rapporto collaborativo tra il CAE e il Top Management.

L'approvazione da parte del Board del budget e del piano delle risorse è importante al fine di dimostrare che la funzione Internal Audit dispone delle risorse necessarie per completare le attività di audit pianificate. I dettagli forniti al Board sono decisi dal CAE.

Esempi di conformità

- Verbali delle riunioni del Board che indicano la revisione e l'approvazione del piano di Audit, del budget e del piano delle risorse.
- Verbali o altra documentazione che attestino il confronto tra il Board e il Top Management in merito all'accesso illimitato della funzione Internal Audit.
- Una griglia o documentazione analoga che indichi quali informazioni dovrebbero essere comunicate dal CAE al Board e al Top Management e la frequenza prevista.

Principio 7 Indipendente

Il Board stabilisce e tutela l'indipendenza e le qualifiche della funzione Internal Audit.

Il Board ha il compito di garantire l'indipendenza della funzione Internal Audit. L'indipendenza è definita come l'assenza di condizioni che compromettano la capacità della funzione Internal Audit di svolgere le proprie responsabilità in modo imparziale. La funzione Internal Audit è in grado di realizzare il Purpose dell'Internal Auditing solo quando il CAE riferisce direttamente al Board, è qualificato ed è posizionato a un livello all'interno dell'organizzazione che consente alla funzione Internal Audit di svolgere i propri servizi e responsabilità senza interferenze.

Standard 7.1 Indipendenza organizzativa

Requisiti

Il CAE deve confermare al Board l'indipendenza organizzativa della funzione Internal Audit almeno una volta all'anno. Ciò include la comunicazione di eventi che potrebbero aver compromesso l'indipendenza e le azioni o le misure di sicurezza impiegate per affrontare tali eventi.

Il CAE deve documentare nell'Internal Audit Charter le linee gerarchiche e il posizionamento organizzativo della funzione Internal Audit, come definito dal Board (si veda anche lo Standard "6.2 Internal Audit Charter").

Il CAE deve discutere con il Board e il Top Management eventuali ruoli e responsabilità attuali o proposti che potrebbero compromettere l'indipendenza della funzione Internal Audit, di fatto o solo apparentemente. Il CAE deve indicare al Board e al Top Management le misure a salvaguardia dell'indipendenza per gestire le compromissioni della stessa (reali, potenziali o presunte).

Quando il CAE ha uno o più ruoli oltre all'Internal Audit, le responsabilità, la natura del lavoro e le tutele stabilite devono essere documentate nell'Internal Audit Charter. Se tali aree di responsabilità sono oggetto di attività di Internal Audit, devono essere stabiliti processi alternativi per garantirne l'assurance, come, ad esempio, stipulare un contratto con un fornitore esterno obiettivo e competente che riferisca in modo indipendente al Board.

Quando le responsabilità diverse dall'Internal Auditing sono temporanee, la tutela su tali aree deve essere fornita da una terza parte indipendente durante l'incarico ad interim del CAE e per i successivi 12 mesi. Inoltre, il CAE deve definire un piano per trasferire tali responsabilità al management.

Se la struttura organizzativa non supporta l'indipendenza, il CAE deve documentare le motivazioni che limitano l'indipendenza e le eventuali garanzie che possono essere adottate per soddisfare questo principio.

Condizioni essenziali

Il Board

- Istituisce una relazione di riporto diretto con il CAE per consentire alla funzione Internal Audit di adempiere al proprio Mandato.
- Nomina e revoca il CAE.
- Fornisce input al Top Management per supportare la valutazione delle performance e la remunerazione del CAE.
- Offre al CAE l'opportunità di discutere questioni significative e sensibili, comprese le riunioni senza la presenza del Top Management.

- Richiede che il CAE sia posizionato a un livello dell'organizzazione che consenta di svolgere i servizi e le responsabilità di Internal Auditing senza interferenze da parte del management. Questo posizionamento fornisce l'autorità e lo status organizzativo per portare questioni direttamente al Top Management e inoltrarle al Board, quando necessario.
- Individua le possibili cause di compromissione effettiva o potenziale dell'indipendenza della funzione Internal Audit nel momento in cui si assegnano ruoli o responsabilità al CAE che esulano dall'ambito dell'Internal Audit.
- Si impegna a stabilire, con il Top Management e il CAE, adeguate misure di tutela dell'indipendenza della funzione Internal Audit nel caso in cui ruoli e responsabilità del CAE compromettano o sembrino compromettere l'indipendenza della stessa.
- Si impegna con il Top Management per garantire che la funzione Internal Audit sia priva di interferenze nella determinazione del suo perimetro di intervento, nell'esecuzione degli incarichi di Internal Audit e nella comunicazione dei risultati.

Il Top Management

- Posiziona la funzione Internal Audit a un livello all'interno dell'organizzazione che le consenta di svolgere i propri servizi e le proprie responsabilità senza interferenze, come indicato dal Board.
- Riconosce il rapporto diretto del CAE con il Board.
- Si impegna con il Board e il CAE per comprendere eventuali casi di compromissione dell'indipendenza della funzione Internal Audit causate dall'attribuzione di ruoli diversi dall'Internal Auditing o da altre circostanze e per supportare l'implementazione di tutele appropriate per gestire tali compromissioni.
- Fornisce input al Board in merito alla nomina e alla revoca del CAE.
- Sollecita il parere del Board sulla valutazione delle performance e sulla remunerazione del CAE.

Indicazioni per l'implementazione

L'Internal Auditing è più efficace quando la funzione Internal Audit risponde direttamente al Board (noto anche come "reporting funzionale al Board"), piuttosto che quando risponde direttamente al management responsabile delle attività su cui fornisce assurance e advisory. Il riporto diretto al Board consente alla funzione Internal Audit di eseguire i servizi di Internal Auditing e di comunicare i risultati dell'incarico senza interferenze o limitazioni. Esempi di interferenza includono la mancata fornitura tempestiva delle informazioni richieste da parte del management e la limitazione dell'accesso alle informazioni, al personale o agli spazi fisici. Limitare il budget o le risorse in modo da interferire con la capacità della funzione Internal Audit di operare in modo efficace è un esempio di indebita limitazione (si veda anche lo Standard "11.3 Comunicazione dei risultati").

Mentre il CAE riferisce funzionalmente al Board, il riporto amministrativo è spesso verso un esponente del management. Ciò consente l'accesso al Top Management e, al contempo, l'autorità di mettere in discussione le scelte del management. Per conseguire tale autorità, è prassi che il CAE riferisca amministrativamente al CEO o equivalente, sebbene il riporto a un altro Top Manager possa raggiungere lo stesso obiettivo, se vengono attuate adeguate misure di salvaguardia dell'indipendenza. I responsabili delle funzioni di Internal Audit di controllate, aree e divisioni dell'organizzazione, dovrebbero essere in grado di comunicare direttamente con il Top Management di tali aree.

Nel valutare se l'indipendenza possa essere compromessa, il CAE dovrebbe prendere in considerazione le relazioni, i ruoli e i riporti per determinare se esistono compromissioni effettive, potenziali o percepite. Inoltre, attraverso il confronto con le parti interessate, il CAE può essere in grado di risolvere eventuali situazioni di compromissione percepita che di fatto non incidono sulla capacità della funzione Internal Audit di svolgere le proprie responsabilità in modo indipendente.

L'indipendenza può essere compromessa quando:

- il CAE non ha comunicazione diretta o interazione con il Board;
- il management tenta di limitare il perimetro di intervento dei servizi di Internal Auditing che sono stati precedentemente approvati dal Board e documentati nell'Internal Audit Charter;
- il management tenta di limitare l'accesso ai dati, alle registrazioni, alle informazioni, al personale e agli spazi fisici necessari per eseguire i servizi di Internal Auditing;
- il management esercita pressioni sugli Internal Auditor affinché cancellino o modifichino i risultati dell'incarico di audit;
- il budget per la funzione Internal Audit è ridotto a un livello che rende la funzione incapace di adempiere alle proprie responsabilità, come delineato nell'Internal Audit Charter;
- un incarico di assurance è svolto dalla funzione Internal Audit o supervisionato dal CAE in un'area funzionale della quale egli è responsabile o sulla quale esercita la supervisione o un'influenza significativa;
- la funzione Internal Audit svolge, o il CAE supervisiona, i servizi di assurance relativi a un'attività gestita da un dirigente (non CEO) a cui il CAE riporta amministrativamente; ad esempio, il CAE riporta al Chief Financial Officer (CFO) ed è responsabile dell'audit sulla tesoreria, funzione che riporta allo stesso CFO.

Oltre alle responsabilità di gestione della funzione Internal Audit, al CAE viene talvolta chiesto di assumere ruoli diversi che possono compromettere o sembrano compromettere l'indipendenza della funzione Internal Audit. Alcuni esempi:

- un nuovo requisito normativo richiede la necessità immediata di sviluppare controlli e altre attività di risk management per essere conformi;
- il CAE dispone delle competenze più adeguate ad adattare le attività di risk management esistenti a un nuovo segmento di business o mercato;
- le risorse dell'organizzazione sono troppo limitate o l'organizzazione è troppo piccola per permettersi una funzione Compliance separata.

Quando si discutono i ruoli e le responsabilità diversi dall'audit con il Board e il Top Management, il CAE dovrebbe identificare le tutele appropriate a seconda che i ruoli siano permanenti o temporanei e destinati ad essere trasferiti al management.

Quando il Board concorda sul fatto che è compromessa l'indipendenza, il CAE dovrebbe suggerire al Board e al Top Management possibili misure per gestire i conseguenti rischi. È, inoltre, importante specificare una tempistica per il passaggio delle responsabilità temporanee diverse dall'audit al management.

Il requisito prevede che le attività di assurance siano supervisionate da una terza parte indipendente per i successivi 12 mesi dopo che il CAE ha lasciato le responsabilità temporanee in quell'area. Tuttavia, è necessaria una valutazione in quanto possono esserci circostanze in cui la percezione di una compromissione può continuare a presentarsi oltre i 12 mesi. Il CAE dovrebbe discutere con il Board e il Top Management se 12 mesi siano appropriati o meno.

Per determinare le altre parti alle quali comunicare eventuali compromissioni dell'indipendenza, il CAE dovrebbe considerare la natura delle stesse, l'impatto sull'affidabilità dei risultati dei servizi di Internal Auditing e sulle aspettative degli stakeholder. Se, dopo il completamento di un incarico di audit, viene rilevata una potenziale compromissione dell'indipendenza che può influire sull'affidabilità dei rilievi, delle raccomandazioni e/o delle valutazioni dell'incarico, il CAE dovrebbe discutere il caso con il management responsabile dell'attività oggetto dell'incarico, il Board, il Top Management e/o altri stakeholder interessati e determinare le azioni appropriate per risolvere la situazione (si vedano anche gli Standard "2.3 Comunicazione di limitazioni all'obiettività" e "11.4 Errori e omissioni").

Prima dell'assunzione di un CAE, il Board dovrebbe essere coinvolto nel processo di selezione e nomina. Ad esempio, il Board può discutere le qualifiche e le competenze necessarie per guidare la funzione Internal Audit e svolgere eventuali ruoli e responsabilità aggiuntivi previsti dall'organizzazione. Inoltre, il Board dovrebbe prendere in considerazione la possibilità di esaminare i curriculum dei candidati e partecipare ai colloqui prima che uno di essi venga selezionato.

Esempi di conformità

- L'Internal Audit Charter che comprenda l'indicazione delle linee gerarchiche relative alla funzione Internal Audit.
- Verbali di riunioni o altre evidenze che attestino la comunicazione del CAE con il Board e il Top Management in merito a potenziali compromissioni dell'indipendenza e delle misure di tutela previste.
- Verbali delle riunioni del Board o altra documentazione che dimostri che il CAE ha confermato con il Board il mantenimento dell'indipendenza della funzione Internal Audit o ha discusso di eventuali compromissioni dell'indipendenza che incidono sulla capacità della funzione Internal Audit di adempiere al proprio Mandato e sulle misure di tutela volte alla gestione di tali compromissioni.
- L'Internal Audit Charter che documenta l'approvazione da parte del Board dei ruoli e delle responsabilità a lungo termine diversi dall'audit e le corrispondenti tutele dell'indipendenza, compresa la durata prevista dei ruoli, delle responsabilità e delle tutele e il modo in cui l'efficacia delle stesse è valutata periodicamente.
- Metodologie documentate da seguire quando si sospetta o si identifica una compromissione dell'indipendenza.
- Piani d'azione formali che delineano le tutele specifiche per affrontare i problemi di indipendenza.
- Documentazione dei servizi di assurance erogati da altri fornitori interni o esterni a tutela dell'indipendenza.
- Verbali o altra documentazione comprovante l'approvazione da parte del Board della nomina o della revoca del CAE.

Standard 7.2 Qualifiche del Chief Audit Executive

Requisiti

Il CAE deve fornire tutte le informazioni e gli esempi necessari affinchè il Board possa comprendere quali competenze e qualifiche sono necessarie per gestire efficacemente la funzione Internal Audit.

Il CAE deve inoltre impegnarsi non solo a mantenere tali qualifiche e competenze, ma anche a migliorarle continuamente, in modo da poter ricoprire adeguatamente il ruolo e adempiere alle responsabilità che il Board gli ha conferito (si veda anche il Principio "3 Dimostrare la competenza").

Condizioni essenziali

Il Board

- Valuta i requisiti necessari affinché il CAE possa gestire efficacemente la funzione Internal Audit, come descritto nella Sezione "IV: Gestione della funzione Internal Audit".
- Approva il ruolo e le responsabilità del CAE e identifica qualifiche, esperienze e competenze che deve possedere per poterli ricoprire.
- Seleziona, in accordo con il Top Management, un CAE che possegga le qualifiche e le competenze necessarie per gestire efficacemente la funzione di Internal Audit e garantire la qualità dei servizi di Internal Audit.

Il Top Management

- Identifica insieme al Board qualifiche, esperienze e competenze che il CAE deve avere.
- Attiva la nomina, lo sviluppo e la retribuzione del CAE tramite i processi di gestione delle risorse umane dell'organizzazione.

Indicazioni per l'implementazione

Il Board e il Top Management collaborano per individuare le qualifiche e le competenze richieste al CAE. Tali competenze possono variare sia in base al Mandato di Internal Audit, sia in base alle caratteristiche dell'organizzazione in cui opera (complessità, esigenze, profilo di rischio, settore di business, area geografica, etc.). Le competenze e le qualifiche richieste vengono generalmente documentate nella job description e includono:

- la completa conoscenza e comprensione dei Global Internal Audit Standards e delle principali pratiche di Internal Audit;
- l'esperienza nella costituzione e nella gestione di una funzione di Internal Audit, dalla selezione degli Internal Auditor, fino alla loro assunzione, formazione e sviluppo continuo delle competenze;
- il conseguimento di certificazioni professionali riconosciute come ad es. il CIA, Certified Internal Auditor®;
- la leadership;
- l'esperienza pregressa nel settore/business dell'organizzazione.

Il CAE può essere selezionato anche sulla base di caratteristiche e competenze diverse da queste che possono essere completate da quelle già presenti nella funzione, soprattutto nel caso in cui provenga da un ruolo o un settore di business diversi. In questi casi, dovrebbe collaborare con gli altri professionisti della funzione al fine di sviluppare la necessaria esperienza.

Il Board può rivedere e approvare la job description del CAE per garantire che rifletta le qualifiche e le competenze richieste.

Il Board dovrebbe spingere il CAE a seguire regolarmente corsi di formazione, ad iscriversi alle associazioni professionali, a conseguire le certificazioni e a perseguire uno sviluppo professionale continuo (si veda anche il Principio "3 Dimostrare la competenza").

Data l'importanza di questo ruolo, dovrebbe essere delineato un piano di successione al fine di identificare candidati interni o esterni all'organizzazione che possano sostituire il CAE in caso di necessità. Questo piano dovrebbe essere in linea con le policy di successione dell'organizzazione e dovrebbe essere condiviso con il Board e il Top Management.

Esempi di conformità

- Approvazione documentata da parte del Board della job description del CAE e della relativa valutazione delle qualifiche e competenze ritenute necessarie.
- Piani di formazione professionale del CAE e relativi attestati di partecipazione.
- Attestati di partecipazione ad attività di associazioni professionali.
- Conversazioni documentate tra il CAE, il Board, il Top Management e/o la funzione Risorse Umane in merito al piano di successione.

Principio 8 Sottoposta alla supervisione del Board

Il Board supervisiona la funzione di Internal Audit per garantirne l'efficacia.

La supervisione del Board è essenziale per garantire l'efficacia della funzione di Internal Audit. Per soddisfare questo principio è necessario che tra il Board e il CAE si instauri una relazione interattiva e collaborativa e che il Board assicuri alla funzione risorse sufficienti ad adempiere al Mandato. Il Board riceve inoltre una valutazione delle performance del CAE e della funzione di Internal Audit attraverso il programma di assurance e miglioramento della qualità e revisiona direttamente i risultati del quality assessment esterno.

Standard 8.1 Interazione con il Board

Requisiti

Il CAE deve fornire al Board le informazioni necessarie per adempiere alle proprie responsabilità di supervisore. Queste informazioni possono essere richieste direttamente dal Board o selezionate dal CAE, in base alla sua valutazione di rilevanza.

Il CAE deve riportare al Board e al Top Management:

- il piano di Audit, il budget e le successive revisioni ritenute più significative (si vedano anche gli Standard "6.3 Supporto dal Board e dal Top Management" e "9.4 Piano di Audit");
- le modifiche al Mandato o al Charter (si vedano anche gli Standard "6.1 Mandato di Internal Audit" e "6.2 Internal Audit Charter");
- le potenziali limitazioni all'indipendenza (si veda anche lo Standard "7.1 Indipendenza organizzativa");
- i risultati delle attività di Internal Auditing, assurance, advisory, approfondimento e monitoraggio, comprese le conclusioni e le tematiche di rilievo (si vedano anche gli Standard "11.3 Comunicazione dei risultati", "14.5 Giudizio dell'incarico" e "15.2 Conferma dell'attuazione delle raccomandazioni o piani d'azione");
- i risultati del programma di assurance e miglioramento della qualità (si vedano anche gli Standard "8.3 Qualità", "8.4 Quality assessment esterno", "12.1 Quality assessment interno" e "12.2 Misurazione delle performance").

Ci possono essere casi in cui il CAE non è d'accordo con il Top Management o con altri stakeholder in merito all'ambito, ai rilievi o altri aspetti di un incarico, che possono influire sulla capacità della funzione di Internal Audit di adempiere alle proprie responsabilità. In questi casi, il CAE deve fornire al Board i fatti e le circostanze sulla base dei quali decidere se intervenire.

Condizioni essenziali

Il Board

- Comunica con il CAE per comprendere come la funzione di Internal Audit stia adempiendo al proprio Mandato.
- Condivide con il CAE la propria visione sulle strategie, gli obiettivi e i rischi dell'organizzazione per supportarlo nella definizione delle priorità dell'Internal Audit.
- Definisce con il CAE le proprie aspettative in merito a:
  - frequenza delle comunicazioni al Board stesso;
  - criteri per l'individuazione delle questioni che devono essere portate all'attenzione del Board, ad esempio i rischi significativi che superano la soglia di risk tolerance;
  - processo per l'escalation di questioni rilevanti per il Board.

- Acquisisce informazioni in merito all'efficacia dei processi di governance, risk management e controllo dell'organizzazione in base ai risultati degli incarichi di Internal Audit e alle discussioni con il Top Management.
- Discute con il CAE eventuali punti di disaccordo con il Top Management o altri stakeholder e gli fornisce il supporto necessario per adempiere alle responsabilità delineate nel Mandato di Internal Audit.

Il Top Management

- Condivide con il CAE la propria visione sulle strategie, gli obiettivi e i rischi dell'organizzazione per supportarlo nella definizione delle priorità dell'Internal Audit.
- Supporta il Board nel comprendere l'efficacia dei processi di governance, risk management e controllo dell'organizzazione.
- Collabora con il Board e il CAE nel processo di escalation di questioni rilevanti per il Board.

Indicazioni per l'implementazione

Per fornire al Board le informazioni necessarie per adempiere alle proprie responsabilità di supervisione, è necessario che la comunicazione sia bidirezionale. Il CAE può utilizzare molteplici mezzi, come report e presentazioni scritte e orali, riunioni formali e discussioni informali e può, inoltre, includere le aspettative del Board nelle metodologie di Internal Audit. Periodicamente, il CAE e il Board dovrebbero confermare che la frequenza, la natura e il contenuto delle comunicazioni soddisfano le aspettative del Board e gli forniscono il supporto necessario per adempiere alle proprie responsabilità di supervisione.

La scelta della frequenza delle comunicazioni tra il Board e il CAE dovrebbe tenere conto della necessità di comunicare tempestivamente le questioni rilevanti. Il CAE dovrebbe chiedere al Board quali sono le sue aspettative in merito alla comprensione e supervisione non solo dei rischi finanziari, ma anche di quelli non finanziari, come ad esempio, iniziative strategiche, cybersecurity, salute e sicurezza, sostenibilità, resilienza aziendale e reputazione.

Per identificare le questioni per le quali il CAE è tenuto a fare escalation al di sopra del Top Management, possono essere definiti criteri di rilevanza e di materialità rispetto al livello di risk tolerance. I criteri dovrebbero essere corredati anche dal processo che il CAE segue per presentare le comunicazioni al Board. In genere, le questioni su cui il CAE e il Top Management si trovano in disaccordo, dovrebbero essere preventivamente condivise in modo da presentare al Board informazioni complete e accurate.

Solitamente, le sedute del Board consentono una comunicazione formale con cadenza almeno trimestrale. Inoltre, il CAE e i membri del Board spesso comunicano anche tra una riunione e l'altra, talvolta in maniera informale.

Esempi di conformità

- Ordini del giorno delle riunioni del Board e relativi verbali che documentano la natura, gli argomenti e la frequenza delle discussioni con il CAE.
- Presentazioni del CAE al Board.
- Comunicazioni di Internal Audit ai membri del Board.
- Documentazione dei criteri per l'identificazione delle questioni rilevanti da portare all'attenzione del Board e definizione di un processo di comunicazione o escalation.

Standard 8.2 Risorse

Requisiti

Il CAE deve valutare se le risorse di Internal Audit sono sufficienti per soddisfare il Mandato di Internal Audit e per realizzare il piano di Audit. Se non lo sono, deve sviluppare una strategia per ottenere risorse sufficienti e deve informare il Board in merito all'impatto dell'insufficienza delle risorse e alle soluzioni che intende implementate per affrontarla.

Condizioni essenziali

Il Board

- Collabora con il Top Management per fornire alla funzione di Internal Audit le risorse sufficienti per soddisfare il Mandato di Internal Audit e realizzare il piano di Audit.
- Almeno una volta all'anno, condivide con il CAE la sufficienza, sia in termini numerici, sia di capacità, delle risorse di Internal Audit per soddisfare il Mandato di Internal Audit e realizzare il piano di Audit.
- Considera l'impatto dell'insufficienza di risorse sia sul Mandato, che sul piano di Audit.
- Si impegna, con il Top Management e il Chief Audit Executive, a trovare soluzioni all'insufficienza di risorse.

Il Top Management

- Collabora con il Board per fornire alla funzione Internal Audit risorse sufficienti per soddisfare il Mandato di Internal Audit e realizzare il piano di Audit.
- Si impegna, con il Board e il CAE, a trovare soluzioni all'insufficienza di risorse.

Indicazioni per l'implementazione

Per valutare se le risorse sono sufficienti per soddisfare il Mandato di Internal Audit e realizzare il piano, il CAE può eseguire una gap analysis tra le risorse disponibili all'interno della funzione Internal Audit e quelle necessarie per svolgere le attività di Internal Auditing (si vedano anche il Principio "10 Gestire le risorse" e i relativi Standard). La strategia del CAE dovrebbe prevedere un piano delle risorse, che può includere una richiesta di budget, e dovrebbe prendere in considerazione sia le opzioni di inserimento di personale, sia l'utilizzo della tecnologia per l'esecuzione delle attività di audit. Questo piano può anche includere un'analisi dei costi e benefici dei vari approcci da presentare al Board.

Sebbene il Board e il CAE si confrontino sulle risorse almeno una volta all'anno in occasione della presentazione del piano di Audit, è una buona pratica avere una discussione trimestrale sul tema. Il confronto dovrebbe includere l'esame delle opzioni per ottenere la copertura di Internal Audit desiderata, ad esempio l'esternalizzazione o i prestiti di risorse, nonché l'implementazione di tecnologie per migliorare l'efficienza e l'efficacia della funzione.

Esempi di conformità

- Ordini del giorno, verbali delle riunioni e comunicazioni tra il CAE e il Board e/o il Top Management, che documentano i confronti su quante e quali risorse di Internal Audit siano da considerare sufficienti.
- Piani che indicano quante e quali risorse di Internal Audit sono necessarie per realizzare il piano di Audit.

- Richieste di budget relative alle risorse di Internal Audit.
- Documentazione relativa alle gap analysis tra il piano di Audit e le risorse disponibili.
- Documentazione relativa all'analisi costi-benefici.
- Documentazione relativa alla strategia del CAE per il reperimento delle risorse.

Standard 8.3 Qualità

Requisiti

Il CAE deve sviluppare, implementare e mantenere un programma di assurance e miglioramento della qualità che copra tutti gli aspetti della funzione di Internal Audit. Il programma prevede due tipi di valutazioni:

- Assessment esterno (si veda lo Standard "8.4 Quality assessment esterno");
- Assessment interno (si veda lo Standard "12.1 Quality assessment interno").

Almeno una volta all'anno, il CAE deve comunicare i risultati del quality assessment interno al Board e al Top Management. I risultati del quality assessment esterno devono essere comunicati una volta completati. In entrambi i casi, la comunicazione comprende:

- l'attestazione di conformità della funzione Internal Audit agli Standard e il relativo raggiungimento degli obiettivi di performance;
- se applicabile, l'attestazione di compliance alle leggi e/o ai regolamenti pertinenti;
- se necessario, i piani per affrontare le carenze della funzione Internal Audit e le opportunità di miglioramento.

Condizioni essenziali

Il Board

- Condivide con il CAE il programma di assurance e miglioramento della qualità, come descritto nella Sezione "IV: Gestione della funzione Internal Audit".
- Approva, almeno una volta all'anno, gli obiettivi della funzione Internal Audit (si veda lo Standard "12.2 Misurazione delle performance").
- Esamina l'efficacia e l'efficienza della funzione Internal Audit. Ciò include:
  - la revisione degli obiettivi di performance della funzione Internal Audit, tra cui la conformità agli Standard e a leggi o regolamenti, la capacità di adempiere al Mandato, lo stato di avanzamento del piano di Audit;
  - l'analisi dei risultati del programma di assurance e miglioramento della qualità della funzione Internal Audit;
  - la valutazione del grado di raggiungimento degli obiettivi di performance della funzione Internal Audit.

Il Top Management

- Fornisce input in merito agli obiettivi di performance della funzione Internal Audit.
- Partecipa, insieme al Board, alla valutazione annuale del CAE e della funzione Internal Audit.

Indicazioni per l'implementazione

Le comunicazioni del CAE al Board e al Top Management in merito al programma di assurance e miglioramento della qualità della funzione Internal Audit dovrebbero includere:

- l'ambito, la frequenza e i risultati dei quality assessment interni ed esterni condotti sotto la direzione o con l'assistenza del CAE;
- i piani, concordati con il Board, che definiscono come gestire le carenze e implementare le opportunità di miglioramento;
- lo stato di completamento delle azioni concordate.

Il quality assessment della funzione Internal Audit può prendere in considerazione:

- il contributo apportato al miglioramento dei processi di governance, risk management e controllo;
- la produttività del personale della funzione Internal Audit (ad esempio, il confronto tra le ore pianificate e le ore effettive sui progetti o tra il tempo speso per i progetti di audit e quello speso per le pratiche amministrative);
- la conformità a leggi e/o regolamenti in materia di Internal Audit;
- l'efficienza, in termini di costi, dei processi di Internal Audit;
- la solidità delle relazioni con il Top Management e gli altri stakeholder principali;
- altri indicatori di performance (si veda anche lo Standard "12.2 Misurazione delle performance").

Esempi di conformità

- Ordini del giorno e verbali delle riunioni del Board che documentano le discussioni con il CAE in merito al programma di assurance e miglioramento della qualità della funzione Internal Audit.
- Presentazioni, o altro, del CAE in merito ai risultati dei quality assessment e lo stato d'avanzamento dei piani per implementare le opportunità di miglioramento.
- Carte di lavoro del programma di assurance e miglioramento della qualità o altre evidenze che dimostrino il completamento delle attività correlate.

Standard 8.4 Quality assessment esterno

Requisiti

Il CAE deve sviluppare un piano per il quality assessment esterno e discuterlo con il Board. Il quality assessment esterno deve essere effettuato almeno una volta ogni cinque anni da un valutatore o da un team di valutatori qualificati e indipendenti. Il requisito può essere soddisfatto anche mediante un'autovalutazione con convalida indipendente.

Il CAE deve assicurarsi che almeno una persona all'interno del team di assessment sia in possesso della certificazione CIA® in corso di validità.

Condizioni essenziali

Il Board

- Discute con il CAE i piani del quality assessment esterno della funzione Internal Audit svolto da valutatori indipendenti e qualificati.
- Collabora con il Top Management e il CAE per definire l'ambito e la frequenza del quality assessment esterno.
- Valuta le responsabilità e i requisiti della funzione Internal Audit e del CAE, come indicati nell'Internal Audit Charter, nella definizione dell'ambito del quality assessment esterno.
- Esamina e approva il piano definito dal CAE per l'esecuzione del quality assessment esterno in merito a:
  - ambito e frequenza delle valutazioni;
  - competenze e indipendenza dei valutatori;
  - motivazioni della scelta di condurre un'autovalutazione con convalida indipendente, anziché un quality assessment esterno.
- Richiede i risultati completi del quality assessment esterno o della convalida esterna dell'autovalutazione.
- Esamina e approva i piani definiti dal CAE per gestire le carenze identificate e le opportunità di miglioramento, se applicabile.
- Approva la tempistica per il completamento dei piani e ne monitora l'avanzamento effettivo.

Il Top Management

- Collabora con il Board e il CAE per la definizione dell'ambito e della frequenza del quality assessment esterno.
- Esamina i risultati del quality assessment esterno, collabora con il CAE e il Board per la definizione dei piani relativi alla gestione delle carenze identificate e all'implementazione delle opportunità di miglioramento, laddove applicabili, e le relative tempistiche di completamento.

Indicazioni per l'implementazione

Il Board e il CAE possono decidere in merito all'opportunità di condurre l'assessment esterno con una frequenza superiore a quella quinquennale. I motivi di questa decisione possono essere molteplici: cambiamenti nelle nomine (ad esempio, per il Top Management o il CAE), cambiamenti significativi nelle metodologie di Internal Audit, fusione di due o più funzioni di Internal Audit, un significativo turnover del personale o altri ancora. Inoltre, alcune organizzazioni, come quelle che operano in settori fortemente regolamentati, potrebbero preferire o essere tenute ad aumentare la frequenza o l'ambito dei quality assessment esterni.

Il quality assessment esterno dovrebbe includere un riesame completo dell'adeguatezza della funzione Internal Audit per quanto riguarda:

- la conformità ai Global Internal Audit Standards;
- il Mandato, il Charter, la strategia, le metodologie, i processi, il risk assessment e il piano di Audit;
- la conformità alle leggi e/o ai regolamenti di riferimento;
- i criteri e i parametri di misurazione delle performance, nonché i risultati dell'assessment;
- le competenze, la diligenza professionale, l'utilizzo di strumenti e tecniche adeguati e l'attenzione allo sviluppo professionale continuo;
- le qualifiche e le competenze, comprese quelle del Chief Audit Executive, come definito nella job description e nel profilo di selezione dell'organizzazione;
- l'integrazione nei processi di governance dell'organizzazione, incluse le relazioni con i soggetti coinvolti nel posizionare la funzione Internal Audit in maniera tale da permetterle di operare in modo indipendente;
- il contributo ai processi di governance, risk management e controllo dell'organizzazione;
- il contributo al miglioramento delle attività operative dell'organizzazione e alla sua capacità di raggiungere gli obiettivi;
- la capacità di soddisfare le aspettative del Board, del Top Management e degli stakeholder.

Oltre al requisito che almeno un membro sia certificato CIA®, bisogna considerare anche altre importanti qualifiche del team di valutazione:

- conoscenza teorica e pratica degli Standard e delle principali pratiche di Internal Audit;
- esperienza come CAE o livello senior analogo;
- esperienza nel settore di attività dell'organizzazione;
- esperienza pregressa nell'esecuzione di quality assessment esterni;
- completamento della formazione esterna riconosciuta dall'Institute of Internal Auditors sul quality assessment;
- evidenze che dimostrano l'assenza di conflitti di interesse, reali o potenziali, di chi svolge l'assessment.

Il CAE dovrebbe prendere in considerazione le potenziali limitazioni all'indipendenza dei valutatori dovute a relazioni passate, presenti o future con l'organizzazione, il suo personale o la sua funzione Internal Audit. Se un potenziale valutatore è un ex collaboratore dell'organizzazione, si dovrebbe valutare il periodo di tempo in cui lo stesso è stato indipendente. Esempi di potenziali limitazioni sono:

- audit esterno di bilancio;
- supporto alla funzione Internal Audit;
- relazioni personali;
- partecipazione precedente o programmata a quality assessment interni;
- servizi di advisory su processi di governance, risk management e controllo, financial reporting o altre aree.

Soggetti appartenenti a una diversa funzione dell'organizzazione, sebbene distinti dalla funzione Internal Audit, non sono considerati indipendenti ai fini della conduzione di un assessment esterno. Allo stesso modo, soggetti di un'organizzazione correlata (ad esempio, la controllante, una controllata, una filiale) non sono considerati indipendenti. Nel settore pubblico, le funzioni Internal Audit in entità distinte all'interno della stessa istituzione non sono considerate indipendenti se riferiscono allo stesso CAE.

Gli assessment tra due organizzazioni analoghe non sono considerati indipendenti. Tuttavia, gli assessment a rotazione tra tre o più organizzazioni analoghe (ovvero operanti nello stesso settore di business, associazioni a livello geografico o altri gruppi) possono essere considerati indipendenti. Si dovrebbe comunque controllare che l'indipendenza e l'obiettività non siano compromesse e che tutti i membri del team siano in grado di adempiere alle proprie responsabilità.

Un'autovalutazione con convalida indipendente include in genere:

- un assessment interno completo e documentato che simula il processo di quality assessment esterno in termini di valutazione della conformità della funzione Internal Audit agli Standard;
- la convalida indipendente, da parte di un valutatore o di un team di valutatori esterni qualificati che l'assessment interno sia stato condotto in modo completo e accurato;
- benchmarking, best practice e interviste con i principali stakeholder, come i membri del Board, il Top Management e il management di linea.

Esempi di conformità

- Verbali delle riunioni in cui il piano di quality assessment esterno è condiviso e approvato dal CAE e dal Board.
- Report del quality assessment esterno redatto e convalidato da un valutatore qualificato e indipendente.
- Presentazioni dei valutatori esterni al Board sui risultati del quality assessment esterno.
- Presentazioni del CAE al Board sui risultati del quality assessment esterno e sui piani d'azione.

Sezione IV: Gestione della funzione Internal Audit

Il **CAE** ha la responsabilità di gestire la funzione Internal Audit in conformità con l'Internal Audit Charter e i Global Internal Audit Standards, realizzare una pianificazione strategica, ottenere e impiegare risorse adeguate, costruire relazioni, comunicare con gli stakeholder e garantire lo svolgimento delle attività di auditing e il miglioramento delle performance della funzione.

Che sia un dipendente dell'organizzazione o che abbia un contratto a termine come fornitore esterno di servizi, ci si aspetta che il CAE agisca conformemente agli Standard e ottemperi alle responsabilità descritte in questa Sezione. Job title e responsabilità specifiche possono variare da un'organizzazione all'altra.

Anche se il CAE può delegare compiti specifici ad altri professionisti qualificati della funzione Internal Audit, la responsabilità finale è comunque sua.

La relazione di riporto diretto del CAE al Board consente alla funzione Internal Audit di soddisfare il proprio Mandato (si veda anche lo Standard "7.1 Indipendenza organizzativa"). Inoltre, il CAE generalmente riporta in maniera diretta al Top Manager di più alto livello, ad es. al Chief Executive Officer, per il necessario supporto nelle attività quotidiane e per conferirgli status e autorità necessari a garantire che i risultati dell'Internal Audit siano tenuti in debita considerazione.

Principio 9 Pianificare strategicamente

Il CAE pianifica strategicamente al fine di garantire alla funzione Internal Audit un posizionamento che permetta di adempiere al suo Mandato e raggiungere un successo sostenibile nel tempo.

La pianificazione strategica richiede che il CAE comprenda il Mandato di Internal Audit e i processi di governance, risk management e controllo dell'organizzazione. Una funzione Internal Audit dotata di risorse e posizionamento adeguati sviluppa e implementa una strategia che supporti il successo dell'organizzazione. Inoltre, il CAE definisce e implementa metodologie per guidare la funzione e sviluppare il piano di Audit.

Standard 9.1 Comprensione dei processi di governance, risk management e controllo

Requisiti

Per sviluppare una strategia e un piano di Audit efficaci, il CAE deve comprendere la governance, il risk management e i processi di controllo dell'organizzazione.

Per comprendere i processi di governance, il CAE deve considerare in che modo l'organizzazione:

- stabilisce gli obiettivi e prende decisioni strategiche e operative;
- supervisiona il risk management e il controllo;
- promuove una cultura etica;
- attua un'efficace gestione delle performance e delle responsabilità;
- struttura le proprie funzioni manageriali e operative;
- comunica le informazioni sui rischi e sui controlli al proprio interno;
- coordina le attività e le comunicazioni tra il Board, i fornitori interni ed esterni di servizi di assurance e il management.

Per comprendere il risk management e i processi di controllo, il CAE deve considerare il modo in cui l'organizzazione identifica e valuta i rischi significativi, seleziona i processi di controllo appropriati, identifica e gestisce le seguenti aree di rischio:

- affidabilità e integrità delle informazioni economico-finanziarie e operative;
- efficacia ed efficienza delle operazioni e dei programmi;
- salvaguardia del patrimonio aziendale;
- conformità a leggi e regolamenti.

Indicazioni per l'implementazione

La comprensione del CAE è costruita mediante la raccolta di informazioni ad ampio spettro e la loro osservazione in modo complessivo. Le fonti di informazioni sono rappresentate dai confronti con il Board e il Top Management, dalle revisioni dei verbali e delle presentazioni del Board e del Top Management, dai report e dalle carte di lavoro degli incarichi di Internal Audit, nonché dalle valutazioni e dalle relazioni degli altri fornitori di servizi di assurance e advisory.

Comprensione dei processi di governance

Il CAE dovrebbe essere ben informato sui più rilevanti principi, framework e modelli di governance nel loro complesso e sulle linee guida professionali specifiche per l'industry e il settore di business in cui l'organizzazione opera. Sulla base di queste informazioni, il CAE dovrebbe comprendere se qualcuno di questi riferimenti è stato adottato e dovrebbe valutare la maturità dei processi di governance dell'organizzazione. La struttura di governance, i processi e le pratiche possono essere influenzati da caratteristiche specifiche quali il tipo di organizzazione, le dimensioni, la complessità, la struttura, la maturità dei processi, così come i requisiti legali e/o normativi ai quali l'organizzazione è soggetta.

Il CAE può esaminare gli statuti e gli ordini del giorno del Board e dei comitati e i verbali delle loro riunioni per ottenere ulteriori informazioni sul ruolo che il Board ricopre nella governance aziendale, in particolare per quanto riguarda il processo decisionale strategico e operativo.

Il CAE può parlare con le figure chiave della governance (ad esempio, il Presidente del Board, un alto funzionario eletto o nominato in un'organizzazione governativa, il Direttore Risorse Umane, il Compliance Officer e il Risk Officer) per raggiungere una più chiara comprensione dei processi e delle attività di assurance dell'organizzazione. Il CAE può esaminare i report e/o i risultati delle revisioni di governance precedentemente completate, prestando particolare attenzione a eventuali problemi individuati.

Comprensione dei processi di risk management

Il CAE dovrebbe comprendere i principi, i framework e i modelli di risk management nel loro complesso, nonché le linee guida professionali specifiche per l'industry e il settore di business in cui l'organizzazione opera. Il CAE dovrebbe raccogliere informazioni per valutare la maturità dei processi di risk management dell'organizzazione e per capire se ha definito un risk appetite e implementato una strategia e/o un framework di risk management. I confronti con il Board e il Top Management aiutano il CAE nella comprensione delle loro prospettive e priorità relative al risk management dell'organizzazione.

Per raccogliere informazioni sui rischi, il CAE dovrebbe esaminare i risk assessment recenti e le comunicazioni al riguardo effettuate dal management, dai responsabili del risk management, dagli Auditor esterni, dai regulator e dagli altri fornitori interni ed esterni di servizi di assurance.

Comprensione dei processi di controllo

Il CAE dovrebbe acquisire familiarità con i framework di controllo internazionalmente adottati ed esaminare quelli utilizzati dall'organizzazione. Per ogni ambito organizzativo, il CAE dovrebbe sviluppare e mantenere un'ampia comprensione dei processi di controllo dell'organizzazione e della loro efficacia. Il CAE potrebbe, inoltre, sviluppare una matrice di rischi e controlli a livello dell'intera organizzazione per:

- documentare i rischi identificati che possono influire sulla capacità di raggiungere gli obiettivi dell'organizzazione;
- indicare la significatività dei rischi stessi;
- comprendere i controlli chiave nei processi aziendali;
- comprendere quali controlli sono stati attuati per verificarne l'adeguatezza del disegno e il corretto funzionamento.

Una conoscenza approfondita dei processi di governance, risk management e controllo dell'organizzazione consente al CAE di identificare e valorizzare quelle opportunità di fornire servizi di Internal Audit che possano contribuire al successo dell'organizzazione e che costituiscono la base della strategia e del piano di Audit.

Esempi di conformità

- Documentazione a supporto della ricerca, raccolta e valutazione da parte del CAE dei framework e dei processi di governance, risk management e controllo utilizzati dall'organizzazione, tra cui:
  - gli statuti del Board e dei comitati, che delineano le aspettative di governance dell'organizzazione;
  - la valutazione di leggi, regolamenti e altri requisiti relativi alla governance, al risk management e ai processi di controllo.
- Revisione degli ordini del giorno e dei verbali delle riunioni del Board che documentano la discussione dei processi di governance, risk management e controllo dell'organizzazione, comprese le strategie, gli approcci e la supervisione di ciascuno di essi.

- Verbali di riunioni o appunti di confronti tra il CAE e le figure che ricoprono ruoli nella governance e nel risk management dell'organizzazione.
- Revisione della dichiarazione di risk appetite dell'organizzazione o evidenze delle comunicazioni con il Board e il Top Management in merito ai livelli di risk appetite e risk tolerance dell'organizzazione.
- Documentazione della formazione o informazione fornita al personale dell'Internal Audit in merito ai processi di governance, risk management e controllo dell'organizzazione.
- Revisione delle strategie aziendali e dei business plan.
- Revisione delle comunicazioni ricevute dai regulator.
- Evidenze della comprensione della matrice di rischi e controlli dell'organizzazione.

Standard 9.2 Strategia dell'Internal Audit

Requisiti

Il CAE deve sviluppare e implementare una strategia per la funzione Internal Audit, che supporti gli obiettivi strategici e il successo dell'organizzazione e sia in linea con le aspettative del Board, del Top Management e degli altri stakeholder chiave.

La strategia di Internal Audit è un piano progettato per raggiungere obiettivi complessivi e sostenibili nel tempo. La strategia di Internal Audit deve includere la vision, gli obiettivi strategici e le iniziative di supporto e aiuta la funzione Internal Audit nell'adempimento del Mandato.

Il CAE deve riesaminare periodicamente la strategia di Internal Audit con il Board e il Top Management.

Indicazioni per l'implementazione

Per sviluppare la vision e gli obiettivi della strategia di Internal Audit, il CAE dovrebbe inizialmente considerare la strategia e gli obiettivi dell'organizzazione e le aspettative del Board e del Top Management. Il CAE può anche prendere in considerazione i tipi di servizi da svolgere e le aspettative degli altri stakeholder della funzione Internal Audit, come concordato nell'Internal Audit Charter.

La vision descrive lo stato a tendere della funzione Internal Audit – ad es. a tre/cinque anni - e fornisce indicazioni per adempiere al Mandato. La vision ha inoltre l'obiettivo di spingere gli Internal Auditor verso il miglioramento continuo. Gli obiettivi strategici definiscono traguardi raggiungibili al fine di realizzare la vision. Le iniziative di supporto delineano tattiche e passi più specifici per raggiungere ciascun obiettivo strategico.

Un metodo per sviluppare una strategia consiste nell'identificare e analizzare i punti di forza, le debolezze, le opportunità e le minacce della funzione Internal Audit, un esercizio utilizzato per individuarne le aree di miglioramento. Un altro approccio consiste nell'eseguire una gap analysis tra lo stato attuale e quello desiderato della funzione Internal Audit.

Le iniziative a supporto della strategia dovrebbero includere:

- opportunità di sviluppo delle competenze per gli Internal Auditor;
- l'introduzione e l'applicazione della tecnologia per migliorare l'efficienza e l'efficacia della funzione Internal Audit;
- opportunità di miglioramento della funzione Internal Audit nel suo complesso (es. metodologie, organizzazione, ecc.).

Quando il CAE determina gli obiettivi strategici e le iniziative a supporto, è necessario assegnare ad ogni attività delle priorità e delle tempistiche.

La strategia di Internal Audit dovrebbe essere adattata ogni volta che si verificano cambiamenti negli obiettivi strategici dell'organizzazione o nelle aspettative degli stakeholder. Alcuni fattori che possono indurre a una revisione più frequente della strategia di Internal Audit sono:

- i cambiamenti nella strategia dell'organizzazione o nella maturità dei suoi processi di governance, risk management e controllo;
- i cambiamenti nelle policy e nelle procedure dell'organizzazione o nelle leggi e/o regolamenti a cui l'organizzazione è soggetta;
- i cambiamenti relativi ai membri del Board, del Top Management o la sostituzione del CAE;
- i risultati degli assessment interni ed esterni della funzione Internal Audit.

Il CAE potrebbe definire una tempistica per l'attuazione della strategia di Internal Audit e delle relative misure di performance (si veda anche lo Standard "12.2 Misurazione delle performance"). Una revisione periodica della strategia di Internal Audit dovrebbe includere un confronto con il Board e il Top Management sui progressi compiuti dalla funzione Internal Audit nelle diverse iniziative.

Esempi di conformità

- Un documento di strategia di Internal Audit che comprenda la vision, gli obiettivi strategici e le iniziative a supporto.
- I verbali o la corrispondenza delle riunioni in cui sono state condivise le aspettative del Board, del Top Management e/o altri stakeholder.
- Note che mostrano le informazioni e le analisi alla base della strategia.
- Le metodologie di Internal Audit per l'elaborazione e la revisione della strategia di Internal Audit e il relativo monitoraggio.
- I risultati di self-assessment periodici o di altre revisioni dello stato di avanzamento delle iniziative.

Standard 9.3 Metodologie

Requisiti

Il CAE deve stabilire metodologie per guidare la funzione Internal Audit in modo sistematico e disciplinato al fine di implementare la strategia di Internal Audit, sviluppare il piano di Audit e conformarsi agli Standard. Deve valutare l'efficacia delle metodologie e aggiornarle, se necessario, per migliorare la funzione Internal Audit e rispondere a cambiamenti significativi che interessano la funzione stessa. Il CAE deve, inoltre, fornire agli Internal Auditor opportunità di formazione sulle metodologie (si vedano anche i Principi "13 Pianificare gli incarichi in modo efficace", "14 Condurre l'incarico", "15 Comunicare i risultati dell'incarico e monitorare i piani d'azione" e i relativi Standard).

Indicazioni per l'implementazione

La forma, il contenuto, il livello di dettaglio e la documentazione relativa alle metodologie possono variare in base alle dimensioni, alla struttura, alla complessità, ai requisiti settoriali e normativi e alla maturità, sia dell'organizzazione, sia della funzione Internal Audit. Le metodologie possono consistere in singoli documenti (come le procedure operative standard) o possono essere raccolte in un manuale di Internal Audit o integrate in un software di gestione dell'Internal Audit. Le metodologie di Internal Audit forniscono istruzioni e criteri specifici che supportano gli Internal Auditor nell'implementare gli Standard e nello svolgere servizi di qualità. Inoltre, le metodologie di Internal Audit descrivono i processi e le procedure per la comunicazione, la gestione delle questioni operative e amministrative e la supervisione della funzione Internal Audit (si vedano anche gli Standard "14.3 Valutazione dei rilievi", "14.5 Giudizio dell'incarico" e "15.2 Conferma dell'attuazione delle raccomandazioni o piani d'azione").

Per implementare la strategia, attuare il piano di Audit ed essere conformi agli Standard, le metodologie dovranno, per esempio, documentare l'approccio della funzione Internal Audit rispetto alle seguenti attività:

- valutare rischi dell'organizzazione e di ogni singolo incarico;
- sviluppare e aggiornare il piano di Audit;
- definire il bilanciamento tra assurance e advisory;
- coordinarsi con i fornitori di assurance interni ed esterni;
- gestire i fornitori di servizi esterni, se utilizzati;
- eseguire gli incarichi di Internal Audit;
- comunicare durante le attività di Internal Audit;
- conservare e rilasciare documenti e altre informazioni, secondo le linee guida dell'organizzazione e i requisiti normativi o di altro tipo pertinenti;
- monitorare e confermare l'attuazione delle raccomandazioni degli Internal Auditor e/o dei piani d'azione indicati dal management;
- garantire la qualità e il miglioramento della funzione Internal Audit;
- sviluppare un sistema di misurazione delle performance per valutare i progressi verso il raggiungimento degli obiettivi;
- eseguire servizi aggiuntivi identificati nel Mandato di Internal Audit.

L'efficacia delle metodologie di Internal Audit dovrebbe essere rivalutata in occasione dei quality assessment della funzione Internal Audit. I motivi che portano all'aggiornamento di metodologie consolidate includono cambiamenti significativi negli Standard e nelle linee guida dell'Internal Audit, nei requisiti legali e/o normativi, nella tecnologia e nelle dimensioni o nella composizione della funzione. Anche l'arrivo di un nuovo CAE o un nuovo Presidente del Board possono giustificare una revisione delle metodologie di Internal Audit.

Esempi di conformità

- Documentazione di software che incorporano le metodologie.
- Ordini del giorno e verbali delle riunioni, e-mail, attestati firmati, programmi di formazione o documentazione analoga che provi che gli Internal Auditor sono stati informati sulle metodologie.
- Documentazione delle quality review del lavoro di audit che dimostri che le metodologie vengono seguite.
- Note a piè di pagina o note di chiusura all'interno delle metodologie o del manuale di Internal Audit che citano gli Standard di riferimento.
- Documentazione degli aggiornamenti delle metodologie.

Standard 9.4 Piano di Audit

Requisiti

Il CAE deve definire un piano di Audit che supporti l'organizzazione nel raggiungimento dei propri obiettivi.

Il CAE deve basare il piano di Audit su un assessment documentato delle strategie, degli obiettivi e dei rischi dell'organizzazione, che consideri anche il contributo del Board e del Top Management, nonché la comprensione del CAE della governance, del risk management e dei processi di controllo dell'organizzazione. L'assessment deve essere effettuato almeno una volta all'anno.

Il piano di Audit deve:

- tenere in considerazione il Mandato di Internal Audit e la totalità dei servizi di Internal Auditing concordati;
- specificare i servizi di Internal Auditing che supportano la valutazione e il miglioramento dei processi di governance, risk management e controllo dell'organizzazione;
- tenere in considerazione la governance delle tecnologie informatiche, il rischio frode, l'efficacia dei programmi di compliance ed etica dell'organizzazione e altre aree ad alto rischio;
- identificare le risorse umane, finanziarie e tecnologiche necessarie a completare il piano;
- essere dinamico e aggiornato tempestivamente in risposta ai cambiamenti nel business dell'organizzazione, nei rischi, nelle operazioni, nei programmi, nei sistemi, nei controlli e nella cultura organizzativa.

Il CAE deve rivedere il piano di Audit, se necessario, e comunicare tempestivamente al Board e al Top Management:

- l'impatto di eventuali carenze di risorse sulla copertura dell'Internal Audit;
- la motivazione per non includere nel piano un incarico di assurance in una determinata area o su un'attività ad alto rischio;
- richieste concomitanti di servizi tra le principali parti interessate, come le richieste ad alta priorità basate sui rischi emergenti e le richieste di sostituire gli incarichi di assurance pianificati con incarichi di advisory;
- limitazioni all'ambito o restrizioni all'accesso alle informazioni.

Il CAE deve condividere il piano di Audit e le modifiche intermedie più significative con il Top Management e il Board. Quest'ultimo dovrà approvare sia il piano che le modifiche.

Indicazioni per l'implementazione

Questo Standard richiede che, come base per il piano, venga completato un risk assessment a livello dell'intera organizzazione almeno una volta all'anno. Tuttavia, il CAE dovrebbe tenersi costantemente informato sui rischi e aggiornare di conseguenza il risk assessment e il piano di Audit. Se il contesto dell'organizzazione è dinamico, potrebbe essere necessario aggiornare il piano di Audit con una frequenza semestrale, trimestrale o addirittura mensile. Le dimensioni, la complessità e il tipo dei cambiamenti che si verificano rispetto alla maturità dei processi di governance, risk management e controllo dell'organizzazione dovrebbero essere presi in considerazione quando si determina l'impegno necessario per aggiornare il risk assessment.

Un metodo di predisposizione del piano di Audit consiste nell'organizzare le aree potenzialmente oggetto di audit all'interno dell'organizzazione in un audit universe per facilitare l'identificazione e la valutazione dei rischi. Un audit universe è più utile quando si basa sulla comprensione degli obiettivi e delle iniziative strategiche dell'organizzazione ed è allineato con la struttura o il framework dei rischi dell'organizzazione. Le aree oggetto di audit possono includere business unit, processi, programmi e sistemi. Il CAE può collegare tali aree ai rischi chiave in preparazione di un risk assessment completo e dell'identificazione della copertura di assurance di tutta l'organizzazione. Questo processo consente al CAE di stabilire le priorità dei rischi da valutare ulteriormente durante gli incarichi di Internal Audit.

Per garantire che l'audit universe e il risk assessment coprano i rischi chiave dell'organizzazione, la funzione Internal Audit dovrebbe esaminare e convalidare in modo indipendente i rischi chiave identificati nel sistema di Risk Management dell'organizzazione. La funzione di Internal Audit dovrebbe basarsi sulle informazioni del management sui rischi solo se ha concluso che i processi di risk management dell'organizzazione sono efficaci.

Per completare il risk assessment sull'intera organizzazione, il CAE dovrebbe considerare gli obiettivi e le strategie non solo a livello organizzativo in generale, ma anche a livello di specifiche aree oggetto di audit. Inoltre, il CAE dovrebbe tenere in debita considerazione i rischi, come quelli relativi all'etica, alle frodi, all'information technology, alle relazioni con le terze parti e alla non conformità ai requisiti normativi, che possono essere legati a più di una business unit o di un processo e possono richiedere una valutazione più complessa.

A supporto di questo risk assessment, il CAE può raccogliere informazioni dagli incarichi di Internal Audit completati di recente, nonché dagli incontri con i membri del Board e del Top Management (si vedano anche gli Standard "9.1 Comprensione dei processi di governance, risk management e controllo" e "11.3 Comunicazione dei risultati"). Il CAE può implementare una metodologia per la valutazione continua dei

rischi. I rischi dovrebbero essere considerati non solo in termini di effetti negativi e ostacoli, ma come opportunità per migliorare la capacità dell'organizzazione di raggiungere i propri obiettivi.

Il CAE dovrebbe sviluppare un processo per identificare e valutare i rischi significativi, nuovi ed emergenti che dovrebbero essere presi in considerazione per la copertura nel piano di Audit. Ad esempio, la scarsità di risorse può rendere impossibile per la funzione Internal Audit valutare annualmente ogni singolo rischio dell'audit universe. In questi casi, il CAE potrebbe dover fare maggiore affidamento su fonti di informazione quali i risk assessment del management, le riunioni con il Board e il Top Management e i risultati di precedenti incarichi e altre attività di audit.

Per creare il piano di Audit, il CAE considera il livello di rischio identificato in ciascuna delle aree potenzialmente oggetto di audit rispetto al livello noto di efficacia del controllo. A influenzare il piano di Audit sono anche le richieste avanzate dal Board e dal Top Management, la copertura di assurance prevista in tutta l'organizzazione, gli incarichi richiesti da leggi o regolamenti e la possibilità per la funzione Internal Audit di fare affidamento sul lavoro di altri fornitori di servizi di assurance. Il CAE dovrebbe pianificare di rivalutare periodicamente la reliance.

Quando definisce il piano di Audit, il CAE dovrebbe considerare:

- incarichi previsti da leggi o regolamenti;
- incarichi critici per la mission o la strategia dell'organizzazione;
- aree e attività con un significativo livello di rischio;
- se tutti i rischi significativi hanno una copertura sufficiente da parte dei fornitori di assurance;
- servizi di advisory e richieste ad hoc;
- il tempo e le risorse necessarie per ogni potenziale incarico;
- i potenziali benefici di ogni incarico per l'organizzazione, ad esempio il potenziale contributo dell'incarico al miglioramento della governance, del risk management e dei processi di controllo dell'organizzazione.

Per pianificare gli incarichi di Internal Audit, il CAE dovrebbe considerare:

- le priorità operative dell'organizzazione;
- il calendario degli incarichi di audit esterno e delle revisioni previste dai regolamenti;
- le competenze e disponibilità degli Internal Auditor;
- la possibilità di accesso all'attività oggetto di audit.

Il piano di Audit proposto dovrebbe includere:

- le risorse e le ore disponibili per gli incarichi rispetto ad altre attività amministrative e non di audit o iniziative incentrate sul miglioramento della funzione Internal Audit;
- l'elenco degli incarichi proposti e la relativa analisi, specificando in che misura gli incarichi sono:
  - di assurance o advisory;
  - focalizzati su determinati reparti, aree o obiettivi dell'organizzazione;
  - orientati a obiettivi finanziari, di compliance, operational, di cybersecurity o di altro tipo;
- la logica per la selezione di ciascun incarico proposto; ad esempio, significatività del rischio, tematiche o tendenze (root cause) dell'organizzazione, requisiti normativi o tempo trascorso dall'ultimo incarico;
- lo scopo e l'ambito preliminare di ciascun incarico proposto;
- la percentuale di ore da riservare a imprevisti e richieste ad hoc;
- la lista di incarichi successivi che sarebbero eseguiti se fossero disponibili risorse aggiuntive; la discussione in merito a tali incarichi può aiutare il Board a valutare l'adeguatezza delle risorse a disposizione della funzione Internal Audit.

Il CAE, il Board e il Top Management dovrebbero concordare i criteri che definiscono i cambiamenti significativi che richiedono una revisione del piano di Audit. I criteri e il protocollo concordati dovrebbero essere integrati nelle metodologie della funzione Internal Audit. Esempi di cambiamenti significativi includono l'annullamento o il rinvio di incarichi relativi a rischi significativi o obiettivi strategici critici. Se emergono rischi che richiedono revisioni del piano prima che possa essere programmata una discussione formale con il Board, questo dovrebbe essere informato immediatamente delle modifiche, per poter procedere con un'approvazione formale il prima possibile.

Esempi di conformità

- Un piano di Audit approvato.
- Un risk assessment documentato e la definizione delle priorità, compresi gli input su cui si basa il piano.
- Verbali di riunioni in cui il CAE ha condiviso con il Board e il Top Management l'audit universe, il risk assessment dell'organizzazione, il piano di Audit e i criteri e il protocollo per la gestione di modifiche significative al piano.
- Note che attestano la raccolta delle informazioni utili al fine del risk assessment e della definizione del piano di Audit dell'organizzazione.
- Elenco documentato dei soggetti ai quali è stato distribuito il piano di Audit.
- Metodologie documentate per il risk assessment dell'organizzazione e protocollo per la gestione dei cambiamenti significativi.

Standard 9.5 Coordinamento e reliance

Requisiti

Il CAE deve coordinarsi con i fornitori interni ed esterni di servizi di assurance e deve tenere in considerazione la possibilità di fare affidamento sul loro lavoro. Il coordinamento dei servizi riduce al minimo la duplicazione degli sforzi, evidenzia le lacune nella copertura dei rischi più significativi e aumenta il valore aggiunto complessivo dei servizi.

Se non è in grado di raggiungere un livello adeguato di coordinamento, il CAE deve sollevare eventuali preoccupazioni con il Top Management e, se necessario, con il Board.

Quando la funzione Internal Audit si affida al lavoro di altri fornitori di servizi di assurance, il CAE deve documentare le motivazioni su cui si fonda il rapporto di reliance ed è comunque responsabile delle conclusioni della funzione Internal Audit.

Indicazioni per l'implementazione

Il CAE dovrebbe sviluppare una metodologia per valutare altri fornitori di servizi di assurance e advisory che includa le motivazioni su cui si fonda la reliance. La valutazione dovrebbe prendere in considerazione i ruoli, le responsabilità, l'indipendenza organizzativa, la competenza e l'obiettività, nonché la loro diligenza professionale.

Il CAE dovrebbe identificare i fornitori di servizi di assurance e advisory dell'organizzazione mediante confronto con il Top Management e dovrebbe esaminare la struttura organizzativa e gli ordini del giorno o i verbali delle riunioni del Board. I fornitori interni di servizi di assurance e advisory includono funzioni che possono riferire o far parte del Top Management, come la funzione Compliance, Sostenibilità, Controllo di Gestione, Salute e Sicurezza, Cybersecurity, l'Ufficio Legale, il Risk

Management e la Qualità. I fornitori esterni di servizi di assurance possono riferire al Top Management, a stakeholder esterni o al CAE.

Alcuni esempi di coordinamento sono:

- la sincronizzazione delle attività pianificate in base alla loro natura, estensione e tempistica;
- una comprensione comune delle tecniche, dei metodi e della terminologia di assurance;
- l'accesso reciproco ai programmi di lavoro e ai report;
- l'utilizzo delle informazioni del risk management per elaborare un risk assessment integrato;
- la creazione di un risk register o elenco dei rischi condiviso;
- la combinazione dei risultati per il reporting integrato.

Il processo di coordinamento delle attività di assurance varia a seconda dell'organizzazione, da informale nelle piccole organizzazioni a formale e complesso nelle organizzazioni grandi o fortemente regolamentate. Il CAE considera i requisiti di riservatezza dell'organizzazione prima di incontrare i vari fornitori di assurance per raccogliere le informazioni necessarie per coordinare i servizi. Spesso, si condividono gli obiettivi, l'ambito e la tempistica degli incarichi imminenti e i risultati di quelli precedenti. I fornitori di assurance discutono anche della possibilità di affidarsi ad altri.

Un metodo per coordinare la copertura consiste nel creare un'assurance map o una matrice dei rischi dell'organizzazione e dei fornitori interni ed esterni di servizi di assurance che coprono tali rischi. L'assurance map collega le categorie di rischio significative identificate con le fonti di assurance pertinenti e fornisce una valutazione del livello di assurance per ciascuna categoria di rischio. Poiché la mappa è completa, mette in luce le lacune e le duplicazioni nella copertura di assurance, consentendo al CAE di valutare l'adeguatezza dei servizi di assurance in ciascuna area di rischio. I risultati possono essere discussi con gli altri fornitori di servizi di assurance in modo che le parti coinvolte possano raggiungere un accordo su come coordinare le attività. Secondo un approccio di combined assurance, il CAE coordina gli incarichi di assurance della funzione Internal Audit con altri fornitori di assurance per ridurre la frequenza e la ridondanza degli incarichi, massimizzando così l'efficienza della copertura di assurance.

Il CAE può scegliere di fare affidamento su altri fornitori di assurance per vari motivi, ad esempio per valutare aree specialistiche al di fuori delle competenze della funzione Internal Audit, per ridurre la quantità di test necessari per completare un incarico e per migliorare la copertura del rischio impiegando risorse aggiuntive rispetto a quelle della funzione Internal Audit.

Per determinare se la funzione Internal Audit possa fare affidamento sul lavoro di un altro fornitore di assurance, la metodologia dovrebbe prendere in considerazione:

- i potenziali o effettivi conflitti di interesse e la loro eventuale comunicazione;
- le relazioni gerarchiche che potrebbero impattare sull'accordo;
- la pertinenza e validità dell'esperienza professionale, delle qualifiche e delle certificazioni;
- la metodologia e la diligenza professionale applicate nelle fasi di pianificazione, supervisione, documentazione e revisione del lavoro;
- rilievi e conclusioni e se questi sono ragionevoli, basati su prove sufficienti, affidabili e pertinenti.

Dopo aver valutato il lavoro di un altro fornitore di servizi di assurance, il CAE può stabilire se la funzione Internal Audit non può fare affidamento su di lui. Gli Internal Auditor possono riesaminare il lavoro, raccogliere ulteriori informazioni o eseguire in modo indipendente i servizi di assurance.

Se la funzione Internal Audit intendesse fare affidamento sul lavoro di un altro fornitore di assurance su base continuativa o a lungo termine, le parti dovrebbero documentare il rapporto concordato e le specifiche per l'assurance da fornire, nonché le verifiche e le prove necessarie a evidenza dell'assurance.

Esempi di conformità

- Comunicazioni relative a ruoli e responsabilità distinti in materia di assurance e advisory, che possono essere documentate nelle minute delle riunioni con i singoli fornitori di servizi di assurance e advisory o nei verbali delle riunioni con il Board e il Top Management.
- Assurance map e/o piani di combined assurance che identificano quale fornitore è responsabile dei servizi di assurance in ciascuna area.
- Documentazione e implementazione della metodologia per determinare se fare affidamento su un altro fornitore di assurance.
- Accordi documentati con altri fornitori di assurance che confermano le specifiche del lavoro che svolgeranno.

Principio 10 Gestire le risorse

Il CAE gestisce le risorse per attuare la strategia della funzione Internal Audit e realizzarne il piano e il Mandato.

La gestione delle risorse prevede l'ottenimento e l'impiego efficace di risorse finanziarie, umane e tecnologiche. Il CAE deve ottenere le risorse necessarie per adempiere alle responsabilità e deve impiegarle secondo le metodologie stabilite per la funzione Internal Audit.

Standard 10.1 Risorse finanziarie

Requisiti

Il CAE deve gestire le risorse finanziarie della funzione Internal Audit.

Il CAE deve sviluppare un budget che consenta l'implementazione efficace della strategia di Internal Audit e lo svolgimento del piano. Il budget comprende le risorse necessarie per il funzionamento della funzione, compresa la formazione e l'acquisizione di tecnologie e tool. Il CAE deve gestire le attività quotidiane della funzione Internal Audit in modo efficace ed efficiente, in linea con il budget.

Il CAE deve cercare di portare l'approvazione del budget al livello del Board e deve comunicare tempestivamente al Board e al Top Management l'impatto di risorse finanziarie insufficienti.

Indicazioni per l'implementazione

Il CAE dovrebbe seguire i processi di budget stabiliti dall'organizzazione. Indipendentemente dal fatto che la funzione Internal Audit sia interna o esternalizzata, il Board dovrebbe comunque approvare un budget adeguato.

Periodicamente, il CAE dovrebbe rivedere il budget pianificato rispetto all'andamento e analizzare gli scostamenti significativi per determinare se sono necessari aggiustamenti. Il budget può includere delle riserve per modifiche impreviste, ma necessarie, al piano di Audit. Se il budget di una funzione Internal Audit è parte di un budget più ampio gestito da un altro dipartimento, business unit o organo, il CAE dovrebbe comunque essere a conoscenza dei fondi assegnati alla funzione Internal Audit, tenere traccia delle spese e monitorare la sufficienza delle risorse finanziarie messe a disposizione della funzione Internal Audit.

Se, a causa di circostanze impreviste, fossero necessarie significative risorse aggiuntive, il CAE dovrebbe discutere tempestivamente tali circostanze con il Board e il Top Management.

Esempi di conformità

- Documentazione del piano di Audit rispetto al budget, alle previsioni e alle spese effettive.
- Verbali delle riunioni in cui il CAE ha discusso il budget della funzione con il Board e il Top Management.
- Verbale delle riunioni del Board in cui si discute il budget della funzione Internal Audit e si formalizza la sua approvazione.

Standard 10.2 Risorse umane

Requisiti

Il CAE deve stabilire un approccio per selezionare, sviluppare e trattenere Internal Auditor qualificati per implementare con successo la strategia e realizzare il piano di Audit.

Il CAE deve sforzarsi di garantire che le risorse umane siano adeguate, sufficienti ed impiegate efficacemente per realizzare il piano di Audit approvato. *Adeguate* si riferisce al mix di conoscenze, competenze e abilità; *sufficienti* si riferisce alla quantità delle risorse; *impiegate efficacemente* si riferisce all'assegnazione ottimale delle risorse per il raggiungimento del piano di Audit.

Il CAE deve discutere con il Board e il Top Management in merito all'adeguatezza e alla sufficienza delle risorse umane della funzione Internal Audit. Se la funzione non dispone di risorse umane adeguate e sufficienti per realizzare il piano di Audit, il CAE deve capire come ottenere le risorse o comunicare tempestivamente al Board e al Top Management l'impatto delle limitazioni (si veda anche lo Standard "8.2 Risorse").

Il CAE deve valutare le competenze dei singoli Internal Auditor della funzione e incoraggiare lo sviluppo professionale. Deve collaborare con gli Internal Auditor per aiutarli a sviluppare le loro competenze individuali attraverso la formazione, il feedback dei supervisori e/o il mentoring (si veda anche lo Standard "3.1 Competenza").

Indicazioni per l'implementazione

La struttura e l'approccio alla gestione delle risorse della funzione di Internal Audit dovrebbero essere in linea con l'Internal Audit Charter e sostenere la realizzazione della strategia della funzione e l'attuazione del piano di Audit.

Nel formulare un approccio per la gestione delle risorse umane della funzione di Internal Audit, il CAE dovrebbe:

- considerare le caratteristiche dell'organizzazione, come la struttura e la complessità, l'articolazione geografica, la diversità di culture e lingue e la volatilità del profilo di rischio in cui opera l'organizzazione;
- considerare il budget per l'Internal Audit, l'adeguatezza in termini di costi e la flessibilità dei vari approcci al personale (ad esempio, l'assunzione di un dipendente o la stipula di un contratto con un fornitore esterno di servizi);
- comprendere le opzioni per ottenere le risorse umane necessarie per adempiere all'Internal Audit Charter e realizzare il piano di Audit;
- comunicare con il Board e il Top Management per concordare un approccio;
- prevedere la pianificazione della successione per la posizione di CAE anche mediante discussioni con il Board.

Al fine di favorire l'assunzione di Internal Auditor competenti, il CAE dovrebbe:

- collaborare con la funzione Risorse Umane per elaborare adeguate job description e specifiche del ruolo, in linea con lo Standard "3.1 Competenza" e i pertinenti competency framework professionali;
- considerare i benefici derivanti dall'assunzione di Internal Auditor con background, esperienze e prospettive diverse e dalla creazione di un ambiente di lavoro inclusivo che consenta una collaborazione efficace e la condivisione di punti di vista diversi;
- partecipare ad attività di recruiting, quali fiere del lavoro, eventi per studenti, momenti di networking professionale e colloqui con potenziali candidati.

Per sviluppare e trattenere gli Internal Auditor, il CAE dovrebbe:

- implementare policy di remunerazione, promozione e riconoscimento legate al raggiungimento degli obiettivi strategici della funzione Internal Audit;
- implementare metodologie per la formazione, la misurazione delle performance, il miglioramento delle competenze e la promozione dello sviluppo professionale degli Internal Auditor;
- considerare gli obiettivi della funzione Internal Audit e dell'organizzazione in materia di risorse umane, come ad es. la condivisione tra le diverse funzioni aziendali delle conoscenze e l'identificazione di piani di successione;
- coltivare un ambiente etico e professionale in cui gli Internal Auditor siano adeguatamente formati e collaborino in modo efficace (si veda anche la Sezione "II: Etica e professionalità").

Per valutare se le risorse umane sono adeguate e sufficienti per realizzare il piano di Audit, il CAE dovrebbe considerare:

- le competenze dei singoli Internal Auditor e quelle necessarie per svolgere i servizi di Internal Auditing;
- la natura e la complessità dei servizi;
- il numero di Internal Auditor e il numero delle ore disponibili;
- i vincoli alla pianificazione, tra cui la disponibilità di Internal Auditor, le informazioni, le persone e le proprietà dell'organizzazione;
- la possibilità di fare affidamento sul lavoro di altri fornitori di servizi di assurance (si veda anche lo Standard "9.5 Coordinamento e reliance").

Oltre alle competenze, il CAE considera la tempistica e il calendario degli incarichi di Audit, basati sulla programmazione dei singoli Internal Auditor e la disponibilità del personale responsabile delle attività oggetto di Audit. Se un incarico fosse pianificato per un momento specifico, le risorse necessarie per completarlo dovrebbero essere disponibili in quel momento.

Se le risorse sono insufficienti per coprire gli incarichi pianificati, il CAE può formare il personale esistente, richiedere a un esperto all'interno dell'organizzazione di fungere da Auditor ospite, assumere personale aggiuntivo, affidarsi ad altri fornitori di assurance, sviluppare un programma di audit basato sulla rotazione o stipulare un contratto con un fornitore di servizi esterno. I fornitori di servizi esterni possono fornire competenze specialistiche, completare progetti speciali o eseguire incarichi.

Quando la funzione Internal Audit è interna, il personale può essere integrato da un modello di rotazione del personale, in base al quale i dipendenti di altre business unit entrano temporaneamente a far parte della funzione Internal Audit. I dipendenti che si trasferiscono nella funzione Internal Audit possono fornire competenze e conoscenze specialistiche, nonché prospettive e approfondimenti unici e quando tornano nelle business unit di provenienza, le loro esperienze di Internal Audit favoriscono una comprensione più approfondita dei processi di governance, risk management e controllo dell'organizzazione. Quando si utilizza un modello a rotazione, il CAE dovrebbe essere consapevole delle potenziali limitazioni all'obiettività e dovrebbe attuare le relative misure di salvaguardia (si veda anche lo Standard "2.2 Protezione dell'obiettività").

La metodologia di Internal Audit per la supervisione degli incarichi dovrebbe prevedere sufficienti occasioni per gli Internal Auditor di ricevere feedback costruttivi da parte di Internal Auditor più esperti con ruoli di supervisione. Questi feedback possono essere forniti mediante osservazioni scritte o verbali nelle revisioni delle carte di lavoro e altre comunicazioni. I programmi di mentorship offrono esperienze sul campo attraverso le quali gli Internal Auditor meno esperti possono seguire e osservare direttamente i più esperti durante lo svolgimento degli incarichi. Il monitoraggio continuo e le autovalutazioni periodiche, che comprendono anche i quality assessment interni della funzione Internal Audit, rappresentano occasioni aggiuntive per gli Internal Auditor di ricevere feedback e suggerimenti che aumentino l'efficacia del loro operato (si veda anche lo Standard "12.1 Quality assessment interno"). Le misurazioni delle performance individuali effettuate a intervalli regolari, ad esempio annualmente, sono un'altra fonte di input che può contribuire allo sviluppo professionale degli Internal Auditor.

Il CAE dovrebbe seguire le policy delle risorse umane dell'organizzazione o, come nel settore pubblico, seguire i framework normativi o contrattuali. In questi casi, per supportare la funzione, il CAE dovrebbe comprendere a fondo i framework di riferimento e ottimizzare la classificazione delle mansioni, i processi di assessment e altri framework previsti per supportare la funzione Internal Audit. Il Board e il Top Management dovrebbero essere informati quando questi framework perdono la loro capacità di soddisfare le esigenze di risorse umane della funzione Internal Audit.

Esempi di conformità

- Analisi documentata dei gap tra le competenze degli Internal Auditor in organico e quelle richieste.
- Job description dettagliate.
- Curriculum Vitae degli Internal Auditor impiegati dall'organizzazione.
- Piani di formazione documentati ed evidenze del completamento della formazione.
- Contratti con fornitori di servizi esterni e Curriculum degli Internal Auditor assegnati dal fornitore.
- Il piano di Audit, con indicazione delle scadenze stimate degli incarichi e delle risorse allocate.
- Verbali di riunione che documentano le discussioni relative al bilancio dell'Internal Audit.
- Confronto post-incarico tra le ore di lavoro preventivate e le ore effettive.
- Misurazione delle performance della funzione Internal Audit e dei singoli Internal Auditor.

Standard 10.3 Risorse tecnologiche

Requisiti

Il CAE deve adoperarsi per garantire che la funzione Internal Audit disponga della tecnologia necessaria per supportare il processo di Internal Audit. Il CAE deve regolarmente valutare la tecnologia utilizzata dalla funzione Internal Audit e perseguire le opportunità per migliorarne l'efficacia e l'efficienza.

Nell'implementazione di nuove tecnologie, il CAE deve prevedere un'adeguata formazione per gli Internal Auditor. Il CAE deve collaborare con le funzioni di Information Technology e Information Security dell'organizzazione per sviluppare correttamente le risorse tecnologiche.

Il CAE deve comunicare al Board e al Top Management l'impatto delle limitazioni tecnologiche sull'efficacia o sull'efficienza della funzione Internal Audit.

Indicazioni per l'implementazione

La funzione Internal Audit dovrebbe utilizzare la tecnologia per migliorare la propria efficacia ed efficienza. Alcuni esempi di tecnologia sono:

- sistemi di gestione degli audit;
- applicazioni per il mapping dei processi di governance, risk management e controllo;
- tool di data science e analytics;
- tool che facilitano la comunicazione e la collaborazione.

Per valutare se la funzione Internal Audit dispone di risorse tecnologiche per adempiere alle proprie responsabilità, il CAE dovrebbe:

- valutare la fattibilità di realizzare miglioramenti abilitati dalla tecnologia in tutti i processi della funzione Internal Audit;
- collaborare con altri reparti a progetti per sistemi condivisi di governance, risk management e controllo;
- presentare all'approvazione del Board e del Top Management richieste documentate di finanziamento per le tecnologie;
- sviluppare e implementare piani per l'introduzione di tecnologie approvate (i piani dovrebbero includere la formazione degli Internal Auditor e la presentazione dei benefici ottenuti al Board e al Top Management);
- identificare e gestire i rischi derivanti dall'uso della tecnologia, compresi quelli relativi alla sicurezza delle informazioni e alla privacy dei dati personali.

Esempi di conformità

- Estratti della strategia di Internal Audit che descrivono le iniziative in corso o pianificate per l'utilizzo della tecnologia al fine di supportare gli obiettivi della funzione Internal Audit.
- Discussioni o piani documentati relativi alle richieste e all'implementazione delle tecnologie.
- Evidenze dell'implementazione, della formazione e dell'uso della tecnologia, comprese le carte di lavoro che dimostrano l'impiego della tecnologia durante gli incarichi.
- I nomi degli Internal Auditor con le rispettive certificazioni e qualifiche relative alla tecnologia.

- Sicurezza delle informazioni, gestione dei record e altre policy e procedure rilevanti per l'uso delle risorse tecnologiche da parte della funzione Internal Audit.

Principio 11 Comunicare in modo efficace

Il CAE definisce le linee guida della funzione Internal Audit per comunicare in modo efficace con i propri stakeholder.

Una comunicazione efficace richiede la costruzione di relazioni, la creazione di fiducia e la possibilità per gli stakeholder di beneficiare dei risultati dei servizi di Internal Auditing. Il CAE ha la responsabilità di aiutare la funzione Internal Audit a stabilire una comunicazione continua con gli stakeholder per creare fiducia e per favorire le relazioni. Inoltre, il CAE, rivede le comunicazioni formali della funzione Internal Audit con il Board e il Top Management per garantirne la qualità e fornire approfondimenti sulla base dei risultati dei servizi di Internal Auditing.

Standard 11.1 Costruzione di relazioni e comunicazione con gli stakeholder

Requisiti

Il CAE deve sviluppare un approccio che permetta alla funzione Internal Audit di costruire relazioni e fiducia con i principali stakeholder, tra cui il Board, il Top Management, il management di linea, gli enti regolatori e i fornitori di servizi di assurance interni ed esterni e altri consulenti.

Il CAE deve promuovere la comunicazione formale e informale tra la funzione Internal Audit e gli stakeholder, contribuendo alla comprensione reciproca di:

- aspetti di interesse e criticità relative all'organizzazione;
- approcci per identificare e gestire i rischi e per fornire assurance;
- ruoli e responsabilità dei soggetti rilevanti e opportunità di collaborazione;
- requisiti normativi significativi;
- processi rilevanti dell'organizzazione, incluso il reporting finanziario.

Indicazioni per l'implementazione

Una comunicazione regolare e continua tra il Board, il Top Management e la funzione Internal Audit contribuisce a una comprensione comune dei rischi e delle priorità di assurance dell'organizzazione e promuove l'adattabilità ai cambiamenti. Il CAE dovrebbe essere incluso nei flussi di comunicazione dell'organizzazione che riguardano i principali sviluppi e le attività pianificate che potrebbero influenzare gli obiettivi e i rischi dell'organizzazione. Il CAE dovrebbe anche partecipare alle riunioni con il Board e i principali comitati di governance, nonché con il Top Management e i team che riportano direttamente al Top Management, come la Compliance, il Risk Management e la Qualità.

Inoltre, il CAE dovrebbe discutere una metodologia per la comunicazione con il Board e il Top Management, per determinare i criteri di significatività delle questioni che richiedono una comunicazione formale, il formato e il contenuto della comunicazione formale e la frequenza con cui tale comunicazione dovrebbe avvenire.

Incontrare individualmente i top manager e i membri del Board consente al CAE di costruire relazioni e conoscere le loro preoccupazioni e prospettive. Per comprendere meglio gli obiettivi e i processi aziendali, gli Internal Auditor dovrebbero incontrare il management di linea, come i responsabili delle business unit e delle attività operative. Nei settori fortemente regolamentati, possono essere opportuni incontri tra il CAE e gli Auditor esterni e le autorità regolatorie.

Il CAE e gli Internal Auditor possono confrontarsi con il management e il Board su strategie, obiettivi e rischi, nonché in relazione a novità che riguardano il settore, le tendenze e gli aggiornamenti normativi. Tali confronti, insieme a sondaggi, interviste e workshop di gruppo, sono strumenti utili per ottenere input, in particolare sui rischi di frode e su quelli emergenti. Siti web, newsletter, presentazioni e altre forme di comunicazione possono essere metodi efficaci per condividere il ruolo e l'apporto della funzione Internal Audit con i dipendenti e gli altri stakeholder.

Il CAE può delegare ai singoli Internal Auditor la responsabilità di mantenere una comunicazione continua con il management delle funzioni chiave come i responsabili delle business unit, delle operations, dei sistemi informativi, della funzione amministrazione e finanza, della compliance e delle risorse umane (si veda anche lo Standard "9.5 Coordinamento e reliance").

La comunicazione dovrebbe includere occasioni di interazione continua e informale tra gli Internal Auditor e i dipendenti dell'organizzazione. Quando tali interazioni informali si verificano in modo costante, i dipendenti acquisiscono fiducia negli Internal Auditor e aumentano le possibilità di confronti aperti che potrebbero non verificarsi nelle riunioni formali. Come parte della costruzione di relazioni, l'interazione informale può migliorare la comprensione completa dell'organizzazione e del suo ambiente di controllo da parte degli Internal Auditor. La rotazione degli Internal Auditor nell'ambito degli incarichi in specifiche business unit o sedi può bilanciare i vantaggi della comunicazione informale con la necessità di proteggere l'obiettività degli Internal Auditor.

Esempi di conformità

- Documentazione del piano della funzione Internal Audit per la gestione delle relazioni con gli stakeholder.
- Ordini del giorno o verbali delle riunioni tra i membri della funzione Internal Audit e gli stakeholder.
- Sondaggi, interviste e workshop di gruppo attraverso i quali gli Internal Auditor richiedono input da parte degli stakeholder interni.
- Siti web o pagine web, newsletter, presentazioni e altri canali attraverso i quali la funzione Internal Audit comunica con gli stakeholder dell'organizzazione.

Standard 11.2 Comunicazione efficace

Requisiti

Il CAE deve stabilire e implementare metodologie per promuovere una comunicazione accurata, obiettiva, chiara, concisa, costruttiva, completa e tempestiva.

Indicazioni per l'implementazione

Le metodologie possono prevedere politiche, criteri, linee guida e procedure per indirizzare la comunicazione della funzione Internal Audit e mantenerne la coerenza. Tali metodologie dovrebbero tenere conto delle aspettative del Board, del Top Management e di altri stakeholder rilevanti (si vedano anche gli Standard "9.3 Metodologie" e "15.1 Comunicazione finale dell'incarico"). Il CAE può promuovere per gli Internal Auditor corsi di formazione in materia di comunicazione, ad esempio prevedendo corsi di scrittura o per la presentazione dei risultati conclusivi.

Le metodologie, accompagnate dalla revisione del supervisore, dovrebbero migliorare la comunicazione nell'ambito di un incarico assicurando che abbia le caratteristiche di seguito illustrate.

- Accurata: priva di errori e distorsioni e fedele ai fatti sottostanti. Quando comunicano, gli Internal Auditor dovrebbero utilizzare termini e descrizioni precise, supportate dalle informazioni raccolte e dovrebbero anche prendere in considerazione altri Standard relativi all'accuratezza, tra cui lo Standard "11.4 Errori e omissioni".
- Obiettiva: imparziale e frutto di una valutazione equa ed equilibrata di tutti i fatti e le circostanze pertinenti. I rilievi, le conclusioni, le raccomandazioni e/o i piani d'azione e gli altri risultati dei servizi di Internal Auditing dovrebbero basarsi su valutazioni equilibrate delle circostanze pertinenti. Le comunicazioni dovrebbero concentrarsi sull'individuazione di informazioni fattuali e permettere il collegamento delle informazioni agli obiettivi. Gli Internal Auditor dovrebbero evitare termini che possano essere percepiti come tendenziosi (si vedano anche il Principio "2 Mantenere l'obiettività" e i relativi Standard).
- Chiara: logica e facilmente comprensibile per i principali stakeholder, evitando un linguaggio tecnico non necessario. La chiarezza aumenta quando gli Internal Auditor adottano un linguaggio coerente con la terminologia utilizzata nell'organizzazione e facilmente comprensibile. Gli Internal Auditor dovrebbero evitare un linguaggio tecnico non necessario e fornire le definizioni di eventuali termini importanti non comuni o utilizzati in modo specifico o particolare per la comunicazione o la presentazione. Gli Internal Auditor migliorano la chiarezza delle loro comunicazioni includendo dettagli significativi a supporto di rilievi, valutazioni, raccomandazioni e/o piani d'azione.
- Concisa: sintetica e priva di dettagli e prolissità inutili. Gli Internal Auditor dovrebbero evitare ridondanze ed escludere le informazioni non necessarie, insignificanti o non correlate all'incarico.
- Costruttiva: utile per gli stakeholder e l'organizzazione e orientata al miglioramento. Gli Internal Auditor dovrebbero esprimere le informazioni in un modo collaborativo e utile, che faciliti la collaborazione nell'ambito dell'attività in esame per determinare le opportunità di miglioramento.
- Completa: informazioni ed evidenze pertinenti, affidabili e sufficienti a sostegno dei risultati dei servizi di Internal Auditing. La completezza consente al lettore di giungere alle stesse conclusioni raggiunte dagli Internal Auditor. Gli Internal Auditor dovrebbero adattare le comunicazioni per soddisfare le esigenze dei vari destinatari e prendere in considerazione le informazioni di cui gli stessi hanno bisogno per intraprendere le azioni di cui sono responsabili. Ad esempio, le comunicazioni al Board e al Top Management possono differire da quelle al management di un'attività oggetto di audit.
- Tempestiva: temporalmente appropriata, in base all'importanza del problema, consentendo al management di intraprendere azioni correttive. La tempestività può essere diversa per ogni organizzazione e dipendere dalla natura dell'incarico.

Il CAE può stabilire dei key perfomance indicator per monitorare l'efficacia della comunicazione dell'Internal Audit, che possono essere utilizzati come parte del programma di assurance e miglioramento della qualità della funzione (si vedano anche lo Standard "8.3 Qualità" e il Principio "12 Migliorare la qualità" e i relativi Standard).

Esempi di conformità

- Linee guida, template e altre metodologie documentate per una comunicazione efficace.
- Tracciabilità della partecipazione a corsi di formazione o incontri sulla comunicazione efficace.
- Comunicazioni finali e altri documenti approvati dal CAE, nonché documentazione a supporto che dimostrino di soddisfare le caratteristiche di una comunicazione efficace.
- Presentazioni o verbali di riunione che dimostrino le caratteristiche di una comunicazione efficace.
- Evidenze a supporto della tempestività delle comunicazioni.
- Carte di lavoro che dimostrano di soddisfare caratteristiche di una comunicazione efficace.
- Carte di lavoro con note di revisione del supervisore su come migliorare l'efficacia della comunicazione.
- Risultati delle indagini presso gli stakeholder sulla qualità delle comunicazioni degli audit.
- Risultati del programma di assurance e miglioramento della qualità.

Standard 11.3 Comunicazione dei risultati

Requisiti

Il CAE deve comunicare i risultati dei servizi di Internal Auditing al Board e al Top Management periodicamente e al termine di ciascun incarico, come opportuno. Il CAE deve comprendere le aspettative del Board e del Top Management in merito alla natura e alla tempistica delle comunicazioni.

I risultati dei servizi di Internal Auditing possono includere:

- conclusioni dell'incarico;
- tematiche di rilievo come pratiche efficaci o root cause;
- giudizi a livello di business unit o di organizzazione.

Valutazioni dell'incarico

Il CAE deve esaminare e approvare le comunicazioni finali dell'incarico, che includono le valutazioni dell'incarico, e decidere a chi e come saranno diffuse, prima che vengano emesse. Se questi compiti sono delegati ad altri Internal Auditor, il CAE ne mantiene la responsabilità generale. Il CAE deve chiedere il parere di un consulente legale e/o del Top Management, come richiesto, prima di rilasciare comunicazioni finali all'esterno dell'organizzazione, a meno che non sia diversamente richiesto o vincolato da leggi e/o regolamenti (si vedano anche gli Standard "11.4 Errori e omissioni", "11.5 Comunicazione dell'accettazione dei rischi" e "15.1 Comunicazione finale dell'incarico").

Tematiche di rilievo

I rilievi e le conclusioni di più incarichi, se visti nell'insieme, possono rivelare schemi o tendenze, così come anche le root cause. Quando il CAE identifica tematiche di rilievo inerenti alla governance, al risk management e ai processi di controllo dell'organizzazione, queste devono essere comunicate tempestivamente, insieme ad approfondimenti, consigli e/o conclusioni, al Board e al Top Management.

Giudizi a livello di business unit o di organizzazione

Al CAE può essere richiesto di esprimere un giudizio a livello di business unit o dell'intera organizzazione sull'efficacia della governance, del risk management e/o dei processi di controllo, in linea con i requisiti del settore, le leggi e/o regolamenti o le aspettative del Board, del Top Management e/o di altri stakeholder. Tale giudizio riflette il giudizio professionale del CAE sulla base degli incarichi svolti e deve essere supportato da informazioni pertinenti, affidabili e sufficienti.

Nel comunicare tale giudizio al Board o al Top Management, il CAE deve includere:

- un riepilogo della richiesta;
- i criteri utilizzati come base per il giudizio, ad esempio un modello di governance o un framework dei rischi e controlli;
- l'ambito di applicazione, comprese le limitazioni e il periodo a cui si riferisce il giudizio;
- un riassunto delle informazioni che supportano il giudizio;
- una dichiarazione di affidabilità del lavoro di altri fornitori di servizi di assurance, se presenti.

Indicazioni per l'implementazione

I risultati dei servizi di Internal Auditing possono basarsi sui singoli incarichi, su più incarichi e sulle interazioni con il Board e il Top Management avvenute nel corso del tempo.

Valutazioni dell'incarico

Mentre lo Standard "13.1 Comunicazione dell'incarico" richiede che gli Internal Auditor comunichino durante un incarico con i responsabili dell'attività oggetto di audit, il CAE è responsabile della comunicazione dei risultati dell'incarico agli opportuni destinatari. I destinatari possono includere il Board, il Top Management e/o i responsabili della definizione e implementazione dei piani d'azione (si veda anche lo Standard "15.1 Comunicazione finale dell'incarico").

Il CAE dovrebbe incoraggiare gli Internal Auditor a riconoscere i risultati soddisfacenti e gli aspetti positivi nelle comunicazioni relative a un incarico. Esempi di buone pratiche identificate negli incarichi possono essere trasferibili ad altre parti dell'organizzazione o fungere da punto di riferimento in tutta l'organizzazione.

Tematiche di rilievo

Il monitoraggio dei rilievi e delle valutazioni di più incarichi può consentire l'identificazione di tendenze, come il miglioramento o il peggioramento di determinate situazioni rispetto ai criteri, una root cause alla base delle situazioni riscontrate o l'opportunità di condividere una pratica che aumenta l'efficacia o l'efficienza. Tali tendenze possono anche portare a svolgere ulteriori incarichi sul tema all'interno dell'organizzazione.

Le comunicazioni al Board e al Top Management dovrebbero includere:

- analisi delle debolezze di controllo più significative e delle root cause;
- tematiche o rilievi sistematici, azioni o miglioramenti emersi nell'ambito di più incarichi o di business unit.

Le informazioni ottenute dalle altre funzioni di assurance dovrebbero essere tenute in considerazione quando si identificano le tematiche rilevanti (si veda anche lo Standard "9.5 Coordinamento e reliance").

Valutazioni a livello di business unit o di organizzazione

Quando si comunicano giudizi a livello di business unit o di intera organizzazione, il CAE dovrebbe considerare in che modo un giudizio si collega alle strategie, agli obiettivi e ai rischi dell'organizzazione. Il CAE dovrebbe anche considerare se il giudizio fornisce la soluzione a un problema, genera valore e/o fornisce al management o ad altri stakeholder garanzie in merito a un tema o a una situazione generale.

Il CAE considera anche il periodo di tempo a cui si riferisce il giudizio e le eventuali limitazioni dell'ambito per determinare quali incarichi sarebbero pertinenti per il giudizio complessivo. Vengono presi in considerazione tutti gli incarichi o i progetti, compresi quelli completati da altri fornitori di servizi di assurance interni ed esterni (si veda anche lo Standard "9.5 Coordinamento e reliance").

Ad esempio, un giudizio complessivo può basarsi su conclusioni aggregate di incarichi a livello locale, regionale e nazionale, insieme ai risultati comunicati da enti esterni come terze parti indipendenti o autorità di regolamentazione. La definizione dell'ambito fornisce il contesto per la conclusione generale, specificando il periodo, le attività, le limitazioni e altre variabili che descrivono i confini della conclusione.

Il CAE dovrebbe riassumere le informazioni su cui si basa il giudizio complessivo e identificare il framework dei rischi o dei controlli o altri criteri utilizzati come base per il giudizio complessivo. Il CAE dovrebbe articolare in che modo il giudizio complessivo si riferisce alle strategie, agli obiettivi e ai rischi dell'organizzazione. I giudizi sono di solito comunicati per iscritto, ma possono anche essere forniti oralmente.

Esempi di conformità

- Comunicazioni finali dell'incarico, inclusi i rilievi, le raccomandazioni e le valutazioni.
- I verbali delle riunioni, le note degli interventi, gli appunti, le presentazioni o i documenti del CAE ad evidenza della comunicazione con il Board e il Top Management.
- Analisi che includono report di dati, diagrammi e grafici ad evidenza dei trend.
- Framework dei rischi e dei controlli o altri criteri utilizzati come base per il giudizio complessivo.

Standard 11.4 Errori e omissioni

Requisiti

Se la comunicazione finale di un incarico contiene un errore o un'omissione significativi, il CAE deve comunicare tempestivamente le informazioni corrette a tutti i destinatari che hanno ricevuto la comunicazione originale.

La significatività è determinata in base a criteri concordati con il Board.

Indicazioni per l'implementazione

Il CAE e il Board dovrebbero concordare un protocollo per comunicare la correzione. Per determinare la significatività, il CAE dovrebbe valutare se le informazioni errate o omesse potrebbero avere conseguenze legali o normative oppure modificare i rilievi, le valutazioni, le raccomandazioni o i piani d'azione.

Il CAE determina il metodo di comunicazione più appropriato in modo che le informazioni corrette siano ricevute da tutti i destinatari che avevano ricevuto la comunicazione originale. Oltre a comunicare le informazioni corrette, il CAE dovrebbe identificare la causa dell'errore o dell'omissione e intraprendere azioni correttive per evitare che una situazione simile si verifichi in futuro.

Esempi di conformità

- Metodologie di Internal Audit per la gestione di errori e omissioni.
- Criteri concordati con il Board e utilizzati dal CAE per determinare il livello di significatività.
- Evidenze che mostrano come il CAE ha determinato l'importanza e la causa dell'errore o dell'omissione.
- L'agenda, i verbali delle riunioni con il Board o di altre riunioni, gli appunti e le e-mail che dimostrano che il CAE ha discusso un errore o un'omissione.
- I documenti di comunicazione finali, originali e corretti.
- Documentazione attestante che i destinatari hanno ricevuto le comunicazioni corrette.

Standard 11.5 Comunicazione dell'accettazione dei rischi

Requisiti

Il CAE deve comunicare livelli di rischio inaccettabili.

Quando il CAE ritiene che il management abbia accettato un livello di rischio superiore al risk appetite o alla risk tolerance dell'organizzazione, la questione deve essere discussa con il Top Management. Se il CAE conclude che non è stata risolta dal Top Management, la questione deve essere inoltrata al Board. Non è responsabilità del CAE risolvere il rischio.

Indicazioni per l'implementazione

Il CAE acquisisce una comprensione dei rischi e della risk tolerance dell'organizzazione attraverso le discussioni con il Board e il Top Management, le relazioni e la comunicazione continua con gli stakeholder e i risultati dei servizi di Internal Auditing (si vedano anche gli Standard "8.1 Interazione con il Board", "9.1 Comprensione dei processi di governance, risk management e controllo" e 11.1 "Costruzione di relazioni e comunicazione con gli stakeholder"). Questa comprensione fornisce al CAE una prospettiva sul livello di rischio che l'organizzazione considera accettabile. Se l'organizzazione disponesse di un processo formale di risk management, il CAE dovrebbe comprendere le policy del management per l'accettazione del rischio.

Il CAE può discutere e ottenere l'accordo del Board sulle metodologie per documentare e comunicare l'accettazione dei rischi che superano i livelli di risk appetite e risk tolerance. Oltre ai requisiti degli Standard, le metodologie dovrebbero considerare il processo, le policy e le procedure di risk

management dell'organizzazione. Il processo di risk management può includere un approccio preferenziale per comunicare i problemi connessi ai rischi significativi. Le specifiche possono includere la tempestività della comunicazione, i livelli gerarchici destinatari del reporting e i requisiti per la consultazione con il Responsabile Legale o il Responsabile Compliance dell'organizzazione. La metodologia di Internal Audit dovrebbe inoltre includere procedure per documentare le discussioni e le azioni intraprese, compresa una descrizione del rischio, il motivo della preoccupazione, il motivo per cui il management non attua le raccomandazioni degli Internal Auditor o altre azioni, il nome della persona responsabile dell'accettazione del rischio e la data della discussione.

Il CAE può rendersi conto che il management ha accettato un rischio esaminando la sua risposta ai rilievi dell'incarico e monitorando lo stato di avanzamento nell'attuazione delle raccomandazioni e dei piani d'azione. Costruire relazioni e mantenere attiva la comunicazione con gli stakeholder sono ulteriori mezzi per rimanere informati sulle attività di risk management, compresa l'accettazione del rischio da parte del management.

Quando i rischi superano il risk appetite, gli impatti possono riguardare:

- danni alla reputazione dell'organizzazione;
- danni ai dipendenti dell'organizzazione o ad altri stakeholder;
- sanzioni amministrative significative, limitazioni nel business o altre penali finanziarie o contrattuali;
- errori significativi;
- conflitti di interesse, frodi o altri atti illeciti;
- impedimenti significativi al raggiungimento degli obiettivi strategici.

Il giudizio professionale del CAE contribuisce a determinare se il management abbia accettato un livello di rischio superiore a risk appetite o risk tolerance. Ad esempio, se il management non ha compiuto progressi sufficienti nei piani d'azione, il CAE può concludere che il management ha accettato un livello di rischio superiore al risk appetite o alla risk tolerance. Prima di comunicare tale criticità al Board e/o al Top Management, il CAE dovrebbe affrontare la questione direttamente con il responsabile dell'area di rischio per condividere le criticità, comprendere il punto di vista del management e concordare un piano d'azione aggiornato.

I requisiti di questo Standard si applicano nei casi in cui il CAE non riesce a raggiungere un accordo con il responsabile della gestione del rischio in questione. Se il rischio identificato come inaccettabile rimane irrisolto dopo una discussione con il Top Management, il CAE inoltra la criticità al Board. Questo è responsabile di decidere come affrontare la criticità con il management.

Esempi di conformità

- Evidenze a supporto delle discussioni e dell'accordo con il Board sulle metodologie per la comunicazione delle criticità sui rischi.
- Evidenze a supporto delle discussioni sul rischio e sulle azioni raccomandate al management e al Top Management, compresi i verbali delle riunioni.
- Documentazione che spieghi il rischio e le azioni intraprese dall'Internal Audit per affrontare il problema, compreso il processo di escalation della discussione dal management al Top Management.
- Verbali delle riunioni con il Board, comprese le sessioni private o chiuse durante le quali la criticità è stata inoltrata al Board.

Principio 12 Migliorare la qualità

Il CAE è responsabile della conformità della funzione Internal Audit ai Global Internal Audit Standards e del miglioramento continuo delle performance.

La qualità è un valore che combina la conformità ai Global Internal Audit Standards e il raggiungimento degli obiettivi di performance della funzione Internal Audit. Pertanto, un programma di assurance e miglioramento della qualità è progettato per valutare e promuovere la conformità della funzione Internal Audit agli Standard, il raggiungimento degli obiettivi di performance e il perseguimento del miglioramento continuo. Il programma prevede assessment interni ed esterni (si vedano anche gli Standard "8.3 Qualità" e "8.4 Quality assessment esterno").

Il CAE ha la responsabilità di garantire che la funzione Internal Audit sia costantemente alla ricerca di miglioramenti. Ciò richiede lo sviluppo di indicatori per valutare le performance degli incarichi di Internal Audit, degli Internal Auditor e della funzione Internal Audit. Questi indicatori costituiscono la base per valutare i progressi verso gli obiettivi di performance, compreso il miglioramento continuo.

Standard 12.1 Quality assessment interno

Requisiti

Il CAE deve sviluppare e condurre assessment interni sulla conformità della funzione Internal Audit ai Global Internal Audit Standards e sui progressi rispetto agli obiettivi di performance.

Il CAE deve stabilire una metodologia per questi assessment interni, come descritto nello Standard "8.3 Qualità", che includa:

- monitoraggio continuo della conformità della funzione Internal Audit agli Standard e dei progressi rispetto agli obiettivi di performance;
- self-assessment periodici o assessment da parte di altre persone all'interno dell'organizzazione con una conoscenza sufficiente delle pratiche di Internal Auditing per valutare la conformità agli Standard;
- comunicazione con il Board e il Top Management in merito ai risultati degli assessment interni.

Sulla base dei risultati dei self-assessment periodici, il CAE deve sviluppare piani d'azione per affrontare le non conformità agli Standard e le opportunità di miglioramento, con una tempistica prevista per l'implementazione delle azioni. Il CAE deve comunicare i risultati dei self-assessment periodici e dei piani d'azione al Board e al Top Management (si vedano anche gli Standard "8.1 Interazione con il Board", "8.3 Qualità" e "9.3 Metodologie").

Gli assessment interni devono essere documentati e inclusi nella valutazione condotta da una terza parte indipendente come parte del quality assessment esterno (si veda anche lo Standard "8.4 Quality assessment esterno").

Se la non conformità agli Standard influisce sullo scopo o sull'operatività della funzione Internal Audit, il CAE deve comunicare al Board e al Top Management la non conformità e il suo impatto.

Indicazioni per l'implementazione

Monitoraggio continuo

Il monitoraggio continuo comporta la quotidiana supervisione, revisione e misurazione della funzione Internal Audit. Il monitoraggio continuo è incorporato nelle policy e nelle pratiche di routine adottate per la gestione della funzione Internal Audit e include i processi, gli strumenti e le informazioni necessarie per valutare la conformità agli Standard.

I progressi della funzione Internal Audit verso gli obiettivi di performance e la conformità agli Standard sono monitorati in primo luogo mediante le metodologie adottate nelle revisioni per la supervisione dell'incarico, relativamente alla pianificazione, alle carte di lavoro e alle comunicazioni finali. Queste metodologie consentono di identificare i punti deboli o le aree che necessitano di miglioramenti e i piani d'azione per affrontarli. Il CAE può sviluppare template per le carte di lavoro, eventualmente implementati nei sistemi informativi, da utilizzare durante gli incarichi per promuovere la standardizzazione e la coerenza nell'applicazione delle metodologie.

Un'adeguata supervisione dell'incarico è un elemento fondamentale di un programma di assurance e miglioramento della qualità. La supervisione inizia con la pianificazione e continua per tutta la durata dell'incarico. La supervisione può includere la definizione delle aspettative, l'impulso alla comunicazione tra i membri del team durante l'incarico e la revisione e approvazione tempestiva delle carte di lavoro (si veda anche lo Standard "12.3 Supervisione e miglioramento delle performance dell'incarico").

Altri meccanismi comunemente utilizzati per il monitoraggio continuo includono:

- checklist o sistemi informativi per garantire la conformità degli Internal Auditor alle metodologie stabilite e per facilitare l'esecuzione dei servizi di Internal Auditing in conformità con gli Standard (questi possono essere particolarmente importanti in funzioni Internal Audit con risorse umane limitate per la supervisione);
- feedback dagli stakeholder dell'Internal Audit in merito all'efficienza e all'efficacia del team di Internal Audit; il feedback può essere richiesto immediatamente dopo l'incarico o periodicamente (ad esempio, semestralmente o annualmente) attraverso survey o discussioni tra il CAE e il management;
- altre misurazioni che possono essere utili per determinare l'efficienza e l'efficacia della funzione Internal Audit includono metriche che indicano l'adeguatezza dell'allocazione delle risorse (come lo scostamento tra budget e consuntivi), le tempistiche di esecuzione dell'incarico, il completamento del piano di Audit e survey volte a misurare la soddisfazione degli stakeholder.

Oltre a convalidare la conformità agli Standard, il monitoraggio continuo può evidenziare opportunità per migliorare la funzione Internal Audit. In tali casi, il CAE può cogliere queste opportunità sviluppando un piano d'azione.

Self-assessment periodici

I self-assessment periodici forniscono una revisione più completa, su tutti gli Standard e sull'intera funzione Internal Audit. I self-assessment periodici, infatti, riguardano la conformità a tutti gli Standard, mentre il monitoraggio continuo può essere incentrato sugli Standard rilevanti per l'esecuzione degli incarichi. Le autovalutazioni periodiche possono essere condotte da membri senior della funzione Internal Audit, da un team dedicato al controllo della qualità, da persone all'interno della funzione Internal Audit che hanno ottenuto la certificazione Certified Internal Auditor® o hanno un'importante esperienza riguardo agli Standard oppure da persone con competenze di audit provenienti da altri settori dell'organizzazione. Il CAE dovrebbe prendere in considerazione il coinvolgimento degli Internal Auditor nel processo di self-assessment periodico per migliorare la loro comprensione degli Standard.

I self-assessment periodici consentono alla funzione Internal Audit di confermare la propria conformità agli Standard. Quando un self-assessment periodico viene eseguito poco prima di un assessment esterno, la durata dello stesso e l'impegno necessario per il suo svolgimento possono essere ridotti.

I self-assessment periodici valutano:

- l'adeguatezza delle metodologie della funzione Internal Audit;
- in che misura la funzione Internal Audit supporta il raggiungimento degli obiettivi dell'organizzazione;
- la qualità dei servizi di Internal Auditing e della relativa supervisione;
- il livello di soddisfacimento delle aspettative degli stakeholder e il raggiungimento degli obiettivi di performance.

L'individuo o il team che conduce il self-assessment periodico valuta la conformità della funzione Internal Audit rispetto a ciascuno Standard e può raccogliere riscontri dagli stakeholder della funzione Internal Audit mediante interviste e survey. Attraverso questo processo, il CAE può valutare la qualità e l'aderenza alle metodologie della funzione Internal Audit.

Esempi di conformità

- Checklist completate a supporto della revisione delle carte di lavoro, risultati delle survey e misurazione delle performance relative all'efficienza e all'efficacia della funzione Internal Audit.
- Documentazione dei self-assessment periodici completati, che includono il piano, le carte di lavoro e le comunicazioni.
- Presentazioni al Board e al management e verbali delle riunioni relative ai risultati degli assessment interni.
- Documentazione a supporto dell'attività di monitoraggio continuo e dei self-assessment periodici, compresi i piani delle azioni correttive.
- Azioni intraprese per migliorare l'efficienza, l'efficacia e la conformità della funzione Internal Audit agli Standard.

Standard 12.2 Misurazione delle performance

Requisiti

Il CAE deve definire degli obiettivi per valutare le performance della funzione Internal Audit e, nello sviluppo di questi obiettivi, deve considerare gli input e le aspettative del Board e del Top Management.

Il CAE deve sviluppare una metodologia di misurazione delle performance per valutare i progressi nel raggiungimento degli obiettivi e per promuovere il miglioramento continuo della funzione Internal Audit.

Nel valutare le performance della funzione Internal Audit, il CAE deve chiedere anche feedback da parte del Board e/o del Top Management.

Il CAE deve sviluppare un piano d'azione per affrontare le criticità e le opportunità di miglioramento.

Indicazioni per l'implementazione

La definizione degli obiettivi di performance è fondamentale per determinare se una funzione Internal Audit stia adempiendo al proprio Mandato in conformità con gli Standard e per ottenere miglioramenti in linea con la strategia della funzione.

La definizione degli obiettivi di performance dovrebbe prendere in considerazione quanto previsto da:

- i Principi dei Global Internal Audit Standards;
- l'Internal Audit Charter;
- la strategia della funzione Internal Audit.

Il CAE può identificare una serie di obiettivi di performance mirati da riportare al Board e al Top Management, mantenendo al contempo un insieme più completo di obiettivi di performance per la gestione della funzione Internal Audit. È necessario prestare attenzione all'identificazione di obiettivi di performance che promuovano i risultati desiderati e siano bilanciati tra le diverse aree, quali: aspettative degli stakeholder, distribuzione dei risultati all'interno della business unit o dell'intera organizzazione, gestione delle risorse umane, efficienza finanziaria e operativa, formazione e sviluppo.

Dopo averli identificati, il CAE dovrebbe stabilire dei target, sia quantitativi che qualitativi, per verificare i progressi nel raggiungimento degli obiettivi di performance. Il CAE dovrebbe disporre di una metodologia per convalidare periodicamente l'accuratezza delle misurazioni in essere e aumentare i livelli attesi di performance.

I piani d'azione per affrontare le criticità e per raggiungere gli obiettivi di performance dovrebbero essere monitorati dal CAE e comunicati al Board e al Top Management. Esempi di tipologie di performance da considerare quando si stabiliscono gli obiettivi e i criteri di misurazione possono includere:

- la copertura degli obiettivi di audit previsti dal Mandato di Internal Audit;
- la misura di quanto le conclusioni dell'Internal Audit a livello di business unit o organizzazione affrontino obiettivi significativi dell'organizzazione (si veda anche lo Standard "11.3 Comunicazione dei risultati");
- la percentuale di raccomandazioni o piani d'azione completati dal management che si traducono nei risultati attesi, come accertato dal monitoraggio della funzione di Internal Audit. Tale misura non riflette esclusivamente le performance della funzione Internal Audit. Mentre le funzioni Internal Audit possono monitorare l'attuazione delle raccomandazioni o dei piani d'azione, il management è responsabile del completamento di tali azioni e di garantire il raggiungimento dei risultati desiderati (si veda anche lo Standard "15.2 Conferma dell'attuazione delle raccomandazioni o piani d'azione");
- la percentuale dei rischi e dei controlli chiave dell'organizzazione esaminati;
- la soddisfazione degli stakeholder per quanto riguarda la comprensione degli obiettivi, le tempistiche di esecuzione dell'incarico e la chiarezza delle conclusioni;
- la percentuale del piano di Audit (da ultima revisione approvata) completato in tempo;
- il bilanciamento degli incarichi di assurance e advisory nel piano di Audit rispetto alla strategia di Internal Audit;
- le quality assurance review esterne che attestano la conformità della funzione Internal Audit agli Standard;
- le quality assurance review che confermano l'esistenza di competenze adeguate a svolgere gli incarichi di Internal Auditing pianificati;
- i piani di formazione e sviluppo degli Internal Auditor legati alla strategia di Internal Audit e ai rischi dell'organizzazione;
- il personale in possesso di almeno una certificazione professionale rilevante ai fini dell'Internal Audit.

Esempi di conformità

- Obiettivi di performance chiave per la funzione Internal Audit formalizzati, che soddisfino i Principi degli Standard, l'Internal Audit Charter e la strategia della funzione stessa.
- Key performance indicator che forniscono l'andamento rispetto agli obiettivi e ai relativi target.
- Piani d'azione per affrontare le criticità individuate e per raggiungere gli obiettivi di performance definiti.

Standard 12.3 Supervisione e miglioramento delle performance dell'incarico

Requisiti

Il CAE deve stabilire e implementare metodologie per la supervisione dell'incarico, la quality assurance e lo sviluppo delle competenze.

- Il CAE o un supervisore dell'incarico deve guidare gli Internal Auditor durante l'incarico, verificare che i programmi di lavoro siano completi e confermare che le carte di lavoro dell'incarico supportino adeguatamente i rilievi, le valutazioni e le raccomandazioni.
- Per garantire la qualità, il CAE deve verificare se gli incarichi sono svolti in conformità con gli Standard e le metodologie della funzione Internal Audit.
- Per sviluppare le competenze, il CAE deve fornire agli Internal Auditor un feedback sulle loro performance e sulle opportunità di miglioramento.

L'entità della supervisione richiesta dipende dalla maturità della funzione Internal Audit, dalla competenza e dall'esperienza degli Internal Auditor e dalla complessità degli incarichi.

Il CAE è responsabile della supervisione degli incarichi, indipendentemente dal fatto che l'incarico sia svolto dal personale dell'Internal Audit o da altri fornitori di servizi. Le responsabilità di supervisione possono essere delegate a persone appropriate e qualificate, ma il CAE mantiene la responsabilità ultima.

Il CAE deve garantire che le evidenze della supervisione siano documentate e conservate, secondo le metodologie stabilite dalla funzione Internal Audit.

Indicazioni per l'implementazione

Quando si pianificano gli incarichi, il CAE, o un supervisore designato per l'incarico, dovrebbe esaminare gli obiettivi dell'incarico. La supervisione può includere momenti dedicati allo sviluppo del personale, come riunioni post-incarico tra gli Internal Auditor che hanno svolto l'incarico e il CAE.

La valutazione delle competenze degli Internal Auditor è un processo continuo che va oltre la revisione delle carte di lavoro dell'incarico. Sulla base dei risultati delle valutazioni delle competenze, il CAE può identificare quali Internal Auditor siano qualificati per supervisionare gli incarichi e assegnare i compiti di conseguenza.

Durante la fase di pianificazione, il supervisore dell'incarico approva il programma di lavoro dell'incarico e può assumersi la responsabilità di altri aspetti dell'incarico (si veda anche il Principio "13 Pianificare gli incarichi in modo efficace" e i relativi Standard).

Il criterio principale per l'approvazione del programma di lavoro è verificare se raggiunge gli obiettivi dell'incarico in modo efficiente. Il programma di lavoro include procedure per l'identificazione, l'analisi, la valutazione e la documentazione delle informazioni relative all'incarico. La supervisione dell'incarico comporta anche il monitoraggio del completamento del programma di lavoro e l'approvazione delle modifiche al programma di lavoro.

Il supervisore dell'incarico dovrebbe mantenere una comunicazione costante con gli Internal Auditor assegnati all'incarico e il management dell'attività oggetto di audit. Il supervisore dell'incarico esamina le carte di lavoro dell'incarico, che descrivono le procedure di audit eseguite, le informazioni identificate e i rilievi e le conclusioni preliminari emersi durante l'incarico. Il supervisore valuta se le informazioni, le attività di test e le evidenze dei risultati sono pertinenti, affidabili e sufficienti per raggiungere gli obiettivi dell'incarico e per supportare le conclusioni dello stesso. Nelle funzioni Internal Audit che non dispongono di auditor per la supervisione e il monitoraggio continuo, il CAE può prendere in considerazione l'uso di strumenti quali checklist o sistemi informativi a supporto, per garantire in ogni incarico l'aderenza agli Standard.

Lo Standard "11.2 Comunicazione efficace" richiede che le comunicazioni dell'incarico siano accurate, obiettive, chiare, concise, costruttive, complete e tempestive. Un supervisore dell'incarico verifica questi elementi nelle comunicazioni dell'incarico e nelle carte di lavoro, poiché le carte di lavoro costituiscono la base delle comunicazioni dell'incarico.

Per tutta la durata dell'incarico, il supervisore dell'incarico e/o il CAE si incontrano con gli Internal Auditor assegnati all'incarico e discutono del processo, il che offre l'opportunità di formare, sviluppare e valutare gli Internal Auditor. Un supervisore può chiedere ulteriori evidenze o chiarimenti durante la revisione delle comunicazioni e delle carte di lavoro dell'incarico. Gli Internal Auditor possono essere messi in condizione di migliorare il proprio lavoro dando seguito alle richieste formulate dal supervisore dell'incarico.

Di solito, i commenti del supervisore vengono cancellati dalla documentazione finale una volta che sono state fornite evidenze adeguate o le carte di lavoro sono state integrate con le informazioni aggiuntive che rispondono alle questioni sollevate dal supervisore e alle sue richieste. In alternativa, la funzione Internal Audit può conservare una versione separata dei documenti con i commenti del supervisore, i passi seguiti per indirizzarli e i conseguenti esiti.

Il CAE è responsabile di tutti gli incarichi di Internal Audit e di tutte le scelte significative basate sul giudizio professionale nel corso degli stessi, indipendentemente dal fatto che il lavoro sia stato svolto dalla funzione Internal Audit o da altri fornitori di servizi di assurance. Il CAE sviluppa metodologie per ridurre al minimo il rischio che gli Internal Auditor esprimano giudizi o intraprendano azioni che non sono coerenti con il giudizio professionale del CAE e possono influire negativamente sull'incarico. Il CAE stabilisce regole per risolvere eventuali divergenze di giudizio professionale. Ciò può includere la discussione dei fatti pertinenti, l'estensione delle indagini o delle ricerche e la documentazione dei diversi punti di vista nelle carte di lavoro dell'incarico, incluse le eventuali conclusioni raggiunte. Se c'è una differenza di giudizio professionale su una questione etica, la questione può essere riportata ai soggetti dell'organizzazione che sono responsabili degli aspetti etici.

Esempi di conformità

- Carte di lavoro dell'incarico con evidenza della supervisione.
- Checklist completate che supportano la revisione delle carte di lavoro.
- Risultati di interviste e survey che includono feedback su come gli stessi Internal Auditor e altre persone direttamente coinvolte hanno svolto l'incarico.
- Documentazione della comunicazione tra il supervisore e gli Internal Auditor in merito all'incarico.

Sezione V: Svolgimento delle attività di Internal Auditing

Lo **svolgimento delle attività di Internal Auditing** richiede che gli Internal Auditor pianifichino gli incarichi in maniera efficace, svolgano l'incarico al fine di determinare rilievi e valutazioni, collaborino con il management per identificare raccomandazioni e/o piani d'azione che sanino i rilievi e comunichino con il management e il personale responsabili dell'attività oggetto di audit durante e dopo l'incarico.

Sebbene gli Standard per lo svolgimento degli incarichi siano presentati in sequenza, i passaggi non sono sempre distinti, lineari e sequenziali. In pratica, l'ordine in cui vengono eseguiti può variare in base all'incarico e avere sovrapposizioni e iterazioni. Ad esempio, la pianificazione dell'incarico include la raccolta di informazioni e la valutazione dei rischi, che possono continuare per tutta la durata dello stesso. Ogni passaggio può influire su un altro o sull'incarico nel suo complesso. Pertanto, gli Internal Auditor dovrebbero esaminare e comprendere tutti gli Standard presentati in questa sezione prima di iniziare un incarico.

L'Internal Audit offre servizi di assurance, advisory o entrambi. Ci si aspetta che gli Internal Auditor applichino e rispettino gli Standard quando svolgono gli incarichi, sia che forniscano assurance, sia advisory, salvo quando diversamente specificato nei singoli Standard.

I servizi di assurance hanno lo scopo di garantire l'affidabilità dei processi di governance, risk management e controllo agli stakeholder dell'organizzazione, in particolare al Board, al Top Management e ai responsabili dell'attività oggetto di audit. Tramite i servizi di assurance, gli Internal Auditor forniscono valutazioni oggettive delle differenze tra la condition (situazione reale, "as-is") di un'attività oggetto di audit e i criteri di valutazione. Gli Internal Auditor valutano le differenze per determinare se vi sono rilievi da evidenziare e per fornire un giudizio sui risultati dell'incarico, comunicando anche quali processi risultano efficaci.

Gli Internal Auditor possono avviare servizi di advisory o svolgerli su richiesta del Board, del Top Management o dei responsabili di un'attività. La natura e l'ambito dei servizi di advisory possono essere oggetto di accordo con la parte che richiede i servizi. Esempi di servizi di advisory includono: la consulenza sul disegno e l'implementazione di nuove procedure, processi, sistemi e prodotti; la fornitura di servizi forensi; l'erogazione di formazione; il supporto nelle discussioni sui rischi e sui controlli. Nell'esecuzione di servizi di advisory, ci si aspetta che gli Internal Auditor mantengano l'obiettività non assumendosi responsabilità di gestione. Ad esempio, gli Internal Auditor possono svolgere servizi di advisory, ma se il CAE si assume anche responsabilità che vanno oltre quelle di Internal Auditing, devono essere implementate misure adeguate per mantenere l'indipendenza della funzione Internal Audit (si veda anche lo Standard "7.1 Indipendenza organizzativa").

I servizi di Internal Auditing sono svolti secondo le modalità descritte nelle metodologie stabilite dal CAE (si veda anche lo Standard "9.3 Metodologie"). Egli può delegare la responsabilità ad altri professionisti qualificati nella funzione Internal Audit, ma mantiene la responsabilità finale.

Principio 13 Pianificare gli incarichi in modo efficace

Gli Internal Auditor pianificano ogni incarico utilizzando un approccio sistematico e disciplinato.

I Global Internal Audit Standards, insieme alle metodologie stabilite dal CAE, costituiscono la base dell'approccio sistematico e disciplinato degli Internal Auditor alla pianificazione degli incarichi. Gli Internal Auditor sono responsabili di comunicare in modo efficace in tutte le fasi dell'incarico.

La pianificazione dell'incarico inizia con la comprensione delle aspettative iniziali per l'incarico stesso e del motivo per cui l'incarico è stato incluso nel piano di Audit. Durante la pianificazione degli incarichi, gli Internal Auditor raccolgono le informazioni che consentono loro di comprendere l'organizzazione e l'attività in esame e di valutare i rischi rilevanti per l'attività. Il risk assessment consente agli Internal Auditor di identificare e classificare in ordine di priorità i rischi per determinare gli obiettivi e l'ambito dell'incarico. Gli Internal Auditor identificano inoltre i criteri e le risorse necessari per eseguire l'incarico e sviluppano un programma di lavoro, che descrive gli specifici passi da seguire.

Standard 13.1 Comunicazione dell'incarico

Requisiti

Gli Internal Auditor devono comunicare in modo efficace in tutte le fasi dell'incarico (si vedano anche il Principio "11 Comunicare in modo efficace" e relativi Standard e lo Standard "15.1 Comunicazione finale dell'incarico").

Gli Internal Auditor devono comunicare gli obiettivi, l'ambito e la tempistica dell'incarico al management. Le modifiche successive devono essere comunicate tempestivamente al management (si veda anche lo Standard "13.3 Obiettivi e ambito dell'incarico").

Al termine di un incarico, se gli Internal Auditor e il management non concordano sui risultati dell'incarico, gli Internal Auditor devono discutere e cercare di raggiungere un'intesa in merito alla questione con il management coinvolto nell'attività oggetto di audit. Se non è possibile raggiungere un'intesa comune, gli Internal Auditor non devono essere obbligati a modificare alcuna parte dei risultati dell'incarico, a meno che non vi sia una valida ragione per farlo. Gli Internal Auditor devono seguire una procedura condivisa per consentire a entrambe le parti di esprimere le proprie posizioni in merito ai contenuti della comunicazione finale dell'incarico e alle ragioni di eventuali divergenze di opinione in merito ai risultati dell'incarico (si vedano anche gli Standard "9.3 Metodologie" e "14.4 Raccomandazioni e piani d'azione").

Indicazioni per l'implementazione

Le comunicazioni rivolte al management dell'attività oggetto di audit possono svolgersi all'avvio, nel corso, alla chiusura e dopo la conclusione dell'incarico. La tipologia dell'incarico può influire sulle comunicazioni necessarie.

Per garantire una comunicazione efficace, dovrebbero essere utilizzate modalità diverse: formali, informali, scritte e orali.

Le comunicazioni dell'incarico possono svolgersi tramite riunioni, presentazioni, scambio di e-mail e altri documenti nonché attraverso discussioni informali. I requisiti sulla qualità e sul contenuto

delle comunicazioni dovrebbero essere definiti dal CAE in linea con le aspettative del Board e del Top Management e documentati nelle metodologie di Internal Audit (si vedano anche gli Standard "9.3 Metodologie" e "11.2 Comunicazione efficace").

La portata delle comunicazioni durante l'incarico dipende dalla natura e dalla durata dello stesso e può prevedere:

- la comunicazione dell'avvio dell'incarico;
- l'illustrazione del risk assessment, degli obiettivi, dell'ambito e delle tempistiche dell'intervento;
- la richiesta delle informazioni e delle risorse necessarie per eseguire l'incarico;
- la definizione delle aspettative per ulteriori comunicazioni dell'incarico;
- l'aggiornamento sull'avanzamento dell'incarico, incluse le criticità relative alla governance, risk management o controllo che richiedono un'attenzione immediata e modifiche all'ambito, agli obiettivi, alle tempistiche dell'incarico;
- i risultati dell'incarico, compresi i rilievi, le raccomandazioni e/o i piani d'azione del management individuati per risolvere i rilievi stessi;
- le scadenze temporali e i responsabili dell'attuazione delle raccomandazioni e/o dei piani d'azione.

Gli Internal Auditor dovrebbero informare in anticipo dell'esecuzione dell'incarico gli stakeholder rilevanti, compresi il management e il personale coinvolto, al fine di costruire le basi per la cooperazione e il dialogo. Gli Internal Auditor dovrebbero seguire quanto stabilito dal CAE per determinare i tempi e le modalità di preavviso. La comunicazione dell'avvio dell'incarico dovrebbe informare il management sul motivo dell'audit, sulla data di avvio proposta e sulla durata approssimativa dell'incarico per pianificare un programma che non sia in conflitto con altri eventi significativi che riguardano l'attività oggetto di audit. Inoltre, gli Internal Auditor dovrebbero richiedere le informazioni e la documentazione necessarie per valutare i rischi e iniziare a sviluppare il programma di lavoro.

Un'altra comune modalità di comunicazione di avvio dell'incarico è l'organizzazione di un kick-off meeting. Quando gli Internal Auditor svolgono un risk assessment dell'incarico, dovrebbero comunicare i risultati al management coinvolto. Dovrebbero anche comunicare gli obiettivi e l'ambito dell'incarico, preferibilmente in una riunione. Questa discussione offre agli Internal Auditor l'opportunità di confermare che il management dell'attività oggetto di audit abbia compreso e supporti gli obiettivi, l'ambito e le tempistiche dell'incarico. La discussione consente alle parti di apportare le modifiche necessarie all'approccio e di definire le aspettative per ulteriori comunicazioni, compresa la frequenza delle stesse e chi riceverà la comunicazione finale. Gli Internal Auditor dovrebbero assicurarsi che questa discussione venga documentata nelle carte di lavoro.

La comunicazione durante l'incarico tra gli Internal Auditor e il management dell'attività oggetto di audit è essenziale per trasmettere informazioni che richiedono un'attenzione immediata e aggiornare le parti coinvolte in merito all'andamento dell'incarico o alle modifiche degli obiettivi o dell'ambito. Questa comunicazione continua abilita la trasparenza e aiuta gli Internal Auditor e il management dell'attività a identificare e risolvere eventuali incomprensioni o differenze.

A seconda del tipo di incarico, gli Internal Auditor possono organizzare una riunione di chiusura dell'incarico (chiamata anche "exit meeting"), che rappresenta un'opportunità per gli Internal Auditor, il management dell'attività oggetto di audit e il personale coinvolto di finalizzare i risultati dell'incarico prima di emettere la comunicazione finale. L'exit meeting offre l'opportunità al management e agli Internal Auditor di discutere eventuali differenze di opinione o divergenze sui risultati dell'incarico con l'obiettivo di raggiungere un accordo.

La discussione in merito alla fattibilità delle raccomandazioni degli Internal Auditor o dei piani d'azione definiti dal management può includere la valutazione dei relativi costi, così come della gravità del rischio rispetto ai benefici derivanti dall'attuazione delle raccomandazioni o dei piani d'azione (si veda anche lo Standard "14.4 Raccomandazioni e piani d'azione"). Il piano delle azioni del management potrebbe non essere completamente sviluppato prima della comunicazione conclusiva, ma il management potrebbe avere idee sulle azioni che intraprenderà per risolvere i rilevi. Anche se il management non ha completamente definito il piano d'azione, le proposte possono essere discusse e valutate. Dopo la discussione, il management può confermare il proprio piano, le tempistiche di attuazione previste e i responsabili dell'implementazione delle azioni.

Esempi di conformità

- Documentazione (e-mail, verbali di riunione, note o appunti) ad evidenza delle comunicazioni intercorse durante l'incarico.
- Documentazione dei feedback ricevuti (ad esempio tramite sondaggi) dal management dell'attività oggetto di audit.

Standard 13.2 Risk assessment dell'incarico

Requisiti

Gli Internal Auditor devono acquisire un'adeguata conoscenza dell'attività oggetto di audit per valutarne i rischi rilevanti. Per i servizi di advisory, potrebbe non essere necessario un risk assessment formale e documentato, a seconda dell'accordo con le parti interessate.

Per una conoscenza adeguata, gli Internal Auditor devono identificare e raccogliere informazioni affidabili, pertinenti e sufficienti riguardanti:

- le strategie, gli obiettivi e i rischi dell'organizzazione rilevanti per l'attività oggetto di audit;
- la risk tolerance dell'organizzazione, se definita;
- il risk assessment a supporto del piano di Audit;
- i processi di governance, risk management e controllo dell'attività oggetto di audit;
- i framework, le linee guida e altri criteri applicabili che possono essere utilizzati per valutare l'efficacia di tali processi.

Gli Internal Auditor devono esaminare le informazioni raccolte per comprendere il disegno dei processi.

Gli Internal Auditor devono identificare i rischi da includere nell'audit attraverso:

- l'identificazione dei rischi potenzialmente significativi per il raggiungimento degli obiettivi dell'attività oggetto di audit;
- la considerazione dei rischi specifici legati alle frodi;
- la valutazione della significatività dei rischi e la relativa prioritizzazione ai fini dell'audit.

Gli Internal Auditor devono identificare i criteri che il management utilizza per determinare in che misura l'attività raggiunge i suoi obiettivi.

Se gli Internal Auditor avevano identificato i rischi rilevanti per l'attività oggetto di audit in occasione di incarichi precedenti, è richiesta solo una revisione e un aggiornamento del precedente risk assessment dell'incarico.

Indicazioni per l'implementazione

Gli Internal Auditor dovrebbero consultarsi con il supervisore dell'incarico durante la pianificazione.

Per sviluppare una comprensione dell'attività oggetto di audit e quindi valutare i rischi rilevanti, gli Internal Auditor dovrebbero iniziare dall'analisi del piano di Audit, dalle discussioni che hanno portato alla sua predisposizione e dal motivo per cui l'incarico è stato incluso nel piano. Gli incarichi inclusi nel piano di Audit possono derivare dall'attività di risk assessment o dalle richieste degli stakeholder.

Quando avviano un incarico, gli Internal Auditor dovrebbero considerare i rischi applicabili allo stesso e informarsi se si sono verificati cambiamenti da quando il piano di Audit è stato sviluppato. La revisione del risk assessment dell'organizzazione e di qualsiasi altra recente valutazione dei rischi svolta (come quelle svolte dal management) può aiutare gli Internal Auditor a identificare i rischi rilevanti per l'attività oggetto di audit. Gli Internal Auditor dovrebbero comprendere tutte le aspettative degli stakeholder in merito allo scopo, agli obiettivi e all'ambito dell'incarico.

Gli Internal Auditor dovrebbero esaminare l'allineamento tra l'organizzazione e l'attività oggetto di audit. Gli Internal Auditor raccolgono ed esaminano le informazioni dell'organizzazione riguardanti le strategie e i processi di governance, risk management e controllo, nonché i suoi obiettivi, policy e procedure. Dovrebbero considerare in che modo questi aspetti dell'organizzazione si relazionano con l'attività oggetto di audit e con l'incarico quando iniziano a sviluppare il risk assessment dell'incarico.

Per raccogliere informazioni, gli Internal Auditor possono:

- esaminare i risk assessment svolti di recente dalla funzione Internal Audit, dal management o dai fornitori esterni di servizi (gli obiettivi presi in considerazione dovrebbero includere la compliance, il financial reporting, le attività operative, le frodi, l'information technology);
- esaminare le comunicazioni relative agli incarichi precedentemente svolti dalla funzione Internal Audit e da altri fornitori di servizi di assurance e advisory, quali quelli in ambito financial, ambientale, di responsabilità sociale e di governance;
- esaminare le carte di lavoro degli incarichi precedenti;
- esaminare i riferimenti pertinenti, quali le linee guida dell'IIA o di altri organismi e le leggi e i regolamenti applicabili al settore, all'industria e all'ambito giurisdizionale dell'organizzazione;
- prendere in considerazione le categorie di rischio rilevanti dell'organizzazione, tra cui strategico, operativo, finanziario e di compliance;
- considerare la risk tolerance, se è stata definita;
- utilizzare gli organigrammi e le descrizioni delle mansioni per determinare chi è responsabile delle informazioni, dei processi e di altri aspetti rilevanti dell'attività oggetto di audit;
- visitare fisicamente le sedi o le strutture dell'attività oggetto di audit;
- esaminare la documentazione interna o esterna, comprese le policy, le procedure, i flow chart e i report del management;
- esaminare siti web, i database e i sistemi;
- acquisire informazioni tramite interviste, discussioni o survey;
- osservare un processo nel suo svolgimento (walkthrought);
- effettuare incontri con altri fornitori di servizi di assurance e advisory.

Sondaggi, interviste, sopralluoghi e walkthrought consentono agli Internal Auditor di osservare lo stato attuale dell'attività oggetto di audit.

Per effettuare il risk assessment dell'incarico, gli Internal Auditor utilizzano le informazioni raccolte per comprendere e documentare gli obiettivi dell'attività oggetto di audit, i rischi che potrebbero influenzare il raggiungimento di ciascun obiettivo e i controlli volti a gestire ciascun rischio (si veda anche lo Standard "14.6 Documentazione dell'incarico").

Gli Internal Auditor possono costruire un grafico, un foglio excel, una matrice di rischi e controlli, una descrizione dei processi o un altro strumento per documentare i rischi e i controlli implementati per gestirli. Tale documentazione supporta gli Internal Auditor nell'applicare il giudizio professionale, l'esperienza e la logica per considerare le informazioni raccolte nel contesto dell'attività oggetto di audit e per stimare la significatività dei rischi in termini di impatto, probabilità ed eventualmente altri fattori di rischio.

Determinare la significatività dei rischi richiede che gli Internal Auditor applichino le loro conoscenze, esperienze e pensiero critico per formulare giudizi sull'organizzazione, sull'attività oggetto di audit, sullo scopo e sul contesto dell'incarico. Nell'ambito della diligenza professionale, gli Internal Auditor dovrebbero raccogliere il contributo del management dell'attività oggetto di audit per ottenere informazioni sugli obiettivi aziendali, sui rischi significativi e sui controlli. Stabilire una comprensione reciproca dei rischi dell'attività oggetto di audit aumenta l'utilità del risk assessment dell'incarico.

I rischi da affrontare durante l'incarico dovrebbero essere classificati in ordine di priorità in base alla significatività. Questo viene spesso illustrato mappando i rischi su un grafico, ad esempio una heat map, in base alla probabilità che il rischio si verifichi e al suo impatto potenziale. Tale documentazione dovrebbe essere conservata come parte delle carte di lavoro dell'incarico. Per i rischi più significativi, la valutazione dell'adeguatezza del disegno dei controlli aiuta gli Internal Auditor a determinare quali controlli continuare a testare per verificarne l'efficacia operativa.

Quando utilizzata, la matrice dei rischi e controlli si sviluppa durante l'incarico. Al progredire delle attività durante la fase di test, la matrice può essere utilizzata per descrivere uno specifico evento di rischio, un controllo e la sua tipologia (ovvero preventive, detective, directive, corrective), la causa, l'effetto (conseguenza) e la valutazione del rischio residuo.

Esempi di conformità

Carte di lavoro relative a:

- strategie, obiettivi e rischi dell'organizzazione;
- obiettivi dell'attività oggetto di audit;
- processi di governance, risk management e controllo dell'attività oggetto di audit;
- organigrammi e job description;
- note e/o fotografie provenienti da osservazioni o ispezioni dirette;
- policy e procedure;
- leggi e/o regolamenti pertinenti e valutazioni di compliance documentate;
- informazioni rilevanti raccolte da siti web, database e sistemi;
- minute di interviste o discussioni, risultati di sondaggi;
- informazioni pertinenti provenienti da risk assessment e incarichi completati in precedenza e dal lavoro svolto da altri fornitori di assurance;
- significatività di ciascun rischio e adeguatezza del disegno dei controlli.

Standard 13.3 Obiettivi e ambito dell'incarico

Requisiti

Gli Internal Auditor devono stabilire e documentare gli obiettivi e l'ambito di ciascun incarico.

Gli obiettivi dell'incarico devono articolare lo scopo dell'incarico e descrivere gli obiettivi specifici da raggiungere, compresi quelli imposti da leggi e/o regolamenti.

L'ambito deve definire il focus e il perimetro dell'incarico specificando le attività, i siti, i processi, i sistemi, i componenti, il periodo di tempo da coprire nell'incarico e altri elementi da esaminare e deve essere sufficiente per raggiungere gli obiettivi.

Gli Internal Auditor devono valutare se l'incarico è finalizzato a fornire assurance o advisory, poiché le aspettative degli stakeholder e i requisiti degli Standard differiscono a seconda del tipo di incarico.

Le limitazioni dell'ambito devono essere discusse con il management quando emergono, con l'obiettivo della loro risoluzione. Le limitazioni dell'ambito sono condizioni degli incarichi di assurance, ad esempio relative a vincoli di risorse o restrizioni all'accesso al personale, alle strutture, ai dati e alle informazioni, che impediscono agli Internal Auditor di eseguire l'incarico come previsto nel programma di lavoro (si veda anche lo Standard "13.5 Assegnazione delle risorse").

Se non è possibile la risoluzione con il management, il CAE deve portare la questione della limitazione dell'ambito all'attenzione del Board secondo una procedura stabilita.

Gli Internal Auditor devono avere la flessibilità di apportare modifiche agli obiettivi e all'ambito dell'incarico quando nel corso dello stesso se ne identifichi la necessità.

Il CAE deve approvare gli obiettivi e l'ambito dell'incarico e qualsiasi cambiamento che si verifichi durante l'incarico.

Indicazioni per l'implementazione

Gli obiettivi e l'ambito degli incarichi di assurance sono definiti principalmente dagli Internal Auditor, mentre gli obiettivi e l'ambito degli incarichi di advisory sono generalmente stabiliti congiuntamente dagli Internal Auditor e dal management dell'attività oggetto di audit.

Gli Internal Auditor dovrebbero allineare gli obiettivi dell'incarico agli obiettivi di business dell'attività oggetto di audit, nonché a quelli dell'organizzazione. Definire correttamente gli obiettivi e l'ambito dell'incarico prima dell'inizio dello stesso consente agli Internal Auditor di:

- concentrare gli sforzi sui rischi rilevanti per l'attività oggetto di audit sulla base dei risultati del risk assessment dell'incarico (si veda anche lo Standard "13.2 Risk assessment dell'incarico");
- sviluppare il programma di lavoro dell'incarico;
- evitare di duplicare gli sforzi o di eseguire lavori che non aggiungono valore;
- definire le tempistiche dell'incarico;
- allocare risorse appropriate e sufficienti per completare l'incarico (si veda anche lo Standard "13.5 Assegnazione delle risorse");
- comunicare chiaramente con il management e il Board.

Gli incarichi di assurance sono volti a verificare che i controlli in essere siano adeguatamente disegnati e implementati per gestire i rischi che potrebbero impedire all'attività oggetto di audit di raggiungere i propri obiettivi di business. Gli obiettivi di questi incarichi indirizzano le priorità nei test sui controlli dei processi e dei sistemi durante l'incarico. Questi includono controlli disegnati per gestire i rischi relativi a:

- attribuzione di poteri e responsabilità;
- conformità a policy, piani, procedure, leggi e regolamenti;
- accuratezza e affidabilità del reporting;
- utilizzo efficace ed efficiente delle risorse;
- salvaguardia degli asset.

Una volta stabiliti gli obiettivi dell'incarico, gli Internal Auditor dovrebbero utilizzare il giudizio professionale e consultarsi con il supervisore dell'incarico, se necessario, per determinare l'ambito dell'incarico. L'ambito di applicazione dovrebbe essere sufficientemente ampio da raggiungere gli obiettivi dell'incarico. Nel determinare l'ambito, gli Internal Auditor dovrebbero considerare separatamente ciascun obiettivo dell'incarico per garantire che possa essere raggiunto.

Gli Internal Auditor dovrebbero valutare se le richieste da parte degli stakeholder di elementi da includere o escludere dall'ambito o le restrizioni sulla durata dell'incarico costituiscano una limitazione dell'ambito.

Esempi di conformità

- Memorandum di pianificazione dell'incarico.
- Carte di lavoro dell'incarico che documentino:
  - l'allineamento tra gli obiettivi e il risk assessment dell'incarico;
  - l'ambito che permette il raggiungimento degli obiettivi dell'incarico;
  - il programma di lavoro approvato contenente gli obiettivi e l'ambito dell'incarico;
  - i verbali delle riunioni con gli stakeholder sugli obiettivi e l'ambito dell'incarico;
  - le limitazioni dell'ambito e le richieste da parte degli stakeholder dell'incarico per gli elementi da includere o escludere;
  - comunicazione finale dell'incarico.

Standard 13.4 Criteri di valutazione

Requisiti

L'Internal Auditor deve individuare i criteri più adatti da utilizzare per valutare gli aspetti dell'attività oggetto di audit definiti negli obiettivi e nell'ambito dell'incarico. Per i servizi di advisory, l'individuazione di criteri di valutazione può non essere necessaria, a seconda dell'accordo con gli stakeholder coinvolti.

Gli Internal Auditor devono valutare in che misura il Board e il Top Management abbiano stabilito criteri adeguati per determinare se l'attività oggetto di audit raggiunga i suoi obiettivi. Se tali criteri sono adeguati, gli Internal Auditor devono utilizzarli per la valutazione. Se i criteri sono inadeguati, gli Internal Auditor devono identificare i criteri appropriati mediante il confronto con il Board e/o il Top Management.

Indicazioni per l'implementazione

Nell'ambito della raccolta delle informazioni e della pianificazione dell'incarico, gli Internal Auditor individuano i criteri utilizzati dall'organizzazione per valutare l'efficacia e l'efficienza dei processi di governance, risk management e controllo dell'attività oggetto di audit. Gli Internal Auditor dovrebbero concentrarsi sui criteri di valutazione più pertinenti per l'incarico. Tali criteri dovrebbero rappresentare lo stato desiderato dell'attività ed essere specifici e pratici. Gli Internal Auditor confrontano i criteri con lo stato esistente (detto anche condition). Ad esempio, se l'obiettivo di un incarico è quello di valutare l'efficacia dei processi di controllo nell'attività oggetto di audit, i criteri potrebbero essere i risultati o gli esiti attesi dei processi di controllo dell'attività, mentre la condition è ciò che emerge dai risultati effettivi.

Criteri adeguati sono essenziali per identificare le differenze tra lo stato desiderato e la condition, che rappresentano i rilievi potenziali. Inoltre, sono necessari criteri adeguati per determinare la significatività dei rilievi e giungere a conclusioni valide. Gli Internal Auditor utilizzano il giudizio professionale per determinare se i criteri dell'organizzazione sono adeguati. Criteri adeguati sono pertinenti, allineati con gli obiettivi dell'organizzazione e dell'attività oggetto di audit e permettono confronti affidabili. Esempi di criteri adeguati includono:

- criteri interni (policy, procedure, key performance indicator o obiettivi specifici dell'attività);
- criteri esterni (leggi, regolamenti e clausole contrattuali);
- pratiche autorevoli (framework, Standard, linee guida e benchmark specifici per un settore, un'attività o una professione);
- prassi organizzative consolidate;
- aspettative basate sul disegno di un controllo;
- procedure che potrebbero non essere formalizzate.

Nel valutare l'adeguatezza dei criteri, gli Internal Auditor dovrebbero determinare se l'organizzazione ha stabilito i principi di base per definire processi appropriati di governance, risk management e controllo. Gli Internal Auditor dovrebbero considerare se l'organizzazione ha sviluppato e definito chiaramente la propria risk tolerance, comprese le soglie di rilevanza per le varie unità aziendali, funzioni o processi. Gli Internal Auditor dovrebbero verificare se l'organizzazione ha adottato o ha chiaramente definito un livello di controllo soddisfacente.

Ad esempio, soddisfacente potrebbe significare che una determinata percentuale di operazioni in riferimento ad un obiettivo di controllo è condotta in conformità con le procedure definite o che una determinata percentuale di controlli nel complesso funziona come previsto.

Inoltre, gli Internal Auditor dovrebbero ricercare best practice e confrontare i criteri di gestione con quelli utilizzati da altre organizzazioni. La determinazione dei criteri migliori per il raggiungimento degli obiettivi dell'incarico richiede che gli Internal Auditor esercitino il giudizio professionale. Gli Internal Auditor possono stabilire che le policy, le procedure e/o altri criteri documentati mancano di dettagli o sono inadeguati per altri motivi. Gli Internal Auditor possono supportare il management nella determinazione dei criteri adeguati o possono chiedere il contributo di esperti per aiutare a identificare o sviluppare i criteri pertinenti. I criteri del management possono sembrare adeguati in generale, ma gli Internal Auditor possono suggerire criteri migliori per l'incarico.

Quando i criteri utilizzati nell'attività oggetto di audit sono inadeguati o inesistenti, gli Internal Auditor possono raccomandare al management di attuare i criteri da loro individuati. La discussione sull'assenza di criteri adeguati può portare alla decisione di fornire servizi di advisory.

Gli Internal Auditor dovrebbero informare il management dell'attività oggetto di audit in merito ai criteri da utilizzare durante l'incarico. I criteri concordati dovrebbero essere documentati in modo da evitare interpretazioni errate o contestazioni da parte del management coinvolto.

Esempi di conformità

- Carte di lavoro che documentano le fonti dei criteri considerati e il processo utilizzato per determinare l'adeguatezza dei criteri utilizzati.
- Documentazione, come verbali di riunione, memorandum di pianificazione o e-mail, che attestino il confronto sui criteri da parte dell'Internal Auditor con il management dell'attività oggetto di audit e/o con il Board.

Standard 13.5 Assegnazione delle risorse

Requisiti

Quando pianificano un incarico, gli Internal Auditor devono identificare le tipologie e la quantità di risorse necessarie per raggiungere gli obiettivi dell'incarico.

Gli Internal Auditor devono considerare:

- la natura e la complessità dell'incarico;
- il periodo di tempo entro il quale l'incarico deve essere completato;
- se le risorse finanziarie, umane e tecnologiche disponibili sono adeguate e sufficienti per raggiungere gli obiettivi dell'incarico.

Se le risorse disponibili sono inadeguate o insufficienti, gli Internal Auditor devono discutere le criticità con il CAE per ottenere le risorse.

Indicazioni per l'implementazione

L'identificazione e l'assegnazione delle risorse durante la pianificazione di un incarico è in genere gestita da un Internal Auditor designato per guidare e supervisionare l'incarico. Per determinare le tipologie e la quantità di risorse necessarie per un incarico, il supervisore dovrebbe analizzare le informazioni raccolte e sviluppate durante la pianificazione dell'incarico, prestando particolare attenzione alla natura e alla complessità del lavoro da svolgere. Il supervisore esercita il giudizio professionale per assegnare le risorse in base alle fasi identificate nel programma di lavoro per raggiungere gli obiettivi dell'incarico e al tempo che ogni fase dovrebbe richiedere (si veda lo Standard "13.6 Programma di lavoro"). È anche importante considerare i vincoli che possono influire sulle prestazioni dell'incarico, come il numero di ore preventivate, i tempi, la logistica e le comunicazioni in più lingue.

Quando pianificano gli incarichi, gli Internal Auditor dovrebbero considerare l'utilizzo più efficiente ed efficace delle risorse finanziarie, umane e tecnologiche disponibili. Il supervisore dell'incarico potrebbe avere accesso alle informazioni del CAE sulle competenze specialistiche dai membri della funzione Internal Audit, che possono aiutare nell'assegnazione delle risorse. La pianificazione dell'incarico richiede di determinare se le risorse disponibili sono adeguate e sufficienti o se sono necessarie risorse aggiuntive per completare l'incarico.

Quando la limitazione delle risorse interferisce con la capacità della funzione Internal Audit di raggiungere gli obiettivi dell'incarico, il supervisore dell'incarico è responsabile di riportare tale criticità al CAE. Il CAE è responsabile di discutere con il Top Management e il Board le implicazioni dei limiti nella disponibilità di risorse e di determinare le azioni da intraprendere. Ad esempio, quando il CAE non è in grado di ottenere le risorse necessarie, potrebbe essere necessario ridurre l'ambito dell'incarico (si vedano anche il Principio "10 Gestire le risorse" e i relativi Standard).

Per migliorare l'efficace utilizzo delle risorse, gli Internal Auditor possono documentare il tempo effettivo impiegato per eseguire l'incarico rispetto al tempo preventivato. La documentazione può essere rivista per migliorare la pianificazione futura delle risorse.

Esempi di conformità

- Programma di lavoro approvato che attesta l'utilizzo di risorse adeguate e sufficienti.
- Documentazione di pianificazione che analizza i fabbisogni di risorse per l'incarico e l'assegnazione delle stesse.
- Sondaggio post incarico compilato dal management dell'attività oggetto di audit per ottenere un riscontro sulle tempistiche e sull'adeguatezza delle risorse.
- Contratti e/o rapporti documentati con fornitori di servizi esterni.

Standard 13.6 Programma di lavoro

Requisiti

Gli Internal Auditor devono sviluppare e documentare un programma di lavoro per raggiungere gli obiettivi dell'incarico.

Il programma di lavoro dell'incarico deve essere basato sulle informazioni ottenute durante la pianificazione dell'incarico, inclusi, se disponibili, i risultati del risk assessment dell'incarico.

Il programma di lavoro deve identificare:

- i criteri da utilizzare per valutare ciascun obiettivo;
- le attività per raggiungere gli obiettivi dell'incarico;
- le metodologie, comprese le procedure analitiche da utilizzare e gli strumenti per svolgere le attività;
- gli Internal Auditor assegnatari di ciascuna attività.

Il CAE deve rivedere e approvare il programma di lavoro preventivamente all'avvio dell'incarico e quando vengono apportate modifiche successive.

Indicazioni per l'implementazione

Nella fase di pianificazione di un incarico, gli Internal Auditor raccolgono e organizzano le informazioni al fine di definire un programma di lavoro. Questo è costruito sulla base delle informazioni raccolte e sviluppate durante la pianificazione dell'incarico e descrive nel dettaglio le attività e le procedure che verranno utilizzate per il raggiungimento degli obiettivi dell'incarico e per l'analisi e la valutazione delle informazioni raccolte a mano a mano che gli Internal Auditor sviluppano i rilievi, le raccomandazioni e le conclusioni dell'incarico. Per i servizi di advisory, il programma di lavoro dovrebbe essere sviluppato in collaborazione con gli stakeholders che hanno richiesto il servizio.

Il lavoro svolto durante la fase di pianificazione dovrebbe essere documentato in carte di lavoro e referenziato nel programma di lavoro (si veda anche lo Standard "14.6 Documentazione dell'incarico"). I programmi di lavoro dovrebbero prevedere gli spazi nei quali indicare i nomi degli Internal Auditor che hanno svolto le attività, le date in cui le attività sono state completate e un'indicazione della review e approvazione delle attività completate durante l'esecuzione dell'incarico.

Gli Internal Auditor possono creare il programma di lavoro collegando i rischi e i controlli identificati nell'attività di risk assessment con i test da svolgere. Durante lo svolgimento delle analisi e delle valutazioni, gli Internal Auditor possono collegare i rischi e i controlli ai rilievi e alle conclusioni.

Il livello di analisi e di dettaglio applicato durante la fase di pianificazione varia a seconda della funzione Internal Audit e dell'incarico in questione. Per gli eventuali test a campione, il programma di lavoro dovrebbe indicare la metodologia utilizzata per la definizione del campione, la popolazione, la dimensione del campione analizzato e se i risultati possono essere estesi all'intera popolazione.

La valutazione dell'adeguatezza del disegno dei controlli potrebbe essere completata nella fase di pianificazione dell'incarico, in quanto aiuta gli Internal Auditor a identificare chiaramente i controlli chiave da sottoporre a ulteriori test per verificarne l'efficacia. La valutazione dell'adeguatezza del disegno dei controlli dovrebbe essere documentata nel programma di lavoro o in una carta di lavoro separata (si veda anche lo Standard "14.6 Documentazione dell'incarico"). Tuttavia, il momento più appropriato per eseguire questa valutazione dipende dalla natura dell'incarico. Se non viene svolta durante la pianificazione, la valutazione del disegno dei controlli può essere svolta come una fase a sé stante dell'incarico, oppure gli Internal Auditor possono valutare il disegno dei controlli durante lo svolgimento dei test di efficacia dei controlli.

Esempi di conformità

Carte di lavoro a supporto dello sviluppo del programma di lavoro, quali:

- risk and control matrix con disegno dei test da effettuare;
- mappe o descrizioni dei processi di controllo;
- note sulla valutazione dell'adeguatezza del disegno del controllo;
- pianificazione di test aggiuntivi;
- verbali, note o documentazione delle riunioni di pianificazione durante le quali sono state definite attività e modalità operative;
- programma di lavoro approvato;
- approvazione delle modifiche al programma di lavoro.

Principio 14 Condurre l'incarico

Gli Internal Auditor svolgono il programma di lavoro per raggiungere gli obiettivi dell'incarico.

Per svolgere il programma di lavoro, gli Internal Auditor raccolgono informazioni e svolgono analisi e valutazioni per produrre risultati. Questi passaggi consentono agli Internal Auditor di:

- fornire assurance e identificare i potenziali rilievi;
- determinare le cause, gli effetti e la significatività dei rilievi;
- sviluppare raccomandazioni e/o collaborare con il management per definire piani d'azione;
- formulare conclusioni.

Standard 14.1 Raccolta delle informazioni per l'analisi e la valutazione

Requisiti

Per lo svolgimento delle analisi e valutazioni, gli Internal Auditor devono raccogliere informazioni con le caratteristiche di seguito descritte.

- Rilevanti - coerenti con gli obiettivi e l'ambito dell'incarico e che contribuiscano all'ottenimento dei risultati.
- Affidabili - fattuali e attuali. Gli Internal Auditor utilizzano lo scetticismo professionale per valutare se le informazioni sono affidabili; l'affidabilità è rafforzata quando le informazioni sono:
  - ottenute direttamente da un Internal Auditor o da una fonte indipendente;
  - confermate;
  - raccolte da un sistema con processi di governance, risk management e controllo efficaci.
- Sufficienti - quando permettono agli Internal Auditor di eseguire analisi e valutazioni complete e consentono a una persona prudente, informata e competente di ripetere il programma di lavoro e ottenere le stesse conclusioni dell'Internal Auditor.

Gli Internal Auditor devono valutare se le informazioni raccolte sono rilevanti e affidabili e se sono sufficienti in modo tale che le analisi forniscano una base ragionevole su cui formulare i potenziali rilievi e conclusioni dell'incarico (si veda anche lo Standard "14.2 Analisi e rilievi potenziali").

Gli Internal Auditor devono decidere se raccogliere ulteriori informazioni per le analisi e la valutazione quando le evidenze non sono rilevanti, affidabili o sufficienti a supportare i rilievi dell'incarico. Se non è possibile ottenere prove adeguate, gli Internal Auditor devono valutare se ciò costituisce un rilievo.

Indicazioni per l'implementazione

Durante la raccolta delle informazioni per completare ogni fase del programma di lavoro, gli Internal Auditor si concentrano su quelle coerenti con gli obiettivi e l'ambito dell'incarico. Applicando lo scetticismo professionale, gli Internal Auditor dovrebbero valutare criticamente se le informazioni sono fattuali, aggiornate e ottenute direttamente (ad esempio mediante osservazione diretta) o da una fonte indipendente dai responsabili delle attività oggetto dell'incarico. Confermare le informazioni confrontandole con più di una singola fonte è un altro modo per aumentarne l'affidabilità.

Le modalità per raccogliere informazioni per le analisi possono prevedere:

- interviste o questionari alle persone coinvolte nell'attività;
- osservazione diretta di un processo, anche detta walkthrough;
- acquisizione della conferma o della verifica delle informazioni da parte di una persona indipendente dall'attività oggetto di audit;
- ispezione o analisi di evidenze fisiche come documenti, magazzini o attrezzature;
- accesso diretto ai sistemi dell'organizzazione per osservare o estrarre dati;
- collaborazioni con gli utenti e gli amministratori di sistema per ottenere i dati.

Durante la raccolta delle informazioni, gli Internal Auditor dovrebbero valutare se testare una popolazione di dati completa o un campione rappresentativo. L'utilizzo di software di analisi dei dati facilita la possibilità di testare popolazioni di dati complete o mirate. Se scegliessero di selezionare un campione, gli Internal Auditor dovrebbero applicare una metodologia per garantire che il campione sia il più rappresentativo possibile dell'intera popolazione.

Esempi di conformità

- Programma di lavoro, che include le modalità per la raccolta delle informazioni rilevanti per gli obiettivi dell'incarico.
- Descrizione delle informazioni raccolte, compresa la fonte, la data in cui sono state raccolte e il periodo a cui si riferiscono.
- Evidenza documentale di come l'Internal Auditor ha stabilito che le informazioni raccolte erano sufficienti per eseguire un'analisi.

Standard 14.2 Analisi e rilievi potenziali

Requisiti

Gli Internal Auditor devono analizzare informazioni rilevanti, affidabili e sufficienti per sviluppare i rilievi potenziali dell'incarico. Per i servizi di advisory, la raccolta di evidenze per sviluppare rilievi potrebbe non essere necessaria, a seconda dell'accordo con gli stakeholder coinvolti.

Gli Internal Auditor devono analizzare le informazioni per determinare se esiste una differenza tra i criteri di valutazione e la situazione reale dell'attività oggetto di audit, nota come condition (si veda anche lo Standard "13.4 Criteri di valutazione").

Gli Internal Auditor devono analizzare la condition utilizzando le informazioni e le evidenze raccolte durante l'incarico.

Una differenza tra i criteri e la condition indica un potenziale rilievo dell'incarico che deve essere considerato e ulteriormente valutato. Se le analisi iniziali non forniscono elementi sufficienti a sostegno di un potenziale rilievo dell'incarico, gli Internal Auditor devono esercitare la diligenza professionale per determinare se sono necessarie ulteriori analisi.

Se sono necessarie ulteriori analisi, il programma di lavoro deve essere aggiornato di conseguenza e approvato dal CAE.

Se gli Internal Auditor stabiliscono che non sono necessarie ulteriori analisi e non vi è alcuna differenza tra i criteri e la condition, gli Internal Auditor devono fornire assurance nella valutazione dell'incarico in merito all'efficacia dei processi di governance, risk management e controllo dell'attività.

Indicazioni per l'implementazione

Il programma di lavoro può includere un elenco di analisi specifiche da condurre, come ad esempio:

- test in merito all'accuratezza o all'efficacia di un processo o di un'attività;
- rapporti, tendenze e analisi di regressione;
- confronti tra le informazioni del periodo corrente e i budget, le previsioni o le informazioni analoghe dei periodi precedenti;
- analisi delle relazioni tra le diverse informazioni (ad esempio, informazioni finanziarie come il valore degli stipendi e le informazioni non finanziarie come le variazioni del numero medio di dipendenti);
- benchmarking interno, confronto delle informazioni tra le diverse aree all'interno dell'organizzazione;
- benchmarking esterno, confronto di informazioni provenienti da organizzazioni simili.

Gli Internal Auditor dovrebbero comprendere e utilizzare tecnologie che migliorino l'efficienza e l'efficacia delle analisi, come le applicazioni software che consentono di testare un'intera popolazione piuttosto che solo un campione.

Le analisi dovrebbero fornire un confronto significativo tra i criteri di valutazione e la condition. Quando le analisi indicano una differenza tra i criteri e la condition, devono essere applicate le conseguenti procedure per determinare la causa e l'effetto della differenza e la significatività dei potenziali rilievi. Esempi comuni di potenziali rilievi includono errori, irregolarità, atti illegali e opportunità per migliorare l'efficienza o l'efficacia.

Gli Internal Auditor esercitano la diligenza professionale per determinare l'entità e il tipo di procedure aggiuntive che dovrebbero essere utilizzate per valutare i potenziali rilievi e determinarne la causa, l'effetto e la significatività. Il CAE e le metodologie di Internal Audit possono fornire indicazioni per determinare se effettuare ulteriori analisi. Le considerazioni includono:

- i risultati della valutazione dei rischi dell'incarico, inclusa l'adeguatezza dei processi di controllo;
- la significatività dell'attività oggetto di audit e dei potenziali rilievi;
- la misura in cui le analisi supportano potenziali rilievi;
- la disponibilità e l'affidabilità di informazioni per ulteriori valutazioni;
- i costi rispetto ai benefici derivanti dall'esecuzione di analisi aggiuntive.

Esempi di conformità

- Carte di lavoro che documentino le analisi eseguite, inclusi i data analytics o i software utilizzati, la popolazione oggetto dell'attività di testing, i processi e i metodi di campionamento.
- Carte di lavoro con i riferimenti opportuni nel programma di lavoro e/o nella comunicazione finale.
- Documentazione relativa alla comunicazione conclusiva.
- Evidenze dell'attività di supervisione dell'incarico.

Standard 14.3 Valutazione dei rilievi

Requisiti

Gli Internal Auditor devono valutare ogni potenziale rilievo dell'incarico per determinarne la sua significatività. Quando si valutano i potenziali rilievi, gli Internal Auditor devono collaborare con il management per identificare le root cause, se possibile, determinarne i potenziali effetti e valutare la rilevanza del problema.

Per determinare la significatività del rischio, gli Internal Auditor devono considerare la probabilità che il rischio si verifichi e l'impatto che il rischio può avere sui processi di governance, risk management o controllo dell'organizzazione.

Se gli Internal Auditor stabiliscono che l'organizzazione è esposta a un rischio significativo, questo deve essere documentato e comunicato come rilievo.

Gli Internal Auditor devono determinare se segnalare altri rischi come rilievi, sulla base delle circostanze e delle metodologie stabilite.

Gli Internal Auditor devono determinare la priorità di ciascun rilievo dell'incarico in base alla significatività, utilizzando metodologie stabilite dal CAE.

Indicazioni per l'implementazione

Per sviluppare i rilievi dell'incarico, gli Internal Auditor confrontano i criteri stabiliti con la condition dell'attività oggetto di audit (si veda anche lo Standard "14.2 Analisi e rilievi potenziali"). Se c'è una differenza, gli Internal Auditor sono tenuti a indagare ulteriormente il potenziale rilievo. L'indagine dovrebbe approfondire sia le cause, sia gli effetti.

- Le cause della differenza spesso si riferiscono a carenze del sistema di controllo ed è il motivo per cui esiste la condition; per quanto possibile, gli Internal Auditor dovrebbero determinare la root cause, che è un problema sottostante o più profondo che ha contribuito alla condition (nella sua forma più semplice, determinare la root cause comporta porsi una serie di domande sul perché esiste la differenza e l'identificazione della root cause richiede la collaborazione con il management, che potrebbe essere in una posizione migliore per comprendere le cause alla base della differenza).
- L'impatto della differenza è da quantificare; in molti casi, l'entità dell'esposizione è una stima basata sul giudizio professionale degli Internal Auditor con il contributo del management dell'attività oggetto di audit (si vedano anche il Principio "4 Esercitare la diligenza professionale" e i suoi Standard).

Per determinare la significatività di un rilievo, gli Internal Auditor identificano e valutano i controlli esistenti per verificarne l'adeguatezza e l'efficacia; quindi, determinano il livello di rischio residuo, ovvero il rischio che permane nonostante i controlli in atto. Sebbene gli Internal Auditor siano tenuti a comunicare i rischi significativi come rilievi, possono anche comunicare altri rischi come rilievi o comunicarli in altro modo.

Gli Internal Auditor assegnano una priorità ai rilievi, in base alla metodologia stabilita dal CAE, per garantire la coerenza in tutti gli incarichi di Internal Audit. Un rating o una graduatoria possono essere strumenti efficaci di comunicazione per descrivere la significatività di ciascun rilievo e potrebbero aiutare il management a definire le priorità dei piani d'azione. Nel determinare la significatività, gli Internal Auditor dovrebbero considerare:

- l'impatto e la probabilità del rischio;
- la risk tolerance;
- eventuali fattori aggiuntivi importanti per l'organizzazione.

Il CAE potrebbe fornire template agli Internal Auditor da utilizzare per formalizzare i rilievi dell'incarico, garantendo un'adeguata documentazione di vari elementi quali:

- criteri;
- condition;
- root cause (quando possibile);
- effetto (rischio o esposizione potenziale);
- significatività e priorità.

I risultati dovrebbero essere redatti in modo sintetico, in un linguaggio semplice, in modo tale che il management dell'attività in esame comprenda la valutazione degli Internal Auditor. I risultati dovrebbero illustrare la differenza tra la condition e i criteri e dovrebbero fornire evidenze documentali che supportino la valutazione degli Internal Auditor e il loro giudizio sulla significatività dei risultati.

Esempi di conformità

- Carte di lavoro che spieghino i criteri utilizzati per valutare i rilievi.
- Carte di lavoro che elenchino i criteri, la condition, la root cause (quando possibile), l'effetto (rischio o esposizione potenziale) e la priorità di ciascun rilievo.
- Carte di lavoro o altra documentazione che spieghino la materialità, la risk tolerance e gli elementi di eventuali analisi costi-benefici utilizzati come base dell'analisi dei rilievi.
- Metodologie, modelli e linee guida pertinenti.
- Documentazione relativa alla comunicazione finale dell'incarico.

Standard 14.4 Raccomandazioni e piani d'azione

Requisiti

Gli Internal Auditor devono decidere se sviluppare raccomandazioni, richiedere piani d'azione al management o collaborare con il management stesso per concordare azioni al fine di:

- risolvere le differenze tra i criteri stabiliti e le condition;
- mitigare a un livello accettabile i rischi identificati;
- indirizzare la root cause del rilievo;
- rafforzare o migliorare l'attività oggetto di audit.

Nell'elaborare le raccomandazioni, gli Internal Auditor devono discuterne con il management coinvolto nell'attività oggetto di audit.

Se gli Internal Auditor e il management non sono d'accordo sulle raccomandazioni e/o sui piani d'azione dell'incarico, gli Internal Auditor devono seguire la procedura definita per consentire a entrambe le parti di esprimere le proprie posizioni e motivazioni e arrivare a una risoluzione (si veda anche lo Standard "9.3 Metodologie").

Indicazioni per l'implementazione

Gli Internal Auditor dovrebbero discutere tempestivamente i rilievi e le potenziali raccomandazioni o piani d'azione con il management che ha il potere di effettuare e supervisionare i cambiamenti all'attività oggetto di audit. Il CAE può definire una regola per aiutare gli Internal Auditor nell'identificazione del management da coinvolgere. Ad esempio, la regola può prevedere che solo un determinato ruolo o livello (come un Manager, un Direttore o un Direttore Generale) abbia tale autorità.

Se gli Internal Auditor individuano un'azione correttiva specifica in risposta ad un rilievo, possono proporla come raccomandazione. In alternativa, possono presentare al management diverse opzioni. In alcuni casi, gli Internal Auditor possono suggerire che sia il management a cercare le opzioni e a determinare le azioni appropriate. Un singolo rilievo può avere più raccomandazioni o azioni correttive.

Se gli Internal Auditor e il management dell'attività oggetto di audit non fossero d'accordo sui risultati dell'incarico, il CAE dovrebbe collaborare con il Top Management per individuare una soluzione. Inoltre, una dichiarazione formale di ciascuna parte può essere allegata alla comunicazione finale dell'incarico o resa disponibile su richiesta.

Gli Internal Auditor dovrebbero valutare e discutere con il management la fattibilità e la ragionevolezza delle raccomandazioni e/o dei piani d'azione. La valutazione dovrebbe includere un'analisi dei costi e dei benefici e determinare se le raccomandazioni e/o i piani d'azione mitighino il rischio in modo soddisfacente in conformità con la risk tolerance dell'organizzazione.

Sebbene gli Internal Auditor debbano collaborare con il management nel definire come affrontare i rilievi dell'incarico, è responsabilità del management implementare azioni per risolvere i rilievi stessi (si veda anche lo Standard "15.1 Comunicazione finale dell'incarico").

Esempi di prove di conformità

- Carte di lavoro per ciascun rilievo, con i criteri, la condition, la root cause (quando possibile), l'effetto (rischio o impatto anche potenziale) e le raccomandazioni e/o i piani d'azione.
- Note, carte di lavoro o altra documentazione che evidenzi le discussioni con il management in merito ai rilievi e alla fattibilità delle raccomandazioni e/o dei piani d'azione.
- Documentazione relativa alla comunicazione finale.

Standard 14.5 Valutazioni dell'incarico

Requisiti

Gli Internal Auditor devono elaborare una valutazione che riassuma i risultati dell'incarico rispetto agli obiettivi dell'incarico e del management. La valutazione deve rappresentare il giudizio professionale di sintesi degli Internal Auditor sulla significatività dei rilievi nel loro complesso.

La valutazione dell'incarico di assurance deve includere una valutazione degli Internal Auditor in merito all'efficacia dei processi di governance, risk management e/o di controllo dell'attività oggetto di audit compresa l'attestazione di quando sono efficaci.

Indicazioni per l'implementazione

Le metodologie del CAE per la funzione Internal Audit possono fornire una scala di valutazione per indicare se si possa dare una ragionevole assurance dell'efficacia dei controlli. Ad esempio, una scala può indicare soddisfacente, parzialmente soddisfacente, necessita di miglioramenti o insoddisfacente a seconda delle valutazioni degli Internal Auditor (si veda anche lo Standard "14.3 Valutazione dei rilievi").

La valutazione potrebbe comprendere informazioni aggiuntive in relazione agli impatti dei rilievi per l'attività oggetto di audit e per l'intera organizzazione. Ad esempio, alcuni rilievi possono avere un impatto significativo sul raggiungimento degli obiettivi o sulla gestione dei rischi a livello di attività, ma non a livello di organizzazione.

La valutazione dell'incarico di advisory dovrebbe essere in linea con gli obiettivi e l'ambito di d'intervento.

Esempi di conformità

- Documentazione che illustri i fondamenti del giudizio complessivo dell'incarico.
- Una dichiarazione con il giudizio dell'incarico nella comunicazione finale.

Standard 14.6 Documentazione dell'incarico

Requisiti

Gli Internal Auditor devono documentare le informazioni e le evidenze per supportare i risultati dell'incarico. Le analisi, le valutazioni e le informazioni a supporto devono essere documentate in modo tale che un Internal Auditor informato e prudente o una qualunque persona similmente informata e competente, possa replicare il lavoro e giungere agli stessi risultati.

Gli Internal Auditor e il supervisore dell'incarico devono esaminare la documentazione relativa all'incarico per verificarne l'accuratezza, la pertinenza e la completezza. Il CAE deve esaminare e approvare la documentazione relativa all'incarico. Gli Internal Auditor devono conservare la documentazione relativa all'incarico in conformità alle leggi e/o ai regolamenti applicabili, nonché alle policy e alle procedure della funzione Internal Audit e dell'organizzazione.

Indicazioni per l'implementazione

La documentazione dell'incarico attraverso le carte di lavoro è una parte importante di un processo sistematico e disciplinato di gestione dell'incarico, perché organizza le informazioni in modo tale da consentire di ripetere l'incarico e di supportare i risultati. La documentazione fornisce la base sia per la supervisione individuale degli Internal Auditor, sia per consentire al CAE e ad altri di valutare la qualità del lavoro della funzione Internal Audit. La documentazione serve anche a dimostrare la conformità della funzione Internal Audit agli Standard.

La documentazione relativa all'incarico dovrebbe includere:

- data o periodo dell'incarico;
- risk assessment;
- obiettivi e ambito;
- programma di lavoro;
- descrizione delle analisi, compresi i dettagli delle procedure e le fonti dei dati;
- risultati dell'incarico;
- nomi o iniziali delle persone che hanno eseguito e supervisionato il lavoro;
- evidenza della comunicazione alle parti coinvolte.

Le carte di lavoro possono essere organizzate in base alla struttura sviluppata nel programma di lavoro e collegate tramite referenze alle informazioni pertinenti. Possono essere utilizzati template o software per lo sviluppo di carte di lavoro e può essere adottato un sistema per l'archiviazione della documentazione. Il risultato è una raccolta completa della documentazione informativa ottenuta, delle procedure completate, dei risultati dell'incarico e delle assunzioni logiche per ogni passaggio. Tale documentazione costituisce la fonte principale della comunicazione degli Internal Auditor con gli stakeholder, tra cui il Board, il Top Management e il management dell'attività oggetto di audit. In particolare, le carte di lavoro contengono informazioni pertinenti, affidabili e sufficienti per consentire a una persona prudente, informata e competente, come un altro Internal Auditor o un Auditor esterno, di giungere alle stesse conclusioni degli Internal Auditor che hanno condotto l'incarico.

Le carte di lavoro comunemente includono:

- documentazione di pianificazione;
- mappa dei processi, flowchart o descrizioni dei processi chiave;
- sintesi delle interviste condotte o dei questionari utilizzati;
- matrice dei rischi e dei controlli;
- dettagli dei test effettuati e delle analisi eseguite;
- conclusioni, che riportano i riferimenti dei rilievi ai documenti;
- proposta di follow-up dell'incarico da svolgere;
- comunicazione finale dell'Internal Audit con le risposte del management.

Un formato di base per le carte di lavoro:

- indice o numero di riferimento;
- titolo o intestazione che identifica l'attività oggetto di audit;
- data o periodo dell'incarico;
- ambito dell'incarico;
- dichiarazione dello scopo dell'ottenimento e dell'analisi dei dati;
- fonte(i) dei dati trattati nelle carte di lavoro;
- descrizione della popolazione valutata, comprese le dimensioni del campione e il metodo di selezione utilizzato per analizzare i dati (approccio di test);
- nome degli Internal Auditor che hanno svolto l'incarico;
- evidenza della revisione delle carte di lavoro e il nome degli Internal Auditor che hanno rivisto il lavoro svolto.

Esempi di conformità

- Carte di lavoro che documentano il lavoro svolto in conformità con la metodologia stabilita.
- Risultati delle review del quality assessment interno che attestano la conformità delle carte di lavoro e le procedure di supervisione.

Principio 15 Comunicare i risultati dell'incarico e monitorare i piani d'azione

Gli Internal Auditor comunicano i risultati dell'incarico alle parti interessate e controllano i progressi del management nell'attuazione di raccomandazioni o piani d'azione.

Gli Internal Auditor sono responsabili dell'emissione di una comunicazione finale dopo aver completato l'incarico e della trasmissione dei risultati dell'incarico al management. Gli Internal Auditor continuano a comunicare con il management dell'attività in esame per confermare l'attuazione dei piani d'azione.

Standard 15.1 Comunicazione finale dell'incarico

Requisiti

Per ogni incarico, gli Internal Auditor devono elaborare una comunicazione finale che includa gli obiettivi, l'ambito, le raccomandazioni e/o i piani d'azione dell'incarico, se applicabili, e le conclusioni.

La comunicazione finale per gli incarichi di assurance deve inoltre includere:

- i rilievi con la loro significatività e la loro priorità;
- una spiegazione delle eventuali limitazioni dell'ambito;
- un giudizio in merito all'efficacia dei processi di governance, risk management e controllo dell'attività esaminata.

La comunicazione finale deve specificare i responsabili della risoluzione dei rilievi e la data prevista entro la quale le azioni dovrebbero essere completate.

Quando gli Internal Auditor vengono a conoscenza del fatto che il management ha avviato o completato azioni per affrontare un rilievo prima della comunicazione finale, ne deve essere data evidenza nella comunicazione.

La comunicazione finale deve essere accurata, obiettiva, chiara, concisa, costruttiva, completa e tempestiva, come descritto nello Standard "11.2 Comunicazione efficace".

Gli Internal Auditor devono garantire che la comunicazione finale sia esaminata e approvata dal CAE prima dell'emissione.

Il CAE deve diffondere la comunicazione finale ai destinatari che ne possono garantire la dovuta considerazione (si veda anche lo Standard "11.3 Comunicazione dei risultati").

Se l'incarico non è condotto in conformità con gli Standard, la comunicazione finale dell'incarico deve fornire i seguenti dettagli sulla non conformità:

- Standard per i quali non è stata raggiunta la conformità;
- motivo della non conformità;
- eventuali impatti della non conformità sui risultati e sulle conclusioni dell'incarico.

Indicazioni per l'implementazione

Nella comunicazione finale dell'incarico dovrebbe essere inclusa una dichiarazione che ne attesti la conduzione in conformità con i Global Internal Audit Standards. È lecito indicare che l'incarico di Internal Auditing è conforme agli Standard solo se l'affermazione è supportata dai risultati della supervisione e del programma di assurance e miglioramento della qualità.

Lo stile e il formato della comunicazione finale dell'incarico variano da un'organizzazione all'altra. Il CAE può definire modelli e procedure.

Possono essere emesse più versioni di comunicazione finale, con formati, contenuti e livello di dettaglio personalizzati per destinatari specifici, in base alla loro conoscenza dell'attività oggetto di audit, al modo in cui i rilievi e le conclusioni li influenzano e a come si prevede che utilizzino le informazioni.

Quando è presentata sotto forma di relazione, la comunicazione finale, oltre a quanto indicato nei requisiti, potrebbe riportare:

- titolo;
- contesto (breve sinossi dell'attività oggetto di audit);
- riconoscimenti (aspetti positivi e/o apprezzamento della cooperazione);
- lista di distribuzione.

La revisione della comunicazione finale dovrebbe verificare se:

- il lavoro svolto e documentato è stato coerente con gli obiettivi e l'ambito dell'incarico e con gli Standard (si vedano anche gli Standard "8.3 Qualità" e "12.1 Quality assessment interno");
- i risultati dell'incarico sono riportati chiaramente e supportati da informazioni pertinenti, affidabili e sufficienti (si veda anche lo Standard "14.1 Raccolta delle informazioni per l'analisi e la valutazione");
- sono stati rispettati i requisiti per la comunicazione con il management dell'attività oggetto di audit.

Il CAE determina come e a chi è distribuita la comunicazione finale dell'incarico. Le presentazioni in forma orale sono solitamente supportate da una copia digitale o stampata della presentazione e/o da una relazione scritta.

Esempi di conformità

- Comunicazioni finali scritte.
- Slide e/o note della riunione di presentazione quando la comunicazione finale è orale.
- Documentazione a supporto della revisione e dell'approvazione della comunicazione finale.
- Documentazione che dimostri il rispetto dei requisiti per la comunicazione con il management dell'attività oggetto di audit.

Standard 15.2 Conferma dell'attuazione delle raccomandazioni o piani d'azione

Requisiti

Gli Internal Auditor devono confermare l'implementazione delle raccomandazioni o piani d'azione da parte del management seguendo una metodologia definita, che preveda:

- la richiesta di informazioni sullo stato di avanzamento dell'implementazione;
- l'esecuzione di verifiche di follow-up secondo un approccio risk-based;
- l'aggiornamento dello stato delle azioni del management in un registro.

L'entità di queste procedure deve tenere conto della significatività dei rilievi.

Se il management non ha implementato le azioni entro le date stabilite, gli Internal Auditor devono ottenere e documentare una spiegazione dal management e discutere la questione con il CAE . Il CAE ha la responsabilità di determinare se il Top Management, per ritardo o mancata azione, abbia accettato un rischio che supera la risk tolerance (si veda anche lo Standard "11.5 Comunicazione dell'accettazione dei rischi").

Indicazioni per l'implementazione

Gli Internal Auditor potrebbero utilizzare un software, un foglio elettronico o un altro sistema per registrare l'avanzamento del piano d'azione da parte del management rispetto alle tempistiche stabilite. Un registro di questo tipo indica se le azioni rimangono aperte o sono scadute e fornisce uno strumento utile per gli Internal Auditor per comunicare con Board e Top Management. Inoltre, un programma o un sistema potrebbero permettere di digitalizzare l'intero flusso, dal risk assessment fino all'implementazione dell'azione correttiva. Ad esempio, potrebbero prevedere l'invio automatico di e-mail che notificano alle parti interessate l'avvicinarsi della data di implementazione delle azioni.

La metodologia per confermare l'implementazione dei piani d'azione a cura del management dovrebbe includere criteri per determinare quando effettuare le attività di follow-up per confermare che le azioni abbiano effettivamente risolto i rilievi. Le valutazioni di follow-up possono essere eseguite per una selezione delle azioni, a seconda della significatività del rischio. In alcuni casi, gli enti o organi di vigilanza possono richiedere di essere informati sui piani d'azione del management.

Se il management decide un piano di azioni alternativo e gli Internal Auditor concordano sul fatto che l'alternativa è soddisfacente o migliore dell'originale, l'avanzamento del piano alternativo dovrebbe essere monitorato fino all'implementazione.

Esempi di conformità

- Un sistema di monitoraggio aggiornato con regolarità (ad esempio, un foglio excel, un database o un altro strumento), che contiene i rilievi, le azioni correttive associate, lo stato d'avanzamento e la conferma dell'Internal Audit.
- Un report per il Board e il Top Management sullo stato di avanzamento delle azioni correttive.

Applicazione dei Global Internal Audit Standards nel Settore Pubblico

Sebbene i **Global Internal Audit Standards** si applichino a tutte le funzioni Internal Audit, gli Internal Auditor nel settore pubblico operano in un ambiente politico caratterizzato da strutture di governance, organizzative e di finanziamento che possono differire da quelle del settore privato. La natura di tali strutture e le relative condizioni possono essere influenzate dalla giurisdizione e dal livello di articolazione del settore pubblico in cui opera la funzione Internal Audit (nazionale, locale, ecc.). Inoltre, anche la terminologia utilizzata nel settore pubblico differisce da quella del settore privato. Tali diversità potrebbero influenzare il modo in cui le funzioni Internal Audit nel settore pubblico applicano gli Standard. Per tali ragioni, il quality assessment esterno di una funzione Internal Audit del settore pubblico dovrebbe essere effettuato da un team di valutazione che possegga le conoscenze sulle attività e le strutture di governance del settore pubblico (si veda anche lo Standard "8.4 Quality assessment esterno").

Il settore pubblico è istituito ed è governato da un quadro giuridico che include leggi, regolamenti, ordini e norme amministrative e altri tipi di requisiti governativi specifici per le giurisdizioni all'interno delle quali opera un'organizzazione. In tutti i Global Internal Audit Standards, il termine "leggi e/o regolamenti" viene utilizzato per rappresentare il quadro giuridico. Le leggi e/o i regolamenti possono stabilire il Mandato, la posizione organizzativa, le linee di riporto, l'ambito di copertura, le risorse finanziarie e altri requisiti della funzione Internal Audit.

Sulla base di tali indicazioni, le funzioni Internal Audit nel settore pubblico sono spesso chiamate a concentrare la propria attività nel:

- garantire la conformità a leggi e/o regolamenti;
- identificare le opportunità per migliorare l'efficienza, l'efficacia e l'economicità dei processi e dei programmi dell'amministrazione pubblica;
- determinare se le risorse pubbliche sono adeguatamente salvaguardate e utilizzate in modo appropriato per fornire servizi in base a principi di equità;
- valutare se le prestazioni di un'organizzazione sono in linea con le finalità e gli obiettivi strategici della stessa.

I paragrafi seguenti descrivono situazioni in cui l'applicazione degli Standard può differire per gli Internal Auditor che operano nel settore pubblico.

Leggi e/o regolamenti

Il CAE deve essere consapevole delle leggi e/o dei regolamenti che incidono sulla capacità della funzione Internal Audit di conformarsi pienamente a tutte le disposizioni degli Standard. Un Charter o altra documentazione può essere utilizzata per spiegare in che modo la funzione Internal Audit soddisfa i requisiti di leggi e/o regolamenti, così come le finalità degli Standard. Quando la conformità non è possibile, il CAE deve documentare il motivo, fornire informazioni appropriate e conformarsi a tutti gli altri requisiti degli Standard (si vedano anche gli Standard "4.1 Conformità ai Global Internal Audit Standards", "6.1 Mandato di Internal Audit", "6.2 Internal Audit Charter", "8.3 Qualità", "8.4 Quality assessment esterno", "12.1 Quality assessment interno" e "15.1 Comunicazione finale dell'incarico").

L'elenco seguente descrive situazioni in cui le leggi e/o i regolamenti possono influenzare la capacità delle funzioni Internal Audit nel settore pubblico di conformarsi agli Standard:

- quando le leggi e/o i regolamenti fungono da Mandato e Charter dell'Internal Audit, il CAE potrebbe non avere l'autorità o la capacità di apportare modifiche. Pertanto, il requisito di cui allo Standard "6.1 Mandato di Internal Audit" di riesaminare periodicamente il Mandato per aggiornamenti potrebbe non essere garantito. Tuttavia, il CAE potrebbe periodicamente condurre e documentare una revisione mirata del Mandato e del Charter per determinare che il percorso stabilito verso la conformità legale e/o normativa sia definito in modo accurato;
- le leggi e/o i regolamenti sulla divulgazione al pubblico possono disciplinare i tipi di documenti che devono essere resi pubblici e quelli che non possono essere resi pubblici. Le metodologie delle funzioni Internal Audit nel settore pubblico dovrebbero includere tali requisiti (si vedano anche gli Standard "5.1 Utilizzo delle informazioni" e "5.2 Protezione delle informazioni");
- le leggi e/o i regolamenti possono limitare il tipo di discussioni private che il CAE può avere con il Board (si vedano anche la definizione di "Board" del glossario, nonché gli Standard "6.3 Supporto dal Board e dal Top Management" e "7.1 Indipendenza organizzativa");
- le leggi e/o i regolamenti possono richiedere alle funzioni Internal Audit nel settore pubblico di presentare i risultati dell'Internal Audit in occasione di incontri pubblici. Le metodologie per la diffusione delle comunicazioni finali dovrebbero rispettare tali requisiti (si vedano anche gli Standard "11.2 Comunicazione efficace" e "15.1 Comunicazione finale dell'incarico");
- nel settore pubblico l'audit esterno è spesso previsto per legge. In alcune giurisdizioni, l'autorità di un'istituzione superiore di controllo (Corte dei conti) può sostituirsi a quella della funzione Internal Audit e le funzioni Internal Audit possono essere tenute a seguire la pianificazione come stabilito e a svolgere lavori congiunti. Nello Standard "11.1 Costruzione di relazioni e comunicazione con gli stakeholder", la funzione Internal Audit è tenuta a coordinarsi con il fornitore esterno di servizi e tale autorità può sostituire il ruolo di coordinamento (si vedano anche gli Standard "6.1 Mandato di Internal Audit" e "9.5 Coordinamento e reliance").

Gli Internal Auditor nel settore pubblico hanno molteplici stakeholder, tra cui la collettività all'interno della giurisdizione e i funzionari nominati ed eletti. La funzione Internal Audit può essere tenuta per legge a rendere conto del proprio operato e a essere trasparente nei confronti della collettività. Per servire adeguatamente i propri stakeholder, gli Internal Auditor possono prendere in considerazione il contributo del pubblico (collettività) durante la pianificazione e l'esecuzione dei servizi di Internal Audit. Un contributo può essere fornito dai fruitori dei servizi pubblici quali i servizi di utilità (gas, energia, gestione rifiuti, ecc.), i sistemi di trasporto pubblico, i parchi e le strutture ricreative, gli sportelli per l'edilizia e altri (si vedano anche gli Standard "9.4 Piano di Audit", "11.1 Costruzione di relazioni e comunicazione con gli stakeholder" e "13.2 Risk assessment dell'incarico").

Governance e struttura organizzativa

Le funzioni Internal Audit nel settore pubblico sono governate da un'ampia varietà di strutture. Alcune organizzazioni del settore pubblico possono essere soggette a più livelli di governance, sia all'interno che all'esterno dell'organizzazione, il che può complicare le relazioni di reporting del CAE, nonché la supervisione e il finanziamento della funzione.

I Global Internal Audit Standards fanno riferimento alle responsabilità relative al "Board" e al "Top Management". Il glossario definisce il "Board" utilizzando concetti che comprendono varie strutture di governance nel settore pubblico. Poiché il Board del settore pubblico può essere un organismo legislativo, potrebbe non avere autorità su aspetti del CAE e della funzione Internal Audit come descritto negli Standard. Ad esempio, tale organismo potrebbe non essere in grado di nominare, rimuovere o fissare una retribuzione per il CAE. In tali situazioni, il Board dovrebbe comunque fornire input al management in merito alle valutazioni delle performance e alle decisioni di nomina e revoca del CAE. In altre organizzazioni del settore pubblico, il termine "Top Management" può essere definito

in modo diverso rispetto agli Standard. Quando il termine è utilizzato per riferirsi alla gestione dell'attività oggetto di audit, devono essere implementate misure di salvaguardia dell'indipendenza per mitigare il rischio di interferenza con l'attività della funzione Internal Audit.

Il CAE dovrebbe evitare di ricevere direttive dai funzionari eletti senza prima consultare il Board e il Top Management, che sovrintendono direttamente alla funzione Internal Audit, a meno che tali funzionari non abbiano responsabilità dirette di supervisione.

Nell'elenco che segue sono riportati alcuni esempi che descrivono le strutture di governance e organizzative in cui le funzioni Internal Audit possono aver bisogno di adattare l'applicazione di alcuni Standard:

- le funzioni Internal Audit possono essere separate dalle altre parti dell'organizzazione e il CAE riferisce direttamente a un organo legislativo che funge da Board;
- le funzioni Internal Audit possono essere collocate al livello più alto dell'organizzazione governativa e il CAE riferisce direttamente al vertice dell'organizzazione;
- le funzioni Internal Audit possono essere collocate all'interno di un'altra componente dell'organizzazione complessiva (come un dipartimento o un'altra unità all'interno di un'organizzazione governativa) e il CAE riporta al capo dell'organizzazione o a un Board non esecutivo/di sorveglianza. Ciò può verificarsi quando esiste una struttura di governance a più livelli e quando è presente più di un organo di governo;
- le funzioni Internal Audit possono essere separate da altre parti dell'organizzazione perché il CAE è eletto e riconfermato dagli elettori all'interno di una giurisdizione e non riporta a nessuno specifico organo di supervisione o persona dell'organizzazione;
- le funzioni Internal Audit possono essere collocate più in basso nell'organizzazione e il CAE riferisce a un singolo Responsabile di quel dipartimento.

Sebbene alcune di queste situazioni non soddisfino i requisiti di indipendenza previsti dai Global Internal Audit Standards, l'istituzione di un Audit Committee composto da membri pubblici, indipendenti dal management, può salvaguardare l'indipendenza e fornire supervisione, consulenza e feedback continui (si vedano anche gli Standard "6.2 Internal Audit Charter" e "6.3 Supporto dal Board e dal Top Management", il Principio "7 Indipendente" e i relativi standard e lo Standard "8.1 Interazione con il Board").

Processi di assegnazione delle risorse umane, tecniche ed economiche

I processi di assegnazione delle risorse umane, tecniche ed economiche delle funzioni Internal Audit variano notevolmente nel settore pubblico. Alcune strutture organizzative e di governance non conferiscono al Board e al Top Management l'autorità sul budget. Tali limitazioni impediscono al CAE di essere in grado di chiedere l'approvazione del budget da parte del Board e del Top Management e condizionano la capacità di cercare o ottenere finanziamenti aggiuntivi a causa di altre priorità di finanziamento all'interno dell'organizzazione.

Ad esempio, alcune funzioni Internal Audit all'interno del settore pubblico possono presentare richieste di budget indipendenti al proprio Board o organo legislativo per l'approvazione. Altrove, i budget fanno parte di un budget organizzativo più ampio e l'assegnazione alla funzione Internal Audit è determinata dal capo dell'organizzazione e spesso approvata da un organo legislativo esterno. In entrambi i casi, il CAE potrebbe richiedere al Board di farsi promotore delle risorse necessarie.

Anche quando il budget è stabilito da leggi e/o regolamenti, il CAE deve rispettare altri requisiti degli Standard relativi alla gestione del budget (si vedano anche gli Standard "6.3 Supporto dal Board e dal Top Management", "7.1 Indipendenza organizzativa", "8.2 Risorse" e "10.1 Risorse finanziarie").

Le seguenti condizioni del settore pubblico possono limitare il modo in cui il CAE può utilizzare i fondi assegnati:

- la struttura di classificazione delle posizioni e/o i contratti di lavoro spesso stabiliscono fasce retributive per ciascuna categoria in base alle conoscenze, alle competenze e alle responsabilità della posizione, che limitano i CAE o il Board nello stabilire la retribuzione per ciascun dipendente. In tali situazioni, il CAE dovrebbe collaborare con la funzione risorse umane, come descritto nello Standard "10.2 Risorse umane";
- alla funzione Internal Audit può essere richiesto di utilizzare solo software approvati dall'organizzazione, il che può limitare la capacità del CAE di ottenere la tecnologia (necessaria) per supportare la funzione Internal Audit. Le funzioni Internal Audit nel settore pubblico dovrebbero coinvolgere i propri Board come sostenitori per supportare le loro esigenze tecnologiche e potrebbero dover utilizzare il software disponibile per realizzare il piano di Audit nel modo più efficiente possibile, mantenendo al contempo la conformità agli Standard (si veda anche lo Standard "10.3 Risorse tecnologiche");
- quando i limiti di finanziamento impediscono al CAE di ottenere risorse adeguate per condurre un quality assessment esterno, le funzioni Internal Audit nel settore pubblico possono trarre vantaggio dalla partecipazione a programmi paritetici per condurre tale assessment (si vedano anche gli Standard "8.4 Quality assessment esterno" e "10.1 Risorse finanziarie");
- quando è un'autorità esterna o un Organismo di Vigilanza a destinare il finanziamento per la funzione Internal Audit nel settore pubblico, il CAE può essere tenuto a fornire le comunicazioni finali dell'incarico all'autorità (si veda anche lo Standard "11.1 Costruzione di relazioni e comunicazione con gli stakeholder", "11.2 Comunicazione efficace" e "15.1 Comunicazione finale dell'incarico").

About The IIA

The Institute of Internal Auditors (IIA) is a nonprofit international professional association that serves more than 245,000 global members and has awarded more than 190,000 Certified Internal Auditor® (CIA®) certifications worldwide. Established in 1941, The IIA is recognized throughout the world as the internal audit profession's leader in standards, certifications, education, research, and technical guidance. For more information, visit theiia.org.

The Institute of
Internal Auditors

1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746 USA
theiia.org