

Allegato alla Delib.G.R. n. 31/16 del 13.10.2022

Linee di indirizzo per l'avvio e
l'espletamento della funzione di
Internal Auditing nel Sistema
Sanitario della Regione
Autonoma della Sardegna

**Mandato di Internal
Auditing ad ARES e a
tutti gli Enti del SSR**

Indice

Premessa	2
1. Standard di connotazione	3
1.1. Standard 1000 –Finalità, Poteri e Responsabilità.....	3
1.2. Standard 1100 - Indipendenza e Obiettività.....	4
1.3. Standard 1200 – Competenza e diligenza professionale	4
1.4. Standard 1230 – Aggiornamento Professionale Continuo	4
2. Standard di prestazione	5
2.1. Standard 2050 – Coordinamento e affidamento.....	5
2.2. Standard 2060 – Comunicazione alla Direzione.....	5
2.3. Standard 2100 – Natura dell’attività	5
2.4. Standard 2110 – Governance.....	6
2.5. Standard 2300 – Svolgimento dell’incarico.....	6
2.6. Standard 2330 – Documentazione delle informazioni.....	7
2.7. Standard 2400 – Comunicazione dei risultati	7
3. Competenze Attribuite alla struttura organizzativa di IA individuata da ARES.....	7
3.1. Standard 1000 –Finalità, Poteri e Responsabilità.....	7
4. Competenze Attribuite alle Funzioni di IA istituite presso le Aziende del SSR.....	8
4.1. Standard 1000 –Finalità, Poteri e Responsabilità.....	8
5. Relazioni con il Collegio Sindacale e l’OIIV	9
Allegato 1: Codice Etico	10
Allegato 2: Glossario.....	13

Premessa

Il presente documento recepisce l'introduzione della funzione di Internal Auditing (d'ora innanzi IA) nel Sistema Sanitario della Regione Sardegna (d'ora innanzi SSR) che, ex art. 3 della L.R. 24/2020, è stata attribuita ad ARES in maniera centralizzata al fine di omogeneizzare la gestione dei bilanci e la contabilità delle singole aziende. Tale documento ha pertanto lo scopo di progettare un sistema di IA su base regionale che rispetti gli standard di connotazione e di prestazione definiti dagli International Professional Practices Framework – IPPF nonché definire le finalità, i poteri, le responsabilità in capo alla struttura organizzativa di IA individuata da ARES, nonché le finalità, i poteri, le responsabilità attribuiti alla funzione di IA attivata presso tutte le Aziende del SSR, le relazioni che le legano e i rapporti con l'organo di indirizzo politico nonché le relazioni tra tale funzione e l'OIV/Collegio Sindacale e ogni altro organo aziendale di controllo.

Si precisa che la funzione di IA nelle aziende del SSR potrà, nel rispetto dell'autonomia organizzativa riconosciuta alle Aziende del SSR, coincidere o con una struttura organizzativa all'uopo destinata o con l'identificazione di uno o più referenti dell' IA, ma, qualunque sia l'articolazione organizzativa scelta dall'Azienda, si sottolinea che deve considerarsi imprescindibile il requisito che il personale assegnato a tale funzione venga dedicato in maniera esclusiva allo svolgimento della funzione di IA al fine di preservarne i requisiti di indipendenza e autonomia.

Il contenuto del presente documento è soggetto a periodiche valutazioni.

Eventuali variazioni dello stesso, a seguito ad esempio del mutamento del contesto organizzativo, dovranno essere autorizzate seguendo l'iter procedurale seguito per l'adozione dello stesso.

Il presente documento è da intendersi quale Mandato di IA: ossia un documento formale che definisce finalità, poteri e responsabilità dell'attività di IA, stabilendone la sua posizione all'interno dell'organizzazione del SSR, autorizzandone l'accesso ai dati, al personale e ai beni aziendali necessari per lo svolgimento dell'incarico e definendone l'ambito di copertura delle attività.

La funzione di IA, secondo la definizione dell'Institute of Internal Auditors - I.I.A, svolge *“un'attività indipendente e obiettiva di assurance e consulenza, finalizzata al miglioramento dell'efficacia e dell'efficienza dell'organizzazione. Assiste l'organizzazione nel perseguimento dei propri obiettivi tramite un approccio professionale sistematico, che genera valore aggiunto in quanto finalizzato a valutare e migliorare i processi di gestione dei rischi, di controllo e di governance”*.

L'intera attività si deve conformare ai principi e alle regole di condotta emanate a livello internazionale dall'Institute of Internal Auditors che rappresentano il cosiddetto International Professional Practices Framework (IPPF) e, in particolare, allo standard internazionale “Internal Control Integrated Framework: CoSO Report”.

L'auditor del SSR deve, inoltre, durante lo svolgimento delle sue mansioni, rispettare il codice di comportamento dei dipendenti pubblici.

Le presenti linee di indirizzo verranno diffuse con le seguenti modalità:

- pubblicazione sul sito della Regione Autonoma della Sardegna;
- pubblicazione sul sito di ARES e delle Aziende del SSR, nell'area “Amministrazione Trasparente, sezione Bilanci e sottosezione denominata PAC così come meglio definito di seguito: **Amministrazione Trasparente >> Bilanci >> Percorsi Attuativi della**

Certificabilità – PAC >> A) Aziende (Standard Organizzativi, Contabili e Procedurali -Requisiti Generali).

Le presenti linee di indirizzo entrano in vigore il giorno successivo alla data di approvazione della delibera di giunta regionale.

1. Standard di connotazione

1.1. Standard 1000 –Finalità, Poteri e Responsabilità

Il presente documento ha lo scopo di definire la finalità, i poteri e le responsabilità della funzione di IA presso tutti gli enti del Servizio Sanitario Regionale ex art. 2 della L.R. 24 del 2020:

- a) ARES: Azienda Regionale della Salute
- b) ASL: le 8 Aziende socio-sanitarie locali
- c) ARNAS: Azienda di rilievo nazionale ed alta specializzazione “G.Brotzu”
- d) AOU: Aziende Ospedaliere Universitarie di Cagliari e Sassari
- e) AREUS: Azienda Regionale dell'emergenza e urgenza della Sardegna
- f) IZS: Istituto zooprofilattico della Sardegna.

Il modello organizzativo della funzione di IA previsto per tutti gli enti di governo suindicati si articola come di seguito:

A) ARES (tramite una struttura organizzativa di IA individuata da ARES), che, nel rispetto di quanto contenuto nell'art. 3 lettera e) della L.R. 24/2020 e ss.mm.ii., deve “*curare l'omogeneizzazione della gestione dei bilanci e della contabilità delle singole aziende ivi compreso il sistema di internal auditing*”.

A tal scopo, ARES, mediante la sua struttura di IA, e in particolare per *curare* l'omogeneizzazione del sistema di IA del SSR, detterà linee guida minime a cui gli altri enti del SSR dovranno conformarsi, coordinerà e darà impulso alle attività di controllo interno e revisione interna e, tramite i suoi audit, proporrà, nell'ambito della sua attività consultiva, le linee di omogeneizzazione contabile del SSR.

Entro al fine dell'anno 2022 ARES dovrà adottare, mediante Delibera del Direttore Generale, un regolamento di IA per tutto il SSR, aggiornabile annualmente in sede di definizione del Piano Annuale di Audit, che definisca i livelli, le metodologie e gli strumenti di controllo nonché la ripartizione operativa dei compiti.

B) le Altre Aziende del SSR (tramite l'attivazione di una funzione che può coincidere o con una struttura organizzativa all'uopo destinata o con l'identificazione di uno o più referenti dell'IA, ma che deve essere comunque composta da personale esclusivamente dedicato allo svolgimento della funzione) dovranno conformarsi, nel rispetto del coordinamento funzionale attribuito ad ARES, alle indicazioni della struttura organizzativa di IA individuata da ARES come di seguito meglio precisato.

1.2. Standard 1100 - Indipendenza e Obiettività

L'attività di IA deve essere indipendente e gli Internal Auditor devono essere obiettivi nell'esecuzione del loro lavoro, pertanto la relativa Funzione, per svolgere il proprio compito, deve godere della necessaria autonomia e deve essere libera da condizionamenti quali potrebbero essere conflitti di interesse individuali, limitazioni del campo di azione, restrizioni nell'accesso a informazioni e rapporto di dipendenza gerarchica nei confronti degli auditati.

Al fine di garantire l'indipendenza dell'attività svolta:

- il personale dedicato alla funzione di IA presso le aziende del SSR redigerà in maniera diretta il piano di audit della propria azienda nel rispetto delle indicazioni del responsabile della struttura organizzativa di IA individuata da ARES, mentre non potrà svolgere gli interventi di audit nell'azienda a cui appartiene ma solo nelle altre aziende del SSR come da convocazione e organizzazione del gruppo di audit che il responsabile della struttura organizzativa di IA individuata da ARES formerà in maniera dettagliata e specifica per ogni intervento di audit programmato nell'ambito del Piano di Audit del SSR, deliberato dal Direttore Generale di ARES, frutto del consolidamento dei piani di audit delle singole aziende del SSR e degli specifici Obiettivi di Audit individuati da ARES.
- Inoltre il personale assegnato allo svolgimento della funzione di IA sia su ARES che sulle altre aziende del SSR potrà svolgere ruoli e responsabilità addizionali purché la Direzione Aziendale, nella fase di affidamento dei nuovi ruoli e responsabilità, adotti le misure compensative di tutela del requisito dell'indipendenza (es. la supervisione), atte a limitare e contenere ogni forma di condizionamento; si precisa comunque che risulta preferibile uno svolgimento del proprio incarico di IA in maniera esclusiva.

Gli Auditor inoltre devono avere un atteggiamento imparziale, senza pregiudizi e devono evitare qualsiasi forma di conflitto di interessi.

1.3. Standard 1200 – Competenza e diligenza professionale

L'attività di IA deve dotarsi delle conoscenze, capacità e altre competenze necessarie all'esercizio delle proprie responsabilità. A tal fine il personale impegnato nelle attività di IA è incoraggiato a dimostrare la propria competenza conseguendo le opportune certificazioni e qualifiche professionali.

Qualora sia ritenuto necessario il responsabile della struttura organizzativa di IA individuata da ARES, al fine di assicurare la massima professionalità e competenza in ogni ambito di intervento, farà presente alla Direzione Aziendale la necessità di avvalersi del supporto di esperti in specifiche materie, che integrino le conoscenze e competenze della funzione.

Tutto il personale dedicato alla funzione di IA applicherà la diligenza e la capacità professionale che ci si attende da un gruppo di IA ragionevolmente prudente e competente, precisando che diligenza professionale non implica infallibilità.

1.4. Standard 1230 – Aggiornamento Professionale Continuo

Le risorse dedicate alla funzione ricevono un programma di formazione professionale continuo ed aggiornato, finalizzato a soddisfare i requisiti previsti per la pratica professionale e migliorare le capacità, le conoscenze e le competenze necessarie all'espletamento delle attività.

Il responsabile della struttura organizzativa di IA individuata da ARES, programma, coordina e predispone il piano di formazione sia per la struttura organizzativa di IA individuata da ARES sia per la funzione di IA attivata nelle Aziende del SSR, oltre a partecipare a specifici corsi di formazione e/o aggiornamento.

La formazione dovrà comprendere anche la presentazione dell'attività di IA a tutte le funzioni di tutte le Aziende del SSR al fine di diffonderne la cultura e acquisirne il necessario consenso con l'obiettivo ultimo di orientare tutta l'organizzazione del SSR verso il miglioramento continuo.

2. Standard di prestazione

2.1. Standard 2050 – Coordinamento e affidamento

Il personale in servizio dedicato alla funzione di IA presso le aziende del SSR formerà un gruppo di auditing su base regionale che, su richiesta e sotto l'organizzazione del responsabile della struttura organizzativa di IA individuata da ARES, verrà coinvolto negli interventi di audit presso le altre aziende del SSR, secondo il piano di audit annuale predisposto e approvato dal Direttore Generale di ARES e condiviso con i Direttori Generali delle altre aziende del SSR, come da art. 4 comma 8 della LR 24/2020¹.

2.2. Standard 2060 – Comunicazione alla Direzione

Il responsabile della struttura organizzativa di IA individuata da ARES riferisce al Direttore Amministrativo ogni sei mesi sullo stato di avanzamento dei lavori svolti. Inoltre, alla fine di ogni anno, entro il 30 novembre, il responsabile della struttura organizzativa di IA individuata da ARES relaziona sui risultati dell'attività svolta alla Direzione Aziendale di ARES che ne trasmette le risultanze all'Assessorato dell'Igiene e Sanità e dell'Assistenza Sociale e contestualmente presenta il Piano di Audit per l'anno successivo.

I referenti delle funzioni di IA presenti nelle aziende del SSR riferiscono sullo stato di avanzamento dei lavori svolti, con cadenza semestrale, al Direttore Amministrativo e al responsabile della struttura organizzativa di IA individuata da ARES. Inoltre, alla fine di ogni anno, entro il 30 ottobre, relazionano sui risultati dell'attività svolta al Direttore Generale, che contestualmente, ossia entro il 30 ottobre, delibera il Piano di Audit per l'anno successivo.

2.3. Standard 2100 – Natura dell'attività

L'attività di IA deve valutare e contribuire al miglioramento dei processi di *governance*, gestione del rischio e controllo dell'organizzazione, tramite un approccio sistematico, rigoroso e *risk based*. La credibilità e il valore dell'IA sono rafforzati quando gli auditor agiscono in maniera proattiva e le loro valutazioni offrono nuove riflessioni e tengono in considerazione gli impatti futuri.

¹Si veda l'art. 4 comma 8 LR 24/2020: "il direttore generale dell'ARES al fine di favorire l'espletamento delle funzioni dell'ARES ed il perseguimento di un'azione omogenea e coordinata tra le aziende di cui all'articolo 2 convoca e presiede il coordinamento dei direttori generali delle medesime"

2.4. Standard 2110 – Governance

La funzione di IA, quale funzione di *assurance* e di consulenza, svolge servizi ad elevato valore aggiunto, quali:

- la mappatura dei processi aziendali, con una codifica comune a tutti gli enti del SSR;
- la promozione in azienda della cultura del processo, dei rischi e dei controlli;
- il supporto per una corretta valutazione dei rischi inerenti e dei rischi residui correlati ai processi aziendali e associati alle strategie aziendali;
- la collaborazione con i responsabili aziendali ai vari livelli, finalizzata alla comprensione e all'analisi dei vari processi secondo un approccio *risk-based* e delle attività necessarie per la mitigazione dei rischi;
- lo sviluppo e l'esecuzione di un piano di Audit basato sull'analisi dei rischi;
- la gestione degli interventi di Audit previsti nel succitato Piano di Audit;
- la generazione di valore aggiunto.

La funzione di IA assume funzioni di supporto alla Direzione Aziendale e ai vari Dirigenti, con responsabilità limitate al controllo e alla valutazione del sistema del controllo interno e, in generale, dei rischi relativi alle attività poste in essere dall'azienda nell'ottica di prevenire eventuali fatti pregiudizievoli rispetto al raggiungimento degli obiettivi istituzionali, col fine di governare i rischi piuttosto che subirli. Si precisa pertanto che la funzione di IA non ha alcuna responsabilità decisionale o autorizzativa.

Qualora, nel corso dell'attività di audit emergano fatti che possano dar luogo a ipotesi di responsabilità civile, penale o amministrativa, il responsabile e i referenti della Funzione di IA sono tenuti ad informare immediatamente il Direttore Generale dell'Azienda di appartenenza, quale rappresentante legale dell'Azienda per l'avvio di eventuali azioni di responsabilità e/o di denuncia qualora gli elementi raccolti siano concreti e attuali o per operare affinché il danno sia evitato.

2.5. Standard 2300 – Svolgimento dell'incarico

La funzione di IA deve raccogliere, analizzare, valutare e documentare informazioni sufficienti al raggiungimento degli obiettivi dell'incarico del responsabile della struttura organizzativa di IA individuata da ARES e dei referenti delle funzioni di IA presenti nelle aziende del SSR.

In particolare il processo di IA si compone di una sequenza coordinata di attività finalizzata ad assistere la Direzione Aziendale nell'attività di conseguimento degli obiettivi programmati e articolato nelle seguenti attività:

- pianificazione dell'incarico del responsabile e/o del referente della funzione di IA
- svolgimento dell'incarico del responsabile e/o del referente della funzione di IA
- comunicazione dei risultati del responsabile e/o del referente della funzione di IA
- monitoraggio delle azioni correttive del responsabile e/o del referente della funzione di IA

La funzione svolge un controllo di terzo livello presidiando i controlli di secondo livello già presenti in azienda e quelli di primo livello attuati direttamente dai responsabili delle strutture.

2.6. Standard 2330 – Documentazione delle informazioni

Per lo svolgimento delle proprie attività la struttura organizzativa di IA individuata da ARES e le Funzioni Aziendali di IA istituite presso le Aziende del SSR si doteranno di opportuni strumenti (*Work Model*), comuni a tutte le Aziende del SSR, che verranno identificati e approvati attraverso specifici provvedimenti del responsabile della struttura organizzativa di IA individuata da ARES.

La struttura organizzativa di IA individuata da ARES e le Funzioni di IA attivate presso le Aziende del SSR devono avere a disposizione e utilizzare idonei strumenti informatici di supporto allo svolgimento delle attività previste nel processo di IA, ivi compreso l'accesso a tutti i moduli del Sistema Amministrativo Contabile in uso (SiSar-AMC), nonché la possibilità di avere un sistema di archiviazione di tutta la documentazione, con particolare riferimento alla necessità di dotare tutte le aziende del SSR di un'area cloud², necessaria per conservare e monitorare lo stato di avanzamento delle attività.

2.7. Standard 2400 – Comunicazione dei risultati

La comunicazione finale dei risultati, ivi compresi gli obiettivi, l'ambito di copertura e i risultati dell'incarico devono essere formalizzati e opportunamente comunicati alle rispettive Direzioni Aziendali e al responsabile della struttura organizzativa di IA individuata da ARES, che a sua volta riferirà all'Assessorato dell'Igiene e Sanità e dell'Assistenza Sociale.

3. Competenze Attribuite alla struttura organizzativa di IA individuata da ARES

3.1. Standard 1000 – Finalità, Poteri e Responsabilità

Nel dettaglio delle finalità, poteri e responsabilità attribuite alla struttura organizzativa di IA individuata da ARES si specifica che le attività che tale struttura dovrà svolgere sono le seguenti:

- predisporre un piano basato sulla valutazione dei rischi al fine di determinare le priorità dell'attività di IA in linea con gli obiettivi dell'ARES ma soprattutto dell'intero SSR (mediante consolidamento dei singoli piani di audit approvati e l'indicazione di specifici obiettivi individuati da ARES) che deve essere sottoposto, dal responsabile della struttura, all'esame e all'approvazione della Direzione Generale di ARES; a tale fine, annualmente, la funzione di IA svolge un'attività di *risk assessment*, propedeutica al piano, coinvolgendo sia il Direttore Amministrativo che il Direttore Sanitario di ARES;
- gestire in maniera efficiente ed efficace l'attività di IA al fine di assicurare che la stessa aggiunga valore all'organizzazione dell'Azienda e del SSR;
- definire le direttive, le procedure, le metodologie e gli strumenti (*work model* e supporti informatici) volti a guidare l'attività di IA sia in ARES che nelle Aziende del SSR;

² tecnologia che permette di elaborare e archiviare dati in rete. In altre parole, attraverso internet il cloud consente l'accesso ad applicazioni e dati memorizzati su un hardware remoto invece che sulla workstation locale.

- valutazione e contributo al miglioramento dei processi di *governance*, gestione del rischio e controllo dell'organizzazione presso ARES tramite un approccio sistematico, rigoroso e *risk based* sulla base di quanto stabilito nel piano di Audit approvato;
- raccolta, analisi, valutazione e documentazione delle informazioni sufficienti, affidabili, pertinenti e utili al fine di conseguire gli obiettivi dell'incarico;
- comunicazione periodica alla Direzione Aziendale in merito allo stato di avanzamento del piano e ogni altra questione che necessita di essere sottoposta all'attenzione della Direzione Aziendale;
- definizione e mantenimento di un sistema di monitoraggio delle azioni intraprese a seguito dei risultati segnalati alla Direzione Aziendale;
- coordinamento e supporto alle Funzioni di IA Aziendali nella valutazione dei processi di *governance*, gestione del rischio e controllo dell'organizzazione;
- coordinamento delle attività svolte dalle Funzioni di IA Aziendali al fine di garantire che gli obiettivi siano raggiunti e che la qualità sia assicurata;
- definizione dei criteri di conservazione e archiviazione della documentazione dell'incarico;
- comunicazione dei risultati dell'incarico alla Direzione Aziendale che la trasmette all'Assessorato dell'Igiene e Sanità e dell'Assistenza Sociale.
- programmazione e coordinamento del piano di formazione previsto per la struttura organizzativa di IA individuata da ARES e per le funzioni di IA delle Aziende del SSR;
- partecipazione a specifici corsi di formazione e/o aggiornamento.

4. Competenze Attribuite alle Funzioni di IA istituite presso le Aziende del SSR

4.1. Standard 1000 –Finalità, Poteri e Responsabilità

La Funzioni Aziendali di IA istituite presso le Aziende del SSR svolgeranno la propria attività sotto la direzione della propria Direzione Amministrativa, alla quale dovranno relazionare e rispondere per le proprie attività e sotto il coordinamento funzionale della struttura organizzativa di IA individuata da ARES alla quale devono relazionare circa le attività svolte.

Alla funzione di IA delle Aziende del SSR competono le seguenti attività:

- Predisposizione, entro il 30 ottobre di ogni anno, di un piano conforme alle strategie e agli obiettivi definiti dalla struttura organizzativa di IA individuata da ARES e definito sulla base della valutazione dei rischi aziendali. Il piano deve essere predisposto nel rispetto delle direttive, procedure, metodologie e gli strumenti definiti dalla struttura organizzativa di IA individuata da ARES, volti a guidare l'attività stessa, verso il miglioramento continuo di tutto il SSR. Il piano deve essere preliminarmente sottoposto al parere di conformità della struttura organizzativa di IA individuata da ARES entro il 30 settembre seguendo il seguente iter. La struttura organizzativa di IA individuata da ARES, entro 10 giorni dalla sua trasmissione, dovrà segnalare eventuali correzioni e/o integrazioni a cui conformarsi, decorso inutilmente tale termine il parere di conformità si dà per rilasciato. La funzione di IA attivata presso le Aziende del SSR, dovrà conformarsi alle indicazioni e ai tempi dettati dalla struttura organizzativa di IA individuata da ARES ritrasmettendo il Piano adeguato

alle suddette indicazioni, da tale momento decoreranno ulteriori 5 giorni per il rilascio del parere di conformità, che nel caso di silenzio della struttura organizzativa di IA individuata da ARES, varrà come silenzio-rilascio del parere di conformità.

Il Piano viene sottoposto di all'esame e all'approvazione della Direzione Generale dell'azienda di riferimento che lo adotterà entro il 30 ottobre con Delibera del Direttore generale, da trasmettere entro il 10 novembre alla struttura organizzativa di IA individuata da ARES;

- gestione efficace dell'attività di IA al fine di assicurare che la stessa aggiunga valore all'organizzazione dell'Azienda e del SSR;
- valutazione e contributo al miglioramento dei processi di *governance*, gestione del rischio e controllo dell'organizzazione presso l'Azienda tramite un approccio sistematico, rigoroso e *risk based* sulla base di quanto stabilito nel piano suddetto;
- raccolta, analisi, valutazione e documentazione delle informazioni sufficienti e utili al fine di conseguire gli obiettivi dell'incarico;
- comunicazione periodica alla Direzione Aziendale dell'azienda alla quale la funzione afferisce e alla struttura organizzativa di IA individuata da ARES in merito allo stato di avanzamento del piano comprensiva dei rischi significativi, dei problemi di controllo e *governance* e ogni altra questione che necessita di essere sottoposta all'attenzione della Direzione Aziendale e alla struttura organizzativa di IA individuata da ARES;
- definizione e mantenimento di un sistema di monitoraggio delle azioni intraprese a seguito dei risultati segnalati alla Direzione Aziendale e alla struttura organizzativa di IA individuata da ARES;
- conservazione della documentazione dell'incarico sulla base dei criteri definiti dalla struttura organizzativa di IA individuata da ARES;
- supporto alla struttura organizzativa di IA individuata da ARES nell'espletamento di attività pianificate nell'ambito di altre aziende sanitarie, consistente per lo più nel rendere disponibile il personale dedicato alla funzione a svolgere gli interventi di audit presso le altre aziende del SSR al fine di preservarne l'indipendenza e l'obiettività;
- partecipazione a specifici corsi di formazione e/o aggiornamento definiti e individuati nel piano di formazione predisposto dalla struttura organizzativa di IA individuata da ARES.

5. Relazioni con il Collegio Sindacale e l'OIV

Il Collegio Sindacale, l'Organismo Indipendente di Valutazione (OIV) e ogni altro Organo di Controllo possono ottenere dalla struttura organizzativa di IA individuata da ARES e dalle funzioni aziendali di IA istituite presso le Aziende del SSR informazioni e comunicazioni formali sull'andamento e sui risultati delle attività svolte.

Allegato 1: Codice Etico

Scopo del Codice Etico dell'Institute of Internal Auditors è di promuovere la cultura etica nell'esercizio della professione di internal auditing.

L'internal auditing è un'attività indipendente ed obiettiva di assurance e consulenza, finalizzata al miglioramento dell'efficacia e dell'efficienza dell'organizzazione.

Assiste l'organizzazione nel perseguimento dei propri obiettivi tramite un approccio professionale sistematico, che genera valore aggiunto in quanto finalizzato a valutare e migliorare i processi di gestione dei rischi, di controllo e di governance.

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

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

- 1) I Principi, fondamentali per la professione e la pratica dell'internal auditing.
- 2) Le Regole di condotta, che descrivono le norme comportamentali che gli internal auditor sono tenuti a osservare. Queste regole sono un aiuto per orientare l'applicazione pratica dei Principi e intendono fornire agli internal auditor una guida di comportamento professionale.

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

Applicabilità e attuazione

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

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

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

Principi

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

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

2) Obiettività - Nel raccogliere, valutare e comunicare le informazioni attinenti l'attività o il processo in esame, l'internal auditor deve manifestare il massimo livello di obiettività professionale. L'internal auditor deve valutare in modo equilibrato tutti i fatti rilevanti, senza venire indebitamente influenzato da altre persone o da interessi personali nella formulazione dei propri giudizi.

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

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

Regole di condotta

1) Integrità - L'internal auditor:

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

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

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

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

2) Obiettività - L'internal auditor:

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

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

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

3) Riservatezza - L'internal auditor:

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

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

4) Competenza - L'internal auditor:

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

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

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

Allegato 2: Glossario

Valore aggiunto

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

Adeguato controllo

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

Servizi di assurance

Consistono in un esame obiettivo delle evidenze allo scopo di ottenere una valutazione indipendente dei processi di governance, di gestione del rischio e di controllo dell'organizzazione. Tra gli esempi si possono citare incarichi di tipo finanziario, di tipo operativo, di conformità, di sicurezza informatica e di due diligence.

Board

Il massimo organo di governo (per esempio consiglio di amministrazione, consiglio di sorveglianza, consiglio dei governatori o dei trustee) che ha la responsabilità di indirizzare e/o di supervisionare le attività dell'organizzazione e di chiederne conto al senior management.

Sebbene le regole di governance possano variare tra le diverse giurisdizioni e i vari settori, generalmente il board comprende membri che non fanno parte del management. Laddove non esista un board, il termine "board" negli Standard fa riferimento ad un gruppo di soggetti o alla persona incaricata della governance dell'organizzazione. Inoltre, il termine "board" negli Standard può riferirsi a un comitato o altro organo al quale l'organo di governo ha delegato determinate funzioni (ad esempio, un comitato di audit, un comitato controllo e rischi...)

Mandato

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

Responsabile internal auditing (CAE - Chief Audit Executive)

Il responsabile internal auditing è la persona con ruolo direttivo che ha la responsabilità di gestire in modo efficace l'attività di internal audit, in conformità al Mandato di internal audit e agli elementi vincolanti dell'International Professional Practices Framework. Il responsabile internal auditing o i collaboratori che riportano al responsabile internal auditing sono in possesso delle opportune qualifiche e certificazioni professionali. La designazione specifica della posizione (Job Title) e/o le responsabilità specifiche del responsabile internal auditing possono variare nelle diverse organizzazioni.

Codice Etico

Il Codice Etico dell'Institute of Internal Auditors (IIA) è composto dai Principi fondamentali per la professione e la pratica dell'internal auditing e dalle Regole di condotta che descrivono le norme comportamentali che gli auditor sono tenuti a osservare. Il Codice Etico si applica sia ai singoli Standard internazionali per la pratica professionale dell'internal auditing (Standard) individui sia agli enti che forniscono servizi di internal audit. Scopo del Codice Etico è quello di promuovere una cultura etica in tutti gli ambiti della professione di internal auditor.

Conformità

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

Conflitto di interessi

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

Servizi di consulenza

Servizi di supporto e assistenza al cliente, la cui natura ed estensione vengono concordate con il cliente, tesi a fornire valore aggiunto e a migliorare i processi di governance, gestione del rischio e controllo di un'organizzazione, senza che l'internal auditor assuma responsabilità manageriali a riguardo. Tra i possibili esempi figurano consulenza, assistenza specialistica, facilitazione e formazione.

Controllo

Qualsiasi azione intrapresa dal management, dal board o da altri soggetti per gestire i rischi e aumentare le possibilità di conseguimento degli obiettivi e dei traguardi stabiliti. Il management pianifica, organizza e dirige l'esecuzione di iniziative in grado di fornire una ragionevole sicurezza sul raggiungimento di obiettivi e traguardi.

Ambiente di controllo

Atteggiamento e azioni del board e del management rispetto all'importanza del controllo all'interno dell'organizzazione. L'ambiente di controllo fornisce la disciplina e l'organizzazione per il raggiungimento degli obiettivi primari del sistema di controllo interno. Gli elementi costitutivi dell'ambiente di controllo sono i seguenti:

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

Processi di controllo

Le politiche, le procedure (manuali e automatizzate) e le attività che fanno parte di un modello di controllo, progettato e gestito per assicurare che i rischi siano contenuti entro il livello che l'organizzazione è disposta a sostenere.

Principi fondamentali per la pratica professionale dell'internal auditing

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

Incarico

La specifica assegnazione di un audit, compito o attività di verifica, siano essi un incarico di internal audit, un'autovalutazione dei controlli, un'investigazione per frode o una consulenza. Un incarico può includere più compiti o attività, concepiti per raggiungere un insieme specifico di obiettivi interrelati.

Obiettivi dell'incarico

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

Giudizio dell'incarico

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

Programma di lavoro dell'incarico

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

Prestatore esterno di servizi

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

Frode

Qualsiasi atto illegale caratterizzato da falsità, dissimulazione o abuso di fiducia. Tali atti non sono legati a minacce di ricorso alla violenza o alla forza fisica. Le frodi sono perpetrate da persone e organizzazioni per ottenere denaro, beni o servizi, per evitare il pagamento o la perdita di servizi o per procurarsi vantaggi personali o commerciali.

Governance

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

Condizionamenti

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

Indipendenza

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

Controlli IT (Information Technology)

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

Governance dei sistemi informativi

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

Attività di internal audit

Reparto, divisione, team di consulenti o altri professionisti che forniscono servizi indipendenti e obiettivi di assurance e di consulenza, concepiti per aggiungere valore e migliorare l'operatività di un'organizzazione. L'attività di internal audit assiste un'organizzazione nel perseguimento dei suoi obiettivi, tramite un approccio professionale sistematico finalizzato a valutare e migliorare l'efficacia dei processi di governance, di gestione dei rischi e di controllo.

International Professional Practices Framework

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

Deve (devono)

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

Obiettività

L'attitudine mentale di imparzialità che consente agli internal auditor di svolgere gli incarichi in un modo che consenta loro di credere nella validità del lavoro svolto e nell'assenza di compromessi sulla qualità. In materia di audit, l'obiettività richiede che gli internal auditor non subordinino il loro giudizio a quello di altri.

Giudizio complessivo

Valutazione, conclusione e/o altra descrizione dei risultati presentata dal responsabile internal auditing che verte, in termini generali, sui processi di governance, di gestione dei rischi e/o di controllo

dell'organizzazione. Per giudizio complessivo si intende il giudizio professionale del responsabile internal auditing, basato sui risultati di una serie di incarichi individuali e di altre attività per un determinato periodo di tempo.

Rischio

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

Livello di accettazione del rischio

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

Gestione del rischio

Processo teso a identificare, valutare, gestire e controllare possibili eventi o situazioni negativi, al fine di fornire una ragionevole assicurazione in merito al raggiungimento degli obiettivi dell'organizzazione.

Dovrebbe (dovrebbero)

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

Significatività

Importanza relativa di un fatto, nel contesto nel quale è considerato. Include elementi quantitativi e qualitativi quali la grandezza, la natura, le conseguenze, la rilevanza e l'impatto.

Agli internal auditor è richiesto un giudizio professionale quando valutano la significatività dei fatti nel contesto degli obiettivi specifici.

Standard

Enunciato professionale emanato dall'International Internal Audit Standards Board che definisce i requisiti per lo svolgimento di una vasta gamma di attività di internal audit e per la valutazione delle prestazioni dell'internal audit.

Strumenti informatici di supporto all'audit

Strumenti di audit automatizzati, quali software generici di audit, generatori di dati di test, programmi informatici di audit e computer-assisted audit techniques (CAAT)