



**Regione Siciliana**  
**Azienda Sanitaria Provinciale di**  
**AGRIGENTO**

**DELIBERAZIONE DIRETTORE GENERALE N. 292 DEL 03.03.2017**

OGGETTO: Adozione Regolamento di Internal Auditing

U.O. PROPONENTE: U.O. INTERNAL AUDIT	
PROPOSTA N. 289 DEL 22/02/2017	
IL RESPONSABILE del PROCEDIMENTO Dott. Salvatore Montante <i>[Signature]</i>	IL RESPONSABILE UOS Controllo di Gestione Dott. F. Adriano Craco <i>[Signature]</i>

<b>VISTO CONTABILE</b>	
Si attesta la copertura finanziaria:	
<input type="checkbox"/> come da prospetto allegato ( ALL. N. _____ ) che è parte integrante della presente delibera.	
<input type="checkbox"/> Autorizzazione n. _____ con comporta ordine di spesa del _____	<input type="checkbox"/> C.E. / <input type="checkbox"/> C.P.
IL RESPONSABILE del PROCEDIMENTO <i>[Signature]</i> S.E.F.P. L'ADDETTO RESPONSABILE Coll. Amm. GLORIA	IL DIRETTORE UOC SEF e P. IL DIRETTORE U. O. C. SERVIZIO ECONOMICO FINANZIARIO e PATRIMONIALE Dr. BEATRICE SALVAGO <i>[Signature]</i>

RICEVUTA DALL'UFFICIO ATTI DELIBERATIVI IN DATA \_\_\_\_\_

L'anno duemiladiciassette il giorno TRE del mese di MARZO  
 nella sede dell'Azienda Sanitaria Provinciale di Agrigento

**IL DIRETTORE GENERALE**

Dott. Salvatore Lucio Ficarra, giusta D.P.R.S. n. 197/serv.1/S.G. del 24/06/2014, coadiuvato dal  
 Direttore Amministrativo Dott. Salvatore Lombardo e dal Direttore Sanitario  
 Dott. Silvio Lo Bosco con l'assistenza del Segretario verbalizzante  
 \_\_\_\_\_  
 Il Direttore Generale Amministrativo Prof. Dr.  
 Salvatore Lombardo

**VISTO** lo statuto della Regione;

**VISTO** il Decreto Legislativo 30 dicembre 1992 n.502, nel testo modificato con il decreto legislativo 7 dicembre 1993 n.517 e s.m.i.;

**VISTA** la L. R. n. 5/2009 di riordino del Servizio sanitario Regionale e s.m.i.;

**VISTO** l'Atto Aziendale di questa ASP, approvato con D.A. n. 220 del 12/02/2016 ed adottato con la Delibera n. 398 del 29/03/2016;

**PREMESSO** che con l'art.1, comma 291, della legge 23/12/2005 n.266, sono stati definiti i criteri e le modalità di certificazione dei bilanci delle aziende sanitarie locali, delle aziende ospedaliere, degli istituti di ricovero e cura, degli istituti zooprofilattici sperimentali e delle aziende ospedaliere universitarie;

**CONSIDERATO** che l'art.11 del nuovo Patto per la Salute 2010-2012 prevede che le regioni le province autonome si impegnino ad avviare le procedure per perseguire la certificabilità dei bilanci, attraverso un processo che dovrà garantire l'accertamento della qualità delle procedure amministrativo-contabile sottostanti alla corretta contabilizzazione dei fatti aziendali, nonché la qualità dei dati contabili;

**VISTO** il Decreto Legislativo 23 giugno 2011 n.118 e s.m.i. recante " Disposizioni in materia di armonizzazione dei sistemi contabili e degli schemi di bilancio delle Regioni, degli enti locali e dei loro organismi, a norma degli articoli 1 e 2 della legge 5 maggio 2009 n.42" ed in particolare il Titolo II recante " Principi contabili generali e applicati per il settore sanitario" nell'ambito del quale è disciplinata, fra l'altro, l'implementazione e la tenuta della contabilità del tipo economico-patrimoniale, nonché l'obbligo di redazione del bilancio di esercizio della gestione sanitaria accentrata e del bilancio sanitario consolidato regionale;

**VISTO** le disposizioni normative in merito ai controlli interni alle Pubbliche Amministrazioni contenute nel Decreto Legislativo n.286/1999 "Riordino e potenziamento dei meccanismi e strumenti di monitoraggio e valutazione dei costi, dei rendimenti e dei risultati dall'attività svolta dalle amministrazioni pubbliche, a norma dell'art.11 della Legge 15 marzo 1997 n.59 e nel Decreto Legislativo n.150/2009 "Attuazione della Legge 4 marzo 2009 n.15 in materia di ottimizzazione della produttività del lavoro pubblico e di efficienza e trasparenza delle pubbliche amministrazioni";

**VISTA** altresì la nota ass.le prot. n.65013 del 02/08/2016, con la quale l'Assessorato della Salute ha fornito chiarimenti ed indicazioni in merito a funzioni e ruolo dell'Internal Audit;

**CONSIDERATO** che con disposizione di servizio n.99025 del 1/06/2016, ratificata con delibera n.1688 del 29/11/2016 è stato individuato l'Internal Audit nella persona del Dr. Salvatore Montante;

**RITENUTO** che occorre procedere ad adottare apposito regolamento che disciplini la funzione di Internal Audit;



**Regione Siciliana**

**Azienda Sanitaria Provinciale di Agrigento**

**REGOLAMENTO DI INTERNAL AUDITING**



## INDICE

1. Introduzione	pag.3
2. Scopo ed oggetto	pag.3
3. Campo di applicazione	pag.4
4. Organizzazione, responsabilità e compiti:	
4.1 Assetto organizzativo della funzione di Internal Auditing	pag.4
4.2 Compiti della funzione di Internal Auditing	pag.4
5. Principi etici, regole di condotta e standard internazionali	
5.1 Principi Etici	pag.5
5.2 Segnalazione di eventuale danno erariale	pag.5
5.3 Segnalazione di eventuale denuncia penale	pag.5
6. Il processo di Internal Auditing	
6.1 Il ciclo di audit	pag.6
6.2 Identificazione delle aree critiche	pag.6
6.2.1 Identificazione dei rischi	pag.6
6.2.2 Risk assessment	pag.7
6.3 Stesura del Piano di Audit	pag.9
6.4 Interventi di Audit	
6.4.1 Pianificazione e comunicazione dell'intervento di audit	pag.9
6.4.2 Programmazione operativa dell'intervento di audit	pag.10
6.4.3 Riunione di apertura	pag.10
6.4.4 Conduzione dell'audit	pag.10
6.4.5 Rapporti di audit	pag.11
7. Follow-up	pag.12
8. Archiviazione della documentazione di audit	pag.12
Allegato 1 Codice Etico – Institute of Internal Auditors	pag.13
Allegato 2 Standard Internazionali di Internal Audit	pag.17



## REGOLAMENTO DI INTERNAL AUDITING

### 1. Introduzione

L'Internal Auditing è una funzione di controllo indipendente preposta alla verifica dell'adeguatezza dei sistemi di controllo aziendali.

L'Internal Auditing (I.A.) svolge un controllo di terzo livello presidiando i controlli di secondo livello svolti dalle altre funzioni aziendali (Controllo di Gestione, Risk management, Qualità, Anticorruzione, ecc.) e quelli di primo livello attuati dai dirigenti responsabili dei processi aziendali.

E' una funzione che ha come fine ultimo la corretta corporate governance aziendale, a patto che sia intesa e riconosciuta come una funzione di management (approccio valutativo) e non come una funzione di tipo ispettivo-vigilanza che si aggiunge a quelle già esistenti, anestetizzando gli slanci organizzativi e scatenando la corsa all'elusione dei controlli stessi (approccio ispettivo). Esiste quindi un equilibrio tra gli obiettivi che l'Azienda si dà, i rischi possono minare il raggiungimento degli obiettivi stessi ed i controlli chiamati a presidiare il rispetto delle procedure attivate in relazione ai vari rischi. Quanto i controlli non sono legati ai rischi e quindi agli obiettivi, ossia quando sono troppi e fini a se stessi, si scivola nella burocrazia. Se i controlli, invece, sono molto limitati rispetto ai rischi da presidiare si rischia l'inefficienza organizzativa-gestionale. Una visione moderna dell'Internal Auditing è certamente quella legata al presidio dei controlli ma con un'attenzione precisa rivolta alle esigenze aziendali e non solo al rigido formalismo normativo, occorre un approccio di tipo flessibile che consenta di tenere alta la guardia e non sottovalutare i potenziali rischi che non sono stati ancora individuati e dei quali non si conoscono né gli elementi scatenanti né le possibili conseguenze.

### 2. Scopo ed Oggetto

Lo scopo della funzione di I.A. è quello di supportare l'organizzazione nel perseguimento dei propri obiettivi attraverso un approccio sistematico volto ad identificare, monitorare e migliorare il sistema di gestione dei rischi.

Il presente Regolamento descrive i principi, le procedure, le metodologie, le fasi e gli strumenti di lavoro utilizzati dalla funzione di I.A. dell'Azienda Sanitaria Provinciale di Agrigento nell'attività di auditing dei processi operativi aziendali.

Il presente Regolamento è adottato con Deliberazione del Direttore Generale e potrà essere soggetto a modifiche e/o integrazioni, nel caso di cambiamento del quadro normativo e del contesto



organizzativo, che dovranno essere approvate seguendo il medesimo iter procedurale previsto per l'approvazione dello stesso.

### **3. Campo di applicazione**

I destinatari del presente Regolamento sono:

- il Responsabile della funzione di Internal Audit;
- il Team di lavoro aziendale a supporto della funzione di I.A.;
- la Direzione Strategica aziendale;
- tutte le Direzioni, Strutture e Servizi dell'Azienda Sanitaria Provinciale di Agrigento interessati dell'attività di audit.

### **4. Organizzazione, Responsabilità e compiti**

#### **4.1 Assetto organizzativo della funzione di Internal Auditing**

La funzione di I.A. è svolta all'interno dell'Azienda da un Responsabile e da un Team di supporto individuato con apposita deliberazione. E' facoltà del coordinatore avvalersi di ulteriori professionalità per favorire la piena implementazione delle attività chiave associate a ciascun processo oggetto di audit. Ciascun componente del Team di audit assicura, per gli audit ai quali è designato a partecipare, l'insussistenza di conflitti di interessi tra la funzione esercitata ed il processo oggetto di audit. Qualora un componente del team di lavoro sia direttamente coinvolto per la propria funzione nell'attività oggetto di analisi il coordinatore propone al Direttore Generale un sostituto e provvede alla sostituzione dello stesso con una diversa figura aziendale nel rispetto dei principi di obiettività, trasparenza ed imparzialità che caratterizzano la funzione di I.A.

Alla funzione di I.A. devono essere resi disponibili ed accessibili tutte le informazioni, i rilievi e tutta la documentazione proveniente da strutture interne e da organi ed organismi di controllo interni ed esterni all'Azienda.

#### **4.2 Compiti della funzione di Interna Auditing**

Alla funzione di Internal Auditing compete:

- Assistere la Direzione Strategica nel valutare il funzionamento del sistema dei controlli e delle procedure operative;
- Coordinare e pianificare le attività di audit;



- Coadiuvare i responsabili delle strutture auditate nella mappatura, identificazione degli ambiti soggetti a rischio ed individuazione delle eventuali modifiche di tipo organizzativo da apportare al processo tali da mitigare il livello di rischio;
- Predisporre il piano annuale di audit e redigere insieme al Team di lavoro il rapporto di audit;
- Eseguire gli audit programmati e gestire l'esecuzione del processo di follow-up;
- Favorire la comprensione dell'importanza di un processo formale, documentale e collaborativo nel quale i responsabili dei processi auditati siano direttamente coinvolti nel giudicare e monitorare l'efficacia dei controlli esistenti;
- Curare la redazione del presente Regolamento e dei successivi aggiornamenti qualora se ne verificano i presupposti;
- Tenere l'archivio della documentazione e delle evidenze necessarie a supporto delle attività di audit.

## **5. Principi etici, regole di condotta e Standard Internazionali**

### **5.1 Principi etici**

L'attività svolta dalla funzione di I.A. si conforma ai principi contenuti nel Codice Etico dell'Institute of Internal Auditors (Allegato 1) ed agli Standard Internazionali di Internal Audit di indipendenza, riservatezza e competenza (Allegato 2).

L'attività di I.A. viene svolta nel rispetto e secondo i limiti previsti dalle vigenti disposizioni in materia di protezione dei dati personali (D. Lgs. 30 giugno 2003 n.196 e s.m.i.).

### **5.2 Segnalazione di eventuale danno erariale**

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

### **5.3 Segnalazione di eventuale denuncia penale**

Qualora nel corso dell'attività di audit, venga acquisita notizia di un reato perseguibile d'ufficio, il Responsabile Internal Audit ed il Team di lavoro che sono venuti a conoscenza dei fatti

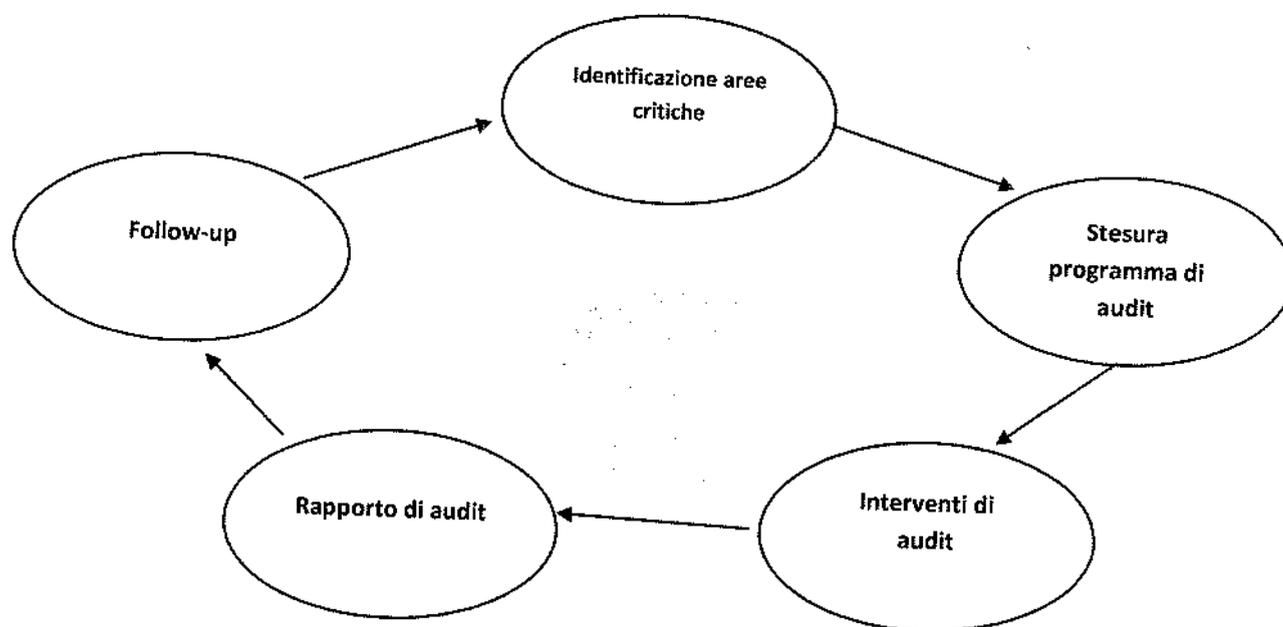


predispongono una relazione indirizzata al Direttore Generale nella quale si dà evidenza delle circostanze riscontrate, i dati circa il giorno di acquisizione della notizia e le fonti di prova già note. Il Direttore Generale disposta l'istruttoria agli uffici competenti provvede a trasmettere gli atti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

## 6. Il processo di Internal Auditing

### 6.1 Il Ciclo di Audit

Il processo descrittivo delle attività della funzione di I.A. e rappresentato nello schema sotto riportato:



### 6.2 Identificazione delle aree critiche

L'identificazione delle aree critiche costituisce l'azione preliminare alla formulazione del Piano Annuale di Audit. L'obiettivo di questa fase consiste nell'individuare le aree (funzione, processi, ecc.) maggiormente critiche, e quindi potenzialmente esposte a rischi che potrebbero pregiudicare il raggiungimento degli obiettivi strategici aziendali.

L'identificazione delle aree critiche si articola nelle seguenti fasi:

- Identificazione dei rischi;
- Risk assessment.



### **6.2.1 Identificazione dei rischi**

In fase di avvio delle attività di I.A., l'individuazione delle aree critiche dell'Azienda avviene tramite l'analisi e la valutazione dell'insieme dei rilievi/ricieste/indicazioni provenienti da strutture interne/organismi esterni all'Azienda, dall'analisi di documenti/dati aziendali, dall'accadimento di fatti dai quali emergono aree di rischio non adeguatamente presidiate. In questo ambito il punto di avvio è rappresentato dalle Aree di Intervento individuate nei Percorsi Attuativi di Certificabilità dei Bilanci (PAC).

Il PAC ha individuato le seguenti Aree organizzativo/gestionali Critiche:

- A) Area Generale;
- D) Immobilizzazioni;
- E) Rimanenze;
- F) Crediti e Ricavi;
- G) Disponibilità liquide;
- H) Patrimonio Netto;
- I) Debiti e Costi.

Altri fonti interne ed esterne sono:

- Verbali del Collegio Sindacale;
- Piano annuale di Risk management;
- Valutazione strumenti di monitoraggio della performance aziendale (es. obiettivi di budget);
- Verbali del Collegio di Direzione;
- Verbali del Comitato Valutazioni Sinistri;
- Confronto con il Servizio Legale;
- Piano Triennale Anticorruzione;
- Confronto con il Referente Anticorruzione aziendale;
- Richieste di informative da parte della Corte dei Conti, del Ministero, della Regione;
- Ufficio Relazioni con il Pubblico.

Il presente elenco è da ritenersi a titolo esemplificativo e non esaustivo.

### **6.2.2 Risk assessment**

Lo strumento metodologico adottato per il Risk assessment (processo di valutazione del rischio) è la matrice di RACM (Risk Assessment Criteria Matrix) che permette di valutare il rischio di probabilità di accadimento e di impatto.



**RISCHIO:** evento potenziale il cui verificarsi potrebbe pregiudicare la capacità dell'Azienda di perseguire gli obiettivi definiti dal Management.

In primo luogo è necessario **VALUTARE IL RISCHIO** in cui l'Azienda incorre misurando lo stesso in termini di **PROBABILITA'** di **ACCADIMENTO** e di **IMPATTO**:

**RISCHIO= PROBABILITA' x IMPATTO**

**PROBABILITA':** frequenza del manifestarsi del rischio o di possibile accadimento dell'evento negativo identificato.

VALUTAZIONE DELLA PROBABILITA'	
<b>QUASI CERTO</b>	E' presumibile che l'evento si manifesti sistematicamente o ripetutamente nell'arco di un periodo definito ( es. anno)
<b>MOLTO PROBABILE</b>	La probabilità di accadimento dell'evento è da considerarsi reale, anche se non con caratteristiche di sistematicità
<b>POCO PROBABILE</b>	L'evento ha qualche probabilità di manifestarsi nel periodo
<b>RARO</b>	La probabilità di accadimento dell'evento è da considerarsi remota

**IMPATTO:** livello in cui il manifestarsi del rischio potrebbe influenzare le strategie per il raggiungimento degli obiettivi aziendali; danno economico potenziale (perdita, mancato raggiungimento dell'equilibrio economico) provocato dal manifestarsi dell'evento negativo.

VALUTAZIONE DELL'IMPATTO	
<b>GRAVE</b>	Impatto rilevante sul raggiungimento degli obiettivi strategici aziendali (es. casi di frode o malversazioni, inefficacia dei sistemi informatici)
<b>SIGNIFICATIVO</b>	Impatto rilevante sulla strategia o sulle attività operative dell'organizzazione
<b>MODERATO</b>	Impatto contenuto sul raggiungimento degli obiettivi strategici dell'Azienda (es. inefficienze o interruzioni nell'operatività, nei pagamenti, problemi temporanei di erogazione del servizio)
<b>IRRILEVANTE</b>	Nessun impatto concreto sul raggiungimento degli obiettivi ma situazioni anomale che, a giudizio del management, possono richiedere interventi correttivi sui controlli a presidio di tali rischi

La **MATRICE DI RACM** è la seguente:

		IMPATTO				
		1	2	3	4	
PROBABILITA'		Irrilevante	Moderato	Significativo	Grave	
	4	Quasi certo	M	A	E	E
	3	Molto probabile	M	M	A	E
	2	Poco Probabile	B	M	M	A
	1	Raro	B	B	M	A



LEGENDA VALUTAZIONE DEL RISCHIO	
B	Rischio basso
M	Rischio medio
A	Rischio alto
E	Rischio elevato

La valutazione dei rischi si conclude con un rapporto riepilogativo conclusivo in cui vengono evidenziati i processi che, sulla base del rischio residuo, si ritiene prioritario analizzare. Il rapporto viene trasmesso alla Direzione Generale.

### 6.3 Stesura del Piano di Audit

Il Piano di Audit è predisposto in base al risultato della identificazione e valutazione dei rischi e del contenuto del rapporto riepilogativo conclusivo. Nel Piano sono definiti gli ambiti di azione e le tipologie di controllo da svolgere sulla base di:

- Risultato del processo di identificazione e valutazione dei rischi;
- E/o ambiti che la Direzione Generale ritenga di sottoporre ad audit (in base alle proprie valutazioni strategiche).

Periodicamente potrà essere sottoposto ad audit anche un processo per il quale la valutazione del controllo operato sullo stesso sia definita adeguata ed il conseguente rischio residuo basso/medio. Ciò al fine di sottoporre a verifica la correttezza/congruità del procedimento di applicazione della RACM sulla valutazione del rischio.

Il Piano di Audit deve contenere le seguenti informazioni:

- Definizione dei processi che saranno sottoposti ad audit ed obiettivi da perseguire;
- Programmazione delle attività e tempi di realizzazione.

Il Piano di Audit è predisposto entro la fine di ogni anno ed è sottoposto alla Direzione Generale per l'approvazione con provvedimento formale.

### 6.4 Interventi di audit

#### 6.4.1 Pianificazione e comunicazione dell'intervento di audit

L'avvio delle attività di audit è comunicata al soggetto auditato attraverso la notifica o del Piano di Audit o dell'audit dedicato a firma del Direttore Generale.

Nel Piano, o comunque in caso di audit dedicato, è specificato:

- Gruppo di audit;
- Attività/Area/Funzione coinvolta;
- Scopo della verifica;
- Luogo della visita;



- Richiesta di messa a disposizione del Gruppo di audit di tutti gli elementi informativi utili alla conoscenza del processo in esame (normativa, procedure operative di supporto, regolamenti, certificazioni, flow-chart organizzativi, manuali, ecc.);
- Cronoprogramma dettagliato.

#### **6.4.2 Programmazione operativa dell'intervento di audit**

In questa fase:

- È contattata la struttura interessata all'audit la quale è stata preventivamente avvisata con la comunicazione di cui al punto precedente per concordare una data per la riunione di apertura;
- Sono studiati gli obiettivi specifici da perseguire, gli ambiti da coprire, i processi e le procedure da esaminare, la metodologia da seguire, le caratteristiche del campione da verificare;
- E' redatto il calendario dei lavori.

#### **6.4.3 Riunione di apertura**

Alla riunione di apertura, il responsabile del gruppo di audit presenta ai componenti del Gruppo gli obiettivi dell'audit, specifica il campo dell'audit, cita le norme di riferimento (criteri) e le altre informazioni necessarie. Sinteticamente si propone il piano dell'audit (tempi, documenti da predisporre, personale da coinvolgere), ove necessario, si definisce un campionamento delle attività o dei documenti da sottoporre a verifica. Si deve dare l'opportunità all'organizzazione auditata di porre domande. L'audit potrà riguardare tutti od alcuni processi dell'organizzazione.

Nel caso in cui sia necessario, o opportuno, procedere all'audit di una selezione di processi o di attività i criteri impiegati per la selezione dovranno essere descritti nel rapporto di audit. In ogni caso il Gruppo di audit dovrà procedere alla raccolta delle evidenze necessarie a permettere l'espressione delle conclusioni dell'audit.

Nel caso di audit particolarmente complessi è opportuno che il Gruppo si confronti in riunioni intermedie per scambiarsi informazioni e valutare il progresso dell'audit ed eventuali problemi insorti. Nel corso della riunione saranno definite le fasi operative da eseguire sul campo.

All'incontro dovrà partecipare il Responsabile della struttura oggetto di audit, con i collaboratori dallo stesso individuati, ed il Gruppo di audit. Una sintesi degli argomenti discussi e delle conclusioni raggiunte nella riunione di apertura sarà formalizzata dal Lead Auditor in un apposito verbale.



#### 6.4.4 Conduzione dell'audit

La conduzione dell'audit è la fase di svolgimento operativo del lavoro sul campo nella quale il Gruppo di audit analizza la normativa, le regole di funzionamento del processo, le procedure, l'organizzazione dell'attività, le risorse impegnate e qualsiasi ulteriore informazione che possa essere utile all'espletamento dell'audit stesso.

Ulteriori strumenti di valutazione di valutazione utilizzati dal Gruppo di audit, anche in combinazione tra di loro, possono essere:

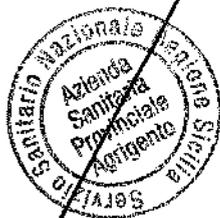
- **Interviste:** il Responsabile della struttura oggetto di verifica potrà essere intervistato dal Team di audit – anche con il supporto di una check list predefinita – quale ulteriore approfondimento delle conoscenze acquisite nel corso dello studio del processo e/o allo scopo di chiarire ulteriori punti e/o dubbi;
- **Workshop:** potranno essere organizzati workshop in forma collegiale per raccogliere informazioni e punti di vista e confrontare le differenti posizioni dei responsabili e dei funzionari che partecipano al processo nelle sue diverse fasi;
- **Questionari a risposta aperta/chiusa:** per richiedere informazioni sulle procedure e sul funzionamento delle diverse fasi del processo saranno utilizzati dei questionari somministrati agli attori del processo della struttura oggetto di analisi previa informazione del Responsabile della struttura;
- **Azioni di re-performance:** con questa tecnica viene testata l'efficacia della procedura di controllo; nel corso dell'audit sarà "provata" e rifatta la procedura di controllo in presenza degli operatori addetti alle attività per determinare l'univocità del risultato;
- **Osservazione diretta:** la tecnica è basata sull'osservazione delle fasi della procedura o dei processi oggetto di audit e consente di ottenere maggiore affidabilità delle evidenze di audit; è spesso utilizzata in presenza di controlli automatici;
- **Campionamento:** si intende l'applicazione delle procedure di verifica ad un campione rappresentativo della popolazione. Il campionamento può essere per quota, ragionato o casuale.

#### 6.4.5 Rapporto di audit

Conclusa la fase di esecuzione dell'audit, il Team di audit provvederà a predisporre un **Rapporto preliminare di audit** sullo stato attuale del sistema di controlli interni dell'attività auditata. Il Rapporto preliminare di audit sarà esaminato e discusso dal Team di Audit e dal Responsabile della struttura auditata; nel corso dell'incontro di chiusura (exit - meeting) saranno valutate le non conformità rilevate e discusse le misure necessarie da intraprendere per conseguire un livello accettabile di rischio.

A seguito dell'incontro di chiusura sarà redatto il **Rapporto finale di audit** inclusivo dei seguenti elementi:

- Risultati dell'audit;
- Rilievi e osservazioni del Responsabile della struttura auditata in sede di exit – meeting;



- Conclusioni e raccomandazioni formulate dal Team di audit;
- Azioni di miglioramento e correzione individuate e suggerite rispetto alle azioni già esistenti.

Il Rapporto finale di audit e la conseguente comunicazione dovranno contenere precisi elementi:

- Destinatari del Rapporto di audit;
- Oggetto dell'audit;
- Data delle sedute di verifica;
- Standard di controllo adottati nella verifica;
- Rilievi;
- Suggerimenti, commenti e possibili azioni di miglioramento;
- Sintesi sul livello di adeguatezza dei sistemi di controllo interni;
- Pianificazione del follow-up;
- Data e firma di chi ha partecipato alla verifica.

Il Rapporto finale di audit sarà inoltrato alla Direzione Generale ed al Responsabile della struttura auditata.

## **7. Follow-up**

Il follow-up rappresenta la fase in cui sarà successivamente verificata l'esecuzione delle azioni di miglioramento e delle correzioni suggerite e contenute nel Rapporto finale di audit. Le tempistiche di follow-up saranno indicate nel Rapporto finale di audit e comunque previste nei successivi Programmi di audit. Il Team di audit definirà il livello di approfondimento e le tempistiche del follow-up sulla base delle criticità riscontrate in fase di esecuzione dell'audit e dell'intervallo di tempo ritenuto congruo per apportare le azioni di miglioramento previste nel Rapporto finale di audit. Gli esiti del follow-up saranno indicati nel Rapporto di follow-up con dettaglio dell'efficacia delle azioni di miglioramento prescritte e raccomandate.

## **8. Archiviazione della documentazione di audit**

Per ogni intervento di audit sarà creato un fascicolo che raccoglie la documentazione utilizzata, i verbali delle sedute, gli atti, la normativa di riferimento, i documenti acquisiti, le informazioni raccolte e le risultanze finali. I fascicoli resteranno agli atti dell'ufficio del Responsabile della funzione di Internal Audit.



**ALLEGATO 1**

**CODICE ETICO – INSTITUTE OF INTERNAL AUDITORS**



## Codice Etico

### Introduzione

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

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

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

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

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

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

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

### Applicabilità e attuazione

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

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

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

### Principi

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



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

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

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

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

### **Regole di condotta**

#### **1) Integrità**

L'internal auditor:

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

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

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

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

#### **2) Obiettività**

L'internal auditor:

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

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

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



### **3) Riservatezza**

L'internal auditor:

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

3.2 Non deve usare le informazioni ottenute né per vantaggio personale, né secondo modalità che siano contrarie alla legge o di nocimento 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**

**STANDARD INTERNAZIONALI DI INTERNAL AUDIT**



### **Introduzione agli *Standard***

Gli *Standard* hanno lo scopo di:

1. delineare i principi base che prescrivono come deve essere svolta l'attività di internal audit;
2. fornire un quadro di riferimento per lo sviluppo e l'effettuazione di una vasta gamma di attività di internal audit a valore aggiunto;
3. definire i parametri per la valutazione delle prestazioni dell'internal audit;
4. promuovere il miglioramento dei processi organizzativi e operativi. Gli *Standard* fissano

requisiti vincolanti, basati su principi, che consistono in:

- Definizioni dei requisiti fondamentali per la pratica professionale dell'internal auditing e per la valutazione dell'efficacia dell'attività, applicabili internazionalmente a diversi livelli organizzativi e individuali.
- Interpretazioni che chiariscono termini e concetti contenuti nelle Definizioni.

Gli *Standard* utilizzano termini cui sono stati attribuiti significati specifici e che sono stati inclusi nel Glossario. Specificamente, gli *Standard* usano la parola "deve" per specificare un requisito vincolante e la parola "dovrebbe" per indicare un requisito vincolante a meno di circostanze ed eventi che, sottoposti a un giudizio professionale, ne giustificano l'inosservanza.

Per comprendere e applicare correttamente gli *Standard*, è necessario considerare sia le Definizioni che le loro Interpretazioni, nonché i significati specifici riportati nel Glossario.

La struttura degli *Standard* è suddivisa in Standard di Connotazione e Standard di Prestazione. Gli Standard di Connotazione precisano le caratteristiche che devono possedere le organizzazioni e gli individui che effettuano attività di internal audit. Gli Standard di Prestazione descrivono la natura dell'attività di internal audit e forniscono criteri qualitativi in base ai quali valutarne l'effettuazione. Gli Standard di Connotazione e gli Standard di Prestazione si applicano a tutti i servizi di internal audit.

Sono inoltre previsti gli *Standard Applicativi* che approfondiscono l'applicazione degli *Standard di Connotazione* e degli *Standard di Prestazione*, stabilendo i requisiti relativi all'assurance (A) o alle attività di consulenza (C).



## **STANDARD DI CONNOTAZIONE**

### **1000 – Finalità, poteri e responsabilità**

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

#### **Interpretazione:**

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

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

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

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

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

### **1100 – Indipendenza e obiettività**

L'attività di internal audit deve essere indipendente e gli internal auditor devono essere obiettivi nell'esecuzione del loro lavoro.

#### **Interpretazione:**

*Indipendenza è la libertà da condizionamenti che minaccino la capacità dell'attività di internal audit di adempiere senza pregiudizio alle proprie responsabilità. Per raggiungere il livello di indipendenza necessario per esercitare in modo efficace le responsabilità dell'attività di internal audit, il responsabile internal auditing ha diretto e libero accesso al senior management e al board. Ciò può essere conseguito tramite un duplice rapporto organizzativo. Casi di limitazione all'indipendenza devono essere gestiti a livello di singolo auditor, di incarico, funzionale e organizzativo.*



*Obiettività è l'attitudine mentale di imparzialità che consente agli internal auditor di svolgere i propri incarichi in un modo che consenta loro di credere nella validità del lavoro svolto e nell'assenza di compromessi sulla qualità. In materia di audit, l'obiettività richiede che gli internal auditor non subordinino il proprio giudizio professionale a quello di altri. Eventuali ostacoli all'obiettività devono essere gestiti a livello di singolo auditor, di incarico, funzionale e organizzativo.*

#### **1110 – Indipendenza organizzativa**

Il responsabile internal auditing deve riportare ad un livello dell'organizzazione che consenta all'attività di internal audit il pieno adempimento delle proprie responsabilità. Il responsabile internal auditing deve confermare al board, almeno una volta l'anno, lo stato di indipendenza organizzativa dell'attività di internal audit.

#### **Interpretazione:**

*Si realizza un'indipendenza organizzativa efficace quando il responsabile internal auditing riferisce funzionalmente al board. Esempi di rapporto funzionale al board comportano che il board:*

- *approvi il Mandato di internal audit;*
- *approvi il piano di attività basato sulla valutazione dei rischi;*
- *approvi il budget e il piano delle risorse dell'attività di internal audit;*
- *riceva comunicazioni dal responsabile internal auditing in merito ai risultati dell'attività di internal audit rispetto al piano e ad altre questioni;*
- *approvi le decisioni relative alla nomina e all'esonero del responsabile internal auditing;*
- *approvi il compenso spettante al responsabile internal auditing;*
- *effettui opportune verifiche con il management e il responsabile internal auditing per stabilire se sono presenti limitazioni non appropriate dell'ambito di copertura e delle risorse.*

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

#### **1111 – Comunicazione con il board**

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

#### **1120 – Obiettività individuale**

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

#### **Interpretazione:**

*Conflitto di interessi è una situazione nella quale gli internal auditor, che godono di una posizione di fiducia, si trovano ad avere un interesse personale o professionale contrario agli interessi dell'organizzazione. Un simile contrasto con l'organizzazione rende difficile l'adempimento dei compiti dell'internal auditor con imparzialità. Un conflitto di interessi può sussistere anche quando non dà luogo a comportamenti non etici o comunque impropri. L'esistenza di un conflitto di interessi può dare l'impressione che vi siano comportamenti*



Azienda Sanitaria Provinciale di Agrigento – Regolamento di Internal Auditing  
*scorretti, con il risultato di compromettere la fiducia verso gli internal auditor, l'attività di internal audit e la professione. Il conflitto di interessi può pregiudicare la capacità individuale di svolgere con obiettività i propri compiti e responsabilità.*

### **1130 – Condizionamenti dell'indipendenza o dell'obiettività**

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

#### **Interpretazione:**

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

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

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

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

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

**1130.C2** – Se gli internal auditor, a fronte di prospettati servizi di consulenza, si trovano in una situazione di potenziale condizionamento della propria indipendenza od obiettività, devono segnalarlo al cliente prima di accettare l'incarico.

### **1200 – Competenza e diligenza professionale**

Gli incarichi devono essere effettuati con la dovuta competenza e diligenza professionale.

#### **1210 – Competenza**

Gli internal auditor devono possedere le conoscenze, capacità e altre competenze necessarie all'adempimento delle loro responsabilità individuali. L'attività di internal audit nel suo insieme deve possedere o dotarsi delle conoscenze, capacità e altre competenze necessarie all'esercizio delle proprie responsabilità.

#### **Interpretazione:**



Azienda Sanitaria Provinciale di Agrigento – Regolamento di Internal Auditing

*I termini conoscenze, capacità e altre competenze si riferiscono nel loro complesso alla competenza professionale richiesta agli internal auditor per adempiere efficacemente alle proprie responsabilità professionali. Gli internal auditor sono incoraggiati a dimostrare la propria competenza conseguendo le opportune certificazioni e qualifiche professionali, come quella di "Certified Internal Auditor" e altre certificazioni rilasciate dal "The Institute of Internal Auditors" e da altri organismi professionali riconosciuti.*

**1210.A1** – Il responsabile internal auditing deve dotarsi di opportuna assistenza e consulenza se gli internal auditor non possiedono le conoscenze, le capacità o altre competenze necessarie per lo svolgimento di tutto o di parte dell'incarico.

**1210.A2** – Gli internal auditor devono possedere conoscenze sufficienti per valutare i rischi di frode e il modo in cui l'organizzazione li gestisce, senza aspettarsi che essi abbiano le competenze proprie di chi ha come responsabilità primaria quella di individuare e investigare frodi.

**1210.A3** – Gli internal auditor devono possedere una sufficiente conoscenza dei rischi e dei controlli chiave dell'Information Technology, nonché degli strumenti informatici di supporto all'attività di audit per svolgere gli incarichi assegnati. Tuttavia, non è richiesto che tutti gli internal auditor posseggano le competenze di chi ha come responsabilità primaria quella dell'Information Technology auditing.

**1210.C1** – Il responsabile internal auditing deve rifiutare l'incarico di consulenza, oppure dotarsi di valido supporto e assistenza nel caso in cui gli internal auditor non posseggano le conoscenze, le capacità o le altre competenze necessarie per lo svolgimento di tutto o di parte dell'incarico.

**1220 – Diligenza professionale**

Gli internal auditor devono applicare la diligenza e le capacità che ci si attende da un internal auditor ragionevolmente prudente e competente. Diligenza professionale non implica infallibilità.

**1220.A1** – L'internal auditor deve esercitare la diligenza professionale tenendo in considerazione:

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

**1220.A2** – Per svolgere l'attività di audit con diligenza professionale, gli internal auditor devono considerare l'utilizzo di strumenti informatici di supporto e di altre tecniche di analisi dei dati.

**1220.A3** – Gli internal auditor devono prestare attenzione ai rischi significativi che



Azienda Sanitaria Provinciale di Agrigento – Regolamento di Internal Auditing

possono incidere su obiettivi, attività o risorse. Comunque, le sole procedure di assurance, anche quando effettuate con la dovuta diligenza professionale, non garantiscono che tutti i rischi significativi vengano individuati.

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

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

### **1230 – Aggiornamento professionale continuo**

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

### **1300 – Programma di assurance e miglioramento della qualità**

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

#### **Interpretazione:**

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

### **1310 – Requisiti del programma di assurance e miglioramento della qualità**

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

### **1311 – Valutazioni interne**

Le valutazioni interne devono includere:

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

#### **Interpretazione:**

*Il monitoraggio continuo costituisce parte integrante dell'attività quotidiana di supervisione, verifica e misurazione dell'attività di internal audit. Il monitoraggio continuo è incorporato nelle procedure utilizzate di norma per gestire l'attività di internal audit e viene svolto utilizzando processi, strumenti e informazioni necessari per valutare la conformità alla Definizione di Internal Auditing, al Codice Etico e agli Standard. Le valutazioni periodiche sono effettuate con l'obiettivo specifico di valutare la conformità alla Definizione di Internal Auditing, al Codice Etico e agli Standard.*



*La comprensione di tutti gli elementi dell'International Professional Practices Framework è necessaria per una adeguata conoscenza della metodologia di internal audit.*

### **1312 – Valutazioni esterne**

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

- la modalità e la frequenza della valutazione esterna;
- le qualifiche e l'indipendenza del valutatore o del team di valutatori esterni, inclusa l'esistenza di qualsiasi possibile situazione di conflitto di interessi.

#### **Interpretazione:**

*Le valutazioni esterne possono essere costituite da valutazioni esterne complete oppure essere condotte sotto forma di autovalutazione con convalida esterna indipendente.*

*Un valutatore o un team di valutatori qualificati devono dimostrare di essere competenti in due ambiti: la pratica professionale dell'internal auditing e il processo di valutazione esterna. La competenza può essere dimostrata attraverso una combinazione di esperienza e conoscenze teoriche. L'esperienza acquisita presso organizzazioni analoghe per dimensioni, complessità, settore o comparto e specializzazione tecnica è più significativa di un'esperienza meno specifica. Nei team di valutatori, non è necessario che tutti i componenti del team posseggano tutte le competenze, in quanto è il team nel suo insieme a risultare idoneo. Nel determinare se un valutatore o un team di valutatori dimostrino competenza sufficiente per essere ritenuti idonei, il responsabile internal auditing applica un giudizio professionale.*

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

### **1320 – Comunicazione del programma di assurance e miglioramento della qualità**

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

#### **Interpretazione:**

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

### **1321 – Uso della dizione “Conforme agli Standard Internazionali per la Pratica Professionale dell'Attività di Internal Auditing”**

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



Azienda Sanitaria Provinciale di Agrigento – Regolamento di Internal Auditing  
affermazione.

**Interpretazione:**

*L'attività di internal audit risulta conforme agli Standard quando raggiunge i risultati descritti nella Definizione di Internal Auditing, nel Codice Etico e negli Standard. I risultati del programma di assurance e miglioramento della qualità comprendono i risultati delle valutazioni interne ed esterne. Tutte le attività di internal audit devono essere oggetto di valutazioni interne, mentre le attività di internal audit che operano da almeno cinque anni devono essere oggetto anche di valutazioni esterne.*

**1322 – Comunicazione di non conformità**

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

**STANDARD DI PRESTAZIONE**

**2000 – Gestione dell'attività di internal audit**

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

**Interpretazione:**

*L'attività di internal audit è gestita efficacemente quando:*

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

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

**2010 – Piano delle attività di internal audit**

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

**Interpretazione:**

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



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

**2010.C1** – Il responsabile internal auditing deve decidere se accettare un incarico di consulenza, sulla base delle possibilità di miglioramento della gestione dei rischi, delle possibilità di aggiungere valore e di migliorare l'operatività dell'organizzazione. Gli incarichi accettati devono essere inclusi nel piano di audit.

#### **2020 – Comunicazione e approvazione del piano**

Il responsabile internal auditing deve sottoporre il piano delle attività di internal audit e delle risorse necessarie, incluse eventuali variazioni significative intervenute, al senior management e al board per il relativo esame e approvazione. Il responsabile internal auditing deve, inoltre, segnalare l'impatto di un'eventuale carenza di risorse.

#### **2030 – Gestione delle risorse**

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

#### **Interpretazione:**

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

#### **2040 – Direttive e procedure**

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

#### **Interpretazione:**

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

#### **2050 – Coordinamento delle attività**

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

#### **2060 – Informazione periodica al senior management e al board**

Il responsabile internal auditing deve informare periodicamente il senior management e il board in merito a finalità, poteri e responsabilità dell'attività di internal audit, nonché comunicare lo stato di avanzamento del piano. Tale comunicazione deve comprendere inoltre i rischi significativi, inclusi quelli di frode, i problemi di controllo, i problemi di governance e ogni altra informazione necessaria o richiesta dal senior management e dal board.



**Interpretazione:**

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

**2100 – Natura dell'attività**

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

**2110 – Governance**

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

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

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

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

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

**2120 – Gestione del rischio**

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

**Interpretazione:**

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

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



Azienda Sanitaria Provinciale di Agrigento – Regolamento di Internal Auditing  
*I processi di gestione del rischio sono monitorati attraverso la gestione manageriale continua, specifiche valutazioni, o entrambi.*

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

- raggiungimento degli obiettivi strategici dell'organizzazione;
- affidabilità e integrità delle informazioni contabili, finanziarie e operative;
- efficacia ed efficienza delle operazioni e dei programmi;
- salvaguardia del patrimonio;
- conformità a leggi, regolamenti, direttive, procedure e contratti.

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

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

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

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

### **2130 – Controllo**

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

**2130.A1** – L'attività di internal audit deve valutare l'adeguatezza e l'efficacia dei controlli introdotti in risposta ai rischi riguardanti la governance, le operazioni e i sistemi informativi dell'organizzazione, relativamente a:

- raggiungimento degli obiettivi strategici dell'organizzazione;
- affidabilità e integrità delle informazioni contabili, finanziarie e operative;
- efficacia ed efficienza delle operazioni e dei programmi;
- salvaguardia del patrimonio;
- conformità a leggi, regolamenti, direttive, procedure e contratti.

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

**2130.A3** – Gli internal auditor dovrebbero verificare operazioni e programmi



Azienda Sanitaria Provinciale di Agrigento – Regolamento di Internal Auditing  
dell'organizzazione al fine di valutarne la coerenza con gli obiettivi stability, e per stabilire se operazioni e programmi sono attuati o eseguiti come previsto.

**2130.A4** – Per valutare i controlli sono necessari adeguati criteri. Gli internal auditor devono accertare che il management abbia stabilito adeguati criteri per valutare il raggiungimento degli obiettivi. Se tali criteri sono adeguati, gli internal auditor devono utilizzarli nell'effettuare la propria valutazione. In caso contrario, devono collaborare con il management nello sviluppo di opportuni criteri di valutazione.

**2130.C1** – Nel corso degli incarichi di consulenza, gli internal auditor devono analizzare i controlli in coerenza con gli obiettivi dell'incarico ed essere attenti all'eventuale presenza di significative problematiche di Controllo.

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

## **2200 – Pianificazione dell'incarico**

Per ciascun incarico gli internal auditor devono predisporre e documentare un piano che comprenda gli obiettivi dell'incarico, l'ambito di copertura, la tempistica e l'assegnazione delle risorse.

## **2201 – Elementi della pianificazione**

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

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

**2201.A1** – Nel pianificare un incarico per conto di terze parti esterne all'organizzazione, gli internal auditor devono definire con queste un accordo scritto che chiarisca obiettivi, ambito di copertura, rispettive responsabilità ed eventuali aspettative e che stabilisca restrizioni alla diffusione dei risultati dell'incarico e all'accesso alla relativa documentazione.

**2201.C1** – Gli internal auditor devono concordare con i clienti di un incarico di consulenza gli obiettivi, l'ambito di copertura, le rispettive responsabilità e ciò che di ulteriore ci si attende. Per gli incarichi di maggiore rilevanza, tale accordo deve essere formalizzato in un documento scritto.



**2210 – Obiettivi dell'incarico**

Per ciascun incarico devono essere fissati obiettivi specifici.

**2210.A1** – Gli internal auditor devono effettuare una valutazione preliminare dei rischi afferenti l'attività oggetto di audit. Gli obiettivi dell'incarico devono rispecchiare i risultati di tale valutazione.

**2210.A2** – Al momento della definizione degli obiettivi dell'incarico, gli internal auditor devono considerare il grado di probabilità che esistano errori significativi, frodi, non conformità e altre situazioni pregiudizievoli.

**2210.A3** – Per valutare la governance, la gestione dei rischi e dei controlli, sono necessari criteri adeguati. Gli internal auditor devono accertare che il management e/o il board abbiano stabilito criteri adeguati per valutare il raggiungimento di obiettivi e traguardi. Se tali criteri sono adeguati, gli internal auditor devono utilizzarli nell'effettuare la propria valutazione. In caso contrario, devono collaborare con il management e/o il board allo sviluppo di opportuni criteri di valutazione.

**2210.C1** – Gli obiettivi degli incarichi di consulenza devono riguardare processi di governance, di gestione dei rischi e di controllo, nella misura concordata con il cliente.

**2220 – Ambito di copertura dell'incarico**

L'ambito di copertura definito, deve essere sufficiente per consentire il raggiungimento degli obiettivi dell'incarico.

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

**2220.A2** – Qualora, nel corso di un incarico di assurance, emergano opportunità significative di incarichi di consulenza, si dovrebbe stipulare uno specifico accordo scritto su obiettivi, ambito di copertura, rispettive responsabilità e su ciò che di ulteriore ci si attenda. I risultati raggiunti vanno comunicati secondo gli standard vigenti per gli incarichi di consulenza.

**2220.C1** – Nello svolgimento di un incarico di consulenza, gli internal auditor devono assicurarsi che l'ambito di copertura dell'incarico sia sufficientemente ampio per conseguire gli obiettivi concordati. Se, nel corso dell'incarico, gli internal auditor ritengono di ridefinire l'ambito di copertura, ne devono discutere con il cliente, per decidere se sia opportuno proseguire.

**2230 – Assegnazione delle risorse**

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



**2240 – Programma di lavoro**

Gli internal auditor devono sviluppare e documentare programmi di lavoro che permettano di conseguire gli obiettivi dell'incarico.

**2240.A1** – I programmi di lavoro devono includere le procedure per raccogliere, analizzare, valutare e documentare le informazioni durante lo svolgimento dell'incarico. I programmi di lavoro devono essere approvati prima della loro utilizzazione e ogni successiva modifica deve essere prontamente approvata.

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

**2300 – Svolgimento dell'incarico**

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

**2310 – Raccolta delle informazioni**

Gli internal auditor devono raccogliere informazioni sufficienti, affidabili, pertinenti e utili per conseguire gli obiettivi dell'incarico.

**Interpretazione:**

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

**2320 – Analisi e valutazione**

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

**2330 – Documentazione delle informazioni**

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

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

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



Azienda Sanitaria Provinciale di Agrigento – Regolamento di Internal Auditing

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

#### **2340 – Supervisione dell'incarico**

Gli incarichi devono essere sottoposti a opportuna supervisione al fine di garantire che gli obiettivi vengano raggiunti, che la qualità sia assicurata e che il personale possa crescere professionalmente.

#### **Interpretazione:**

*Il grado di supervisione richiesta dipende dalla professionalità e dall'esperienza degli internal auditor, nonché dalla complessità dell'incarico. Il responsabile internal auditing ha la completa responsabilità della supervisione dell'incarico, anche nel caso in cui questo sia svolto per conto dell'internal audit. Il responsabile internal auditing può delegare tale supervisione a internal auditor di provata esperienza. Evidenza dell'avvenuta supervisione deve essere documentata e opportunamente conservata.*

#### **2400 – Comunicazione dei risultati**

Gli internal auditor devono comunicare i risultati degli incarico.

#### **2410 – Modalità di comunicazione**

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

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

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

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

**2410.C1** – Le comunicazioni relative allo stato di avanzamento e ai risultati finali degli incarichi di consulenza possono variare, nella forma e nei contenuti, in funzione della natura dell'incarico e delle esigenze del cliente.

#### **2420 – Qualità della comunicazione**

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

#### **Interpretazione:**

*Una comunicazione accurata non presenta errori né distorsioni ed è fedele ai fatti rilevati. Una comunicazione obiettiva è corretta, imparziale e scevra da pregiudizi ed è il risultato di una*



Azienda Sanitaria Provinciale di Agrigento – Regolamento di Internal Auditing  
*valutazione imparziale ed equilibrata di tutti i fatti e le circostanze rilevanti. Una comunicazione chiara ha senso logico ed è facilmente comprensibile. La chiarezza può essere migliorata limitando l'uso di termini tecnici e fornendo sufficienti informazioni di supporto. Una comunicazione concisa è essenziale, evita formulazioni non necessarie, dettagli superflui, ridondanze e prolissità. Una comunicazione costruttiva è utile al committente dell'incarico e all'organizzazione e induce miglioramenti laddove necessari. Una comunicazione completa contiene tutti gli elementi informativi essenziali per i destinatari, nonché tutte le informazioni e le osservazioni significative atte a corroborare raccomandazioni e conclusioni. Una comunicazione tempestiva è puntuale e opportuna nei tempi, in funzione della portata del problema, consentendo al management di intraprendere appropriate azioni correttive.*

#### **2421 – Errori e omissioni nella comunicazione**

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

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

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

#### **2431 – Comunicazione di non conformità di uno specifico incarico**

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

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

#### **2440 – Divulgazione dei risultati**

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

#### **Interpretazione:**

*Il responsabile internal auditing, è tenuto a verificare ed approvare sia la comunicazione finale dei risultati dell’incarico prima dell’emissione degli stessi, sia la lista di distribuzione che la modalità di divulgazione.*

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



Azienda Sanitaria Provinciale di Agrigento – Regolamento di Internal Auditing

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

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

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

**2440.C2** – Nel corso di incarichi di consulenza è possibile che vengano rilevate criticità concernenti la governance, la gestione dei rischi e il controllo. Se tali criticità sono significative per l'organizzazione, esse devono essere segnalate al senior management e al board.

#### **2500 – Monitoraggio delle azioni correttive**

Il responsabile internal auditing deve stabilire e mantenere un sistema di monitoraggio delle azioni intraprese a seguito dei risultati segnalati al management.

**2500.A1** – Il responsabile internal auditing deve impostare un processo di follow-up per monitorare e assicurare che le azioni correttive siano state effettivamente attuate dal management oppure che il senior management abbia accettato il rischio di non intraprendere alcuna azione.

**2500.C1** – L'attività di internal audit deve monitorare le azioni intraprese a seguito di incarichi di consulenza nella misura concordata con il cliente.

#### **2600 – Comunicazione dell'accettazione del rischio**

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

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



## **GLOSSARIO**

### **Adeguato controllo**

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

### **Ambiente di controllo**

È costituito dagli atteggiamenti e dalle azioni del board e del management rispetto all'importanza del controllo all'interno dell'organizzazione. Esso 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 di direzione;
- struttura organizzativa;
- attribuzione di poteri e responsabilità;
- politiche e prassi di gestione del personale;
- competenze del personale.

### **Attività di internal audit**

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

### **Board**

Per board si intende il massimo organo di governo, che ha la responsabilità di indirizzare e/o di sorvegliare le attività e la gestione dell'organizzazione. In genere, il board è costituito da un gruppo indipendente di amministratori (per esempio, consiglio di amministrazione, consiglio di sorveglianza, consiglio dei governatori o dei trustee). Nei casi in cui questo gruppo non è presente, per "board" si può intendere la persona a capo dell'organizzazione. Il termine "board" può anche designare un Audit Committee al quale l'organo di governo abbia delegato determinate funzioni.

### **Codice Etico (o Codice Deontologico)**



Azienda Sanitaria Provinciale di Agrigento – Regolamento di Internal Auditing

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

#### **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).

#### **Conflitto di interessi**

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

#### **Conformità**

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

#### **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.

#### **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.

#### **Deve (devono)**

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

#### **Dovrebbe (dovrebbero)**

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

#### **Frode**

Qualsiasi atto illegale caratterizzato da falsità, dissimulazione e 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.

#### **Gestione del rischio**



Azienda Sanitaria Provinciale di Agrigento – Regolamento di Internal Auditing

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.

### **Giudizio complessivo**

Valutazione, conclusione e/o altra descrizione dei risultati presentata dal responsabile internal auditing; essa 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.

### **Giudizio dell'incarico**

Valutazione, conclusione e/o altra descrizione dei risultati di un incarico di internal audit, con riferimento agli obiettivi e all'ambito di copertura dell'incarico.

### **Governance**

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

### **Governance dei sistemi informativi**

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

### **Incarico**

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

### **Indipendenza**

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

### **International Professional Practices Framework (IPPF)**

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

### **Livello di accettazione del rischio (*risk appetite*)**

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

### **Mandato di internal audit**

Il Mandato di internal audit è un documento formale che definisce finalità, poteri e responsabilità dell'attività di internal audit. Il Mandato deve determinare la posizione dell'internal auditing nell'organizzazione, autorizzare l'accesso ai dati, alle persone e ai beni aziendali



Azienda Sanitaria Provinciale di Agrigento – Regolamento di Internal Auditing  
necessari per lo svolgimento degli incarichi di audit, nonché definire l'ambito di copertura delle attività di audit.

### **Obiettivi dell'incarico**

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

### **Prestatore esterno di servizi**

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

### **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.

### **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.

### **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 alla Definizione di Internal Auditing, al Codice Etico e agli *Standard*. Il responsabile internal auditing o i collaboratori che riferiscono a lui sono in possesso delle opportune qualifiche e certificazioni professionali. La designazione specifica del responsabile internal auditing può variare nelle diverse organizzazioni.

### **Rischio**

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

### **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.

### **Servizi di consulenza**

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

### **Significatività**

Importanza relativa di un fatto, nell'ambito del contesto nel quale è considerato. Include fattori



Azienda Sanitaria Provinciale di Agrigento – Regolamento di Internal Auditing  
quantitativi e qualitativi quali la grandezza, la natura, le conseguenze, la rilevanza e l'impatto.  
Agli internal auditor è richiesto un giudizio professionale quando valutano la significatività dei fatti collocati nell'ambito degli obiettivi considerati.

**Standard**

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

**Strumenti informatici di supporto all'audit**

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

**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.



Con il parere favorevole del Direttore Sanitario e del Direttore Amministrativo;

### DELIBERA

Per le motivazioni espresse in premessa:

1. Di approvare il regolamento Aziendale Internal Auditing della Azienda Sanitaria Provinciale di Agrigento, che si allega come parte integrante del presente provvedimento;
2. Autorizzare il servizio proponente a notificare attraverso la pubblicazione su sito web istituzionale aziendale sezione Atti dell'Azienda – Regolamenti Aziendali il suddetto regolamento a tutti i dirigenti responsabili delle strutture aziendali;
3. Stabilire che nessun onere economico grava dall'adozione del presente provvedimento;
4. Dichiarare il presente atto immediatamente esecutivo stante la necessità di provvedere in materia.



IL DIRETTORE AMMINISTRATIVO  
*Dott. Salvatore Lombardo*

A handwritten signature in black ink, appearing to be "S. Lombardo", written over a horizontal line.

IL DIRETTORE GENERALE  
*Dott. Salvatore Lucio Ficarra*

A handwritten signature in black ink, appearing to be "S. Ficarra", written over a horizontal line.

IL DIRETTORE SANITARIO  
*Dott. Silvio Lo Bosco*

A handwritten signature in black ink, appearing to be "S. Lo Bosco", written over a horizontal line.

Il Segretario Verbalizzante  
il Collaboratore Amministrativo Prof.lla  
Sig.ra Sabrina Torresi

A handwritten signature in black ink, appearing to be "S. Torresi", written over a horizontal line.

**PUBBLICAZIONE**

Si dichiara che la presente deliberazione, su conforme relazione dell'addetto, è stata pubblicata all'albo pretorio on line dell'ASP di Agrigento, ai sensi e per gli effetti dell'art. 53, comma 2, della L.R. n.30 del 03/11/93 e dell'art. 32 della Legge n. 69 del 18/06/09 e s.m.i., dal \_\_\_\_\_ al \_\_\_\_\_

L'Incaricato

Per delega del Direttore Amministrativo  
Il Collaboratore Amm.vo Prof.le  
Titolare di Posizione Organizzativa  
Dott.ssa Patrizia Tedesco

Notificata al Collegio Sindacale il \_\_\_\_\_ con nota prot. n. \_\_\_\_\_

**DELIBERA SOGGETTA AL CONTROLLO**

Dell'Assessorato Regionale della Salute ex L.R. n. 5/09 trasmessa in data \_\_\_\_\_ prot. n. \_\_\_\_\_

**SI ATTESTA**

Che l'Assessorato Regionale della Salute:

- Ha pronunciato l'approvazione con provvedimento n. \_\_\_\_\_ del \_\_\_\_\_
  - Ha pronunciato l'annullamento con provvedimento n. \_\_\_\_\_ del \_\_\_\_\_
- come da allegato.

Delibera divenuta esecutiva per decorrenza del termine previsto dall'art. 16 della L.R. n. 5/09 dal \_\_\_\_\_

**DELIBERA NON SOGGETTA AL CONTROLLO**

- Esecutiva ai sensi dell'art. 65 della L. R. n. 25/93, così come modificato dall'art. 53 della L.R. n. 30/93 s.m.i., per decorrenza del termine di 10 gg. di pubblicazione all'Albo, dal \_\_\_\_\_

X Immediatamente esecutiva dal 03.03.2017

Agrigento, li

**IL FUNZIONARIO INCARICATO**

**REVOCA/ANNULLAMENTO/MODIFICA**

- Revoca/annullamento in autotutela con provvedimento n. \_\_\_\_\_ del \_\_\_\_\_
- Modifica con provvedimento n. \_\_\_\_\_ del \_\_\_\_\_

Agrigento, li

**IL FUNZIONARIO INCARICATO**