Ospedale di Circolo
Fondazione Macchi

Sistema Sanitario Regione Lombardia

Azienda ospedaliera Ospedale di Circolo e Fondazione Macchi - Polo universitario
di rilievo nazionale e ad alta specializzazione

Viale Borri 57 21100 Varese
Tel. 0332-278.111, Fax 0332-261.440

DELIBERAZIONE DEL DIRETTORE GENERALE n. 1000 del 30.11.2015

OGGETTO: ADOZIONE DEL REGOLAMENTO AZIENDALE DI INTERNAL AUDITING.

DELIBERAZIONE ADOTTATA DAL DIRETTORE GENERALE DR. CALLISTO BRAVI

IL DIRETTORE GENERALE

Accertata la competenza procedurale, sottopone in data 20/11/2015 l'allegata proposta di deliberazione n. 1078 sull'argomento all'oggetto specificato, il cui costo rientra nel budget assegnato.

Il Responsabile del procedimento
(Dr. Paolo Michele Covacich)

Il Direttore Generale
(Dr. Callisto Bravi)

IL DIRETTORE S.C. ECONOMICO-FINANZIARIA

ha registrato contabilmente l'importo complessivo di € .....

☐ il costo previsto dalla presente proposta, che trova copertura come segue:
(n. conto economico, n. autorizzazione, BPE dell'esercizio 20.....)
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

☐ l'importo di € ..... che trova adeguata copertura finanziaria tramite.....
.....

☒ non comporta alcun onere

☐ altro .....
.....

data 23.11.2015

Il Direttore S.C. Economico-Finanziaria
Dr. Dario Lorenzon

Ospedale di Circolo
Fondazione Macchi

Sistema Sanitario Regione Lombardia

Azienda ospedaliera Ospedale di Circolo e Fondazione Macchi - Polo universitario
di rilievo nazionale e ad alta specializzazione

Viale Borri 57 21100 Varese
Tel. 0332-278.111, Fax 0332-261.440

DELIBERAZIONE DEL DIRETTORE GENERALE n. 1000 del 30.11.2015

La deliberazione si compone di n. 27 pagine, di cui n. 23 pagine di allegati, parte integrante.

IL DIRETTORE GENERALE

richiamate 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 dell'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 della pubbliche amministrazioni";

richiamata la Legge Regionale n. 17 del 4 giugno 2014 avente ad oggetto "Disciplina del sistema dei controlli interni ai sensi dell'art. 58 dello Statuto d'autonomia" e, in particolare l'art. 6 che definisce la funzione di Internal Auditing;

vista la D.G.R. n. X/2989 del 23.12.2014, "Determinazione in ordine alla gestione del Servizio Socio Sanitario Regionale per l'esercizio 2015", che ha previsto, nell'anno 2015, lo sviluppo della funzione di Internal Auditing all'interno delle aziende sanitarie regionali, l'approvazione di un regolamento aziendale specifico in materia e la predisposizione della pianificazione annuale di attività per l'anno 2016;

richiamata altresì la deliberazione n. 927 del 30.10.2015 con la quale si è provveduto ad attribuire la responsabilità della funzione di Internal Auditing al Dr. Paolo Michele Covacich, responsabile della S.S. Controllo di Gestione e Programmazione, e a rinviare a successivo provvedimento l'adozione di apposito regolamento;

dato atto che il presente regolamento è il risultato di un percorso di collaborazione interaziendale, che ha preso avvio a partire dal mese di maggio c.a., con i referenti di I.A. delle seguenti Aziende Ospedaliere: "Ospedale Civile"di Legnano, "Ospedale di Circolo" di Busto Arsizio, "Ospedale S. Antonio Abate" di Gallarate e "Ospedale Guido Salvini" di Garbagnate;

acquisiti per quanto di competenza, ai sensi dell'articolo 3 del D.Lgs. n. 502/1992 e s.m.i, i pareri favorevoli del Direttore Amministrativo e del Direttore Sanitario;

DELIBERA

Per i motivi di cui in premessa che qui si intendono integralmente trascritti:

1. di approvare il regolamento aziendale di Internal Auditing che si allega quale parte integrante del presente provvedimento (allegato n. 1);

2. di dare atto che il presente provvedimento non comporta oneri economici;

Ospedale di Circolo
Fondazione Macchi
Sistema Sanitario Regione Lombardia

Azienda ospedaliera Ospedale di Circolo e Fondazione Macchi - Polo universitario
di rilievo nazionale e ad alta specializzazione

Viale Borri 57 21100 Varese
Tel. 0332-278.111, Fax 0332-261.440

DELIBERAZIONE DEL DIRETTORE GENERALE n. 1000 del 30.11.2015

3. di dare atto che, ai sensi dell'art. 18, comma 9, della Legge Regionale n. 33 del 30 dicembre 2009, il presente provvedimento deliberativo, non soggetto a controllo, verrà pubblicato nei modi di legge, ed è immediatamente esecutivo.

IL DIRETTORE GENERALE
(Dr. Callisto Bravi)

IL DIRETTORE SANITARIO
(Dr. Gianluca Avanzi)

IL DIRETTORE AMMINISTRATIVO
(Dott.ssa Maria Grazia Colombo)

Ospedale di Circolo
Fondazione Macchi
Sistema Sanitario Regione Lombardia

Azienda ospedaliera Ospedale di Circolo e Fondazione Macchi - Polo universitario
di rilievo nazionale e ad alta specializzazione

Viale Borri 57 21100 Varese
Tel. 0332-278.111, Fax 0332-261.440

DELIBERAZIONE DEL DIRETTORE GENERALE n. 1000 del 30.11.2015

RELATA DI PUBBLICAZIONE

Si certifica che la presente deliberazione è pubblicata all'albo pretorio sul sito aziendale www.ospedalivarese.net così come previsto dall'art. 32, comma 1, L. 69/2009, dal 2.12.2015 e vi rimane per quindici giorni consecutivi.

S.C. AFFARI GENERALI E LEGALI
Il Funzionario addetto
(Claudia Bortolato)
C. Bortolato

La presente deliberazione è stata trasmessa il ....., per il controllo preventivo, alla Giunta Regionale con elenco n. ..... prot. n.....ai sensi della L.R. n. 33 del 30.12.2009, art. 18 comma 6.

- ☐ Approvata dalla Giunta Regionale con DGR n. ..... del .....
- ☐ Esecutiva dal ..... per silenzio assenso
- ☐ .....

IL DIRETTORE AMMINISTRATIVO
(Dott.ssa Maria Grazia Colombo)

La presente copia fotostatica, composta da n. ..... fogli numerati progressivamente dal n. ..... al n. ....., è conforme all'originale.
Varese, lì .....

S.C. AFFARI GENERALI E LEGALI
Il Funzionario addetto
(Claudia Bortolato)

ALLEGATO 1)

Azienda Ospedaliera

OSPEDALE DI CIRCOLO E FONDAZIONE MACCHI VARESE

Regolamento di Internal Auditing

Vers. 1 del 12 novembre
A cura di Controllo di Gestione e Programmazione

5

1. Introduzione

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

Svolge un controllo di terzo livello presidiando i controlli di secondo livello svolti dalle altre funzioni aziendali (Controllo di gestione, Risk management, Qualità, Anticorruzione...) e quelli di primo livello attuati dai dirigenti responsabili dei processi aziendali.

Il suo scopo è quello di supportare l'organizzazione nel perseguimento dei propri obiettivi attraverso un approccio sistematico volto a 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 Internal Auditing dell'Azienda Ospedaliera di Varese nell'attività di auditing sui processi operativi aziendali;

I destinatari del Regolamento sono il Responsabile della funzione di Internal Auditing, il Gruppo di lavoro aziendale a supporto della funzione di Internal Auditing, la Direzione strategica, tutte le Direzioni, Strutture e Servizi dell'Azienda Ospedaliera di Varese interessati all'attività di audit.

2. Organizzazione, responsabilità e compiti

2.1 L'assetto organizzativo

Il responsabile della funzione di Internal auditing individua, per ciascun audit, i componenti del Gruppo le cui competenze professionali sono maggiormente attinenti al processo oggetto di audit, costituendo il Gruppo di audit.

Ciascun componente del Gruppo assicura, per gli audit ai quali è designato a partecipare, l'insussistenza di conflitti di interessi.

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

2.2 Compiti della funzione di Internal auditing

Alla funzione di Internal Auditing compete:

- predisporre il piano annuale di audit e stendere insieme al Gruppo di lavoro il rapporto di audit
- assistere la Direzione nel valutare il funzionamento del sistema dei controlli e delle procedure operative
- coordinare e pianificare l'attività di audit
- coadiuvare i responsabili delle strutture auditate nella mappatura ed identificazione degli ambiti soggetti a rischio e nell'individuazione di modifiche organizzative tali da mitigare il livello di rischio
- eseguire gli audit programmati e l'esecuzione dei follow-up

- stendere insieme al team il rapporto di Audit
- provvedere agli aggiornamenti del Regolamento di Audit qualora necessari

3. Principi etici e regole di condotta

3.1 I principi etici

L'attività svolta dalla funzione di Internal Auditing si conforma ai principi contenuti nel Codice Etico dell'Institute of Internal Auditor (allegato A).

L'attività viene svolta in autonomia, indipendenza di giudizio, obiettività e riservatezza.

L'attività di Internal Auditing non è soggetta alle limitazioni a tutela della privacy.

3.2 Denuncia di danno erariale

Qualora, nel corso dell'attività di audit emergano fatti che possano dar luogo a un'ipotesi di responsabilità per danni causati alla finanza pubblica, il responsabile Internal Auditing informa , il Direttore Generale, che dopo averne accertata la responsabilità, provvederà alla denuncia alla Procura Regionale presso la sezione giurisdizionale della Corte dei Conti.

La denuncia deve contenere tutti gli elementi raccolti per l'accertamento della responsabilità e la determinazione del danno. L'obbligo di denuncia sussiste qualora il danno sia concreto e attuale.

Nel caso di potenzialità lesiva, il Responsabile di Internal Auditing, informerà il Direttore Generale dell'obbligo di operare affinchè il danno sia evitato e, nel caso si verifichi, dell'obbligo di denuncia del fatto alla Procura erariale.

3.3 Denuncia penale

Qualora, nel corso dell'attività di audit, venga acquisita notizia di un reato perseguibile d'ufficio deve esserne fatta denuncia.

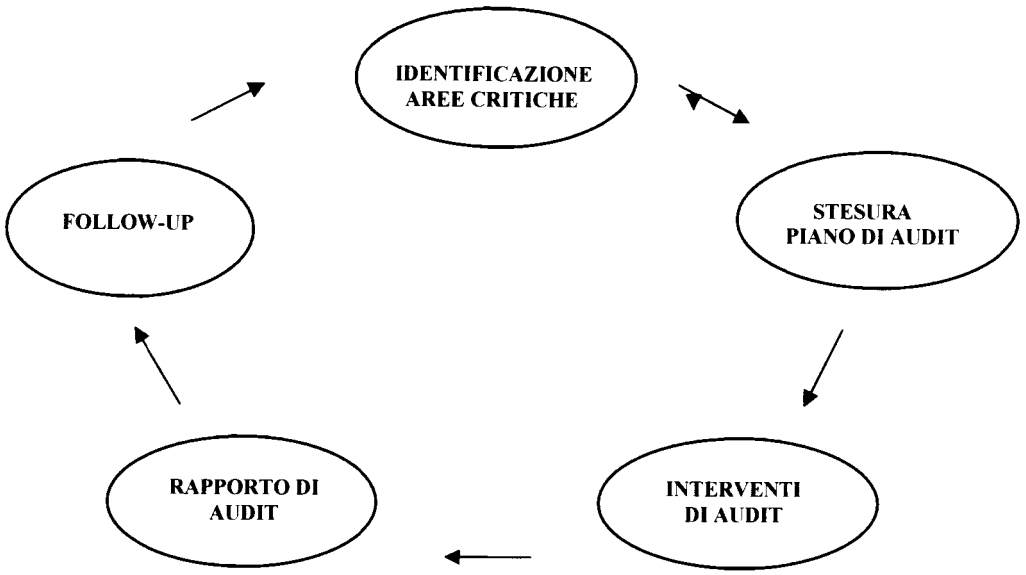
Il Dirigente responsabile dell'I.A. ed il team di auditors che hanno appreso la notizia predispongono una relazione al Direttore Generale nella quale si dà evidenza dei fatti riscontrati e dell'obbligo di denuncia.

La denuncia è inviata a firma del Direttore Generale alla Procura della Repubblica e deve contenere l'esposizione dei fatti, i dati circa il giorno di acquisizione della notizia e le fonti di prova già note. Quando possibile deve contenere gli elementi utili all'identificazione della persona alla quale il fatto è attribuito, della persona offesa e di coloro che siano in grado di riferire su circostanze rilevanti per la ricostruzione dei fatti.

4. Il processo di internal auditing

4.1. Il ciclo di Audit

Il processo descrittivo delle attività della funzione di Internal Auditing è quello dello schema sotto riportato:



4.2. Identificazione delle aree critiche

L'identificazione delle aree critiche costituisce l'azione preliminare all'avvio dell'attività nella quale viene analizzata la struttura organizzativa aziendale ed individuato l'universo di Audit, ovvero le aree per le quali è opportuno condurre l'attività di risk- assessment propedeutica alla definizione del Piano annuale di Audit.

Il risk assessment è il processo attraverso il quale vengono individuati i rischi potenziali e le attività di controllo poste in essere dal management per mitigarli. Si conclude con l'identificazione dei rischi cioè l'evidenza dei fattori interni ed esterni che possono pregiudicare il raggiungimento degli obiettivi. Il Risk Assessment si articola nelle seguenti fasi:

- identificazione dei processi che contribuiscono in modo significativo al raggiungimento degli obiettivi aziendali
- identificazione dei rischi e dei controlli esistenti tesi a ridurre il rischio inerente
- definizione delle prioritarie aree da analizzare in base al livello di rischio individuato e a quanto stabilito dalla Direzione Strategica.

In fase di avvio dell'attività di internal auditing, l'individuazione delle aree critiche dell'Azienda avviene tramite l'analisi e la valutazione dell' insieme dei rilievi/richieste/indicazioni provenienti da strutture interne/organismi esterni all'Azienda, dall'analisi di documenti/dati aziendali, dall'accadimento di fatti dai quali emergano aree di rischio non adeguatamente presidiate.

Tra le principali fonti interne ed esterne si indicano:

1. Verbali del Collegio Sindacale
2. Piano annuale di Risk Management

3. Valutazione strumenti di monitoraggio Performance Aziendale (es. Piano Integrato di Miglioramento dell'Organizzazione, Obiettivi di budget)
4. Verbali del Collegio di Direzione
5. Verbali del Comitato Valutazione Sinistri
6. Controlli dei Nuclei operativi di Controllo delle prestazioni
7. Controlli dei Nuclei Operativi di Controllo Contabile di Regione Lombardia
8. Confronto con l'Ufficio Legale
9. Piano Triennale Anticorruzione
10. Confronto con il Responsabile Anticorruzione aziendale
11. Richiesta di informative da parte della Corte dei Conti, del Ministero, della Regione, dell'Asl
12. Ufficio Relazioni con il Pubblico

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

4.3. La valutazione dei rischi

Lo strumento metodologico adottato per valutare il rischio è la matrice **RACM** (Risk Assessment Criteria Matrix) che permette di valutare il rischio in termini di **PROBABILITA'** di accadimento e di **IMPATTO**.

PROBABILITA' -> frequenza del manifestarsi del rischio

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

IMPATTO -> livello in cui il manifestarsi del rischio potrebbe influenzare il raggiungimento delle strategie e degli obiettivi.

VALUTAZIONE DELL'IMPATTO	
GRAVE	Impatto rilevante sul raggiungimento degli obiettivi strategici aziendali. Es: casi di frode o malversazioni, inefficacia dei sistemi informatici.
SIGNIFICATIVO	Impatto rilevante sulla strategia o sulle attività operative dell'organizzazione.

MODERATO	Impatto contenuto sul raggiungimento degli obiettivi strategici dell'Azienda. Es: inefficienze o interruzioni nell'operatività, nei pagamenti, problemi temporanei di erogazione del servizio.
IRRILEVANTE	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 valutazione complessiva del rischio in termini di probabilità e impatto viene effettuata utilizzando la seguente **Matrice RACM:**

			IMPATTO			
			1	2	3	4
			irrilevante	moderato	significativo	grave
PROBABILITA'	4	Quasi certo	M	A		
	3	molto probabile	M	M	A	
	2	Poco probabile	B	M	M	A
	1	raro	B	B	M	A

LEGENDA VALUTAZIONE DEL RISCHIO	
B	Rischio basso
M	Rischio medio

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 inviato alla Direzione Generale.

4.4. Il Piano di Audit

Il Piano di Audit viene predisposto sulla base del risultato della Valutazione dei rischi e del contenuto del rapporto riepilogativo conclusivo.

Nel Piano vengono definiti gli ambiti di azione e le attività di controllo da svolgere sulla base del risultato della Valutazione dei Rischi (Risk Assessment) e/o dagli ambiti che la Direzione Generale ritenga di sottoporre ad audit, sulla base delle 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 Annuale 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 viene predisposto entro la fine di ogni anno ed è sottoposto alla Direzione Generale per l'approvazione

4.5 Le fasi di un intervento di audit

Nell'intervento di audit si possono identificare le seguenti fasi:

4.5.a) Comunicazione dell'intervento di audit

L'avvio dell'attività di audit viene comunicato al soggetto auditato con nota scritta del Direttore Generale.

Nella nota viene:

- specificato l'obiettivo dell'attività di audit,
- identificato il Gruppo di audit,
- richiesto di mettere a disposizione del Gruppo di audit tutti gli elementi utili alla conoscenza del processo in esame (normativa, procedure di supporto, regolamenti, certificazioni, flowchart organizzativi, manuali ...)

4.5.b) Programmazione operativa dell'intervento di audit

In questa fase:

- viene preso contatto con la struttura interessata dall'audit la quale è stata preventivamente avvisata con la comunicazione di cui al punto precedente per concordare una data per la riunione di apertura,
- vengono studiati gli obiettivi da perseguire, gli ambiti da coprire, i processi e le procedure da esaminare, la metodologia da seguire, le caratteristiche del campione da verificare.
- viene steso il calendario dei lavori e definiti i componenti del gruppo di audit.

4.5.c) Riunione di apertura

L'obiettivo della riunione di apertura è quello di chiarire all'auditato lo scopo e l'ambito dell'audit, nonché le metodologie che saranno seguite nella sua conduzione. Nel corso di tale riunione si definiscono le fasi operative del lavoro sul campo.

All'incontro partecipa il responsabile della struttura auditata con i collaboratori dallo stesso individuati ed il gruppo di audit. Una sintesi degli argomenti discussi e delle conclusioni raggiunte nella riunione di apertura viene formalizzata dall'auditor incaricato dell'intervento in un verbale della riunione.

4.5.d) Conduzione dell'audit

La conduzione dell'audit è la fase di svolgimento 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.

Gli ulteriori strumenti di valutazione utilizzati dal gruppo di audit, anche in combinazione tra di loro, possono essere:

- Interviste: il responsabile della struttura auditata può essere intervistato dal team di audit – anche con il supporto di una chek list predefinita – quale ulteriore approfondimento delle conoscenze acquisite nel corso dello studio del processo e/o allo scopo di chiarire i punti dubbi;

- Work-shop: possono essere organizzati work-shop in forma collegiale per raccogliere i 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. Della somministrazione dei questionari occorre sempre avvisare il responsabile della struttura auditata;

- Azioni di re-performance: con questa tecnica viene testata l'efficacia della procedura di controllo. La stessa viene "provata" alla presenza degli operatori addetti allo scopo di verificare se si perviene allo stesso risultato;

- Osservazione diretta: la tecnica è basata sull'osservazione delle fasi della procedura o dei processi oggetto di audit e consente di avere maggiore affidabilità delle evidenze di audit. E' spesso utilizzata sui controlli automatici.

- Campionamento: si intende l'applicazione delle procedure di verifica a meno del 100% della popolazione in modo da trarre una valida conclusione valutando le caratteristiche del campione esaminato. Il campionamento può essere casuale, mirato, sistematico.

4.5.e) Rapporto di Audit

Conclusa la fase di esecuzione dell'audit il gruppo di audit predispone un Rapporto preliminare sullo stato attuale del sistema di controllo interno dell'attività auditata.

Il Rapporto preliminare viene esaminato e discusso, dal Gruppo di Audit e dal Responsabile della struttura auditata, nel corso di un incontro di chiusura (exit-meeting) nel quale vengono valutate le non conformità rilevate e vengono discusse le misure necessarie da intraprendere per conseguire un livello accettabile di rischio.

A seguito dell'incontro di chiusura viene redatto un Rapporto finale che tiene conto dei risultati dell'audit, dei rilievi, delle osservazioni del responsabile della struttura auditata in sede di exit-meeting, delle conclusioni e raccomandazioni formulate dal gruppo di audit, delle azioni di miglioramento e correzione individuate e suggerite rispetto alle azioni già esistenti.

Il rapporto finale e la comunicazione che ne consegue devono contenere elementi precisi:

- Destinatari del rapporto
- Oggetto dell'audit
- Data delle sedute e delle verifiche
- Standard di controllo adottati nella verifica
- Rilievi emersi
- Suggerimenti, commenti e possibili azioni di miglioramento
- Sintesi sul livello di adeguatezza dei sistemi di controllo interni
- Previsioni di follow-up
- Data e firme di chi ha partecipato alla verifica-

Il rapporto finale è inoltrato alla Direzione Generale ed al responsabile della struttura auditata.

5. Follow-up

E' la fase in cui viene verificata l'esecuzione delle azioni di miglioramento e delle correzioni suggerite e contenute nel Rapporto finale di audit.

Il follow-up è indicato nel Rapporto finale di audit e programmato nei successivi Piani di Audit.

Il Gruppo di Audit definisce il livello di approfondimento e la tempistica del follow-up sulla base dei rilievi emersi in fase di audit e del tempo necessario per approntare le azioni di miglioramento previste dal rapporto finale di audit.

I risultati del follow-up sono esplicitati in un rapporto riportante il livello di attuazione delle azioni correttive.

6. Archiviazione della documentazione di Audit

Per ogni intervento di audit viene creato un fascicolo che raccoglie la documentazione utilizzata, i verbali delle sedute, gli atti, la normativa, i documenti acquisiti, le informazioni raccolte e le risultanze finali.

I fascicoli restano agli atti dell'ufficio del Responsabile della funzione di Internal Auditing.

Allegati:
All. A – Codice Etico dell' Institute of Internal Auditor

ALLEGATO A – STANDARD INTERNAZIONALI

Codice Etico

Introduzione

Lo 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 ed 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 ad 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 ed attuazione

Il Codice Etico si applica sia ai singoli individui sia alle strutture che forniscono servizi di internal auditing.
Il mancato rispetto del Codice Etico da parte dei membri dell'Institute, dei detentori delle certificazioni professionali e di coloro che si candidano a riceverle, sarà valutato e sanzionato secondo le norme previste nello Statuto e nelle "Administrative Directives" dell'Institute.
Il fatto che non siano esplicitamente menzionati nel Codice non toglie che certi comportamenti siano inaccettabili o inducano discredito e quindi che possano essere passibili di azione disciplinare.

Principi

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

1. Integrità

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

2. Obiettività

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

3. Riservatezza

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

4. Competenza

Nell'esercizio dei propri servizi professionali, l'internal auditor utilizza il bagaglio più appropriato di conoscenze,

competenze ed esperienze.

Regole di Condotta

1. Integrità
L'internal auditor:
1.1 Deve operare con onestà, diligenza e senso di responsabilità.

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

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

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

2. Obiettività
L'internal auditor:
2.1 Non deve partecipare ad alcuna attività o avere relazioni che pregiudichino o appaiano pregiudicare l'imparzialità della sua valutazione. In tale novero vanno incluse quelle attività o relazioni che possano essere in conflitto con gli interessi dell'organizzazione.
2.2 Non deve accettare nulla che pregiudichi o appaia pregiudicare l'imparzialità della sua valutazione.
2.3 Deve riferire tutti i fatti significativi a lui noti, la cui omissione possa fornire un quadro alterato delle attività analizzate.

3. Riservatezza
L'internal auditor:
3.1 Deve acquisire la dovuta cautela nell'uso e nella protezione delle informazioni acquisite nel corso dell'incarico.
3.2 Non deve usare le informazioni ottenute né per vantaggio personale, né secondo modalità che siano contrarie alla legge o di nocumento agli obiettivi etici e legittimi dell'organizzazione.

4. Competenza
L'internal auditor:
4.1 Deve effettuare solo prestazioni per le quali abbia la necessaria conoscenza, competenza ed esperienza.
4.2 Deve prestare i propri servizi in pieno accordo con gli Standard internazionali per la Pratica Professionale dell'Internal Auditing
4.3 Deve continuamente migliorare la propria preparazione professionale nonché l'efficacia e la qualità dei propri servizi.

DEFINIZIONE 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.

Standard Internazionali

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 riporto funzionale del responsabile internal auditing al board; autorizza l'accesso ai dati, alle persone e ai beni aziendali che sono necessari per lo svolgimento degli incarichi 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 riporto 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 riporto 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 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:
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 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;
- periodiche auto-valutazioni o valutazioni condotte da altre persone interne all'organizzazione che abbiano conoscenz adeguate 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 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. Il responsabile internal auditing deve rivedere e adeguare opportunamente il piano, in risposta ai cambiamenti intervenuti a livello di attività, rischi, operatività, programmi, sistemi e controllo dell'organizzazione.

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.A2 – Il responsabile internal auditing deve individuare e considerare le aspettative del senior management, del board e degli altri stakeholder verso i giudizi dell'internal audit e le altre conclusioni.

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.

2070 – Prestatore esterno di servizi e responsabilità organizzativa sull'internal auditing
Quando l'attività di internal audit è affidata a un prestatore esterno di servizi, quest'ultimo deve fare in modo che
l'organizzazione sia consapevole di avere la responsabilità di mantenere un'attività di internal audit efficace.
Interpretazione
Questa responsabilità si dimostra attraverso il programma di assurance e miglioramento della qualità, che valuta la conformità alla Definizione di Internal Auditing, al Codice Etico e agli Standard.

2100 – Natura dell'attività
L'attività di internal audit deve valutare e contribuire al miglioramento dei processi di governance, gestione del rischio e 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.

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 es prime 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.

L'attività di internal audit può raccogliere le informazioni necessarie per questa valutazione attraverso molteplici incarich i. I risultati di questi incarichi, visti nel complesso, permettono di capire i processi di gestione del rischio dell'organizzazione e la loro efficacia.
I processi di gestione del rischio sono monitorati attraverso 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.C1 – 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.

2210.C2 – Gli obiettivi degli incarichi di consulenza devono essere coerenti con i valori, le strategie e gli obiettivi dell'organizzazione.

2220 – Ambito di copertura dell'incarico
L'ambito di copertura definito, deve essere sufficiente per consentire il raggiungimento degli obiettivi dell'incarico.

2220.A1 – L'ambito di copertura dell'incarico deve 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.

2220.C2 – Nel corso degli incarichi di consulenza, gli internal auditor devono analizzare i controlli in coerenza con gli obiettivi dell'incarico ed essere attenti all'eventuale presenza di problematiche di controllo significative.

2230 – Assegnazione delle risorse
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 appro

priate.

2330 – Documentazione delle nformazioni
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.

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 venga no 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 incarichi.

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. Quando espressi, il giudizio o la conclusione devono tenere in considerazione le aspettative del senior management, del board e degli altri stakeholder e devono essere corroborati da informazioni sufficienti, affidabili, pertinenti e utili.
Interpretazione:
I giudizi espressi a livello di incarico possono essere valutazioni, conclusioni o altre descrizioni dei risultati. In questi casi, l'incarico può riguardare il controllo su un processo, un rischio o una business unit specifici. Per formulare questi giudizi è necessario considerare i risultati dell'incarico e il loro significato.

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 c omunicazione obiettiva è corretta, imparziale e scevra da pregiudizi ed è il risultato di una 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 costru ttiva 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 i nviare 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. Laddove il responsabile internal auditing deleghi queste funzioni, egli ne rimane comunque totalmente responsabile.

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.
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.

2450 – Giudizi complessivi
Quando si esprime un giudizio complessivo, questo deve tenere in considerazione le aspettative del senior management, del board e degli altri stakeholder e deve essere corroborato da informazioni sufficienti, affidabili, pertinenti e utili. **Interpretazione:** *La comunicazione deve precisare:*
- *l'ambito di copertura, specificando il periodo di tempo cui si riferisce il giudizio;*
- *le limitazioni dell'ambito di copertura;*
- *tutti i progetti connessi che sono stati presi in considerazione, indicando l'eventuale ricorso ad altri fornitori di assurance;*
- *il modello di rischio o di controllo o gli altri criteri usati come fondamento per esprimere il giudizio complessivo;*
- *il parere, il giudizio o la conclusione complessivi formulati.*

È necessario specificare i motivi dell'eventuale giudizio complessivo sfavorevole.

2500 – Monitoraggio delle azioni correttive
Il responsabile internal auditing deve stabilire e mantenere un sistema di monitoraggio delle azioni intraprese a seguito dei risultati segnalati al management.

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

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

2600 – Comunicazione dell'accettazione del rischio
Qualora il responsabile internal auditing concluda che il management abbia accettato un livello di rischio che potrebbe essere inaccettabile per l'organizzazione, ne deve discutere con il senior management. Se il responsabile internal auditing ritiene che la problematica non sia stata risolta, deve informarne il board.
Interpretazione:
È possibile identificare il rischio accettato dal management o attraverso un incarico di assurance o di consulenza che permetta di monitorare lo stato di implementazione delle azioni intraprese dal management in risposta a incarichi precedenti, oppure in altri modi. Il responsabile internal auditing non è responsabile per la gestione del rischio.