Sistema Socio Sanitario
Regione Lombardia
ATS Val Padana

Cl.: 1.1.02

DECRETO n. 69 del 24/08/2016

OGGETTO: ATTIVITÀ DI INTERNAL AUDITING: RESPONSABILITÀ, MANUALE E PIANO ATTIVITÀ 2016

Il DIRETTORE GENERALE – Dott. Aldo Bellini

Acquisito il parere favorevole del
DIRETTORE AMMINISTRATIVO Dott. Giuseppe Albini

Acquisito il parere favorevole del
DIRETTORE SANITARIO F.F. Dott. Renzo Boscaini

Acquisito il parere favorevole del
DIRETTORE SOCIOSANITARIO Dott. Diego Maltagliati

Responsabile del procedimento: BONI CRISTINA

IL DIRETTORE GENERALE

Dato atto che la Regione Lombardia, in esecuzione del Testo Unico in materia di Sanità del 30/12/2009 n. 33, modificato dalla L.R. n. 23 del 11/8/2015 “Evoluzione del sistema socio sanitario lombardo: modifiche al titolo I e II della Legge Regionale 30/12/2009 n. 33”, con Deliberazione n. X/4470 del 10/12/2015 ha costituito l’Agenzia di Tutela della Salute (ATS) della Val Padana con effetto dal 1/1/2016;

Premesso che:

- Il D.Lgs. 286 del 30/7/1999 e il D.Lgs.150 del 27/10/2009 hanno delineato, tra l’altro, un potenziamento dei controlli interni alle Pubbliche Amministrazioni, prevedendo che ogni P.A. adotti dei sistemi di controllo interno;
- Il Decreto regionale n. 2822 del 3/4/2013 con oggetto “Approvazione del Manuale di Internal Auditing della UO Sistema dei Controlli e Coordinamento Organismi Indipendenti” ha approvato il Manuale di Internal Auditing Regionale;
- La L.R. n. 17 del 14/6/2014 “Disciplina del sistema dei controlli interni ai sensi dell’art. 58 dello Statuto d’autonomia” stabilisce, tra l’altro, la funzione di Internal Auditing e le modalità e procedure per il controllo finalizzato a garantire legittimità, regolarità e correttezza dell’azione amministrativa;
- La DGR 2524 del 24/11/2014 “Vigilanza e controllo sugli Enti del sistema regionale, ai sensi dell’art.1 comma 1, comma 1-bis e 5 quarter, L.R. 27 dicembre 2006, n. 30”, con la quale la Regione Lombardia promuove la valorizzazione della rete di Internal Auditing;
- La DGR n. 2989 del 23/12/2014 “Determinazioni in ordine alla gestione del Servizio Socio Sanitario Regionale per l’anno 2015”, con la quale la Regione Lombardia introduce l’obbligo di costruzione di una Rete di Internal Auditing (IA) in tutti gli Enti Sanitari;

Considerato che, in base alla normativa sopra-richiamata, la funzione di Internal Auditing è uno strumento necessario alla valutazione dell’efficacia del sistema dei controlli interni, anche mediante la verifica dei processi, delle procedure e delle operazioni, nonché alla verifica dei sistemi di gestione e di controllo aziendali con la finalità di identificare, mitigare e/o correggere gli eventuali rischi (strategici, di processo e di informativa) presenti nell’organizzazione;

Dato atto che la costituzione della ATS della Val Padana, derivante dalla fusione dell’ASL di Mantova e dell’ASL di Cremona, in conseguenza del riassetto degli ambiti territoriali, e il passaggio di alcune funzioni alle ASST territoriali di riferimento, determina la necessità di rivedere la struttura e la programmazione per l’anno 2016 dell’attività di controllo interno svolta dall’Internal Auditing;

Vista altresì la nota regionale prot. n. 15787/16 del 13/4/2016 di richiesta della rielaborazione del Piano Audit per l’anno 2016 alla luce dei riassetti territoriali ed organizzativi disposti in seguito alla recente riforma del Sistema Sanitario lombardo;

Richiamata la delibera n. 269 del 4/8/2015 della disciolta ASL di Mantova con la quale:

- è stata istituita la funzione di Internal Auditing a partire dal 1° settembre 2015;
- è stato adottato il Manuale di Internal Auditing;
- è stato approvato il Piano delle attività di audit anno 2016;

Richiamati altresì i seguenti provvedimenti della disciolta ASL di Cremona:

- decreto n. 355 del 5/11/2015 con il quale si è approvato il nuovo Manuale di Internal Auditing;
- decreto n. 390 del 9/12/2015 con il quale è stato approvato il Piano delle attività di Audit per l’anno 2016;

Ritenuto quindi opportuno, per dare seguito alle indicazioni regionali, procedere alla ridefinizione della struttura e della programmazione dell'attività di Internal Auditing per l'ATS della Val Padana, provvedendo:

- ad affidare, in via provvisoria, la responsabilità della funzione di Internal Auditing in capo alla dott.ssa Cristina Boni, in possesso delle competenze professionali richieste per lo svolgimento di tale funzione, avendo anche partecipato ai corsi di formazione organizzati nel 2014 da Eupolis Lombardia in materia;
- all'adozione del Manuale di Internal Auditing;
- all'adozione del piano di attività di Internal Auditing, derivante da quanto determinato nelle ex ASL di Cremona e di Mantova;

Visti, come da documenti allegati quali parti integranti e sostanziali del presente atto:

- il Manuale di Internal Auditing che recepisce i principi e i criteri enunciati nel Manuale di Internal Auditing regionale, approvato dal Decreto Regionale n. 2822 del 3/4/2013, cui l'attività di Internal Auditing dell'ATS dovrà ispirarsi;
- il Piano di attività, nei quali sono stati definiti gli obiettivi, le finalità e la programmazione dell'attività dell'ATS Val Padana per l'anno 2016;

Ritenuto altresì opportuno rimandare a dopo la definizione del Piano Organizzativo Aziendale Strategico dell'ATS, la composizione di un gruppo di lavoro, dando atto comunque che la Funzione di IA, per le sue attività, potrà avvalersi di ogni altra professionalità dell'ATS in relazione alla specificità dell'area, delle attività monitorate e delle problematiche oggetto di verifica, che comporranno il team di auditor a supporto del Responsabile, ai quali sarà garantito un processo di formazione e sviluppo;

Vista l'attestazione della dott.ssa Boni Cristina nella veste di Responsabile del procedimento amministrativo e in ordine alla regolarità tecnica ed alla legittimità del presente provvedimento;

Acquisiti i pareri favorevoli del Direttore Amministrativo, Sanitario F.F. e Sociosanitario;

D E C R E T A

1. di affidare, in via provvisoria, la responsabilità della funzione di Internal Auditing dell'ATS Val Padana in capo alla dott.ssa Cristina Boni, in possesso delle competenze professionali richieste per lo svolgimento di tale funzione, avendo anche partecipato ai corsi di formazione organizzati nel 2014 da Eupolis Lombardia in materia;

2. di approvare il Manuale di Internal Auditing dell'ATS Val Padana, che recepisce i principi e i criteri enunciati nel Manuale di Internal Auditing regionale, approvato dal Decreto Regionale n. 2822 del 3/04/2013, cui l'attività di Internal Auditing aziendale dovrà ispirarsi, come da documento allegato al presente atto quale parte integrante e sostanziale;

3. di approvare il Piano di attività dell'ATS Val Padana, nel quale sono stati definiti gli obiettivi, le finalità e la programmazione dell'attività dell'ATS Val Padana per l'anno 2016, come da documento allegato al presente atto quale parte integrante e sostanziale;

4. di rimandare a dopo la definizione del Piano Organizzativo Aziendale Strategico dell'ATS della Val Padana la predisposizione di un Piano triennale e la composizione di un gruppo di lavoro;

5. di dare atto che la Funzione di Internal Auditing, per le sue attività, potrà avvalersi di ogni altra professionalità dell'ATS in relazione alla specificità dell'area, delle attività monitorate e delle problematiche oggetto di verifica, che comporranno il team di auditor a supporto del Responsabile, ai quali sarà garantito un processo di formazione e sviluppo;

6. di garantire al Responsabile Internal Auditing piena indipendenza ed autonomia nello svolgimento delle attività di audit e di assicurare accesso diretto a tutti i dati, alle informazioni ed ai beni aziendali necessari allo svolgimento delle proprie attività;

7. di trasmettere il Piano delle Attività di Audit alla Direzione Generale Welfare;

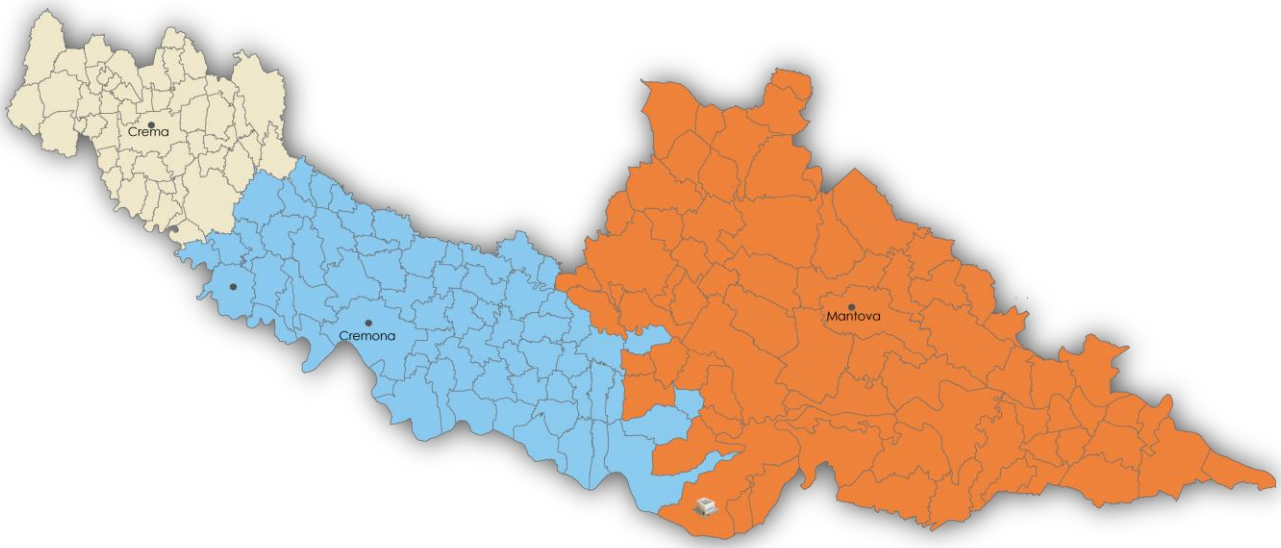
8. di disporre, a cura degli Affari Generali, la pubblicazione all'Albo on-line ai sensi dell'art. 32 della L. n. 69/2009, e nel rispetto del D.Lgs. n. 196/2003.

Firmato digitalmente
Dott. Aldo Bellini

Sistema Socio Sanitario
Regione Lombardia
ATS Val Padana

INTERNAL AUDITING

MANUALE INTERNAL AUTIDING ATS DELLA VAL PADANA 2016



SOMMARIO

1 INTRODUZIONE

1.1 Gli obiettivi del manuale

Il presente Manuale recepisce le indicazioni contenute nella Legge Regionale 4 giugno 2014 n. 17 "Disciplina del sistema dei controlli interni ai sensi dell'art. 58 dello Statuto d'autonomia" ed è stato redatto recependo i principi ed i criteri enunciati nel Manuale di Internal Auditing regionale (approvato con Decreto DDUO Sistema dei Controlli e Coordinamento Organismi Indipendenti n. 2822 del 3 aprile 2013), cui si fa espresso rinvio per quanto non espressamente precisato nel presente Manuale.
Gli scopi principali che si intendono perseguire col presente Manuale sono i seguenti:

- definire la metodologia per assistere i Direttori e Dirigenti nell'identificazione, mitigazione e monitoraggio dei rischi e dei relativi controlli;
- definire le fasi e le tempistiche del processo di audit;
- definire gli ambiti di collaborazione tra la funzione di audit e le strutture organizzative aziendali.

I destinatari del Manuale sono tutte le strutture aziendali. Il contenuto del manuale e dei suoi allegati potranno essere soggetti a revisioni nel caso di mutamento del contesto organizzativo e sulla base dei risultati annuali dell'attività di auditing. Le revisioni del manuale dovranno essere approvate seguendo l'iter procedurale previsto per l'approvazione del manuale stesso.

1.2 Le tipologie di intervento

L'internal auditing - controllo di secondo livello di metodo e di conformità alle linee guida esterne, ai vincoli legislativi e alle direttive che l'Agenzia stessa elabora per regolamentare la propria attività - è di norma articolato nelle seguenti tipologie d'intervento:

Audit tecnico-operativo (Operational Auditing) - o di processo
Analisi critica al fine di stabilire se le risorse siano utilizzate in modo efficace ed efficiente, in relazione agli obiettivi aziendali.

Audit di conformità (Compliance Auditing)
Verifica la conformità di attività e processi a norme, procedure e codici di condotta, al fine di prevenire il rischio di non conformità dell'attività aziendale.

Audit della governance etica (Ethical Auditing)
Attività avente come area di analisi la governance etica dell'azienda.

Audit dei Sistemi Informativi (Information Technology Auditing)
Analisi e verifica dei sistemi informatici a supporto dei diversi processi e delle diverse funzioni aziendali.

Audit antifrode (Fraud Auditing)
Verifiche volte a evitare irregolarità e atti illeciti perpetrati da persone operanti all'interno o all'esterno dell'ente.

Audit direzionale o strategico (Management Auditing)
Verifica la qualità del processo decisionale, con particolare attenzione alla fase di esecuzione da parte del management delle decisioni prese dall'alta Direzione.

Audit sui progetti
Verifica la gestione e lo stato di avanzamento dei progetti, identificandone i rischi e le strategie per ridurli o eliminarli.

Follow-up Auditing
Verifica che tutte le azioni correttive previste nel corso degli audit siano realizzate correttamente.

2 ORGANIZZAZIONE, RESPONSABILITÁ, RUOLI E COMPITI

2.1 **L'assetto organizzativo**

Con Deliberazione n. 3554 del 8/5/2015 la Regione Lombardia prevedeva lo sviluppo della funzione di Internal Auditing presso le Aziende Sanitarie, entro ottobre 2015, in attuazione della L.R. n. 17/2014, prevedendo la sua allocazione ad un livello dell'organizzazione idoneo ad assicurare autonomia della funzione, indipendenza di giudizio ed obiettività delle rilevazioni. La costituzione dell'ATS della Val Padana, con effetto dal 1/01/2016, derivante dalla fusione dell'ASL di Mantova e di Cremona, ha determinato la necessità di adottare un unico Manuale di Internal Auditing, in sostituzione dei Manuali già in precedenza adottati dalle confluite ASL di Cremona (Manuale adottato con Decreto n. 355 del 05.11.2015) e ASL di Mantova (Manuale adottato con Delibera n. 269 del 04.08.2015).
La Funzione di Internal Auditing è formata da un Responsabile che opera in piena indipendenza ed autonomia nello svolgimento delle attività di audit e al quale è assicurato l'accesso diretto a tutti i dati, alle informazioni ed ai beni aziendali necessari allo svolgimento delle proprie attività. Il Responsabile IA potrà predisporre un regolamento di dettaglio per lo svolgimento dell'attività che recepisca principi e criteri enunciati nel manuale di IA regionale avvalendosi di un gruppo operativo composto dalle diverse professionalità aziendali, scelte in funzione della specificità dell'area, delle attività monitorate e delle problematiche oggetto di verifica.
Per quanto riguarda al ruolo, responsabilità e compiti del Responsabile e dei collaboratori della Funzione di Internal Auditing si fa un esplicito rimando a quanto previsto dal Manuale di Internal Auditing di cui al Decreto Regione Lombardia n. 2822 del 03/04/2013.

2.2 **I principi etici, le regole di condotta e gli standard internazionali**

L'attività svolta dalla Funzione di Internal Auditing si conforma ai principi contenuti nel Codice Etico dell'Institute of Internal Auditors e agli Standard Internazionali Professionali di Indipendenza, Obiettività, Riservatezza e Competenza riportati in allegato al presente Manuale.

2.3 **I protocolli di comunicazione**

Le comunicazioni della Funzione di Internal Auditing sono rivolte ai seguenti soggetti:

1. Soggetti auditati: sono i destinatari delle comunicazioni esplicitate nel paragrafo 5 per quanto concerne le diverse fasi degli interventi di audit;
2. Direttore Generale: destinatario dei rapporti di audit;
3. Direttore del Servizio Risorse Umane: destinatario dei rapporti di audit per la valutazione degli eventuali profili disciplinari o di responsabilità dirigenziale del personale dipendente;
4. Responsabili di funzioni cointeressate alla specifica procedura/azione esaminata: destinatari dei rapporti di audit per gli aspetti di loro competenza.

2.3.1 **Denuncia di danno erariale**

Qualora dall'attività di audit emergano fatti che possano dar luogo a responsabilità per danni causati alla finanza pubblica (responsabilità erariale) deve essere presentata denuncia alla Procura Regionale presso la competente Sezione giurisdizionale della Corte dei conti secondo le indicazioni esplicitate nella nota prot. N. PG 9434 del 2.8.2007 "nota interpretativa in materia di denunce di danno erariale ai procuratori regionali presso le Sezioni giurisdizionali regionali della Corte dei Conti". L'obbligo di denuncia sussiste qualora il danno sia concreto e attuale e non quando i fatti abbiano solo una mera potenzialità lesiva. In quest'ultima ipotesi, il dirigente responsabile dell'audit informerà il Direttore Generale dell'obbligo di operare affinché il danno sia evitato e, nel caso si verifichi, dell'obbligo di denunciare il fatto alla Procura erariale.

2.3.2. **Denuncia penale**

Qualora nel corso dell'attività di audit venga acquisita notizia di un reato perseguibile d'ufficio, deve esserne fatta denuncia senza ritardo. La denuncia, redatta dal/i componente/i del gruppo di lavoro che ha/nno preso notizia del reato, è inviata dal responsabile dell'audit al Pubblico ministero o a un Ufficiale di polizia giudiziaria.

3 VALUTAZIONE DEL RISCHIO

3.1. **Il ciclo di Audit**

Il processo legato alle attività della funzione di Internal Audit può essere rappresentato mediante lo schema sotto riportato. Per l'ATS Val Padana il punto di partenza sono le Regole di Sistema, gli obiettivi regionali e quelli aziendali.

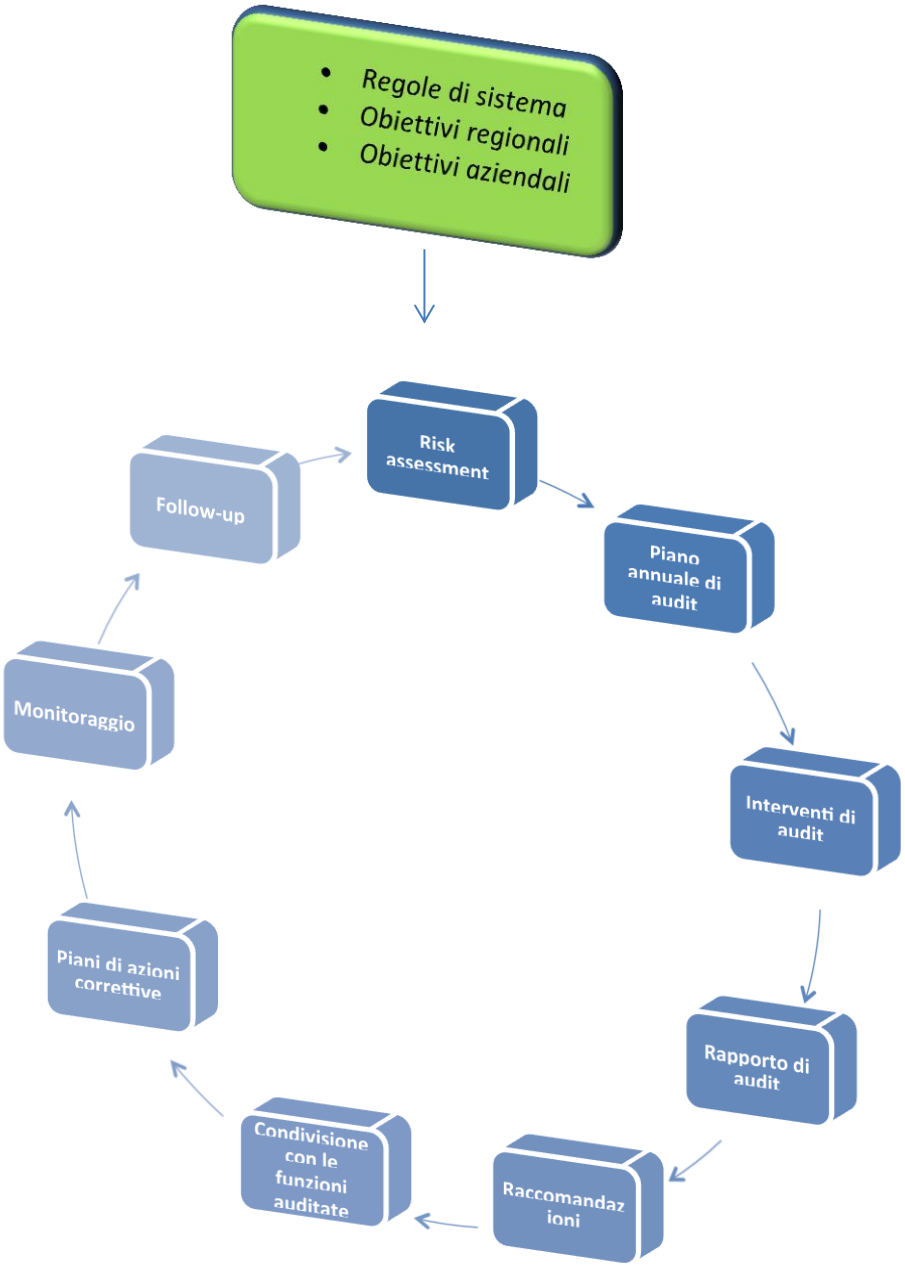


Figura 1 – Il ciclo di audit

3.2 **Il Risk Assessment – La metodologia**

3.2.1 **Definizione e Fasi**

Il Risk Assessment è definito come un processo sistematico di identificazione e valutazione dei rischi, svolto dalla Funzione di Internal Auditing che individua le aree maggiormente esposte a rischio, che potrebbero pregiudicare il raggiungimento degli obiettivi posti dal management.

Il Risk Assessment rappresenta l'attività preliminare alla formazione dei piani pluriennali ed annuali di audit.

L'attività di Risk Assessment sarà svolta dall'ATS Val Padana gradualmente e in progressione.

Le principali fasi in cui si articola il Risk Assessment sono le seguenti:

a) la definizione dell'Universo di Audit;
b) l'identificazione dei rischi dei processi aziendali e la loro valutazione;
c) l'identificazione dei controlli di linea e la loro valutazione;
d) la definizione delle priorità di Audit sulla base del risk scoring (quantificazione del rischio associato a un'attività o all'intero processo);
e) l'elaborazione della relazione di Risk Assessment e condivisione con il management.

3.2.2. **L'universo di Audit**

L'Universo di Audit è costituito da tutti gli obiettivi e le relative azioni attuative identificate dalle regole di Sistema regionali, Obiettivi regionali, obiettivi aziendali, altre attività di Risk Assessment svolte dalle preposte funzioni aziendali.

3.2.3. **Identificazione dei rischi e loro valutazione**

La Funzione di Internal Auditing procede alla definizione dell'elenco dei rischi principali con la relativa valutazione.

Tipologia Rischio	Codice	Descrizione
Rischi strategici	Str	Rischi derivanti dal manifestarsi di eventi che possono condizionare e/o modificare in modo rilevante le strategie e il raggiungimento degli obiettivi dell'Azienda. Possono avere origine esterna ma anche interna.
Rischi di processo	Pro	Rischi connessi alla normale operatività dei processi dell'Azienda, che possono pregiudicare il raggiungimento di obiettivi di efficienza/efficacia, di qualità dei servizi erogati, di salvaguardia del patrimonio pubblico e di conformità normativa.
Rischi di informativa	Inf	Rischi connessi alla possibile inadeguatezza dei flussi informativi interni all'Azienda, che possono impedire una adeguata analisi e valutazione delle diverse problematiche e pregiudicare la correttezza dell'informativa prodotta nonché l'efficacia delle decisioni strategiche e operative.
Rischi di Compliance	Com	Rischi derivanti da eventi che possono comportare un mancato rispetto delle normative esterne ed interne all'Azienda.

Tabella 1 – Macro tipologie di rischio

Generalmente la valutazione dei rischi è effettuata al "lordo" del controllo (rischio inerente), ossia non tenendo conto dell'effetto del controllo di linea realizzato dal responsabile di processo per presidiare quel rischio e ridurne gli impatti negativi sul raggiungimento degli obiettivi.

L'Internal Audit adotta un modello di valutazione dei rischi in termini di probabilità di accadimento e di impatto.

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 probabilità e di impatto, con una valutazione quindi di tipo qualitativo.

Probabilità -> frequenza del manifestarsi del rischio (significativa è l'esperienza e la capacità di giudizio del responsabile di processo e dell'auditor).

VALUTAZIONE DELLA PROBABILITÁ	
QUASI CERTO	È 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.

Tabella 2 – Valutazione della probabilità

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

Anche l'impatto è valutato dal punto di vista qualitativo per ciascun rischio attribuendo le qualifiche di Grave, Significativo, Moderato e Irrilevante secondo il seguente modello.

VALUTAZIONE DELL'IMPATTO	
GRAVE	Impatto rilevante sul raggiungimento degli obiettivi strategici dell'Azienda. 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. 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.

Tabella 3 – Valutazione dell'impatto

La **valutazione complessiva** del rischio in termini di probabilità e impatto viene effettuata utilizzando la seguente matrice:

		Irrilevante	Moderato	Significativo	Grave
		1	2	3	4
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

Figura 3 - Matrice RACM

3.2.4. Valutazione dei controlli di linea

Identificati i rischi occorre individuare e analizzare i controlli, se esistenti, posti in essere dal responsabile di processo e che consentono di attenuare i rischi entro livelli ritenuti accettabili dai responsabili di azioni/processi.

La valutazione del controllo è effettuata in funzione di due aspetti:

- efficacia del controllo nel mitigare il rischio gestito, ossia se il controllo è idoneo ad assicurare il contenimento del rischio nei limiti ritenuti accettabili;
- effettività nello svolgimento del controllo.

L'efficacia dei controlli nel mitigare i rischi è valutata in relazione a ciascun specifico obiettivo di controllo come nella tabella seguente:

Obiettivo	Esempio
Legittimità e regolarità dell'attività	Il controllo in essere garantisce che l'attività sia svolta conformemente ad adeguati percorsi autorizzativi ed alle procedure ed ai dettami giuridici esistenti.
Efficacia dell'attività	Il controllo in essere garantisce che l'attività sia svolta in modo da assicurare il raggiungimento degli obiettivi del processo.
Efficienza dell'attività	Il controllo in essere garantisce che l'attività sia svolta in modo da raggiungere gli obiettivi del processo, nei tempi e con le risorse desiderate.
Correttezza delle operazioni	Il controllo in essere garantisce che le operazioni siano svolte correttamente.
Completezza ed accuratezza delle operazioni	Il controllo in essere garantisce che le operazioni siano svolte completamente e accuratamente.
Tracciabilità delle operazioni	Il controllo in essere garantisce la completezza e la rintracciabilità della documentazione relativa alle transazioni.
Realtà delle operazioni	Il controllo in essere garantisce che le transazioni sono effettivamente realizzate.
Valutazione delle transazioni	Il controllo in essere garantisce che le transazioni sono correttamente valutate.
Imparzialità delle valutazioni	Il controllo in essere garantisce che le valutazioni sono effettuate con imparzialità (indipendenza).
Evidenza del controllo	Il controllo svolto è adeguatamente documentato.

Tabella 4 – Obiettivi dei controlli

La valutazione dei controlli per ciascuno dei rischi gestiti è quindi espressa come nella seguente tabella:

Valutazione del controllo	Descrizione della Valutazione
Sottodimensionato	I controlli previsti non consentono un'efficace riduzione del rischio oppure i controlli previsti non sono effettivamente eseguiti.
Adeguato	I controlli previsti consentono un'efficace riduzione del rischio e sono effettivamente eseguiti.
Sovradimensionato	I controlli previsti sono eseguiti e consentono una riduzione del rischio oltre il livello accettabile in rapporto al loro costo.
Non valutato	Le evidenze disponibili non consentono di valutare l'efficacia e l'effettività dei controlli.

Tabella 5 – Valutazione dei controlli

3.2.5**. Il rischio Residuo**

Dopo la fase di valutazione dei controlli che presidiano i rischi inerenti, si procede alla determinazione del rischio residuo. Il rischio residuo è determinato dal rischio inerente (ossia quello al lordo dei controlli) al netto delle attività di controllo previste o implementate a seguito dell'assessment. Si applica la stessa metodologia di valutazione del rischio lordo a cui pertanto si rinvia.

3.2.6 **L'Universo dei rischi dell'Agenzia**

L'Universo dei rischi dell'ATS Val Padana, utili ai fini della valutazione dei rischi e preliminare alla predisposizione della pianificazione delle attività di Audit è individuato anche attraverso:

- il manuale regionale, che è stato elaborato tenendo conto dei risultati degli audit effettuati, dalle relazioni annuali del Comitato dei Controlli, dai risultati dei controlli operanti a livello centrale della Regione Lombardia e dai macro rischi, opportunamente adattati, che generalmente sono individuati nelle realtà aziendali private approvato con Decreto n. 2822 del 3 aprile 2013;
- le attività di risk assessment già effettuate da altri settori della ATS Val Padana (es. anticorruzione, privacy, salute e sicurezza sul lavoro, ecc.);
- altri rischi eventualmente individuati dal management della ATS nell'ambito dell'attività di Risk Assessment.

L'Universo dei rischi è tenuto ed aggiornato a cura della Funzione Internal Auditing.

Nelle tabelle seguenti sono riportati i rischi o macro rischi che costituiscono, indicativamente, l'Universo dei rischi dell'ATS della Val Padana, ai fini della valutazione dei rischi, preliminare alla predisposizione della pianificazione delle attività di Audit.

RISCHI STATEGICI: ***rischi derivanti dal manifestarsi di eventi che possono condizionare e/o modificare in modo rilevante le strategie ed il raggiungimento degli obiettivi dell'Azienda. Possono avere origini esterne ed interne***	
Fonte esterna	
- Rischio politico	Rischio legato alla manifestazione di situazioni o eventi di natura politica (internazionale, nazionale e regionale) che potrebbero comportare conseguenze negative sull'operatività dell' Azienda; include iniziative ed avvenimenti che potrebbero compromettere la gestione delle attività e l'erogazione dei servizi (e.g. cambiamenti politici, riorganizzazioni politiche, tagli a risorse, dimissioni di figure istituzionali).
- Rischio economico - finanziario	Rischio legato ad avvenimenti nel contesto economico esterno (es. cambiamenti macro-economici, crisi economica-finanziaria,) e all'andamento delle variabili di mercato, che possono incrementare i costi dell'indebitamento dell'Azienda; Essa potrebbe non disporre di adeguati strumenti per monitorare l'andamento del mercato finanziario e delle altre variabili economiche con possibili ripercussioni in termini di errate decisioni strategiche.
- Rischio socio-culturale	Rischio legato all'eventualità che evoluzioni sociali (e.g. cambiamenti demografici, variazioni del tasso di natalità) e/o culturali (e.g. orientamenti educativi, parità di genere, cittadinanza) abbiano un impatto diretto o indiretto alla realizzazione degli obiettivi e strategie del sistema aziendale.
- Rischio tecnologico	Rischio connesso alla possibilità che l' Azienda non colga le opportunità di implementazione delle innovazioni derivanti dall'applicazione di nuove tecnologie disponibili o scelga di utilizzare una tecnologia innovativa che potrebbe non rivelarsi quella più premiante.
- Rischio legislativo	Rischio legato alla necessità di monitorare l'evoluzione normativa, primaria e secondaria (comunitaria e nazionale) che incide per numerosi aspetti sulle regole di esecuzione delle attività e può richiedere significativi aggiornamenti o adeguamenti di carattere operativo.
- Rischio ambientale	Rischio connesso al manifestarsi di eventi incontrollabili (rischio idrogeologico, sismico) oppure al deteriorarsi del contesto ambientale causato dalle attività umane che possano comportare conseguenze rilevanti, danni temporanei e/o permanenti alle strutture ed ai territori con pericolo per la collettività.
- Rischio competitività	Rischio connesso al posizionamento della Azienda rispetto agli altri soggetti istituzionali (regioni, amministrazioni dello Stato, enti locali etc.) con riferimento alla competitività del servizio pubblico / servizio alla collettività erogato dalla Azienda inteso in termini di costi, qualità e tempistiche di erogazione rispetto a quello erogato da altre Aziende o Enti privati.
- Rischio reputazionale	Rischio legato al deterioramento della reputazione propria dell'Azienda intesa come l'insieme di tutte le aspettative, percezioni ed opinioni sviluppate nel tempo nella collettività dove l'Azienda opera, in relazione alla qualità dell'organizzazione e dei servizi erogati, alle caratteristiche e ai comportamenti dei suoi dipendenti e alle osservazioni delle passate azioni dell'organizzazione, ecc.
-Rischio Stakeholder (portatori di interesse)	Rischio legato alla possibilità che le azioni, anche solo di indirizzo, esercitate dai "portatori di interessi" (Governo, Enti, collettività ecc.) che gravitano attorno alla Azienda possano produrre effetti negativi sulle strategie o sulle strutture organizzative, compromettendo il raggiungimento dei suoi obiettivi oppure che le azioni dell'Azienda possano compromettere il suo rapporto con stakeholders significativi ai fini del perseguimento degli obiettivi regionali .
Fonte interna	
- Errata programmazione / pianificazione /ricognizione delle opportunità strategiche	Rischio connesso alla definizione di obiettivi che si rivelino inadeguati, non realizzabili, incoerenti con l'interesse pubblico o non raggiungibili anche a causa di errori o carenze alla base dei processi decisionali alla base di scelte rilevanti e che potrebbe esporre l'Azienda a non cogliere opportunità di tipo strategico.
- Flessibilità strutturale nella gestione dei cambiamenti	Rischio legato all'incapacità da parte della struttura dell'Azienda di reagire con dovuta tempestività ad un eventuale evoluzione del sistema in termini economici, politici, normativi, ecc.
- Disallineamento tra strategie e modello organizzativo	Rischio legato a possibili scelte di tipo organizzativo che potrebbero non consentire la realizzazione di precise strategie o ridurre l'efficacia delle azioni intraprese per mancanza o inadeguatezza delle risorse necessarie (es. la carenza di uno strutturato processo di gestione e controllo potrebbe compromettere l'attività di monitoraggio della programmazione, sia da un punto di vista operativo che finanziario)
- Errata gestione degli investimenti e del patrimonio	Rischio connesso ad una gestione inefficiente / inefficace del patrimonio e degli investimenti, da parte della Azienda. Il rischio rileva anche in caso di errate decisioni in merito alle iniziative di investimento da intraprendere (es. opere di ristrutturazione/rifacimento di strutture dedicate,) con conseguenze di tipo economico per il sistema aziendale.
- Errata definizione del sistema di deleghe e poteri	Rischio connesso a un non adeguato sistema di deleghe e poteri che potrebbe produrre annullamento di provvedimenti sottoscritti da soggetti che non erano "titolati" alla sottoscrizione degli atti o comunque implicare profili di responsabilità per la Azienda.
- Comunicazione non efficace / non tempestiva verso l'esterno	Rischio connesso alla possibilità che errori o carenze alla base dei processi decisionali o delle scelte strategiche, non consentano all'Azienda di cogliere opportunità di tipo strategico.

RISCHI DI PROCESSO: Rischi connessi alla normale operatività dei processi, che possono pregiudicare il raggiungimento di obiettivi di efficienza / efficacia, di qualità dei servizi erogati, di salvaguardia del patrimonio pubblico e di conformità normativa	
RISCHI DI COMPLIANCE: rientrano in questa categoria i rischi di mancata conformità a norme, regole o standard impartiti dal legislatore (comunitario, nazionale e locale), nonché a disposizioni e regolamenti interni alla Regione stessa (istruzioni, procedure etc.).	
- Normativa (comunitaria, nazionale e locale)	Il rischio si configura nella possibilità che vengano compiuti atti contrari alle normative in vigore (comunitarie,nazionali, locali o disposizioni interne) con conseguente esposizione a contenziosi, sanzioni e danni reputazionali.
- Disposizioni interne	Il rischio si configura nella possibilità di prendere decisioni o nel porre in essere azioni contrarie a quanto previsto alle disposizioni interne della Azienda (istruzioni, procedure operative, politiche, indirizzi e linee guida, comunicazioni organizzative ecc.).
- Contrattualistica (inclusi appalti pubblici)	Il rischio si riferisce alla possibilità che vengano commesse irregolarità nell'ambito della gestione degli appalti pubblici (di fornitura, lavori pubblici, servizi, ecc), oppure al mancato rispetto, totale o parziale, di contratti, convenzioni oppure incarichi che regolano i rapporti con soggetti esterni all'Azienda (non rientranti nelle fattispecie normate dal D.Lgs 163/2006), incluse società *in-house, partecipate ed enti regionali* , (ad es. non ottemperanza degli impegni relativi alle modalità e tempistiche di erogazione dei servizi / fornitura di beni, dei pagamenti, omissione di adempimenti contrattuali, ecc).
- Frodi e corruzione	Il rischio è connesso alla possibilità che soggetti esterni o soggetti operanti all'interno della struttura aziendale, agiscano attraverso comportamenti fraudolenti pregiudicando l'attività o i risultati dell' Azienda (il rischio comprende tutte le fattispecie di illecito, inclusa la corruzione soggetta alle specifiche prescrizioni derivanti dal DDL Anticorruzione).
- Trasparenza	Il rischio è connesso alla possibilità che il Sistema aziendale operi non in ottemperanza al principio di trasparenza come metodo della propria azione legislativa e amministrativa e come strumento per consentire l'effettiva partecipazione dei cittadini alle attività dell'Azienda e alla realizzazione delle politiche aziendale.
- Ambiente, salute e sicurezza	Il rischio è connesso alla possibilità che si agisca nel mancato rispetto della normativa da applicarsi sul luogo di lavoro in tema di ambiente, salute e sicurezza.
- Privacy	Il rischio è connesso alla possibilità che si agisca nel mancato rispetto della normativa sulla Privacy.
RISCHI IT: includono i rischi correlati al verificarsi di un insieme di situazioni, interne o esterne, che metterebbero a repentaglio la protezione dell'integrità, della disponibilità, della confidenzialità dell'informazione automatizzata e delle risorse usate per acquisire, memorizzare, elaborare e comunicare tale informazione. Suddette situazioni possono essere causate anche dall'inadeguatezza ed d all'obsolescenza degli strumenti informatici impiegati (hardware) e/o alla scarsa funzionalità dei software, in termini di architettura del sistema, rapidità nei tempi di elaborazione dei dati, facilità di utilizzo, ecc.	
- Integrità e sicurezza dei dati	Il rischio si riferisce all'alterazione, manipolazione e/o perdita dei dati a fronte di elaborazioni errate o non accurate e accessi non autorizzati tali da inficiare la completezza, l'affidabilità, la riservatezza delle informazioni e conseguentemente l'operatività ed i processi decisionali.
- Disponibilità dei sistemi informativi	Il rischio si riferisce all'indisponibilità o inaccessibilità dei dati o dei sistemi informativi con conseguente interruzione dei processi interessati; l'interruzione dei processi critici può comportare significative perdite economiche oppure interruzioni dell'attività e danni di immagine di entità strettamente dipendente dal periodo di indisponibilità dei sistemi informativi a supporto di tali processi.
- Governo, infrastruttura e progetti IT	Il rischio è connesso alla possibilità che: • l'infrastruttura IT (Organizzazione, processi e sistemi) non sia adeguata a supportare le esigenze attuali e future in modo efficiente, economico e ben controllato • la struttura organizzativa dell'IT (funzionale e dimensionale) non sia adeguata a rispondere alle esigenze operative per l'attuazione di tutte le iniziative IT • il Piano delle iniziative IT non sia adeguatamente aggiornato ed allineato con i programmi e le strategie regionali o che i servizi gestiti non siano rispondenti alle esigenze in termini di livelli di servizio e competenze richieste • le attività di manutenzione ordinaria e di modifiche non siano adeguatamente pianificate e/o strutturate. Il rischio è inoltre associato alla possibilità che la gestione dei progetti e iniziative IT (in termini di coordinamento, responsabilità, priorità assegnata, risorse etc.) non sia adeguata, producendo soluzioni non in linea con i tempi, il budget, la qualità e le esigenze del sistema regionale.
RISCHI RISORSE UMANE: I rischi attengono alla gestione delle risorse umane all'interno del sistema regionale nell'ottica di raggiungimento degli obiettivi e riguardano la capacità	

dell'Azienda di disporre di personale adeguato e di processi interni idonei a garantire una corretta gestione e valorizzazione del capitale umano.	
-Competenze	Il rischio è legato alla mancata disponibilità, valorizzazione e/o sviluppo delle necessarie competenze/risorse per lo svolgimento delle attività e la realizzazione degli obiettivi regionali (ivi inclusa la flessibilità e la propensione al cambiamento in caso di processi di radicale trasformazione interna). Tale rischio potrebbe derivare dall'inefficacia dei processi attraverso cui il Gruppo gestisce la selezione, la formazione e la valorizzazione/retention delle risorse/competenze.
-Capitalizzazione delle conoscenze	Il rischio si riferisce ad una possibile situazione di assenza o inadeguata "condivisione" ed "accessibilità" delle informazioni e della conoscenza, con conseguenti problematiche in termini di preparazione del personale e progressivo "depauperamento" del capitale intellettuale. Tale rischio si rileva anche in situazioni dove non è assicurato un adeguato grado di sostituibilità delle risorse chiave, che in caso di fuoruscita non consentono di trasferire il know-how all'interno del sistema.
- Leadership	Il rischio è legato alla possibilità che gli organi direzionali e i vertici non riescano a trasmettere all'interno dell'organizzazione la propria autorevolezza per poter condurre la struttura aziendale al raggiungimento di obiettivi comuni e condivisi.
- Deleghe e procure	Il rischio è attinente alla possibile mancanza di un sistema chiaro e strutturato di deleghe e procure che potrebbe indurre i dipendenti a compiere atti non autorizzati e ad assumere responsabilità inadeguate rispetto al ruolo ricoperto.
- Performance e sistemi premianti	Il rischio deriva dalla possibile presenza di sistemi di misurazione e valutazione delle performance non oggettive (es. obiettivi qualitativi non misurabili), non coerenti con gli obiettivi perseguiti oppure inadeguate e non allineate e ai requisiti normativi (i.e. D.Lgs. 150/09) e agli standard delle altre realtà regionali, anche con riferimento ai livelli intermedi, con conseguenze che possono impattare anche su una non adeguata pianificazione delle carriere e influire sulla motivazione del personale.
- Comportamenti etici	Il rischio deriva da una mancanza o scarsa sensibilità dell'organizzazione nello stimolare e valorizzare comportamenti etici e responsabili
- Abuso di potere/conflitto d'interesse	Il rischio deriva dalla possibilità che venga fatto utilizzo del potere in modo eccessivo, ingiusto (o in estrema ratio, illegale), al di fuori dei limiti circoscritti e conferiti per lo svolgimento di una mansione, al fine di trarne dei vantaggi propri o per conto di terzi.
- Organizzazione e adeguata ripartizione dei compiti	Il rischio è connesso alla possibilità che l'organizzazione preveda una sproporzionata distribuzione dei carichi di lavoro nonché una ripartizione dei compiti non coerente con le competenze, il background e le aspettative professionali dei dipendenti.
- Comunicazione	Il rischio è connesso al possibile utilizzo di mezzi e modalità di comunicazione inefficaci, sia interna che esterna (es. mancanza definizione di regole e ambiti dei flussi informativi, comunicazione interna orizzontale

ALTRI RISCHI OPERATIVI: ***rientrano in questa famiglia tutte le categorie di rischio connesse allo svolgimento delle attività e dei processi "tipici" del sistema, ,non già ricomprese nelle precedenti categorie.***	
- Qualità del servizio	Il rischio si riferisce alla possibilità che i processi interni non presidino adeguatamente la qualità delle attività svolte dei servizi erogati , con conseguenti ripercussioni in termini di servizi non in linea con gli standard necessari e conseguenti danni alla reputazione e all'immagine del sistema aziendale.
- Misurazione della soddisfazione	Il rischio si riferisce alla possibilità che l'Azienda non sia in grado di misurare adeguatamente i bisogni e le aspettative dei cittadini e dei diversi stakeholder, in termini di soddisfazione per i servizi erogati, e conseguentemente di rispondere tempestivamente e in modo adeguato alle esigenze della collettività.
- Gestione provider esterni, incarichi, acquisti, contratti di servizio	Il rischio si riferisce alla possibilità che i servizi resi dagli outsourcer/ fornitori di servizi/società e enti che operano internamente o esternamente al sistema regionale, non siano in linea con le aspettative, le esigenze, gli standard e gli obblighi definiti contrattualmente, e/o il controllo e monitoraggio dell'Azienda sulle attività servizio affidate a terzi risulti inefficace / inefficiente. Il rischio rileva anche in caso di errate decisioni in merito alle valutazioni di economicità delle scelte operate.
- Gestione delle vertenze legali	Il rischio si riferisce alla possibilità che i processi interni di gestione delle vertenze e controversie legali non siano adeguatamente presidiati e gestiti, con conseguenti ripercussioni in termini di possibili maggiori costi sostenuti, situazioni di possibile soccombenza con ricadute di natura reputazionale .
- Gestione delle autorizzazioni e accreditamenti	Il rischio si riferisce alla possibilità che i soggetti accreditati / autorizzati non rispondano ai requisiti previsti oppure non risultino performanti nella gestione delle risorse attribuite, con conseguenze in termini di mancato raggiungimento degli obiettivi, gestione e/o attribuzione non ottimale delle risorse.
- Gestione ed erogazione contributi	Il rischio si riferisce alla possibilità che i processi interni di gestione, erogazione e rendicontazione dei contributi (bandi, convenzioni, sponsorizzazioni, patrocini, doti, voucher, erogazioni liberali ecc) non siano adeguatamente presidiati e gestiti, con conseguenze in termini di mancato raggiungimento degli obiettivi della programmazione, gestione e attribuzione non ottimale delle risorse disponibili
- Gestione contributi di funzionamento	Il rischio si riferisce alla possibilità che i processi interni di gestione ed erogazione dei contributi di funzionamento (intesi come contributi non determinati né da atti bilaterali, né da istanze di terzi) non siano adeguatamente presidiati e gestiti, con conseguenze in termini di mancato raggiungimento degli obiettivi della programmazione, gestione e attribuzione non ottimale delle risorse disponibili .
- Gestione programmazione negoziata	Il rischio si riferisce alla possibilità che i programmi e gli accordi negoziati non siano adeguatamente presidiati e gestiti, con conseguenze in termini di mancato raggiungimento degli obiettivi della programmazione, gestione e attribuzione non ottimale delle risorse disponibili
- Gestione riscossioni	Il rischio si riferisce alla possibilità che i processi interni e/o esternalizzati di gestione delle riscossioni non siano adeguatamente presidiati e gestiti, con possibili conseguenze in termini di perdita di risorse e/o maggiori oneri da sostenere per il sistema aziendale.
- Gestione trasferimenti	Il rischio si riferisce alla possibilità che i processi interni di gestione e controllo dei trasferimenti delle risorse non siano adeguatamente presidiati, con possibili conseguenze in termini di mancato raggiungimento degli obiettivi e gestione non ottimizzata delle risorse (es. fondo sanitario, fondo trasporti, fondo formazione disabili, ecc).
RISCHI DI INFORMATIVA: ***Rischi connessi alla possibile inadeguatezza dei flussi informativi interni, che possono impedire una adeguata analisi e valutazione delle diverse problematiche e pregiudicare la correttezza dell'informativa prodotta nonché l'efficacia delle decisioni strategiche e operative***	
RISCHI DI REPORTING E COMUNICAZIONE: ***includono i rischi che impattano direttamente i contenuti dell'informativa interna, che in qualche modo si riveli non adeguata in termini qualità, completezza, correttezza per la presa di decisioni consapevoli da parte del management, nonché per fornire idonea rendicontazione dell'attività svolta.***	
- Informativa strategica / programmazione	Il rischio è connesso alla carenza o mancanza di informazioni del contesto interno e/o esterno di riferimento necessarie alla formulazione e al disegno della programmazione strategica ed in generale al corretto funzionamento dei processi direzionali. Il manifestarsi di questo rischio potrebbe privare i vertici del necessario quadro d'insieme per procedere a decisioni consapevoli nell'ambito della definizione degli obiettivi strategici o nell'ambito della pianificazione operativa.
- Informativa economico - finanziaria	Il rischio è correlato alla possibilità che l'informativa economico-finanziaria (e.g. bilancio di esercizio e relativi allegati, reporting, prospetti entrate e spese) non sia in linea con i principi contabili di riferimento, oppure includa errori e/o omissioni di fatti significativi e rilevanti.
- Informativa interna ed esterna	Il rischio è connesso alla possibilità che i flussi informativi intercorrenti sia internamente al sistema aziendale sia esternamente (e.g. tra Azienda e Regione e organi dello Stato), non vengano correttamente gestiti in termini di modalità e contenuti, con possibili impatti sull'efficacia/efficienza dei processi interni e/o sulla conformità normativa.
- Misurazione delle performance	Il rischio si riferisce alla potenziale inadeguatezza e inaffidabilità delle informazioni per la misurazione delle performance dei servizi erogati. Tale carenza informativa può precludere al management la possibilità di effettuare le necessarie valutazioni per migliorare i servizi erogati dalla Azienda nonché di fornire un'adeguata informativa agli stakeholders.
- Valutazione del sistema di controllo interno	Il rischio si riferisce alla possibilità che la struttura aziendale non abbia le informazioni necessarie, in termini di qualità e completezza, per consentire un'adeguata analisi e valutazione del proprio sistema di controllo interno. Tale rischio si traduce nella difficoltà (incapacità o impossibilità), del sistema aziendale di accorgersi dei profili di criticità del sistema di controllo interno e di introdurre tempestive azioni correttive ove necessario.

Tabella 6–Universo dei rischi

4 PIANIFICAZIONE DELLE ATTIVITÁ DI AUDIT

Le attività di audit sono pianificate sulla base dei rischi prioritari individuati con il Risk -Assessment. L'attività di Risk Assessment sarà svolta gradualmente, sinergicamente alle aree a rischio individuate dalla L.190/2012 e da altre attività di Risk Assessment svolte nell'ambito dell'ASL.

4.1 **Pianificazione triennale**

Dall'anno 2017 le attività di audit saranno pianificate su base triennale.

La Pianificazione triennale di Audit evidenzia l'ordine, sulla base dei rischi prioritari, delle attività di audit da svolgersi in ciascuno degli anni del triennio di pianificazione.

La Pianificazione triennale delle attività di Audit è approvata con delibera del Direttore Generale entro il 31 gennaio di ogni anno ed è aggiornata annualmente, sulla base degli esiti dell'attività di audit svolta nell'anno precedente e dell'eventuale aggiornamento della valutazione dei rischi.

4.2 **Piano annuale di Audit**

Il Piano Annuale di Audit definisce le azioni e/o procedure che saranno verificate nell'anno e individua i correlati centri responsabilità. Il Piano prevede anche le risorse da destinarsi all'effettuazione di attività di indagine non programmabili da effettuarsi in corso d'anno sulla base di formale mandato.

All'interno del Piano vengono specificate le seguenti informazioni per ogni Audit programmato:

- ✓ Azione/Procedura oggetto dell'audit;
- ✓ Struttura auditata;
- ✓ Ambito dell'audit;
- ✓ Obiettivo dell'intervento
- ✓ Crono - programma delle attività.

Il Piano di Audit deve essere predisposto entro il 31 gennaio di ogni anno e gli interventi in esso previsti fanno riferimento all'anno solare.

Il Piano è approvato con delibera del Direttore Generale sulla base delle proposte del responsabile della funzione di audit ed eventualmente integrato da richieste pervenute da parte degli organi aziendali e di controllo dell'ASL (Direttore Generale, Collegio Sindacale, Nucleo di Valutazione, Responsabile anticorruzione, ecc.) o dalla Regione Lombardia.

Eventuali modifiche significative e rilevanti apportate in corso d'anno dovranno essere approvate con le stesse modalità previste per l'approvazione del piano annuale.

4.3 **Programmazione operativa**

Il Responsabile della funzione di Auditing predispone e aggiorna la programmazione operativa delle attività ed individua:

- risorse dedicate all'esecuzione dei singoli audit;
- nominativi dei responsabili e/o referenti per le singole aree auditate;
- data di inizio e conclusione;
- crono – programma delle attività di ciascuna risorsa.

La programmazione operativa e i suoi aggiornamenti sono comunicati ai collaboratori in riunioni da convocarsi da parte del Responsabile.

5 PROCEDURA DI AUDIT

5.1 **Le fasi di un intervento di audit**

L'incarico di Audit si svolge attraverso le seguenti fasi:

- ✓ programmazione operativa dell'intervento di audit;
- ✓ analisi preliminare;
- ✓ esecuzione del lavoro sul campo;
- ✓ reporting e comunicazione dei risultati.

5.1.1. **Programmazione operativa dell'intervento di audit**

Nella fase di programmazione vengono dettagliati gli obiettivi e le operazioni da eseguire per il singolo intervento di Audit.

La programmazione è volta alla definizione di dettaglio di:

- ✓ obiettivi dell'intervento di Audit;
- ✓ ambito di copertura dell'Audit, ovvero: confini temporali che l'analisi deve coprire, processi e procedure da esaminare, caratteristiche del campione da sottoporre a test;
- ✓ calendario dei lavoro, risorse e definizione del Team di Audit.

Se il perseguimento degli obiettivi dell'audit lo richiede, l'intervento potrà essere esteso a azioni/procedure collegate a quella per il quale l'intervento è stato programmato.

5.1.2 **Notifica dell'intervento di audit**

L'avvio di un'attività di audit deve essere sempre comunicato in forma scritta al soggetto auditato e in copia per conoscenza alla Direzione Strategica.

Preliminarmente alla notifica potrà essere stabilita per le vie brevi una data condivisa per l'incontro di apertura dei lavori e potrà essere anticipata la lista delle informazioni da ottenere.

La notifica deve avere luogo di norma 10 giorni lavorativi prima dell'inizio effettivo delle attività sul campo, salvo casi eccezionali.

La comunicazione d'avvio delle attività di audit deve indicativamente prevedere:

- ✓ Obiettivi dell'attività di Audit
- ✓ Durata ipotizzata del lavoro;
- ✓ Nominativi degli auditor assegnati all'incarico;
- ✓ Per il soggetto auditato, richiesta della nomina di un referente che fungerà da interfaccia con gli auditor;
- ✓ Ipotesi di una data per la realizzazione dell'incontro di apertura ("kick off meeting");
- ✓ Eventuale richiesta di documentazione.

La notifica viene inviata dal Responsabile della Funzione di Audit ai responsabili apicali dell'azione/procedura oggetto di audit e, per conoscenza, alla Direzione Strategica.

La risposta dovrà pervenire nei termini fissati dalla notifica.

5.1.3 **Analisi preliminare**

In fase di analisi preliminare il team di internal auditing deve raccogliere ed analizzare la documentazione necessaria alla comprensione e/o approfondimento dei rischi e dei controlli esistenti nell'ambito del processo oggetto di audit (ad esempio normativa di riferimento, procedure, regolamenti, organigramma, ecc.).

Il team di Internal Auditing deve conseguire una piena comprensione delle attività chiave associate a ciascun processo al fine di assicurare che tutti i rischi siano adeguatamente ed efficacemente identificati. Deve, inoltre, comprendere in che modo ciascun processo influisca sul conseguimento degli

obiettivi della Direzione.

Nella fase di analisi dei processi, gli auditor analizzano la correttezza delle procedure e l'efficacia dei controlli posti a presidio dei rischi inerenti.

L'analisi preliminare deve prevedere lo studio della normativa e delle regole di funzionamento dell'azione/procedura, dell'organizzazione e delle risorse applicate/ impiegate dai responsabili dell'azione o procedura.

Lo studio raccoglie gli elementi di base costituiti da procedure, organizzazione, budget, dotazione di risorse umane e tecnologiche, stato di attuazione dell'azione/procedura.

Gli strumenti di rilevazione utilizzati anche in combinazione tra loro nel corso dell'analisi del processo possono essere:

- ✓ Documentali: risultanti da documentazione prodotta nel corso del processo;
- ✓ Testimoniali: si tratta di informazioni raccolte tramite meeting, interviste o questionari da persone coinvolte nelle varie attività che costituiscono il processo;
- ✓ Analitici: frutto di calcoli e deduzioni effettuate autonomamente dall'auditor;
- ✓ On site: derivano dall'osservazione diretta delle attività svolte dai soggetti auditati.

Nel caso in cui l'attività di analisi del processo avvenga sotto forma di intervista o meeting, gli auditor provvedono a formalizzare il contenuto della stessa in un documento che costituirà carta di lavoro del processo di audit.

L'analisi di processo può essere formalizzata attraverso due metodologie distinte:

- Flowchart: strumento di formalizzazione in forma grafica e sintetica del processo;
- Narrative: strumento di formalizzazione in forma analitica e descrittiva del processo.

La documentazione del processo dovrà:

- ✓ rappresentare sinteticamente il processo nella sua interezza, delineando la sequenza degli eventi/attività;
- ✓ aiutare a chiarire i ruoli e le responsabilità all'interno del processo;
- ✓ fornire indicazioni sui flussi informativi;
- ✓ permettere una facile identificazione dei rischi e controlli associati (o delle carenze degli stessi);
- ✓ aiutare ad identificare punti di debolezza oppure opportunità di miglioramento del processo.

Tali metodologie di documentazione possono essere utilizzate separatamente o in combinazione tra loro.

Studio del processo: L'analisi preliminare deve prevedere lo studio della normativa e delle regole di funzionamento dell'azione/procedura, dell'organizzazione e delle risorse applicate/impiegate dai responsabili dell'azione o procedura.

La ricerca di ulteriori informazioni preliminari di interesse per lo svolgimento dell'audit potrà riguardare:

- documentazione relativa a eventuali precedenti audit: raccomandazioni, referti della Corte dei Conti, Autorità di Vigilanza, Ministeri, altre Autorità di audit, Società di revisione esterna;
- correttivi predisposti dal management della Struttura auditata rispetto a criticità evidenziate in audit precedenti;
- rapporti delle società di certificazione e accreditamento;
- letteratura tecnica concernente l'attività da esaminare;
- l'analisi dei dati di monitoraggio dell'azione/procedura per individuare gli scostamenti tra risultati conseguiti e obiettivi programmati e le anomalie segnalate dall'emergere di andamenti

incongruenti tra le diverse grandezze monitorate (es: scostamento tra le spese rendicontate e le spese approvate, scostamenti frequenti dei risultati delle operazioni rispetto agli obiettivi previsti).

Lo studio raccoglie gli elementi di base costituiti da Procedure, organizzazione, budget, dotazione di risorse umane e tecnologiche, stato di attuazione dell'azione/procedura.

Sulla base dello studio preliminare viene aggiornata la Risk and Control Matrix dell'azione/procedura.

Definizione delle informazioni da richiedere: Il team di audit assegnato al singolo intervento predispone una lista delle informazioni da richiedere ove non siano accessibili attraverso le basi informative disponibili, riferite all'intervento in esecuzione, quali:

- le procedure in essere, eventualmente la documentazione esaminata non risulti esaustiva;
- i flowchart organizzativi, se disponibili;
- stato di attuazione delle azioni / procedure;
- stato di attuazione dei controlli;
- manuali o comunque documentazione inerente ai sistemi informativi in uso;
- strumenti utilizzati per il controllo (checklist, procedure informatizzate, pianificazione, altro).

Tale lista deve essere inviata di norma contestualmente alla lettera di comunicazione dell'inizio dell'attività e presentare il seguente contenuto:

- indicazione della documentazione da ottenere e del supporto sul quale possibilmente ottenerla (supporto cartaceo o elettronico);
- termine entro il quale ottenere la documentazione;
- referente auditor della Funzione Internal Auditing cui inviare la documentazione e/o da contattare per eventuali chiarimenti.

L'auditor incaricato predispone, quindi, una lista per il controllo della ricezione dei documenti richiesti, che aggiornerà in relazione alla documentazione ricevuta.

Entro tre giorni dalla scadenza del termine per l'invio della documentazione l'auditor incaricato contatta, anche in modo informale, il soggetto auditato per verificare lo status dell'invio ed analizzare possibili difficoltà nell'invio della documentazione.

5.1.4. **Lavoro sul campo**

La fase di svolgimento del lavoro sul campo consiste nell'acquisizione delle evidenze necessarie per pervenire a conclusioni fondate relativamente all'efficacia dei controlli di processo.

5.1.4.1 **Strumenti**

L'esecuzione del lavoro sul campo si avvale dei seguenti strumenti.

1. **Interviste**

I responsabili possono essere intervistati con l'ausilio di una lista di controllo predefinita che tenga conto delle conoscenze acquisite nella fase di lavoro preliminare per chiarire i punti dubbi. Le interviste con i Responsabili sono effettuate nella forma di interviste "aperte", senza prevedere un percorso rigido e risposte predefinite. Nel corso dell'intervista dovranno essere esaminati tutti i punti previsti dall'estensione dell'incarico e rientranti nelle competenze del Management.

2. **Workshop**

Per raccogliere i punti di vista dei responsabili e dei funzionari che partecipano in posizione chiave all'attuazione dell'azione/procedura può darsi luogo a workshop organizzati in maniera collegiale.

3. **Questionari a risposta aperta**

Per richiedere informazioni strutturate sul processo in esame possono essere sottoposti ai responsabili dei controlli chiave questionari a risposta aperta relativi al funzionamento delle varie fasi del processo.

4. **Questionari a risposta chiusa**

La raccolta di informazioni e valutazioni di un numero maggiore di partecipanti al processo può essere effettuata a mezzo di questionari, della cui distribuzione sarà data informazione al responsabile della Struttura auditata.

5. **Test di funzionamento**

I test di funzionamento sono predisposti per verificare la conformità e l'efficacia delle procedure adottate rispetto alle procedure e agli obiettivi di controllo formalizzati in tutte le fasi di esecuzione delle operazioni che sono soggette a audit.

I test di funzionamento sono effettuati sulla base di un campione rappresentativo di transazioni selezionate con metodologia statistica oppure sulla base di criteri volti a selezionare le operazioni maggiormente esposte a rischio.

5.1.4.2. **Riunione di apertura dell'Audit**

La riunione di apertura ("kick off meeting") sancisce l'inizio delle attività operative di audit.

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.

A tale riunione partecipano:

- il responsabile apicale del soggetto auditato;
- i collaboratori della Struttura auditata individuati dal Responsabile come referenti;
- il responsabile della funzione di audit oppure persona delegata e gli Internal auditor assegnati all'intervento.

In tale contesto potranno essere esaminate:

- le procedure di verifica (analisi di processo e testing) che saranno effettuate nel corso dell'audit;
- i ruoli e la suddivisione dei compiti all'interno del team di Internal Auditing, nel caso siano coinvolti più auditor nell'intervento di audit;
- la richiesta di informazioni specifiche non contenute nella lista di documentazione inviata con la lettera d'avvio dell'attività;
- gli aspetti logistici della conduzione dell'audit;
- le modalità di accesso a luoghi, documenti e sistemi informatici;
- il processo di comunicazione previsto nel corso dell'audit (tempi e persone incaricate di condividere il lavoro svolto);
- le aree considerate critiche dal management;
- i tempi di lavoro (inclusa una prima proposta di un piano interviste);
- eventuali ulteriori argomenti di particolare interesse dell'auditor;
- l'identificazione nominativa dei referenti del processo o della procedura auditata.

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, che viene sottoposto per mail al responsabile dell'azione/procedura, il quale può osservare e integrare quanto verbalizzato. Il verbale deve essere archiviato nella forma risultante a seguito delle osservazioni e integrazioni del responsabile dell'azione/procedura.

Per approfondire aspetti particolari dell'azione/procedura si potranno tenere ulteriori incontri tra il team di audit e il gruppo di lavoro della struttura auditata. I lavori potranno svolgersi anche con la sola partecipazione di collaboratori dell'IA e referenti della struttura auditata e saranno verbalizzati con le stesse modalità previste per l'incontro di apertura.

5.1.5**. Reporting e comunicazione dei risultati**

Conclusa la fase di esecuzione dell'audit sul campo, il team di audit predispone un rapporto preliminare.
Il rapporto preliminare riassume le constatazioni formulate in fase di analisi di processo e di testing e documentate all'interno dei singoli issue sheet sulla base delle evidenze raccolte.
Il rapporto preliminare di Audit viene inviato al responsabile della Struttura auditata e viene esaminato nel corso di un incontro di chiusura (exit meeting).

5.1.5.1**. Exit meeting**

Le constatazioni contenute nel rapporto preliminare sono discusse dal team di audit e dal responsabile e referenti della Struttura auditata in un exit meeting da svolgersi entro i termini previsti dal Programma di Audit condiviso con il soggetto auditato e comunque non oltre 10 giorni lavorativi dall'invio del rapporto preliminare.
L'incontro è volto a valutare l'importanza delle non conformità rilevate nel corso dell'audit in relazione agli obiettivi programmati per l'azione e le misure necessarie per conseguire un livello accettabile di rischio delle operazioni.
In caso di mancata condivisione di uno o più aspetti del Rapporto, il punto di vista della Struttura auditata dovrà essere documentato nel rapporto definitivo.
In sostituzione dell'exit meeting potrà essere svolto contraddittorio in forma scritta se la complessità degli aspetti controversi lo richiede oppure ancora nel caso risulti impossibile tenere tempestivamente l'exit meeting.
In caso di contraddittorio scritto il responsabile della Struttura auditata farà pervenire le proprie osservazioni entro 10 giorni lavorativi dal ricevimento del rapporto preliminare.

5.1.5.2**. Rapporto definitivo e comunicazione dei risultati**

Dopo la condivisione con le strutture auditate, viene intrapresa la stesura del Rapporto di Audit definitivo.
Il Rapporto di Audit deve essere predisposto ed inviato entro i termini concordati con il soggetto auditato in fase di pianificazione dell'intervento di audit e non oltre 20 giorni lavorativi dall'exit meeting.
Il Rapporto di Audit descrive lo scopo, l'ampiezza ed i risultati dell'audit, evidenzia i rilievi, le conclusioni e le raccomandazioni formulate a seguito del lavoro e riporta l'opinione del responsabile dell'audit sul sistema di gestione e controllo dell'azione/procedura.
Il Rapporto deve contenere almeno le seguenti informazioni:

- ✓ la data dell'audit ed il periodo di tempo coperto dall'audit;
- ✓ l'identificazione dell'attività e del settore d'intervento sottoposti ad auditing;
- ✓ elenco dei partecipanti ai lavori;
- ✓ gli obiettivi ed i criteri rispetto ai quali è stato condotto l'audit;
- ✓ i documenti di riferimento per l'audit;
- ✓ l'esito dei test di funzionamento effettuati;
- ✓ i rischi rilevati e gli adeguamenti raccomandati;

- ✓ il Piano d'azione.

La Struttura del Rapporto di Audit finale è formata dalle seguenti sezioni:

- ✓ executive summary;
- ✓ obiettivo e ambito audit;
- ✓ contesto e informazioni di fondo;
- ✓ metodologia di svolgimento dei lavori;
- ✓ aree di migliormamento;
- ✓ piano d'azione;
- ✓ allegati.

All'occorrenza, alcune sezioni possono essere accorpate o diversamente denominate, fermi restando i contenuti di seguito indicati.

Executive Summary

L'executive summary è una sintesi delle conclusioni raggiunte, predisposta per il Management di vertice degli organismi auditati, allo scopo di fornire le informazioni rilevanti per l'elaborazione e il monitoraggio delle azioni correttive.

L'executive summary contiene:

- ✓ l'opinione sull'efficacia del Sistema di Gestione e Controllo esaminato;
- ✓ le principali osservazioni in ordine di importanza dei rischi rilevati;
- ✓ le raccomandazioni correlate;
- ✓ gli aspetti principali della posizione del responsabile della Struttura auditata se divergente dalle conclusioni del rapporto.

Obiettivi e portata/ambito audit

In questa sezione devono essere indicati gli obiettivi specifici dell'audit, gli ambiti di rischio maggiormente rilevanti e le procedure e/o operazioni e/o processi che sono stati esaminati.

Contesto e informazioni di fondo

Questa sezione ha lo scopo di informare i responsabili ai vari livelli del soggetto auditato relativamente ai seguenti aspetti:

- ✓ materialità delle operazioni esaminate;
- ✓ esiti dell'analisi dei rischi preliminare;
- ✓ esiti delle eventuali missioni di audit effettuate precedentemente dall'Internal Auditing oppure da altri organismi di controllo comunitari e nazionali;
- ✓ esiti dei controlli sulle operazioni

Metodologia di svolgimento lavori

In questa sezione devono essere illustrate le modalità con cui è stato effettuato l'audit con riferimento a:

- ✓ criteri di valutazione adottati;
- ✓ documentazione esaminata;
- ✓ riunioni e /o interviste effettuate;
- ✓ test di funzionamento svolti.

Aree di miglioramento

In questa parte del rapporto sono riportate le carenze del sistema di gestione e controllo, evidenziando la deviazione del suo funzionamento rispetto ai criteri adottati, l'impatto in termini di errori conseguenti alla deviazione riscontrata e l'azione da intraprendere per adeguare il sistema allo standard individuato, secondo il seguente schema:

- ✓ standard
- ✓ scostamento
- ✓ impatto
- ✓ azione correttiva
- ✓ osservazioni del responsabile della Struttura auditata se divergente dalle conclusioni relative a ciascuna constatazione.

Piano d'azione

Il piano d'azione riporta in forma sinottica i seguenti elementi:

- ✓ sintesi delle osservazioni;
- ✓ descrizione delle azioni correttive;
- ✓ responsabile dell'esecuzione dell'azione;
- ✓ data limite prevista per il completamento oppure posizione del responsabile della Struttura auditata se in dissenso con i correttivi indicati;
- ✓ priorità di esecuzione dell'azione.

Le osservazioni e/o obiezioni avanzate in sede di exit meeting relativamente al Piano di Azione sono integrate nel Rapporto finale di Audit.

Il rapporto di audit riporta anche l'evidenza di un'eventuale non condivisione delle azioni correttive da parte del Management che si assume la responsabilità di non presidiare il rischio rilevato.

Occorre, tuttavia, tenere presente che:

- ✓ l'accettazione del rischio deve sempre risultare dalla documentazione dell'audit;
- ✓ il rischio può essere accettato solo da chi è effettivamente responsabile delle eventuali conseguenze.

Nel caso in cui l'attività di audit si discosti significativamente dalle indicazioni degli Standard IIA, è opportuno che si riportino, in calce allo stesso documento, gli Standard IIA che non sono stati rispettati, le motivazioni dello scostamento e le conseguenze di tale condotta sull'attività

Le osservazioni e/o obiezioni avanzate in sede di exit meeting relativamente al Piano di Azione sono integrate nel Rapporto finale di Audit.

Il rapporto di audit riporta anche l'evidenza di un'eventuale non condivisione delle azioni correttive da parte del Management che si assume la responsabilità di non presidiare il rischio rilevato.

Occorre, tuttavia, tenere presente che:

- l'accettazione del rischio deve sempre risultare dalla documentazione dell'audit;
- il rischio può essere accettato solo da chi è effettivamente responsabile delle eventuali conseguenze.

Il Responsabile della Funzione Internal Auditing trasmette il Rapporto di audit al Management auditato e alla Direzione Strategica.

In caso di errori e/o omissioni significative nella comunicazione, sarà cura del Responsabile della Funzione Internal Auditing segnalare la rettifica agli stessi soggetti destinatari dell'invio del Rapporto di Audit.

6. FOLLOW-UP

Il follow-up è il processo di monitoraggio e verifica dell'esecuzione delle azioni correttive contenute nel Piano d'azione.
Spetta al Responsabile dell'Internal Auditing definire natura, grado di approfondimento e tempistica del follow-up, in funzione:

- ✓ della significatività dei rilievi riscontrati;
- ✓ dell'importanza delle conseguenze;
- ✓ del periodo di tempo richiesto.

A seconda della rilevanza delle eccezioni riscontrate:

- ✓ per le azioni di bassa priorità oppure da attuarsi in relazione al verificarsi di nuove iniziative, il follow-up potrà rientrare in un successivo incarico di audit sulla stessa area/materia;
- ✓ per le azioni di priorità media e alta, il follow-up deve essere programmato tempestivamente alla scadenza dei termini previsti nel Piano di Azione. In tale circostanza, l'attività di follow-up viene inclusa nel Piano Annuale di Audit.

6.1 **Monitoraggio del piano d'azione**

Il monitoraggio del piano d'azione avviene sulla base delle informazioni fornite periodicamente dal Management, secondo le scadenze stabile nel rapporto di audit.
In caso di azioni correttive da eseguirsi con l'adozione di procedure, la produzione di reportistica e l'aggiornamento dello stato di attuazione dell'azione/procedura lo stato di attuazione della raccomandazione può essere definito sulle base delle informazioni ricevute.

6.2 **Missione di follow-up**

Se le informazioni fornite dal Management non sono sufficienti per determinare lo stato di attuazione della raccomandazione, sarà programmata una missione di follow-up per verificare le azioni effettivamente intraprese dal Management.
Per organizzare la missione di follow-up si procede mediante:

- ✓ Comunicazione, con almeno 15 giorni lavorativi di anticipo dalla data dell'incontro;
- ✓ Acquisizione della documentazione relativa alle azioni correttive intraprese dal Management;
- ✓ Esame della documentazione acquisita e richiesta di eventuali integrazioni.

Durante la missione di follow-up il responsabile dell'Internal Auditing verifica con il Management l'efficacia delle azioni correttive, adottate a seguito dell'audit e redige uno specifico verbale.
Il responsabile dell'Internal Auditing sulla base della valutazione professionale dell'auditor decide se effettuare un nuovo ciclo di test e la tipologia stessa dei test da effettuare.
Nel caso in cui l'azione correttiva concordata nel Piano di Azione non sia stata eseguita è necessario valutare se il rischio non sussista più o si sia ridotto a causa di altri fattori. Qualora il rischio permanga nella misura iniziale, è necessario farne menzione nel Rapporto di follow-up.

Al termine della missione si redige il Rapporto di follow-up che elenca i rilievi contenuti nel Rapporto di Audit, le azioni correttive poste in essere e i miglioramenti raggiunti, in termini di efficacia, dei controlli effettuati.
Nel caso in cui sussistano dei rischi non ancora mitigati il Rapporto di follow-up riporta le motivazioni, propone nuove azioni correttive ed una nuova data di esecuzione di un nuovo follow-up.
Il Rapporto di follow-up deve essere indirizzato alle stesse persone a cui è stato indirizzato il Rapporto finale di Audit.

6.3 **Risultati di follow-up**
Nel Rapporto di follow-up, il livello di attuazione delle azioni correttive deve essere compendiato in:

1. **Azione attuata**
Sono state attuate le azioni previste per mitigare il rischio in modo efficace o sono state intraprese azioni anche differenti da quelle consigliate che hanno tuttavia raggiunto il medesimo obiettivo di gestione del rischio.

2. **Azione parzialmente attuata**
Le azioni previste per mitigare il rischio in modo efficace sono in corso, ma non ancora completate. Si rende pertanto necessaria l'effettuazione di un successivo intervento di follow-up di verifica.

3. **Azione non attuata**
Le azioni consigliate non sono state implementate. Il rischio, pertanto, non è ridotto entro un livello accettabile.

4. **Azione non più applicabile**
Un cambiamento di scenario rende le nostre raccomandazioni non più applicabili in quanto il rischio precedentemente evidenziato non è più esistente.

6.4. **Tabella di monitoraggio del Piano d'azione**
La tabella di monitoraggio riproduce il Piano d'azione e ne aggiorna lo stato di attuazione sulla base delle informazioni ricevute e dei risultati delle missioni di follow – up.

7 ARCHIVIAZIONE DELLA DOCUMENTAZIONE DI AUDIT

7.1. **Archivio cartaceo**

Il Responsabile dell'Audit raccoglie e conserva le comunicazioni e la documentazione da e verso l'esterno e la documentazione ad uso interno (Manuale operativo, Piano annuale di audit, fascicoli degli audit, ecc.). Il materiale viene fascicolato e custodito all'interno di appositi spazi.
La documentazione è custodita per i 5 anni successivi all'anno di riferimento.

La gestione e conservazione dell'archivio cartaceo è in carico al team di audit con la collaborazione del personale di segreteria.

7.1.1 **Archivio degli interventi di audit**

Per ciascun intervento di audit, viene creato un fascicolo allo scopo di raccogliere e ordinare le evidenze che documentano le attività di pianificazione e di controllo, le informazioni raccolte e le conclusioni cui si è pervenuti.

Il fascicolo viene individuato da un codice, lo stesso che lo contraddistingue all'interno del Piano annuale di audit. Tale codice è il riferimento che consente di identificare tutta la documentazione prodotta o ricevuta nel corso dell'intervento. Pertanto, il suddetto codice viene riportato, oltre che sul fascicolo, anche su tutte le carte in esso archiviate.

Al fine di facilitarne la gestione, in testa al fascicolo viene inserito un sommario, indicante i documenti in esso contenuti.

Gli elementi essenziali da allegare al fascicolo dell'intervento di audit sono:

- ✓ la lettera di pianificazione dell'intervento;
- ✓ le carte di lavoro firmate e referenziate dagli auditor;
- ✓ la corrispondenza e le comunicazioni intercorse con i soggetti auditati;
- ✓ il rapporto di audit.

L'archiviazione cartacea della documentazione può seguire le seguenti specifiche:

A - Pianificazione

- **A 10** - Corrispondenza
- **A 20** - Procedure
- **A 30** - Normativa
- **A 40** - Verbali riunioni preliminari
- **A 50** - kick off meeting
- **A 60** - Matrice e check list

B - Esecuzione

- **B 10** - Corrispondenza
- **B 20** - Campionamento
- **B 30** - Test

C - Reportistica

- **C 10** - Corrispondenza
- **C 20** - Draft report
- **C 30** - Final report
- **C 40** - Exit meeting

7.2 **L'archivio informatico e il Sistema Informativo di Audit**

L'archivio informatico è organizzato in sezioni o cartelle, secondo la seguente architettura:

- ✓ Manuale e carte di lavoro, che contiene il Manuale della Funzione di Internal Auditing (con le sue successive revisioni) e i modelli della documentazione operativa necessaria a supportare lo svolgimento dell'attività di audit;
- ✓ Normativa, con un archivio dei testi aggiornati delle principali normative di riferimento;
- ✓ Mappe dei processi e dei rischi, comprensive degli aggiornamenti e delle correzioni apportate;
- ✓ Pianificazione, con la documentazione e le informazioni inerenti alla programmazione delle attività per ciascun anno;
- ✓ Interventi (per anno di attività), contenente tutta la documentazione prodotta nel corso degli audit effettuati, raccolta in cartelle identificate con il codice assegnato nel Piano annuale a ciascun intervento, quali: lettera di pianificazione e programma di lavoro, rapporto finale;
- ✓ Follow-up (per anno di attività), con le osservazioni effettuate, che, se ancora aperte, vengono riportate nella tavola dell'anno successivo, per essere oggetto di specifici "ri-controlli".

L'archivio informatico è accessibile esclusivamente al personale dell'internal auditing. La gestione e l'aggiornamento delle sezioni/cartelle sono a cura dei soli funzionari incaricati, con il supporto della segreteria.

ALLEGATO 1 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.

- I Principi, fondamentali per la professione e la pratica dell'internal auditing.
- 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 documento 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:

- 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: 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 conoscenze 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 auditù

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 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.

L'attività di internal audit può raccogliere le informazioni necessarie per questa valutazione attraverso molteplici incarichi.
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 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
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 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 comunicazione 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 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.
Gli internal auditor possono indicare che i loro incarichi sono "effettuati in conformità agli Standard Internazionali per la Pratica

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.
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.

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)
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
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 Struttura to 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 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.

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 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.

ALLEGATO 2–MODULISTICA

LETTERA DI NOTIFICA AVVIO AUDIT

(su carta intestata della Funzione)

Oggetto : Piano di Audit 20__ -codice Audit __.__.__ –Avvio attività di verifica ….
Nell'ambito delle attività programmate dal Piano di Audit 20__ (approvato con decreto del _ _____ 20__ n. ____), è prevista l'effettuazione di un intervento di audit sul processo di _____di cui alla _____.
L'obiettivo dell'intervento è quello di verificare la conformità del processo alla normativa di riferimento e la verifica dell'efficacia dei controlli.
Per l'esame di quanto sopra indicato si conferma l'incontro per _____ dalle___ alle____ per una durata di __ circa.
Durante l'incontro i lavori seguiranno il seguente programma:
□□15 minuti per l'esposizione del programma di lavoro;
□□1 ora e 30 minuti per l'esame dei controlli sul processo;
□□……
□□….

All'incontro parteciperanno anche i miei collaboratori incaricati dell'intervento di audit: _____

Preliminarmente all'incontro si prega di far pervenire, entro 10 giorni dalla data della presente, alla scrivente Struttura la seguente documentazione:
1) ……
2)…….
3)……..
Durante l'incontro, si richiede inoltre, la presenza di vostri collaboratori al fine rendere disponibili i fascicoli relativi alle domande di cui si renda eventualmente necessario l'esame.
Cordiali saluti.

Il Responsabile

Data

Sistema Socio Sanitario
Regione Lombardia
ATS Val Padana

Piano delle attività Internal Auditing

Piano delle attività di audit

ATS della Val Padana

-anno 2016-

Piano delle attività Internal Auditing

Premessa

A seguito della riforma sanitaria regionale di cui alla L.R. 23/2015, con D.G.R. n. X/4470 del 10/12/2015 è stata costituita l'Agenzia di Tutela della Salute (ATS) della Val Padana, con effetto dal 1/01/2016, derivante dalla fusione dell'ASL di Mantova e dell'ASL di Cremona. In conseguenza del riassetto degli ambiti territoriali ed organizzativi e il passaggio di alcune funzioni alle ASST territoriali di riferimento, si è reso opportuno rivedere, con il presente atto, la struttura e la programmazione per l'anno 2016 dell'attività di controllo interno svolta dall'Internal Auditing.

Finalità e modalità

Il Piano degli audit per l'anno 2016 è stato predisposto tenendo conto delle seguenti finalità:

- rispondere alle aspettative del *management* in termini di mitigazione dei rischi delle attività e dei processi;
- verificare l'efficacia del sistema dei controlli e la conformità delle procedure e dei processi alla normativa di riferimento;
- accertare, attraverso interventi di *follow-up,* l'effettiva implementazione delle eventuali raccomandazioni e degli eventuali piani d'azione relativi agli audit effettuati.

Le attività di audit verranno svolte nel rispetto dei principi contenuti nel Codice Etico IIA (Institute of Internal Auditors), conformemente agli Standard Internazionali Professionali di Indipendenza, Obiettività, Riservatezza e Competenza. Gli interventi di audit, come previsto nel Manuale di Internal Auditing, si articolano nelle seguenti fasi:

1. programmazione operativa (definizione obiettivi e calendario del lavoro);
2. analisi preliminare (studio della documentazione, somministrazione di questionari agli operatori del sistema, analisi *flowchart*, procedure e punti di controllo, analisi dei dati sulle operazioni, analisi dei dati relativi ad eventuali controlli, analisi dei dati di risposta ai questionari, ecc.);
3. riunione di avvio *(kick–off meeting:* apertura formale dell'intervento, acquisizione documentazione e informazioni utili);
4. *reporting* (stesura rapporto di audit in versione di bozza, fase di condivisione del documento, stesura rapporto audit finale condiviso, rilascio definitivo documento);
5. riunione di chiusura dell'audit (*exit meeting*);
6. eventuale *follow-up.*

Contenuti, criteri di selezione e scelte operative

Gli interventi di audit da effettuare nel corso del 2016, tenute presenti le finalità sopra enunciate, sono stati selezionati unendo i Piani attività 2016 delle due disciolte Aziende ed escludendo i controlli su ambiti di attività transitati alle ASST di riferimento territoriale.

In particolare, gli ambiti da sottoporre ad audit erano stati individuati principalmente sulla base:

- della percezione dei rischi;
- della normativa di riferimento (in particolare l'approfondimento "Sanità" allegato al Piano Nazionale Anticorruzione, aggiornamento 2015);
- dell'analisi dei rischi compiuta, secondo la metodologia prevista nel Piano Nazionale Anticorruzione, sui processi individuati all'interno del "Piano Triennale Prevenzione Corruzione 2016-2018".

Date le premesse, i processi da sottoporre a controllo per l'anno 2016, tenuto conto delle varie tipologie di rischio (strategico, di processo, di informativa, di compliance), sono i seguenti.

➢ ***Attività autorizzativa e vigilanza strutture farmaceutiche –sede territoriale di Cremona***

Il rischio si configura nella possibilità che vengano compiuti interventi non in linea con la normativa in vigore (nazionale, regionale o disposizioni interne), con conseguente esposizione a contenziosi, sanzioni e danni reputazionali. A ciò si aggiunge il rischio di agire nel mancato rispetto della normativa sulla privacy e ai principi di trasparenza e conflitto di interessi.
Inoltre è presente il rischio connesso alla possibilità che soggetti esterni o soggetti operanti all'interno della struttura aziendale agiscano attraverso comportamenti fraudolenti pregiudicando l'attività o i risultati
Verrà valutata l'efficacia, l'appropriatezza ed uniformità dell'attività autorizzativa e di vigilanza, nonché il rispetto della procedura sanzionatoria.
Sarà sottoposto ad audit l'UOD Autorizzazioni e Vigilanza Strutture Farmaceutiche (attività autorizzativa e vigilanza sulle strutture farmaceutiche della sede territoriale di Cremona).

➢ ***Controlli ufficiali nel settore veterinario – sede territoriale di Cremona***

Il rischio si configura nella possibilità che vengano compiuti interventi non in linea con la normativa in vigore (comunitaria, nazionale, regionale o disposizioni interne), con conseguente esposizione a contenziosi, sanzioni e danni reputazionali. A ciò si aggiunge il rischio di agire nel mancato rispetto della normativa sulla privacy e ai principi di trasparenza e conflitto di interessi.
Inoltre è presente il rischio connesso alla possibilità che soggetti esterni o soggetti operanti all'interno della struttura aziendale, agiscano attraverso comportamenti fraudolenti pregiudicando l'attività o i risultati.
Verrà valutata l'efficacia, l'appropriatezza ed uniformità delle attività di controllo ufficiale nell'ambito veterinario, nonché il rispetto della procedura sanzionatoria.
Sarà sottoposto ad audit il Dipartimento Prevenzione Veterinario, della sede territoriale di Cremona, che svolge al suo interno attività di controllo ufficiale secondo le direttive comunitarie, nazionali e regionali.

➢ ***Appalto di lavori per ristrutturazione palazzina sede territoriale di Mantova***

L'area dei contratti pubblici rientra nelle aree di rischio "generali" in ambito sanitario (vedi anche determinazione ANAC n. 12/2015). L'affidamento dell'appalto di lavori per ristrutturare la palazzina n. 8 della sede territoriale di Mantova rende necessaria una valutazione della correttezza e trasparenza delle diverse fasi del processo di affidamento dei lavori con particolare attenzione alla fase dell'esecuzione del contratto con verifica dei tempi e delle modalità di esecuzione del contratto. La presente scelta è legata alla individuazione dell'attività dei contratti pubblici tra quelle ad alto rischio di corruzione.
Sarà sottoposto ad audit l'area economico patrimoniale – Settore patrimonio e ambienti - della sede territoriale di Mantova, responsabile dell'affidamento dei lavori per la ristrutturazione della palazzina n. 8.

Interventi e pianificazione

Gli interventi di audit della ATS della Val Padana per l'anno 2016 sono sintetizzati nella seguente tabella.

Codice audit	Ambito	Motivazione
01.16	**Attività autorizzativa e vigilanza sulle strutture farmaceutiche- sede territoriale di Cremona-** Verifica: • efficacia, appropriatezza e uniformità dell'attività autorizzativa e di controllo svolta sul territorio; • rischio connesso alla possibilità che si agisca nel mancato rispetto della normativa sulla privacy e al principio di trasparenza; • gestione delle non conformità che determinano l'irrogazione di sanzioni amministrative (procedura sanzionatoria).	Possibili rischi: - compimento di atti non in linea con le normative in vigore, con conseguente esposizione a contenziosi, sanzioni e danni reputazionali; - mancato rispetto della normativa sulla privacy e dei principi di trasparenza e conflitto di interessi; - comportamenti fraudolenti da parte di soggetti esterni o soggetti operanti all'interno della struttura aziendale

Codice audit	Ambito	Motivazione
02.16	**Esecuzione dei controlli ufficiali rispetto a quanto stabilito dal Reg. CE 882/2004 che fissa le regole generali – sede territoriale di Cremona** Verifica: • efficacia, appropriatezza e uniformità dell'attività di controllo svolta sul territorio; • rischio connesso alla possibilità che si agisca nel mancato rispetto della normativa sulla privacy e al principio di trasparenza; • gestione delle non conformità che determinano l'irrogazione di sanzioni amministrative (procedura sanzionatoria).	Possibili rischi: - compimento di atti non in linea con le normative in vigore, con conseguente esposizione a contenziosi, sanzioni e danni reputazionali; - mancato rispetto della normativa sulla privacy e dei principi di trasparenza e conflitto di interessi; - comportamenti fraudolenti da parte di soggetti esterni o soggetti operanti all'interno della struttura aziendale

Codice audit	Ambito	Motivazione
03.16	***Appalto di lavori per ristrutturazione palazzina sede territoriale di Mantova*** Verifica: • adempimenti in tema di trasparenza • corretta esecuzione di quanto previsto relativamente alle diverse fasi del processo di affidamento lavori • efficacia delle procedure di monitoraggio e controllo relative all'esecuzione del contratto • efficacia delle procedure di rendicontazione del contratto • controllo sulla applicazione di eventuali penali in caso di ritardo nell' esecuzione del contratto.	Possibili rischi: - compimento di atti non in linea con le normative in vigore, con conseguente esposizione a contenziosi e danni reputazionali; - mancato rispetto della normativa sulla privacy e dei principi di trasparenza e conflitto di interessi Le verifiche verranno effettuate sulle diverse fasi del processo di affidamento dei lavori con particolare attenzione alla fase dell'esecuzione del contratto con verifica dei tempi e delle modalità di esecuzione del contratto.

Le attività di audit previste dal Piano potranno essere ampliate ove, nell'esecuzione di uno degli incarichi programmati, emerga la necessità di esaminare aspetti inerenti ad azioni e procedure non incluse nell'incarico in corso.
Inoltre il presente Piano prevede l'effettuazione, eventuale, delle seguenti attività:

1. Formazione professionale degli internal auditor;
2. Attività di Risk Assessment;
3. Richieste specifiche da parte del Responsabile della prevenzione della corruzione;
4. Richieste da parte della Regione Lombardia;
5. Richieste da parte delle Direzioni.

Modifiche/Integrazioni

Il Piano potrà essere variato ed integrato sulla base di nuove rilevazioni dei rischi e in base allo stato di avanzamento delle azioni o di eventuali esigenze di carattere straordinario.
Il presente Piano inoltre potrà subire modifiche per effetto delle variazioni organizzative di cui alla Riforma Sanitaria prevista dalla L.R. 23/2015 e per l'adozione del Piano Organizzativo Aziendale Strategico.
Gli eventuali scostamenti rispetto al presente Piano saranno comunque giustificati in fase di Relazione Consuntiva Annuale.

Risorse

Le risorse a disposizione per la realizzazione del Piano di audit 2016 sono le seguenti:
Responsabile della Funzione di Internal Audit per circa 300 ore;
Collaborazione di varie professionalità aziendali in relazione alla specificità dell'area da auditare per un impegno da quantificare al bisogno.

Cronoprogramma e ore dedicate

Codice audit	GEN	FEB	MAR	APR	MAG	GIU	LUG	AGO	SET	OTT	NOV	DIC
01.16												
02.16												
03.16												
Formazione												
Risk Assessment												
Richieste specifiche												

*****