MANUALE INTERNAL AUDIT

P.A.C. COMPLIANT

(approvato con Determina n. 671ASURDG del 21/11/2019)

Indice

1. INTRODUZIONE

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

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

Il suo scopo è quello di supportare l'organizzazione nel perseguimento dei propri obiettivi attraverso un approccio sistematico volto a identificare, monitorare e migliorare il sistema di gestione dei rischi.

Il presente Regolamento descrive i principi, le procedure, le metodologie, le fasi e gli strumenti di lavoro utilizzati dalla funzione di Internal Auditing dell'ASUR Marche nell'attività di auditing sui processi operativi aziendali;

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

2. ATTORI E COMPITI DELLA FUNZIONE DI INTERNAL AUDITING

La funzione di Internal auditing è presidiata da un Referente aziendale nominato dal Direttore Generale tra Dirigenti/Funzionari afferenti al suo staff.

Il referente IA individua, per ciascun audit previsto dal Piano di Audit, i componenti del Gruppo le cui competenze professionali sono maggiormente attinenti al processo oggetto di audit, costituendo di volta in volta il Gruppo di audit.

Il Gruppo di Audit è composto dal Referente della funzione e da 3 componenti scelti tra i Direttori/Dirigenti delle Aree Dipartimentali dell'ATL/Aree di Coordinamento Sanitario e Socio Sanitario o Direttori/Dirigenti delle Strutture di Area Vasta ove ne ravvisi la necessità.

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

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

Alla funzione di Internal Auditing compete:

- predisporre il piano annuale di audit e stendere insieme al Gruppo di lavoro di volta in volta costituito il rapporto di audit
- assistere la Direzione nel valutare il funzionamento del sistema dei controlli e delle

procedure operative

- pianificare l'attività di audit
- coadiuvare i responsabili delle strutture auditate nella mappatura ed identificazione degli ambiti soggetti a rischio e nell'individuazione di modifiche organizzative tali da mitigare il livello di rischio;
- eseguire gli audit programmati e l'esecuzione dei follow-up
- provvedere agli aggiornamenti del Regolamento di Audit qualora necessari

3. IL SISTEMA DI CONTROLLO INTERNO E DI GESTIONE DEI RISCHI

Il sistema di controllo interno e di gestione dei rischi (in breve "sistema di controllo interno" o "SCI") è costituito dall'insieme delle regole, delle procedure e delle strutture organizzative adottate dall'ASUR per il raggiungimento degli obiettivi aziendali, quali l'attendibilità dell'informativa economico- finanziaria, l'efficacia e l'efficienza della gestione ed il rispetto della normativa applicabile al settore in cui opera l'Ente.

Il sistema di controllo interno e gestione dei rischi è strutturato per consentire l'identificazione, la misurazione, la gestione e il monitoraggio dei principali rischi. Tale sistema è integrato nei più generali assetti organizzativi e di governo adottati dall'Ente e tiene in adeguata considerazione i modelli di riferimento previsti dal PAC (Percorso attuativo di Certificabilità).

I pilastri su cui si fonda il SCI dell'ASUR sono cosi schematizzati:

Obiettivi	Principi	Componenti
▪ Salvaguardia del patrimonio aziendale; ▪ conformità a leggi e regolamenti; ▪ attendibilità informazioni; ▪ efficacia ed efficienza operazioni gestionali.	▪ Separazione dei ruoli; ▪ *accountability*; ▪ oggettivazione delle scelte; ▪ tracciabilità delle informazioni;	▪ Ambiente di controllo; ▪ valutazione del rischio; ▪ attività di controllo; ▪ informazione e comunicazione; ▪ monitoraggio;

Nei paragrafi successivi si descrivono i significati degli Obiettivi, Principi e Componenti del sistema di controllo.

3.1. Gli obiettivi del sistema di controllo interno

Nella tabella che segue sono riepilogati gli obiettivi del SCI dell'ASUR

	Il sistema di controllo interno dell'ASUR è strutturato per

Salvaguardia del patrimonio aziendale	raggiungere l'obiettivo di salvaguardare il patrimonio aziendale nelle sue diverse configurazioni, ovvero: ▪ patrimonio tangibile: beni materiali (es. immobilizzazioni, disponibilità finanziaria, ecc.); ▪ patrimonio intangibile: beni immateriali (es. *know-how*, reputazione aziendale, ecc.).
Conformità a leggi e regolamenti	Il sistema di controllo interno è strutturato per raggiungere l'obiettivo di garantire che le azioni svolte siano conformi alle leggi e regolamenti, ovvero: ▪ conformità esterna a leggi, normative e regolamenti; ▪ conformità interna a politiche, procedure e istruzioni aziendali.
Attendibilità informazioni	Il sistema di controllo interno è strutturato per raggiungere l'obiettivo di garantire che le informazioni siano attendibili quando esse si riferiscono a: ▪ informazioni economico patrimoniale (annuali e/o periodiche) verso l'esterno; ▪ informazioni gestionali e operative verso l'interno.
Efficacia ed efficienza delle operazioni aziendali	Il sistema di controllo interno è strutturato per raggiungere l'obiettivo di garantire che le operazioni aziendali siano improntate in maniera **Efficace** (raggiungimento degli obiettivi aziendali nello svolgimento delle operazioni) ed **Efficiente** (miglior rapporto costi / benefici nell'impiego delle risorse aziendali).

3.2. I principi del sistema di controllo interno

Nella tabella che segue sono riepilogati i principi del SCI dell'ASUR

Separazione dei ruoli	ASUR, attraverso le procedure e prassi adottate, garantisce che un intero processo non è mai gestito in autonomia da una sola persona. Le procedure prevedono sempre che esecuzione e controllo siano adeguatamente separate. Nei casi in cui la separazione non è possibile si alza il livello di supervisione e di monitoraggio delle operazioni ad opera della funzione IA.
Accountability	Le procedure aziendali e le prassi adottate garantiscono che l'attività e le decisioni sono riconducibili alla responsabilità di un determinato soggetto individuato in modo specifico.
Oggettivazione delle scelte	Le procedure aziendali e le prassi adottate garantiscono che le decisioni derivanti da valutazioni siano il più possibile razionali e oggettive. Il processo decisionale è sempre motivato e condiviso con i soggetti interessati nel rispetto delle norme, regolamenti e procedure interne formalizzate.

Tracciabilità delle informazioni	Le procedure aziendali e le prassi adottate garantiscono che le scelte siano sempre formalizzate e quindi tracciabili. Tutte le operazioni aziendali sono adeguatamente documentate. Il sistema informatico garantisce anche la tracciabilità delle operazioni e la relativa archiviazione.

3.3. Le componenti del sistema di controllo interno

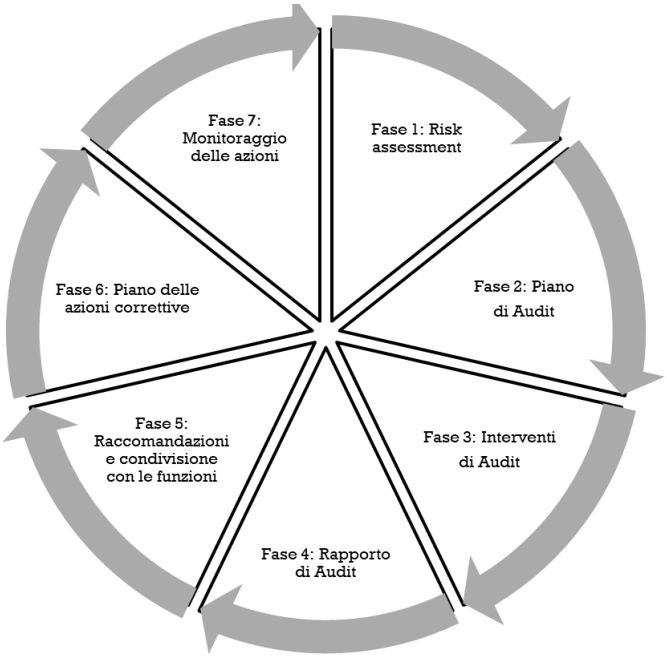
Nella tabella che segue si identificano gli elementi che formano il sistema di controllo interno dell'ASUR.

Ambiente di Controllo	L'ambiente di controllo, inteso quale l'insieme di valori, competenze, stile di direzione, assegnazione di autorità, risorse in campo, ecc. Si realizza attraverso i principi, le linee guida e l'organizzazione dell'ASUR, che costituiscono le fondamenta di tutti gli altri componenti del controllo interno e determina il livello di sensibilità del personale alla necessità di controllo.
Valutazione del Rischio	La valutazione del rischio è una attività volta a garantire la realizzazione di obiettivi e procedure attuative aziendali attraverso l'individuazione e l'analisi dei fattori che possono pregiudicare il raggiungimento degli stessi obiettivi. La valutazione del rischio ha il fine di determinare come questi rischi dovranno essere gestiti.
Attività di Controllo	Le attività di controllo sono quelle attività volte ad individuare ed analizzare i fattori che possono pregiudicare il raggiungimento degli obiettivi. L'ASUR svolge le attività di controllo attraverso l'applicazione di politiche e delle procedure per i principali processi, oppure prassi, che garantiscono al *management* che le sue direttive siano attuate.
Monitoraggio	Il monitoraggio è una attività volta ad assicurare che il sistema di controllo interno sia sempre aggiornato e adatto alle dimensioni della azienda. Il monitoraggio è svolto attraverso l'attività di supervisione continua, in valutazioni periodiche oppure combinazione dei due metodi ed attraverso la valutazione delle *performance* dei sistemi di controllo.
Informazione e comunicazione	L'informazione e comunicazione è un'attività di diffusione delle informazioni di natura contabile, sull'attività operativa e sull'ambiente in cui opera l'Azienda. Tale attività è svolta attraverso la predisposizione di canali informativi aziendali che consentano l'adempimento delle proprie responsabilità e che producano rapporti contenenti dati operativi, contabili e relativi al rispetto degli obblighi legali e regolamentari, che permettono di gestire e controllare l'attività aziendale.

4. IL CICLO DI AUDIT E LA VALUTAZIONE DEL RISCHIO

4.1. Il ciclo di Audit dell'ASUR

Il ciclo di *Audit* opera mediante una funzionalità circolare. Lo stesso prende avvio dalla analisi dei rischi e termina con il monitoraggio delle azioni. Lo schema tipo del processo funzionale del ciclo di *Audit* si può così rappresentare:



4.2. Il Risk Assessment

Il *Risk Assessment* è il processo sistematico di identificazione e valutazione dei rischi, svolto dalla funzione di *Internal audit* che individua le aree maggiormente esposte a rischio. L'identificazione delle aree critiche costituisce l'azione preliminare all'avvio dell'attività nella quale viene analizzata la struttura organizzativa aziendale ed individuate le aree per le quali è opportuno condurre l'attività di risk-assessment propedeutica alla definizione del Piano annuale di Audit.

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

a) l'identificazione dei rischi dei processi aziendali e la loro valutazione;
b) l'identificazione dei controlli operativi e la loro valutazione;
c) la definizione del piano di *audit* sulla base del *risk scoring*;
d) formalizzazione in una relazione del processo seguito.

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

Tra le principali fonti interne ed esterne che si elencano a titolo esemplificativo e non esaustivo si indicano:

- Verbali del Collegio Sindacale
- Esiti verifiche ispettive;
- Rilievi del MEF;
- Rilievi dell'ANAC;
- Valutazione strumenti di monitoraggio Performance Aziendale (es. Obiettivi di budget)
- Verbali del Collegio di Direzione;
- Confronto con l'Ufficio Legale;
- Piano Triennale Anticorruzione;
- Confronto con il Responsabile Anticorruzione aziendale;
- Richiesta di informative da parte della Corte dei Conti, del Ministero, della Regione;
- Ufficio Relazioni con il Pubblico.

4.2.1. Identificazione dei Rischi

Il Referente dell'*Internal audit* procede con il supporto di ciascuna Struttura/Ufficio aziendale alla definizione dell'elenco dei rischi principali con la relativa valutazione. Generalmente la valutazione dei rischi è effettuata al "**lordo**" del controllo ovvero si valuta il rischio inerente e, quindi, non si tiene 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. Nell'ambito della propria azione l'IA dell'ASUR si troverà ad analizzare le seguenti macro tipologie di rischio:

Tipologia di Rischio	Descrizione
Rischi Strategici	Rischi derivanti dal manifestarsi di eventi che possono condizionare e/o modificare in modo rilevante le strategie e il raggiungimento degli obiettivi dell'ASUR. Possono avere origine esterna ma anche interna.
Rischi di Processo	Rischi connessi alla normale operatività dei processi dell'Ente, che possono pregiudicare il raggiungimento di obiettivi di efficienza/efficacia, di salvaguardia del patrimonio e di conformità normativa.

Rischi di informativa	Rischi connessi alla possibile inadeguatezza dei flussi informativi interni e verso l'esterno, 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.
Rischio di Compliance	Rischi derivanti dalla applicazione della normativa di riferimento e/o procedure PAC in termini di errata applicazione o di mancata conoscenza delle stesse, che, ove emergenti, pregiudicano il raggiungimento degli obiettivi dell'ASUR.

4.2.2. Metodologia di valutazione dei Rischi

La funzione IA adotta un modello di valutazione dei rischi in termini di probabilità di accadimento e di impatto. Lo strumento metodologico adottato dall'ASUR, 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.

(P) PROBABILITÀ (*) DI ACCADIMENTO		
RATING	**PROBABILITÀ**	**DESCRIZIONE**
1	**Impossibile**	Evento negativo mai o raramente verificatosi o verificabile (≤ 5 %)
2	**Improbabile**	Evento negativo che si può generare solo in particolari circostanze ad oggi inesistenti per la tipologia di attività svolta (≤ 25%)
3	**Possibile**	Evento che si è verificato in realtà analoghe e che potrebbe presentarsi anche nell'ASUR come conseguenza di particolari circostanze (≤ 60%)
4	**Probabile**	Evento negativo che si è verificato nell'ASUR, seppur raramente, e tale da influenzarne lo svolgimento delle attività (≤ 80%)
5	**Molto Probabile**	Evento negativo quasi certo generato anche da circostanze routinarie e già verificatosi nell'Ente (> 80%)

(*) Probabilità: è la frequenza del manifestarsi del rischio (significativa è l'esperienza e la capacità di giudizio del responsabile di processo e dell'*audit*or).

IMPATTO (**)		
RATING	**IMPATTO**	**DESCRIZIONE**
1	**Immateriale**	Conseguenze praticamente nulle sull'attività e sugli obiettivi
2	**Basso**	Conseguenze minime che non generano una priorità di intervento
3	**Medio**	Conseguenze che influenzano l'efficiente conduzione dell'attività e in

		quanto tali meritevoli di considerazione
4	**Alto**	Conseguenze rilevanti sull'efficienza e adeguatezza dell'attività e che potrebbero comportare modifiche anche di strategie aziendali
5	**Elevato - Significativo**	Conseguenze pericolose per la continuità dell'attività e in quanto tali il presidio deve essere prioritario e costante

(**) Impatto: livello in cui il manifestarsi del rischio potrebbe influenzare il raggiungimento delle strategie e degli obiettivi.

La valutazione complessiva del rischio in termini di probabilità e impatto viene effettuata utilizzando la seguente matrice, moltiplicano il *rating* assegnato all'impatto per quello assegnato alla probabilità.

RACM (Risk Assessment Criteria Matrix)			**IMPATTO**				
			1	**2**	**3**	**4**	**5**
			Immateriale	**Basso**	**Medio**	**Alto**	**Pericoloso**
PROBABILITÀ	**5**	**Molto Probabile**	**5**	**10**	**15**	**20**	**25**
	4	**Probabile**	**4**	**8**	**12**	**16**	**20**
	3	**Possibile**	**3**	**6**	**9**	**12**	**15**
	2	**Improbabile**	**2**	**4**	**6**	**8**	**10**
	1	**Impossibile**	**1**	**2**	**3**	**4**	**5**

Definendo i dati di probabilità ed impatto si ottiene la misurazione del **RISCHIO INERENTE**, ovvero del rischio che non tiene conto delle azioni di controllo.

MISURAZIONE DEL LIVELLO DI RISCHIO INERENTE		
RATING	**RISCHIO INERENTE**	**DESCRIZIONE**
1	**Remoto**	Rischio inerente non rilevante
2 ≤ 5	**Basso**	Rischio inerente esiguo per il quale le azioni di mitigazione non sono una priorità
5,01 ≤ 11	**Medio**	Rischio inerente meritevole di considerazione per il quale è opportuno attivare una risposta al rischio stesso
11,01 ≤ 18	**Alto**	Rischio inerente elevato per il quale è necessario attivare un costante presidio e una efficiente risposta
≥18,01	**Elevato**	Rischio inerente massimo per il quale è indispensabile una risposta efficiente, tempestiva, costante e immediata

4.2.3. Identificazione dei controlli operativi e loro valutazione

Prima di definire il piano di *Audit* e completare l'*iter* previsto del *Risk Assessment* la funzione *Internal*

audit deve valutare i controlli esistenti a presidio dei rischi inerenti identificati. La valutazione delle attività di controllo esistenti a presidio dei rischi devono anche tenere conto delle propensioni al rischio dei referenti. La valutazione è espressa in termini di assorbimento del rischio inerente ossia quanto l'attività/azioni di controllo in essere e la propensione al rischio riescono a mitigare/coprire i rischi stessi.

VALUTAZIONE DEL CONTROLLO ESISTENTE			
RATING	**CONTROLLO**	**RISCHIO RESIDUO**	**DESCRIZIONE**
1	**Adeguato**	10%	Attività di controllo efficiente e adeguata (% di assorbimento del rischio 90%)
2	**Parzialmente Adeguato**	30%	Attività di controllo efficiente ma ottimizzabile (% di assorbimento del rischio 70%)
3	**Debole**	60%	Attività di controllo non sufficiente (% di assorbimento del rischio 40%)
4	**Critico**	80%	Attività di controllo non efficace (% di assorbimento del rischio 20%)
5	**Non adeguato**	100%	Attività di controllo inesistente (% di assorbimento del rischio 0%)

La tabella che segue sintetizza la fase finale di valutazione del rischio inerente dopo la valutazione dei controlli. Il rischio residuo è calcolato attraverso la media delle valutazioni ponderate dei rischi inerenti con i relativi controlli esistenti che mitigano (assorbono) il rischio. Nella valutazione del rischio è considerata anche la percezione dello stesso (propensione al rischio) definita per ciascun *owner* di processo individuato nelle procedure PAC.

MISURAZIONE DEL LIVELLO DI RISCHIO INERENTE RESIDUO		
RATING	**RISCHIO INERENTE**	**DESCRIZIONE**
0 ≤ 1,5	**Remoto**	Rischio residuo trascurabile grazie ad un sistema di controllo efficace e a una irrilevante percezione dello stesso
1,51 ≤ 5	**Basso**	Rischio residuo esiguo grazie alle attività di controllo poste in essere. La percezione del rischio è irrilevante
5,01 ≤ 11	**Medio**	Rischio residuo meritevole di considerazione e percepito come un pericolo per il business. Le attività di controllo non riescono a ridurne l'impatto
11,01 ≤ 18,99	**Alto**	Rischio residuo elevato e percepito in modo significativo e per il quale le attività di controllo non risultano essere sufficienti
≥19	**Elevato (Significativo)**	Rischio residuo massimo percepito come una minaccia per il business e per il quale le attività di controllo risultano essere insufficienti

4.2.4. Definizione delle priorità di Audit sulla base del risk scoring

La funzione IA opera sulla base delle risorse di cui dispone, con la finalità di presidiare i rischi elevati,

ovvero quei rischi che rappresentano una minaccia al raggiungimento degli obiettivi. Verranno anche presidiate le attività ed i processi PAC che presentano dapprima i rischi elevanti, poi quelli alti, medi e così via, sempre nel rispetto delle esigenze di tempo e risorse disponibili.

4.2.5. Elaborazione della relazione di Risk Assessment e condivisione con il management

La relazione di *Risk Assessment* precede l'elaborazione del piano di *Audit*, quest'ultimo verrà elaborato in risposta al *Risk Assessment*. La relazione di *Risk Assessment* verrà condivisa con la Direzione Generale che l'approva prima del piano di *audit*.

4.2.6. Documentazione dell'attività svolta

La funzione di IA per lo svolgimento della sua attività utilizza strumenti di formalizzazione fogli elettronici e documentazione cartacea opportunamente archiviata.

5. DEFINIZIONE DI DETTAGLIO DELLE PRIORITÀ DI AUDIT SULLA BASE RISK SCORING

La funzione IA opera sulla base delle risorse di cui dispone, con la finalità di presidiare i rischi elevati, ovvero quei rischi che rappresentano una minaccia al raggiungimento degli obiettivi. Con specifico riferimento ai PAC, devono essere presidiate le attività ed i processi che presentano dapprima i rischi elevanti, poi quelli alti, medi e così via, sempre nel rispetto delle esigenze di tempo e risorse disponibili.

Le risultanze di Risk Assessment confluiscono appunto nell'elaborazione del piano di Audit. Le stesse vengono condivise con la Direzione Generale.
Le tipologie di intervento dell'Internal Auditing sono sviluppate in base a tre principali direttive:

- Audit di conformità, che tratta l'analisi della conformità dei comportamenti con le procedure e prassi interne con quanto richiesto dal legislatore;
- Audit Operativo, che rispecchia il monitoraggio del rispetto degli obiettivi aziendali a livello di processo, valutando l'efficacia e l'efficienza dei processi e dei controlli previsti;
- Controlli Periodici, che si estrinsecano negli interventi periodici su specifiche aree aziendali utili per la verifica dell'effettiva attuazione dei piani di azione concordati con i responsabili dei processi.

6. PREDISPOSIZIONE E CONDIVISIONE DEL PIANO DI AUDIT

Il Piano Internal Audit viene approvato entro il 31 Dicembre dell'anno precedente rispetto all'anno di riferimento, con provvedimento del Direttore Generale. Il Piano Internal Audit viene predisposto dal Referente dell'Internal Audit. Esso individua l'ambito dell'audit, le modalità di verifica, l'area/struttura

coinvolta, i tempi di svolgimento, senza escludere la possibilità di ulteriori verifiche per esigenze particolari. Il Piano prevede anche le risorse da destinare alle attività comprese al suo interno, in termini quantitativi e di competenza.

La fase di pianificazione rappresenta la risposta ai rischi identificati nella fase del "Risk Assessment".

Il Piano di Audit consente di identificare gli obiettivi di audit a livello di ciclo aziendale e di definire la portata dell'intervento, ovvero di identificare la natura, l'estensione e la tempistica delle procedure riferite agli obiettivi di verifica, al fine di svolgere il lavoro in maniera efficace ed efficiente.

L'azione dell'Internal audit sarà, quindi, improntata alla raccolta delle evidenze documentali che consentano di mostrare che gli obiettivi dei controlli implementati siano raggiunti.

Gli audit previsti nel Piano di audit vengono formalmente notificati alle UU.OO. interessate unitamente al Programma di Audit, che include:

- data verifica;
- sede di verifica;
- attività/area/funzione coinvolta;
- scopo della verifica;
- gruppo di audit;
- tempi presunti di svolgimento;
- documentazione di interesse.

7. RIUNIONE DI APERTURA

L'obiettivo della riunione di apertura dell'incontro di Audit è quello di chiarire alla struttura sottoposta a verifica lo scopo e l'ambito dell'audit nonché le metodologie che saranno seguite nella sua conduzione. Nel corso di tale riunione si definiscono le fasi operative del lavoro sul campo.

All'incontro partecipa il responsabile della struttura sottoposta a verifica, i collaboratori dallo stesso individuati ed il Gruppo di lavoro I.A. Una sintesi degli argomenti discussi e delle conclusioni raggiunte nella riunione di apertura viene formalizzata dal Referente IA in un verbale della riunione.

8. SVOLGIMENTO INTERVENTO DI AUDIT

La fase di conduzione dell'incontro di Audit è quella in cui il Gruppo di lavoro analizza la normativa, le regole di funzionamento del processo, le procedure esistenti, l'organizzazione dell'attività, le risorse impegnate e qualsiasi ulteriore informazione che possa essere utile all'espletamento dell'audit.

Gli ulteriori strumenti di valutazione utilizzati dal Gruppo di I.A., anche in combinazione tra di loro, possono essere:

- Interviste: il Responsabile della struttura sottoposta a revisione può essere intervistato dal team di I.A, anche con il supporto di una check-list predefinita, quale ulteriore approfondimento delle conoscenze acquisite nel corso dello studio del processo e/o allo scopo di chiarire i punti dubbi;
- Work-shop: possono essere organizzati in forma collegiale, per raccogliere i punti di vista e confrontare le differenti posizioni dei responsabili e dei funzionari che partecipano al processo, nelle sue diverse fasi;
- Questionari a risposta aperta/chiusa: utili per richiedere informazioni sulle procedure e sul funzionamento delle diverse fasi del processo. Nel caso si scelga di somministrare questionari, però, occorre sempre avvisare il Responsabile della struttura sottoposta a revisione;
- Azioni di re-performance: tecnica utilizzata per testare l'efficacia della procedura di controllo; nel corso dell'audit viene "provata" e rifatta la procedura di controllo alla presenza degli operatori addetti per determinare se si perviene allo stesso risultato;
- Osservazione diretta: la tecnica è basata sull'osservazione delle fasi della procedura o dei processi oggetto di audit e consente di avere maggiore affidabilità delle evidenze di audit. È spesso utilizzata sui controlli automatici;
- Campionamento: si intende l'applicazione delle procedure di verifica a meno del 100% della popolazione, in modo da trarre una valida conclusione valutando le caratteristiche del campione esaminato. ll campionamento può essere casuale, mirato o sistematico.

9. REPORTING PIANO AZIONI CORRETTIVE

Conclusa la fase di Audit, si procede alla predisposizione di un rapporto preliminare, che riassume le constatazioni formulate in fase di analisi del processo. Nell'incontro di chiusura vengono poi discusse tutte le constatazioni ed i rilievi emersi tramite l'attività del team di lavoro, che ne condivide gli elementi salienti con tutti i referenti dell'azienda; attraverso tale incontro si analizzeranno e discuteranno tutte le non conformità rilevate durante i lavori.

A seguito dell'incontro di chiusura viene redatto il rapporto finale che 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.

10. IL FOLLOW-UP AUDIT

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.

Con la fase del follow-up, vengono verificate le esecuzioni delle azioni di miglioramento e delle correzioni suggerite e contenute nel rapporto finale. Con l'obiettivo di formalizzare adeguatamente le attività svolte e tenere traccia degli interventi correttivi apportati nel corso del tempo, per ogni intervento di audit viene creato un fascicolo che raccoglie la documentazione utilizzata e tutti i documenti redatti.

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.

11. ARCHIVIAZIONE

Per ciascun intervento di audit viene creato un fascicolo contenete tutte le evidenze atte a documentare l'attività di audit.

La Funzione Internal Audit conserva tutta la documentazione relativa all'attività di audit. Il materiale viene fascicolato e custodito all'interno di apposito armadio che consenta di mantenere la segretezza degli atti e in formato informatico facilmente consultabile.

ALLEGATI:

1. Lettera di notifica avvio audit
2. Piano di Audit
3. Verbale di Audit
4. Rapporto di Audit
5. Format Piano di Audit

6. Format Sintesi Rapporto di Audit
7. Codice Etico

Allegato 1: LETTERA DI NOTIFICA AVVIO AUDIT

LETTERA DI NOTIFICA AVVIO AUDIT

Oggetto : Piano di Audit 20__ codice Audit_____ Avvio attività di verifica _____

Nell'ambito delle attività programmate dal Piano di Audit 20__ (approvato con determina del _____20__n.____), è prevista l'effettuazione di un intervento di audit sul processo di _____.
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:

- ✓ esposizione del programma di lavoro;
- ✓ esame dei controlli sul processo;
- ✓ …
- ✓ …

All'incontro parteciperanno:
_____
_____
_____

Preliminarmente all'incontro si prega di far pervenire, entro 10 giorni dalla data della presente, alla scrivente 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.

ALLEGATO 2: PIANO DI AUDIT

INDICE DEL DOCUMENTO

1 PREMESSE

L'Internal Audit nisulta essere un attore chiave nella gestione dei rischi di natura amministrativo-contabile dell'Azienda, con l'obiettivo di consentire l'identificazione, la misurazione, la gestione ed il monitoraggio dei principali rischi nonché, al fine di garantire.

- la salvaguardia del patrimonio aziendale;
- la conformità a leggi e regolamenti;
- l'attendibilità delle informazioni;
- l'efficacia ed efficienza delle operazioni gestionali.

L'istituzione della funzione di Internal Audit all'interno dell'organizzazione delle aziende sanitarie è un obbligo normativo, previsto nel Percorso attuativo di certificabilità dei Bilanci (P.A.C.).

Il Presente Piano di Audit, predisposto dal Responsabile della funzione di Internal Audit, definisce le azioni — procedure - processi che saranno oggetto di controllo durante l'anno, i Servizi Responsabili delle attività oggetto di verifica ed il cronoprogramma delle attività da svolgere.

2 RISULTANZE DEL RISK ASSESSMENT

AI fine di addivenire ad un efficace pianificazione dell'attività di audit, occorre procedere ad un'attività di RISK ASSESSMENT volta alla valutazione ed all'identificazione dei rischi a cui sono esposti i processi aziendali. Nello specifico il Team di Audit procede a:

1) **valutare il rischio intrinseco**: ossia verificare qual'è la probabilità che il rischio si verifichi, qual'è l'impatto (monetario) se il rischio si verifica;

2) **valutare il rischio di controllo**: procedendo all'analisi del Sistema dei Controlli Interni sui singoli processi aziendali e all'individuazione dei controlli di primo livello sulle fasi in cui si articola ciascun processo

Dopo aver valutato il rischio intrinseco e il rischio di controllo, mediante procedure separate e differenziate, la funzione di Internal Audit è tenuta a riesaminare i risultati ottenuti in queste due fasi per poter sintetizzare e valutare i rischi di errori significativi a livello di bilancio e a livello di asserzioni per classi di operazioni, saldi contabili e informativa.

Al termine di tale fase è possibile giungere ad uno dei seguenti risultati del livello del rischio di errori significativi, così come ben esplicitati all'interno del Regolamento di Audit, ciò porta alla compilazione della seguente tabella

		Rischio di Controllo	
		Affidamento sui controlli	Nessun Affidamento sui controlli
Rischio Inerente	Basso	Minimale	Basso
	Moderato	Basso	Moderato
	Alto	Moderato	Elevato
		Rischio Complessivo	

3 PIANIFICAZIONE DELL'ATTIVITA' DI AUDIT

Di seguito la pianificazione degli Audit previsti per l'anno _____ ed il relativo Cronoprogramma delle relative attività

Rif. Audit	Obiettivo	Attività di Audit	UU.OO. coinvolte	Cronoprogramma
1/anno	Verifica operativa del processo previsto all'interno dell'azione E1.4 del PAC	Verifica dello svolgimento, trimestrale degli inventari fisici dei beni sanitari nei Magazzini Centrali e nei reparti	UOC Farmacia Ospedaliera - UU.OO che gestiscono beni a scorta	Mese 4 — Mese 5 - Mese 10 - Mese 12

Pianificazione dell'Attività di Audit

GANTT PROGETTO														
Mese		Mese 1	Mese 2	Mese 3	Mese 4	Mese 5	Mese 6	Mese 7	Mese 8	Mese 9	Mese 10	Mese 11	Mese 12
Attivita' di audit ANNO XXXX													
1/anno	Verifica operativa del processo previsto all'interno dell'azione E1.4 del PAC relativamente all'applicazione della procedura operativa relativa all'effettuazione degli inventari fisici periodici di beni sanitari nei Magazzini Aziendali e nei reparti												

Cronoprogramma attività di Audit

ALLEGATO 3: VERBALE DI AUDIT

VERBALE DI AUDIT		
Ora e luogo	Attivita'	Responsabile UU.OO. presente
Ora: Sede:	Risk assesment - Comprensione dell'azienda e del contesto di riferimento - Analisi dei processi aziendali - Analisi del sistema di controllo interno - Valutazione del rischio intrinseco - Valutazione del rischio di controllo - Valutazione del rischio complessivo - Determinazione del Campione da sottoporre a verifica	
Ora: Sede:	Svolgimento della riunione di aperture - Presentazione del programma di audit - Scopo, obiettivo ed estensione della verifica - Conferma piano di verifica e modalità operative - Individuazione dei referenti di interfaccia - Indicazione nominativa, da parte dei Responsabili degli interlocutori ed eventuali accompagnatori per le fasi successive Conferma di disponibilità dei "mezzi" necessari alla verifica	

Ora: Sede:	Verifica sul "campo" Esame della documentazione, osservazioni sul campo ed incontri con gli operatori per rilevare l'effettiva applicazione e valutazione dei requisiti previsti da procedure, linee guida, norme, ecc...	
Ora: Sede:	Riunione del Gruppo di Verifica per la stesura del "Rapporto di Audit"	
Ora: Sede:	Riunione di chiusura - Presentazione rapporto e verbale di verifica - Definizione programma di monitoraggio sugli eventuali piani di miglioramento - Discussione	

ALLEGATO 4: RAPPORTO DI AUDIT

INDICE DEL DOCUMENTO

1 EXECUTIVE SUMMARY

Tale sezione rappresenta una sintesi dei risultati dell'Audit da fornire ala Direzione Strategica per il monitoraggio e l'eventuale emanazione di Raccomandazioni, Richieste di chiarimenti o qualsiasi altra azione ritenuta necessaria al fine di ottemperare alle indicazioni fornite dal Responsabile Internal Audit.
Tale area deve necessariamente contenere le principali osservazioni in ordine alle criticità rilevate e ai rischi individuati, le raccomandazioni fornite nonché l'indicazione di azioni correttive.

2 OBIETTIVI/AMBITO DI AUDIT

In tale sezione devono essere indicati gli obiettivi specifici dell'attività di Audit; le procedure, i processi e/o operazioni valutate, specificando le UU.OO. oggetto di Audit.

3 METODOLOGIA

In questa sezione devono essere illustrate le modalità utilizzate per lo svolgimento delle verifiche facendo specifico riferimento all'analisi del rischio, condotta in riferimento alle varie aree aziendali, alla documentazione esaminata, al campione utilizzato, ai criteri di valutazione adottati, alle riunioni ed interviste effettuate, alle check list predisposte, ecc....

4 CONSTATAZIONI

In quest'area devono essere dettagliate le criticità individuate sui processi analizzati, evidenziando le carenze e gli scostamenti riscontrati rispetto alle procedure, linee guida e normative di settore. Devono essere riportate in questa sezione le eventuali osservazioni fornite dal Responsabile delle UU.OO. oggetto di audit se divergenti rispetto ai risultati dell'attività.

5 AZIONI CORRETTIVE

In tale area devono essere riportate per ogni criticità rilevate le azioni correttive/migliorative da intraprendere con l'espressa indicazione, per ciascuna di esse, di un Responsabile per lo svolgimento ed una data di scadenza entro la quale occorre adeguarsi all'intervento indicato.
In tale sezione occorre, inoltre, dare specifica evidenza dell'eventuale non condivisione delle Azioni correttive indicate dall'Internal Audit da parte della Direzione Strategica con l'espressa indicazione delle motivazioni di non adesione.

ALLEGATO 5: FORMAT PIANO DI AUDIT

NOME AZIENDA	
RESPONSABILE IA	
COMPONENTI TEAM DI AUDIT	
DATA INIZIO – DATA FINE	
OBIETTIVI DELL'AUDIT	
VALUTAZIONE RISCHIO INTRINSECO	
VALUTAZIONE RISCHIO DI CONTROLLO	
VALUTAZIONE RISCHIO COMPLESSIVO	
ESTENSIONE DELL'AUDIT	
UU.OO. COINVOLTE	

ALLEGATO 6: FORMAT SINTESI RAPPORTO DI AUDIT

NOME AZIENDA	
RESPONSABILE IA	
COMPONENTI TEAM DI AUDIT	
N. RAPPORTO AUDIT	
DATA INIZIO – DATA FINE	
INFORMAZIONI GENERALI	
RIFERIMENTO PIANO DI AUDIT	
OBIETTIVIO DI AUDIT	
OGGETTO DELL'AUDIT	
UU.OO. COINVOLTE – RESPONSABILE DI CIASCUNA UUOO COINVOLTA	
PARTECIPANTI	
STRUMENTI UTILIZZATI	
DOCUMENTAZIONE ACQUISITA	
RISULTANZE	

ID CRITICITA’	DESCRIZIONE CRITICITA’	AZIONE MIGLIORATIVA	REFERENTE/RESPONSABILE	SCADENZA

ALLEGATO 7 – CODICE ETICO

CODICE ETICO

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

L'internal auditing è un'attività indipendente ed obiettiva di assurance e consulenza, finalizzata al miglioramento dell'efficacia e dell'efficienza dell'organizzazione. Assiste l'organizzazione nel perseguimento dei propri obiettivi tramite un approccio professionale sistematico, che genera valore aggiunto in quanto finalizzato a valutare e migliorare i processi di gestione dei rischi, di controllo e di governance.

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

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

1) I Principi, fondamentali per la professione e la pratica dell'*internal auditing*.

2) Le Regole di Condotta, che descrivono le norme comportamentali che gli *internal auditor* sono tenuti a osservare. Queste regole sono un aiuto per orientare l'applicazione pratica dei Principi e intendono fornire agli internal auditor una guida di comportamento professionale.
Il termine *internal auditor* si riferisce ai membri dell'*Institute of Internal Auditors*, ai detentori delle certificazioni professionali rilasciate dall'*Institute*, a coloro che si candidano a riceverle e a tutti coloro che svolgono attività di internal audit secondo la Definizione di *Internal Auditing*.

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

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

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

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

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

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

Regole di condotta
1) Integrità - L'*internal auditor*:

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

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

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

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

2) Obiettività - L'*internal auditor*:

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

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

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

3) Riservatezza - L'*internal auditor*:

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

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

4) Competenza - L'*internal auditor*:

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

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

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