Sommario

INTRODUZIONE 2
1. SCOPO E CAMPO DI APPLICAZIONE 2
2. DIAGRAMMA DI FLUSSO 2
3. SIGLARIO 2
4. DESCRIZIONE DELLE ATTIVITÀ 3
5. ORGANIZZAZIONE 3
5.1 RUOLO, RESPONSABILITÀ E COMPITI 4
5.2 PRINCIPI ETICI E REGOLE DI CONDOTTA 5
5.3 ORGANIZZAZIONE DELLE ATTIVITÀ 5
5.4 PIANO DI AUDIT 6
5.5 CICLO DI INTERNAL AUDITING 6
5.6 PIANIFICAZIONE E PREPARAZIONE DELL'AUDIT 8
5.7 RIUNIONE DI APERTURA 9
5.8 CONDUZIONE DELL'AUDIT 9
5.9 CHIUSURA DELL'AUDIT 9
5.10 FOLLOW-UP 10
5.11 AUDIT DI CONSULENZA 10
5.12 GESTIONE DELLA DOCUMENTAZIONE 10
6. NOTE FINALI 10
6.1 DENUNCIA DI DANNO ERARIALE 10
6.2 DENUNCIA PENALE 11
7. RIFERIMENTI NORMATIVI 11

STATO DELLE REVISIONI

Rev	Data	Modifica	Preparato	Verificato	Approvato
0	15/10/2015	Prima emissione	Coordinatore Internal Auditing Camelia Gaby Tiron	Responsabile Internal Auditing Enrico Burato	Direttore Generale Luca Stucchi
1	05/01/2021	Aggiornamento della normativa di riferimento, modello della rete regionale	Coordinatore Internal Auditing Camelia Gaby Tiron	Responsabile Internal Auditing Enrico Burato	Direttore Generale Raffaello Stradoni
2	14/10/2026	Adeguamento a modifiche organizzative	Responsabile Internal Auditing Maria Saveria Renzulli	Responsabile Internal Auditing Maria Saveria Renzulli	Direttore Generale Anna Gerola

Documento firmato elettronicamente. La copia originale del documento in stato di validità è pubblicata sul sistema informatico Taleteweb e consultabile elettronicamente da tutto il personale autorizzato.

INTRODUZIONE

L'Internal Auditing (di seguito in breve "I.A."), secondo la **definizione** validata dall'organizzazione mondiale cui fa riferimento l'Associazione Italiana Internal Auditors (A.I.I.A.), è *"un'attività indipendente e obiettiva di assurance e consulenza, finalizzata al miglioramento dell'efficacia e dell'efficienza dell'organizzazione. Assiste l'organizzazione nel perseguimento dei propri obiettivi tramite un approccio professionale sistematico, che genera valore aggiunto in quanto finalizzato a valutare e migliorare i processi di gestione dei rischi, di controllo e di governance"*.

L'attività di Internal Auditing è regolata a livello internazionale dai relativi **Standard** professionali emanati dall'I.I.A. (Institute of Internal Auditors) che, tra l'altro, ha redatto un **Codice Etico** con i **Principi** e le **Regole di condotta (Integrità, Obiettività, Riservatezza, Competenza)** cui gli auditors devono conformarsi.

RETE INTERNAL AUDITING DEGLI ENTI DEL SISTEMA REGIONALE (SIREG)

Regione Lombardia con la legge regionale 30/2006 ha isitituito il SIREG. Con le *"Regole di sistema 2015 - ambito sanitario"* (Allegato B della DGR 23 dicembre 2014, n. X/2989) ha, poi, stabilito di inserire nella Rete di Internal Auditing tutti gli Enti Sanitari.

L'art. 1 della L.R. 17/2014 ha attribuito alla Giunta regionale la funzione di promuovere la Rete degli uffici di Internal Auditing degli enti del SIREG e sostenerne la formazione, attraverso le competenze assegnate alla funzione audit regionale in raccordo con l'Organismo Regionale per le attività di controllo (ORAC). Istituito con L.R. 13/2018, l'Organismo ha, infatti, fra le proprie funzioni quella di coordinare la Rete e di fornire indicazioni per lo svolgimento di audit finalizzati a verificare il presidio di alcuni rischi di particolare rilevanza, anche in raccordo con altri organismi operanti a livello regionale, quale ad esempio il Collegio dei Revisori.

Si tratta di un modello organizzativo secondo il quale Regione Lombardia, nel rispetto della professionalità, dell'autonomia e dell'indipendenza delle strutture dedicate della Giunta e degli Enti del sistema, incoraggia la cooperazione tra i punti della rete al fine di conseguire la massima copertura dei rischi con minor impiego di risorse.

1. SCOPO E CAMPO DI APPLICAZIONE

Il presente Regolamento descrive i principi, le procedure, le metodologie e gli strumenti di lavoro utilizzati per l'attività della funzione aziendale di Internal Auditing.

Ad esso devono attenersi il Responsabile Internal Audit, il Team IA e le Direzioni/Strutture aziendali.

2. DIAGRAMMA DI FLUSSO

Non attinente

3. SIGLARIO

ASST	Azienda Socio Sanitaria Territoriale
GIAS	Global Internal Audit Standards
IA	Internal Auditing
IIA	Institute of Internal Auditors
ORAC	Organismo regionale per le Attività di Controllo
POAS	Piano di Organizzazione Aziendale Strategico
RIA	Responsabile Internal Audit
SIREG	Sistema Regionale

4. DESCRIZIONE DELLE ATTIVITÀ

La funzione Internal Auditing all'interno dell'Azienda Socio-Sanitaria Territoriale (ASST) di Mantova è volta a controllare il regolare andamento dell'operatività e l'evoluzione dei rischi in un'ottica di terzo livello.

Il primo livello del sistema è quello dei controlli di linea, ossia di quelle verifiche svolte sia da chi mette in atto una determinata attività, sia da chi ne ha la responsabilità di supervisione. Sono continuativi controlli procedurali, informatici, documentali, amministrativo-contabili, ecc. la cui responsabilità è in capo al Dirigente di ciascuna Struttura Aziendale in ordine a tutte le funzioni che gli sono attribuite dal POAS e dagli atti organizzativi interni.

I controlli di secondo livello, invece, sono affidati a unità operative e funzioni istituzionalmente preposte al controllo (risk management, qualità, accreditamento, controllo di gestione, prevenzione e protezione, prevenzione della corruzione e trasparenza, Sistemi Informativi Aziendali (SIA), Data Protection Officer (DPO), ecc.).

L'Internal Auditing si identifica nel controllo di terzo livello finalizzato a valutare la funzionalità del complessivo sistema dei controlli interni ossia la capacità dell'ente di gestire e controllare i propri rischi.

Il Sistema di Controllo Interno concorre ad assicurare "la salvaguardia del patrimonio sociale, l'efficienza e l'efficacia dei processi aziendali, l'affidabilità delle informazioni, il rispetto di leggi e regolamenti, nonché delle procedure interne" (Comitato per la Corporate Governance, 2018).

La prima elaborazione completa in tema di nozione e struttura dei controlli interni, risalente al 1992 (Cfr. rapporto "Internal Control: Integrated Framework" – 1992 – Committee of Sponsoring Organization of the Treadway Commission - CoSo), definisce il Sistema di Controllo Interno come il processo formato da un insieme di meccanismi, procedure e strumenti, adottati dalla direzione, per assicurare una ragionevole garanzia nel conseguimento degli obiettivi.

Il presente documento si ispira ai Global Internal Audit Standards (GIAS), pubblicati dall'Institute of Internal Auditors (IIA) nel gennaio 2024 ed entrati in vigore il 9 gennaio 2025. Si tratta di un aggiornamento con il quale l'Istituto ha inteso rafforzare il ruolo strategico dell'Internal Audit, evidenziando l'importanza di un approccio proattivo nella valutazione del governo aziendale, della gestione del rischio e dell'efficacia dei controlli interni.

L'applicazione degli standard nel settore pubblico deve tener conto però delle specificità normative e dei vincoli giuridici che regolano il mandato dell'Internal Audit, la trasparenza dei risultati e le modalità di interazione con gli organi di governance. Tali aspetti possono richiedere un adattamento delle metodologie di audit per garantire il rispetto delle disposizioni locali.

La Funzione IA, in definitiva, assiste l'organizzazione nel perseguimento dei propri obiettivi attraverso un approccio professionale e sistematico, generando valore aggiunto grazie alla valutazione e al miglioramento dei processi di gestione dei rischi, dei controlli e della governance. Ne consegue che non riveste un ruolo ispettivo, bensì consultivo e propositivo.

5. ORGANIZZAZIONE

L'I.A. è un'attività indipendente, pertanto la relativa Funzione aziendale, per svolgere il suo compito in modo obiettivo, dovrà godere della necessaria autonomia, ed essere libera da condizionamenti, quali potrebbero essere conflitti di interesse individuali, limitazioni del campo di azione, restrizioni nell'accesso a informazioni, rapporto di dipendenza gerarchica nei confronti di coloro che verifica o difficoltà analoghe.

La responsabilità della Funzione di I.A. è assegnata dal Direttore Generale ad un Responsabile al quale sono altresì attribuite le risorse ritenute necessarie per adempiere al mandato e del quale ne supporta l'attività per consentire di conseguire i relativi obiettivi.

Il RIA si avvale del supporto stabile di un Team di auditors/Team I.A.

L'attività del Team è organizzata da un Coordinatore.

Il Team può essere integrato da ulteriori risorse, interne o esterne all'Azienda, con competenze tecnico/professionali di volta in volta individuate in relazione al processo da auditare.

Il componente del Team direttamente coinvolto per la propria funzione nell'attività oggetto di analisi, si astiene dal partecipare ai lavori.

Le attività di audit possono essere effettuate da tutto il Team di I.A. o da sotto-gruppi individuati dal RIA in accordo con il Coordinatore, in funzione delle singole attività e delle conoscenze degli Auditors, favorendo lo scambio e la formazione tra i diversi componenti.

Il RIA ed i componenti del Team sono individuati dalla Direzione Strategica sulla base delle competenze, dell'expertise maturata e per la presenza delle seguenti soft skills necessarie:

- rapidità di comprensione delle diverse situazioni organizzative dell'Azienda,
- capacità di analisi e di sintesi,
- elevato senso dell'etica ed integrità morale,
- atteggiamento mentale di obiettività,
- attitudine ai rapporti interpersonali e capacità di comunicazione,
- conoscenza delle tecniche di "problem solving",
- creatività nella ricerca di soluzioni per i problemi rilevati,
- determinazione nel conseguimento degli obiettivi.

5.1 RUOLO, RESPONSABILITÀ E COMPITI

Al Responsabile dell'Internal Auditing competono i seguenti compiti:

- supportare la Direzione Strategica nella valutazione del funzionamento del sistema dei controlli, con feedback relativamente alle attività poste in essere e con proposte per la programmazione delle attività future;
- supportare i responsabili delle Unità Operative, dei Servizi e delle Funzioni oggetto di Audit nella mappatura ed identificazione degli ambiti soggetti a rischio e nell'individuazione di modifiche organizzative tali da mitigare il livello di rischio;
- pianificare l'attività di Audit definendo le strategie di medio periodo e i piani annuali delle attività;
- implementare il piano annuale con il supporto del coordinatore del Team di Internal Audit, programmando ed individuando le modalità operative delle attività da svolgere;
- stendere insieme al Team il rapporto di Audit e comunicarlo agli owner del processo ed al Direttore Generale;
- programmare un'adeguata attività di formazione ed informazione volte a far crescere nel Team e nell'organizzazione la cultura del miglioramento continuo nella gestione dei rischi;
- coordinare gli aggiornamenti del presente regolamento e degli strumenti utilizzati nell'attività di Audit;

Al Coordinatore del Team IA competono i seguenti compiti:

- coadiuvare il RIA nella pianificazione e programmazione delle attività e dei follow-up;
- coordinare le attività di audit affiancando gli auditors nell'esecuzione delle verifiche, garantendo la sostenibilità delle proposte formulate a seguito delle conclusioni tratte;
- riportare tempestivamente al RIA eventuali criticità sia nelle modalità di effettuazione che nei risultati dell'audit/follow up;
- collaborare alla predisposizione del piano annuale di audit;
- proporre le collaborazioni con soggetti esterni per gli audit di alta complessità e specificità;
- partecipare agli specifici percorsi di formazione;
- governare l'archiviazione dell'intera documentazione e delle evidenze degli interventi di audit/follow up;
- collaborare agli aggiornamenti del presente regolamento e degli strumenti utilizzati nell'attività di Audit/follow-up.

Ai componenti del Team IA competono i seguenti compiti:

- eseguire gli Audit/follow up programmati;

- raccogliere e ordinare tutta la documentazione necessaria a supportare le conclusioni tratte nel corso degli interventi di audit/follow up;
- individuare e proporre azioni migliorative del sistema dei controlli a seguito degli audit/follow up effettuati;
- redigere le bozze dei rapporti di Audit/follow up;
- partecipare agli specifici percorsi di formazione programmati;
- collaborare agli aggiornamenti del presente regolamento e degli strumenti utilizzati nell'attività di Audit/follow-up.

5.2 PRINCIPI ETICI E REGOLE DI CONDOTTA

Le attività di I.A. sono 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;

- dei limiti previsti dalle vigenti disposizioni in materia di protezione dei dati personali (Regolamento UE 2016/679, cd. GDPR, D. Lgs. 30 giugno 2003 n. 196 cosiddetto "Codice sulla Privacy" come novellato dal recente D. Lgs. 10 agosto 2018 n. 101 e s.m.i.);

- degli obblighi di riservatezza in merito alle informazioni delle quali si venga a conoscenza.

L'internal auditor per poter mantenere l'indipendenza e l'oggettività di giudizio non deve avere responsabilità diretta nei processi oggetto del controllo e, inoltre, deve comunicare tempestivamente al RIA eventuali cause di condizionamento nell'indipendenza organizzativa o nell'obiettività individuale. Nel caso in cui tale situazione riguardi il RIA questi deve provvedere a comucarlo al Direttore Generale.

5.3 ORGANIZZAZIONE DELLE ATTIVITÀ

L'attività di Internal Auditing viene svolta utilizzando la metodologia di tipo risk based e process oriented e assolve alle funzioni principali di:

1. **assurance** (verifica della corretta esecuzione delle attività) ossia controllo di terzo livello, in grado di verificare l'affidabilità e l'efficacia dei controlli di primo e di secondo livello nel contenere i rischi aziendali;

2. **consulenza** (miglioramento della gestione della catena del valore) supporto nell'analisi e gestione dei rischi legati ai processi aziendali.
Questa attività può avvenire attraverso:

a) il confronto e la interazione con le strutture che effettuano controlli trasversali (controlli di II livello);
b) l'affiancamento nella rilevazione di punti di debolezza e/o dei rischi esistenti relativi alle procedure in essere e nell'individuazione delle eventuali misure di contenimento;
c) la formulazione di indicazioni e pareri, in caso di avvio di nuovi processi o a seguito di introduzione di nuove norme;
d) la partecipazione alla definizione di percorsi innovativi strategici per il governo dell'azienda e/o alla revisione di procedure in essere.

5.4 PIANO DI AUDIT

L'Internal Auditing opera sulla base di una pianificazione, individuando i processi che saranno oggetto dell'attività di assurance tra quelli maggiormente strategici ed esposti a rischio.

La programmazione delle attività segue una logica integrata che considera i rischi desumibili da dati, informazioni e conoscenze tratti da diverse fonti (pianificazione delle attività dell'ORAC e conseguenti raccomandazioni, priorità di rischio emerse dalla valutazione effettuata a valle dei servizi di audit assurance e consulenza prestati, documenti di programmazione strategica, elementi di attenzione e definizione di nuovi indirizzi sollecitati dalla Direzione Strategica o altri, ecc.).

Nel Piano di Audit annuale vengono definiti gli ambiti di azione, le attività di controllo e di follow-up da svolgere con il relativo cronoprogramma, gli obiettivi da perseguire. È approvato dal Direttore Generale, al quale il gruppo di I.A. deve riportare i possibili miglioramenti al processo di gestione dei rischi, e può essere sottoposto a modifica, di norma entro settembre, al fine di allineare l'attività svolta e le risultanze con eventuali ulteriori necessità scaturite in corso d'anno. L'aggiornamento segue le medesime modalità con le quali è predisposto ed approvato il Piano annuale.

È possibile attivare degli Audit straordinari, su richiesta della Direzione Strategica e per motivazioni rilevanti, in deroga a quanto previsto nel Piano annuale. Le attività straordinarie possono comportare lo slittamento temporale e/o la rimodulazione di quanto programmato nel Piano annuale.

5.5 CICLO DI INTERNAL AUDITING

Si parla di "rischio" per indicare la possibilità che si verifichi un evento che può influire sul raggiungimento degli obiettivi.

Il processo di I.A. prende avvio con una fase preliminare di Risk Assessment attraverso la quale vengono identificati i fattori che agevolano il mancato raggiungimento degli obiettivi aziendali volta per volta coinvolti (ad esempio: economicità, trasparenza, efficacia, ecc.) e viene valutata l'adeguatezza delle attività di controllo poste in essere dal management per mitigare tali rischi.

I fattori di rischio possono essere raggruppati in funzione della loro origine in:

*Rischi interni (*connessi alle caratteristiche ed all'articolazione dell'organizzazione stessa)
- modello organizzativo;
- regole/prassi di processi e procedure
- fattore umano;

Rischi esterni (quelli che nascono all'esterno dell'Azienda)
- contesto (politico, economico-finanziario, socio-culturale, tecnologico, legislativo, ambientale, competitività);
- terze parti;
- eventi eccezionali.

La Funzione di I.A. analizza nella propria attività le seguenti macro-**tipologie** di rischi:

Rischi strategici: rischi derivanti dal manifestarsi di eventi che possono condizionare e/o modificare in modo rilevante le strategie e il raggiungimento degli obiettivi aziendali. Possono avere origine esterna ma anche interna.

Rischi di processo/Rischi operativi: rischi connessi alla normale operatività dei processi e del Sistema aziendale, 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: è il rischio di incorrere in sanzioni giudiziarie o amministrative o danni di reputazione per effetto della non conformità alle Leggi (incluse fiscali e ambientali), ai Regolamenti regionali o di Autorità di Vigilianza.

Rischio gestionale e/o finanziario: informazioni contabili ed extracontabili non allineate, non corrette, non complete; rischio di contenzioso e perdite finanziarie dovute a:
- inadeguata gestione dei processi aziendali (rischio liquidità, credito, ecc.)
- errata gestione aspetti fiscali

- errata gestione aspetti giuridici

Rischi di informativa: rischi connessi alla possibile inadeguatezza dei flussi informativi interni ed esterni aziendali 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.

Nella prima fase di analisi sarà richiesto al Risk Owner (Direttore di Dipartimento/Presidio/Distretto /Responsabile di Unità Operative, altri referenti identificati) una valutazione dei fattori di rischio a livello potenziale per ciascuna attività del processo a partire dall'*input* (elemento d'ingresso del processo) e fino all'*output* (risultato atteso).

Per rischio inerente o potenziale si intende il rischio valutato a prescindere dai sistemi di controllo interno operanti e dagli strumenti di gestione che sono stati istituiti e messi in atto per ridurne la probabilità di accadimento e/o il relativo impatto.

L'approccio valutativo prescelto per stimare l'esposizione dell'organizzazione ai rischi è di tipo qualitativo. L'esposizione al rischio è stimata, dunque, in base a motivate valutazioni del Risk Owner, tenendo in considerazione la combinazione delle seguenti due dimensioni:

• **Probabilità di accadimento (P)**: possibilità che un evento si verifichi.

• **Impatto (I)**: effetto derivante dal verificarsi dell'evento in termini di maggiori spese o altri effetti non previsti a carico del bilancio aziendale (impatti finanziari) o in termini di deviazioni dal corretto procedimento (impatto da non conformità senza ricadute finanziarie) o, ancora in termini di difficoltà operative, ritardi e/o anomalie nello svolgimento dell'attività e nell'erogazione dei servizi.

La probabilità potrà avere uno dei seguenti valori:

ALTO	È presumibile che l'evento si manifesti sistematicamente o ripetutamente nell'arco di un periodo definito (es: anno)
MEDIO	L'evento ha probabilità di manifestarsi nel periodo anche se non con caratteristiche di sistematicità
BASSO	La probabilità di accadimento dell'evento è da considerarsi remota.

Analogamente anche l'impatto avrà uno dei seguenti valori:

ALTO	Gli effetti derivanti dal verificarsi dell'evento sono altamente negativi
MEDIO	Gli effetti derivanti dal verificarsi dell'evento hanno un'incidenza media negativa.
BASSO	Gli effetti derivanti dal verificarsi dell'evento hanno una bassa incidenza negativa

Effettuata la valutazione della probabilità e dell'impatto va attribuito il valore complessivo utilizzando sempre la scala ordinale (Alto – Medio - Basso).

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.

La metrica di valutazione dei controlli è la seguente

ADEGUATO	Controllo che opera nel suo complesso in modo efficace ed efficiente assicurando monitoraggio e contenimento dei rischi o che presenta circoscritte carenze con lieve esposizione al rischio

PARZIALMENTE ADEGUATO	Controllo con carenze localizzate con esposizione lieve al rischio o per il quale è in essere un intervento correttivo/di mitigazione in fase di conclusione (es. procedura in corso di approvazione)
INADEGUATO	Assenza totale di elementi di controllo, o controllo che presenta gravi criticità con esposizione alta al rischio

Terminata la fase di risk assessment, la Funzione I.A. predispone la Heat Map che, mediante una scala di colori, fornisce la rappresentazione del livello di adeguatezza dei controlli attivati per la mitigazione dei rischi inerenti.
La Heat Map restituisce la valutazione dei rischi residui.

DISEGNO DEI CONTROLLI	**INADEGUATO**			
	PARZIALMENTE ADEGUATO			
	ADEGUATO			
		BASSO	**MEDIO**	**ALTO**

RISCHI INERENTI

La funzione IA ha così gli elementi per definire l'area di intervento. Di norma dall'attività di analisi verranno esclusi i controlli ritenuti adeguati alla mitigazione di rischi inerenti bassi/medi.

5.6 PIANIFICAZIONE E PREPARAZIONE DELL'AUDIT

I responsabili della Unità Operativa, Servizi/Funzioni o altre articolazioni aziendali interessata dall'attività di I.A. vengono informati dell'avvio dell'audit con lettera a firma del RIA.

Con la nota la struttura da auditare viene invitata a mettere a disposizione, entro un termine, tutti gli elementi utili e funzionali alla conoscenza dell'attività (risk register se già disponibile o da predisporre sulla base del modello fornito dalla funzione I.A., documentazione, procedure, regolamenti, atti formali, certificazioni, ecc.).

Ricevuta la documentazione, si procede con l'individuazione dell'area da esaminare, con la stesura del calendario di lavori e con la definizione dei componenti il gruppo di Audit.

Il RIA in questa fase ma anche in corso d'opera valuterà la necessità di richiedere il coivolgimento di esperti in relazione a processi specialistici che non costituiscono patrimonio dei componenti del Team I.A.

Ciascun componente del gruppo di audit dovrà assicurare, per gli audit ai quali partecipa, l'insussistenza di conflitti di interesse.

Le fasi successive sono in sintesi:
1) programmazione dell'incontro di apertura (kick-off meeting);
2) eventuali incontri tecnici intermedi con gli owners del processo per chiarimenti e approfondimenti;
3) predisposizione di una checklist che sarà di supporto nel valutare il livello di conformità ed i margini di miglioramento delle attività di controllo;
4) conduzione dell'audit;
5) riunione di chiusura dell'audit (exit meeting) volta alla condivisione del rapporto di audit predisposto in versione *draft* prima della stesura definitiva;
6) comunicazione del rapporto definitivo agli owner del processo ed al Direttore Generale.

5.7 RIUNIONE DI APERTURA

Nell'incontro di apertura dell'intervento I.A. (kick-off meeting) viene esposto il programma di lavoro, in particolare l'area d'intervento e gli strumenti che verranno utilizzati.

Alla riunione partecipano il responsabile della struttura oggetto di Audit con i propri collaboratori ed il gruppo degli Internal Auditor assegnati all'intervento.

Della riunione viene steso un sintetico verbale.

5.8 CONDUZIONE DELL'AUDIT

L'Audit può essere condotto con tecniche e strumenti differenti che possono essere usati insieme o alternativamente a seconda dell'obiettivo. Si fa riferimento in particolare a:

Interviste – i responsabili delle attività oggetto di Audit possono essere intervistati, anche con il supporto di una check–list predefinita, per approfondire quanto acquisito dal team di Auditors nella fase di conoscenza preliminare;

Questionari – i questionari, sia a risposta aperta che a risposta chiusa, possono essere utilizzati per richiedere informazioni sulle procedure e sul funzionamento delle diverse fasi del processo;

Osservazione diretta – consiste nell'osservazione delle fasi della procedura o dei processi oggetto dell'Audit e consente di avere maggiori affidabilità delle evidenze di Audit;

Azioni di re-performance – nel corso dell'azione di re-performance, viene valutata l'efficacia della progettazione di controlli, in definitiva viene estratto un campione di operazioni relative al processo e viene eseguito il controllo alla presenza degli operatori addetti per determinare se si perviene allo stesso risultato.

La scelta degli strumenti da utilizzare dovrà essere effettua prima dell'avvio dell'audit.

Si potrà decidere ti attivare anche un **work-shop** in forma collegiale tra i vari responsabili delle procedure per raccogliere i diversi punti di vista e confrontare le differenti posizioni sulle questioni oggetto di audit.

Le attività di Audit possono avvenire sia in presenza che utilizzando strumenti di videocall di gruppo, qualora siano compatibili con le attività da svolgere.

5.9 CHIUSURA DELL'AUDIT

L'attività compiuta dal gruppo incaricato dell'Internal Auditing si conclude con un Rapporto preliminare su quanto emerso durante l'attività del singolo Audit. Il Team di I.A. nell'incontro di chiusura (exit–meeting) condivide i contenuti del rapporto preliminare con gli owners del processo auditato procedendo ad una valutazione delle eventuali non conformità rilevate e discutendo le misure necessarie per mitigare il livello di rischio.

Tale attività di condivisione ha lo scopo di favorire un approccio alle attività di I.A. come processo di supporto alla struttura auditata, orientato al miglioramento continuo.

Il Rapporto di audit sintetizza in maniera rigorosa, sintetica e chiara le evidenze raccolte durante l'analisi operativa, le raccomandazioni formulate e le conclusioni finali.

Viene comunicato, con tutti gli allegati, agli owners del processo e al Direttore Generale con nota protocollata del RIA.

I partecipanti all'audit potranno concordare di includere nel rapporto di audit una lista di distribuzione delle stesso ad altre funzioni e figure aziendali coinvolte o potenzialmente interessate.

5.10 FOLLOW-UP

È la fase in cui viene verificata l'esecuzione delle azioni di miglioramento e delle correzioni suggerite. L'attività di follow-up e la relativa tempistica di norma vengono definite nel Rapporto finale di Audit.

La tempistica del follow-up dipende infatti dal tipo di rilievi sollevati nell'attività di Audit e dal tempo necessario alle unità operative per mettere in atto le modifiche alla soluzione del problema o alle mutate condizioni normative e istituzionali.

Il RIA provvederà a proporne la programmazione, di norma, nel piano I.A. dell'anno successivo.

Il follow-up viene attivato tramite comunicazione formale al responsabile del processo coinvolto, seguendo modalità analoghe a quelle dell'audit iniziale.

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

5.11 AUDIT DI CONSULENZA

Gli interventi di audit nella forma consulenziale, di norma, si articolano nelle seguenti fasi:

1. programmazione e definizione dell'incarico in accordo con il responsabile del processo richiedente la consulenza;
2. analisi preliminare *desk* (studio della documentazione, analisi *flow chart*, procedure e punti di controllo, analisi dei dati sulle operazioni, analisi dei dati relativi ad eventuali controlli);
3. analisi dei rischi e proposta di reingegnerizzazione del processo con indicazione dei punti di controllo;
4. report finale comunicato, con tutti gli allegati, al responsabile del processo e al Direttore Generale con nota protocollata del RIA.

5.12 GESTIONE DELLA DOCUMENTAZIONE

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

La documentazione, ove possibile, è creata in formato digitale e non cartaceo.

L'archiviazione della documentazione e della modulistica utilizzata per le attività della Funzione di Internal Audit è affidata al Coordinatore del Team.

Lo scarto della documentazione avviene secondo quanto previsto dal Titolario e Massimario del Sistema Sanitario e Sociosanitario di Regione Lombardia in vigore.

6. NOTE FINALI

L'attività di Internal Auditing non solleva i Direttore di Dipartimento/Presidio/Distretto/Responsabile di Unità Operative e delle funzioni aziendali dalle proprie responsabilità in merito al mantenimento di un sistema di controllo di primo livello efficace ed adeguato rispetto ai rischi connessi alla gestione.

L'attività di Internal Auditing, infatti, si configura come un'integrazione – e non una sostituzione – ai controlli di primo e secondo livello. Questi ultimi restano anch'essi in capo alle strutture preposte le quali ne conservano la piena responsabilità.

6.1 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), la denuncia va redatta sulla base delle rilevazioni del Responsabile I.A. e del Team I.A. e deve contenere tutti gli elementi raccolti per l'accertamento della responsabilità e la determinazione del danno.

L'obbligo di denuncia sussiste qualora il danno sia concreto e attuale e non quando i fatti abbiano solo una mera potenzialità lesiva. In quest'ultima ipotesi, il RIA informerà per iscritto 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.

6.2 DENUNCIA PENALE

Nel caso in cui durante l'attività di audit venga acquisita una notizia di reato perseguibile d'ufficio, il RIA deve farne denuncia senza ritardo. La denuncia va redatta dal RIA unitamente al Team I.A. e, con contestuale

informativa per iscritto al Direttore Generale, va inviata all'Autorità competente (Procura della Repubblica, Ufficiale di Polizia giudiziaria).
Nel caso in cui si rilevino fatti che non integrino le tipologie illecite di cui sopra, ma che presentino potenziali rischi per l'Azienda, il RIA ne dà tempestiva notizia al Direttore Generale, per i provvedimenti del caso.

7. RIFERIMENTI NORMATIVI

- D.Lgs. 20 luglio 1999, n. 286 e il D.Lgs. 30 marzo 2001, n. 165 e ss.mm.ii., nelle rispettive versioni vigenti, per quanto attiene alle disposizioni sui controlli interni alle Pubbliche Amministrazioni;
- D.Lgs. 150/2009 che ha delineato, tra l'altro, un potenziamento dei controlli interni alla P.A.;
- Legge Regionale n. 30 del 27 dicembre 2006 che, in attuazione dello Statuto di Regione Lombardia, ha istituito il Sistema Regionale costituito dalla Regione e dagli Enti individuati negli allegati 1 e 2 della stessa Legge;
- Legge Regionale 6 agosto 2010, n. 14 che ha differenziato la forma di partecipazione degli Enti al Sistema Regionale sulla base della loro tipologia;
- DGR n. X/2524, del 24 novembre 2011, con la quale la Regione ha stabilito le modalità di esercizio dell'attività di vigilanza e controllo sugli Enti appartenenti al Sistema Regionale finalizzati al perseguimento di obiettivi di efficacia, efficienza ed economicità;
- DGR n. 1292, del 30 gennaio 2014, con la quale Regione Lombardia ha definito le direttive agli Enti e alle Societa del sistema regionale in merito alla tipologia dei controlli con particolare riguardo alla funzione di Internal Auditing;
- nota prot. 30876 del 20 marzo 2014, con la quale la Direzione Centrale Legale, Legislativo, Istituzionale e Sistema dei Controlli e Coordinamento Organismi Indipendenti Audit SIREG ha chiesto ad ogni Azienda Sanitaria l'individuazione del responsabile della funzione di Internal Auditing;
- Legge Regionale 4 giugno 2014, n. 17, recante la "Disciplina del sistema dei controlli interni ai sensi dell'articolo 58 dello Statuto d'autonomia", che ha istituito, tra l'altro, la funzione di Internal Auditing e stabilito le modalità e le procedure per il controllo finalizzato a garantire la legittimità, la regolarità e la correttezza dell'azione amministrativa;
- DGR n. X/2989, del 23 dicembre 2014, avente ad oggetto "Determinazioni in ordine alla gestione del Servizio Socio Sanitario Regionale per l'esercizio 2015" (Regole 2015), che ha introdotto l'obbligo di costruzione di una Rete di Internal Auditing in tutti gli enti sanitari e previsto che ogni Azienda approvi un proprio regolamento di Internal Auditing e rediga la Pianificazione annuale dell'attività di audit;
- Legge Regionale 13 del 2018 istitutiva dell'Organismo regionale per le Attività di Controllo (ORAC);
- D.G.R. n. 5737 del 21 dicembre 2021, con la quale sono state approvate le "Direttive agli enti dipendenti e società in house di Regione Lombardia di cui all'allegato a1 della l.r. 30/2006";
- DGR n. XI/6387, del 16 maggio 2022 ("Determinazioni in ordine agli indirizzi di programmazione per l'anno 2023 – di concerto con gli assessori Caparini e Lucchini"), il cui Allegato 9 ("La funzione di Internal Auditing") introduce alcune indicazioni operative in materia di audit;
- Decreto del Segretario Generale n. 7968/2025 del 5 giugno 2025, con il quale sono stati approvati il Mandato e il Manuale di internal auditing di Regione Lombardia.