Sistema Socio Sanitario
Regione Lombardia
ASST Lariana

REGOLAMENTO DI INTERNAL AUDITING DELL'ASST LARIANA

PRINCIPI, PROCEDURE, METODOLOGIE, STRUMENTI DI LAVORO
(Deliberazione 260 del 31 marzo 2016)

INDICE

1. PREMESSA

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 controllo, di gestione dei rischi e di Corporate Governance" The Institute of Internal Auditors (IIA)

L'Internal Auditing (IA) è quindi 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, Trasparenza, Anticorruzione, …) e quelli di primo livello attuati dai dirigenti responsabili dei processi aziendali.

Gli scopi principali che si intende perseguire attraverso il Regolamento sono i seguenti:

- definire la **metodologia** per assistere il management nell'identificazione, mitigazione e monitoraggio dei rischi e dei relativi controlli;
- armonizzare e standardizzare le **fasi** e le **modalità operative** nonché gli **output** dell'attività di Internal Auditing;
- definire le **fasi** e le **tempistiche** del processo di audit ;
- definire gli ambiti di **collaborazione** tra funzione di audit e le strutture organizzative aziendali.

così come previsto dalla L.R. 17 del 04/06/2014, avente ad oggetto "Disciplina dei controlli interni ai sensi dell'art. 58 dello Statuto di autonomia" e dalla D.G.R. X/2989 del 23/12/2014, avente ad oggetto "Determinazioni in ordine alla gestione del Servizio Socio Sanitario Regionale per l'esercizio 2015" che prevede, tra l'altro, l'ingresso di tutti gli Enti sanitari a fare data dall'anno 2015 nella rete di Internal Audit regionale.

2. ASSETTO ORGANIZZATIVO DELLA FUNZIONE DI INTERNAL AUDITING

L'ASST Lariana ha individuato un gruppo di lavoro, individuato sulla base delle competenze, delle professionalità e dell'esperienza maturata all'interno dell'organizzazione che affiancherà il responsabile IA in tutte le fasi dell'attività di audit. L'Azienda ha attribuito il coordinamento, e la responsabilità alla dr.ssa Anna Sannino Responsabile qualità, accreditamento e rischio clinico .
I componenti del gruppo di lavoro e gli ulteriori professionisti, di volta in volta coinvolti, sono tenuti a prestare la propria collaborazione.

Ogni componente del gruppo assicura, per gli audit cui è designato a partecipare, l'insussistenza di conflitti di interesse.
Il responsabile di IA ha comunque la possibilità di avvalersi di ulteriori professionisti per conseguire la piena comprensione delle attività chiave associate a ciascun processo che possa essere oggetto di audit.

Il responsabile IA individua, per ciascun audit, i componenti del gruppo di lavoro le cui competenze siano le più attinenti al processo in oggetto di audit.

Ogni componente del gruppo di audit assicura, per gli audit cui è designato a partecipare, l'insussistenza di conflitti di interesse.

Alla funzione di IA, su richiesta, deve essere resa disponibile ed accessibile la documentazione, interna e/o esterna, che si ritiene necessaria per l'espletamento dell'audit.

3. CONTENUTO DEL REGOLAMENTO

Il presente Regolamento descrive i principi, le procedure, le metodologie e gli strumenti di lavoro utilizzati dal Gruppo operativo dell'ASST Lariana per svolgere l'attività di auditing sui processi operativi aziendali volti alla realizzazione degli obiettivi del Programma Aziendale di Sviluppo (Audit Operativi) e sulle procedure attivate dalle UU.OO. dell'ASST così come definiti dalla l.r. 30 del 2006 e s.m.i. (Audit di Conformità).
Tale Regolamento recepisce i principi e i criteri enunciati nel Manuale di Internal Auditing regionale approvato con Decreto DDUO Sistema dei Controlli e Coordinamento Organismi indipendenti n. 2822 del 3.4.2013.).

Il Regolamento IA (e suoi allegati) viene adottato con deliberazione del Direttore Generale e potrà essere oggetto di revisioni nel caso di mutamenti normativi e del contesto organizzativo aziendale e sulla base dei risultati annuali dell'attività di auditing.
Le revisioni del Regolamento dovranno essere approvate seguendo l'iter procedurale previsto per l'approvazione del Regolamento stesso.

4. DESTINATARI DEL REGOLAMENTO

I destinatari del Regolamento sono il responsabile IA, i componenti del gruppo di lavoro, la Direzione Aziendale, tutti i responsabili di struttura semplice e complessa dell'intera azienda.

5. COMPITI DELLA FUNZIONE DI INTERNAL AUDITING

Alla funzione di IA compete:

- Assistere la Direzione Aziendale nel valutare il funzionamento del sistema dei controlli e delle procedure operative;
- Collaborare con i responsabili delle strutture oggetto di audit nella mappatura ed identificazione degli ambiti soggetti a rischio e nella individuazione di modifiche organizzative tali da mitigare il livello di rischio;
- Effettuare la valutazione dei rischi ed aggiornare la mappatura complessiva dei rischi;
- Predisporre il piano annuale di audit, pianificare l'attività di audit e stendere il rapporto di audit;
- Eseguire gli audit programmati e l'esecuzione dei follow-up;
- Favorire la comprensione dell'importanza di un processo formale, documentato e collaborativo nel quale i responsabili dei processi oggetto di audit siano direttamente coinvolti nel giudicare e monitorare l'efficacia dei controlli esistenti;
- Curare la redazione del Regolamento di IA e dei suoi aggiornamenti qualora se ne verifichino i presupposti;

- Tenere l'archivio della documentazione e delle evidenze necessarie a supporto dell'attività di audit;
- Partecipare a corsi di formazione in merito al tema dell'IA.

6. I PRINCIPI ETICI E LE REGOLE DI CONDOTTA

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, nonché ai principi e valori enunciati nel Codice Etico aziendale. (vedi Allegato 1).
L'attività viene svolta in autonomia, indipendenza di giudizio, obiettività e riservatezza.
L'attività di IA non è soggetta alla limitazioni previste a tutela della privacy.

7. DENUNCIA DI DANNO ERARIALE

Qualora, nel corso dell'attività di audit emergano fatti che possano dar luogo a responsabilità per danni causati alla finanza pubblica, il responsabile IA ed i componenti del gruppo di lavoro inoltrano al Direttore Generale una relazione dalla quale si evincano tutti gli elementi raccolti per la determinazione del danno e l'accertamento delle responsabilità e dell'obbligo di denuncia alla Procura Regionale presso la 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 informa la Direzione aziendale di riferimento del settore auditato affinché sia avviata un'azione correttiva per evitare il danno.
Ove, malgrado ciò, il danno si verifichi sussiste l'obbligo di informare la Direzione Generale ai fini della conseguente presentazione di denuncia alla Corte dei Conti.

8. DENUNCIA PENALE

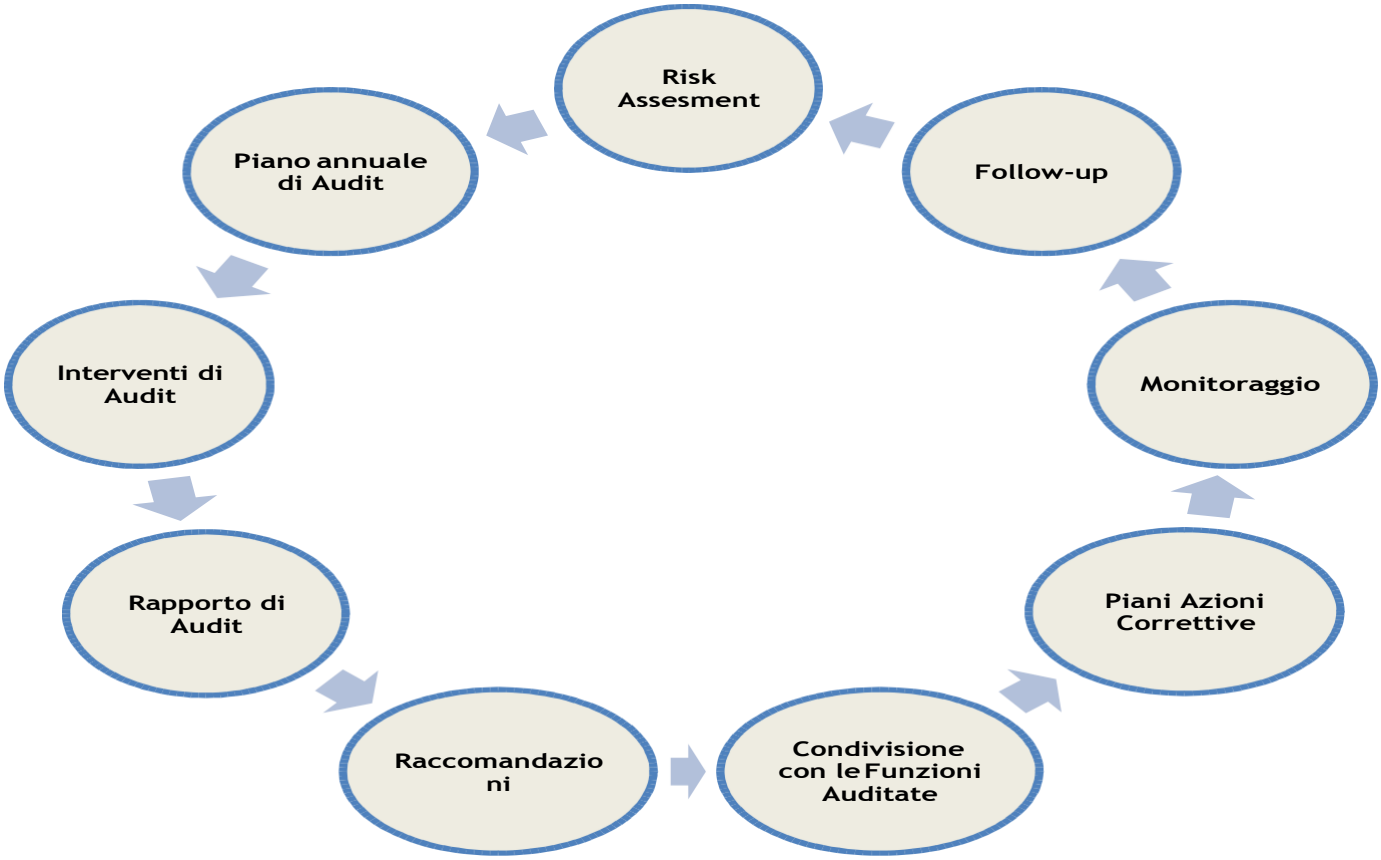
Qualora nel corso dell'attività di audit venga acquisita notizia di un reato perseguibile d'ufficio, deve esserne fatta denuncia.

Il responsabile IA ed i componenti del gruppo di lavoro che ne hanno appreso notizia, inoltrano la denuncia alla Procura della Repubblica o ad ufficiale di Polizia Giudiziaria, informando contestualmente il Direttore Generale tramite relazione che dia evidenza dei fatti riscontrati e dell'obbligo di denuncia.

La denuncia deve contenere i dati circa il giorno di acquisizione delle notizia e le fonti di prova già note; quando possibile deve contenere gli elementi utili all'identificazione della persona alla quale il fatto è attribuito e di coloro che siano in grado di riferire su circostanze rilevanti per la ricostruzione dei fatti.

9. PROCESSO DI INTERNAL AUDITING

Il processo legato alle attività della funzione di *Internal Audit* può essere rappresentato mediante lo schema sotto riportato.



9.1 Il Risk Assessment – La metodologia

9.1.1 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 del Piano di audit.

Le principali fasi in cui si articola il *Risk Assessment* dell'ASST Lariana 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 ;
e) l'elaborazione della relazione di *Risk Assessment* e condivisione con il management.

a) Definizione Universo di Audit
L'Universo di Audit è costituito da:
- l'insieme di tutti i processi individuati da norme nazionali e regionali in materia sanitaria, dalle Regole di gestione del SSR, dalle deliberazioni regionali di definizione degli obiettivi aziendali operativi e strategici di sistema, dai contratti stipulati con la ASL/ATS di competenza, dal P.O.A., dai provvedimenti organizzativi , dai regolamenti e dai documenti di programmazione aziendale e

in particolare il Documento di Programmazione dei servizi sanitari e socio-sanitari, il Piano Performance e il Documento di Budget per quanto riguarda l'analisi delle operazioni;
- l'insieme delle procedure poste in essere dalle diverse strutture della ASST Lariana per quanto attiene agli Audit di Conformità.

b) Identificazione dei rischi e loro valutazione

La Funzione di Internal Auditing procede alla definizione dell'elenco dei rischi principali con la relativa valutazione dall'analisi e valutazione delle fonti interne ed esterne, ovvero dall'insieme delle evidenze di criticità riportate da strutture interne o esterne, quali, in via esemplificativa e non esaustiva:

- ✓ Verbali del Collegio Sindacale
- ✓ Piano annuale di Risk Management
- ✓ Indicazioni provenienti da strumenti di valutazione della performance aziendale (quali il P.I.M.O., monitoraggio degli obiettivi strategici del Direttore Generale ecc.)
- ✓ Verbali del Collegio di Direzione
- ✓ Evidenze emerse dagli Audit della funzione Qualità, accreditamento, Rischio Clinico
- ✓ Controlli dei NOC della ATS di competenza
- ✓ Controlli dei NOCC regionali
- ✓ Osservazioni del Comitato Trasparenza Appalti
- ✓ Verbali del Nucleo di Valutazione delle Prestazioni
- ✓ Piano Triennale Anticorruzione
- ✓ U.R.P. e Mediazione
- ✓ Piano Anticorruzione

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

LE TIPOLOGIE DI RISCHI		
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. Possono avere origine esterna ma anche interna.
Rischi di processo	Pro	Rischi connessi alla normale operatività dei processi della A S S T 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'ASST, 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.

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

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. 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. 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

c) Identificazione e 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:

a) efficacia del controllo nel mitigare il rischio gestito, ossia se il controllo è idoneo ad assicurare il contenimento del rischio nei limiti ritenuti accettabili;
b) 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	Descrizione
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 ed è quindi espressa come nella seguente tabella:

Valutazione del controllo	Descrizione
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

c1) 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.

9.1.2 L'Universo dei rischi dell'ASST Lariana

L'"Universo dei rischi" dell'ASST Lariana, coerente con l'Universo dei rischi previsti dal Manuale di Regione Lombardia, da integrare con i rischi descritti nel Modello organizzativo del Codice Etico Comportamentale e identificati nel Piano anticorruzione, è preliminare alla predisposizione della pianificazione delle attività di Audit.

9.2 Pianificazione delle attività i audit

Le attività di audit sono pianificate sulla base dei rischi prioritari individuati con il Risk Assessment.
Il Piano aziendale si articola in Programmi Operativi, che a loro volta individuano, per ciascuna area (economica, sociale e territoriale), obiettivi specifici, operativi e azioni.
La metodologia esposta nel seguito, pur di carattere generale, può essere facilmente adattata alla predisposizione di un *Risk Assessment in conformità con la* procedura aziendale di "Gestione

Audit" , strumento idoneo a presidiare le procedure attivate per il raggiungimento degli obiettivi e creare valore aggiunto per il miglioramento dell'efficacia e dell'efficienza dei processi.

La Pianificazione dell'attività di Audit presso l'ASST Lariana è approvata dal Direttore Generale entro il 30 aprile di ogni anno sulla base della proposta del responsabile della funzione di audit e delle informazioni fornite nel corso dell'anno precedente dai sistemi in uso di aggiornamento delle procedure, monitoraggio dei risultati e dei costi, rilevazione delle irregolarità, monitoraggio del contenzioso, raccolta delle segnalazioni inerenti a difformità e malfunzionamenti di procedure e operazioni, selezioni rese disponibili da rassegne della stampa e degli altri media e dell'eventuale aggiornamento della valutazione dei rischi.
La Pianificazione annuale è comunicata a tutti i Direttori delle UOC dell'ASST con nota del Responsabile della funzione di Internal Auditing.
Il Programma di Audit definisce i processi/procedure e/o azioni che saranno verificati nell'anno e individua i correlati centri di responsabilità. Il Programma 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.

Eventuali modifiche significative e rilevanti apportate in corso d'anno dovranno essere approvate con le stesse modalità previste per l'approvazione del piano annuale.
Il Piano Annuale è comunicato ai Direttori delle UOC destinatari degli interventi programmati, con nota del Dirigente responsabile dell'attività di IA.

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

- Obiettivo dell'audit (conformità alle norme /standard/principi etici; miglioramento; rischio,etc.)
- Processi/ Attività oggetto dell'audit;
- Direzione/Struttura aziendale auditata;
- Responsabile del gruppo di audit;
- Periodo di effettuazione dell'audit

9.2.1 Programmazione operativa

Il Dirigente della funzione di Auditing in collaborazione con i componenti del Gruppo Operativo predispone e aggiorna la programmazione operativa delle attività che individua:

- risorse dedicate all'esecuzione dei singoli audit;
- nominativi dei responsabili e/o referenti per le singole aree auditate;
- data di inizio e conclusione.

L'attività di audit deve essere svolta coerentemente alla procedura aziendale di "Gestione audit interni".

Le fasi di un intervento di audit

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

- analisi preliminare;
- redazione piano di audit per ciascun intervento;
- esecuzione del lavoro sul campo;

- reporting e comunicazione dei risultati.

1) Analisi preliminare

Strumenti di rilevazione

Il team aziendale 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.

In tale fase la Risk and Control Matrix preliminare, predisposta in fase di programmazione dell'intervento di audit, viene adattata al processo oggetto di analisi, al fine di evidenziare in modo completo rischi e relativi controlli.
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.

Documentazione del processo auditato

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, richieste dell'Autorità Giudiziaria, 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: tassi elevati di rinunce o revoche, tassi particolarmente bassi oppure elevati di 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 p rocedure, 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.

<u>Definizione delle informazioni da richiedere</u>

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 infomatizzate, pianificazione, altro)

Tale lista deve essere inviata 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;
- responsabile 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.

Notifica dell'intervento di audit ed invio del Piano di audit

L'avvio di un'attività di audit deve essere sempre comunicato in forma scritta al soggetto auditato nel Piano di Audit. 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 almeno 10 giorni lavorativi prima dell'inizio effettivo delle attività sul campo, salvo casi eccezionali.

Nella comunicazione d'avvio delle attività di audit devono essere necessariamente indicati:

- 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;
- Programma dei lavori dell'incontro;
- Richiesta di documentazione integrativa e scadenza per adempiere;
- Eventuale questionario riguardante il funzionamento della azione/procedura.

La notifica viene inviata dal Responsabile della Funzione di Audit ai responsabili apicali dell'azione/procedura oggetto di audit e, per conoscenza, al Direttore aziendale sovraordinato.

La risposta dovrà pervenire nei termini fissati dalla notifica, anche in caso negativo o di richiesta di termine ulteriore, via posta elettronica interna oppure via mail recante quale mittente il responsabile dell'azione/procedura .

2) Redazione Piano di audit

Sono dettagliati gli obiettivi e le operazioni da eseguire per il singolo intervento di Audit.
Nello specifico sono definiti:

- la struttura aziendale da auditare;
- 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 lavori, 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,

3) 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.

Strumenti

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

1. Interviste
I responsabili degli Organismi o delle operazioni 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 il Management 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 degli operatori che partecipano in posizione chiave all'attuazione dell'azione/procedura possono essere organizzati workshop organizzati in maniera collegiale.

3. Questionari a risposta aperta
Per richiedere informazioni Strutturate sul processo in esame ai responsabili dei controlli chiave possono essere sottoposti 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. Verifica degli indicatori di monitoraggio procedurale, finanziario e fisico
i dati raccolti nella fase preliminare relativamente agli indicatori di monitoraggio procedurale, finanziario e fisico sono verificati sulla base delle registrazioni tenute dalla Struttura auditata.

6. 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.

<u>Riunione di apertura dell'Audit</u>
La riunione di apertura 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 saranno esaminate di norma:

- le procedure di verifica che saranno effettuate nel corso dell'audit;
- i ruoli e la suddivisione dei compiti all'interno del *team* di *Internal Auditing*, nel caso in cui 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);
- i tempi di lavoro (inclusa una prima proposta di un piano interviste);
- le aree considerate critiche dal *management*;
- eventuali ulteriori argomenti di particolare interesse dell'auditor;
- l'identificazione nominativa dei referenti del processo o della procedura auditata.

Nella riunione potrà essere svolta l'intervista con il responsabile dall'azione/procedura oppure il *workshop* per verificare, sulla base delle informazioni raccolte, le valutazioni dei rischi e dei controlli formulate nella Risk and Control Matrix .
Completata l'analisi di processo e identificati i relativi controlli, gli auditor valutano con metodologia di campionamento l'efficacia del controllo da un punto di vista operativo ossia se il controllo opera effettivamente. Qualsiasi metodologia di campionamento si basa sull'assunzione che non è necessario esaminare tutte le evidenze per confermare la correttezza di un'asserzione. La tipologia di campionamento utilizzata è prettamente un metro di giudizio: più critiche sono le asserzioni da validare, più forte è il grado di precisione richiesto all'analisi, più estensiva e popolata di item deve essere l'attività .
Nello specifico tengono in considerazione i seguenti elementi:

- Numero e significatività dei rischi che vengono mitigati dal controllo;
- Tipologia di controllo;
- Esistenza di controlli compensativi che, in caso di fallimento del controllo in esame, potrebbero ridurre l'impatto del manifestarsi del rischio;
- Probabilità che il controllo operi in modo efficace;
- Eventuali cambiamenti significativi all'interno dell'ambiente di controllo per il periodo considerato.

I singoli elementi del campione sono definiti come componenti individuali facenti parte dell'intera popolazione e possono corrispondere a documenti, registrazioni, transazioni, righe d'ordine e altro.

I principali aspetti oggetto di verifica sono: l'effettiva conformità dell'operazione agli obiettivi dell'azione e alla procedura; il rispetto degli adempimenti richiesti per l'approvazione, durante l'esecuzione dell'operazione e successivamente alla sua conclusione.

In caso sussistano i presupposti e la necessità di effettuare controlli presso la sede di soggetti terzi, sottoposti a controllo in quanto destinatari di provvedimenti della ASST Lariana oppure di Enti e Società del Sistema regionale oppure di effettuare circolarizzazione, si procederà con le modalità esposte in appendice.

Le constatazioni e le relative raccomandazioni che emergono nel corso dell'esecuzione del lavoro sul campo devono essere formalizzate mediante la compilazione di un rapporto di audit.

4) Reporting e comunicazione dei risultati

Conclusa la fase di esecuzione dell'audit sul campo, il team di audit predispone il rapporto preliminare di audit. Tale documento contiene l'indicazione della problematica rilevata

dall'auditor, la descrizione del rischio, la raccomandazione per migliorare il Sistema di Controllo Interno.
Riassume le constatazioni formulate in fase di analisi di processo documentate sulla base delle evidenze raccolte.

Riunione finale
Le constatazioni contenute nel rapporto preliminare di audit sono discusse dal team di audit e dal responsabile e referenti della Struttura auditata in una riunione finale da svolgersi entro i termini previsti dal Programma di Audit condiviso con il soggetto auditato. 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.

Rapporto definitivo e comunicazione dei risultati
Dopo la condivisione con le strutture auditate, viene intrapresa la stesura del Rapporto definitivo di Audit .

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 dalla riunione finale.

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:
- obiettivi/ambito audit;
- riferimenti per raccolta evidenze
- processi/attività sottoposte ad audit;
- rilevazioni generali (evidenze e risultanze dell'audit)
- eventuali osservazioni del responsabile dell'area soggetta ad audit
- eventuali allegati.

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

Rilevazioni generali
Le Rilevazioni generali costituiscono 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. Contengono le evidenze raccolte in sede di audit e le risultanze in base all'esame della documentazione e della verifica sul campo con indicazione di non conformità e/o osservazioni e7o commenti/raccomandazioni. Inoltre sono riportati gli aspetti principali della posizione del responsabile della Struttura auditata se divergente dalle conclusioni del rapporto.

Obiettivi /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.

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 riunione finale 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 al Direttore dell'area di competenza.

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.

9.3 Gli interventi di audit riguardanti Enti e Società del Sistema Regionale

Il responsabile dell'audit assicura, comunque, adeguata comunicazione all'auditato circa modalità e fasi di svolgimento del'audit.

10. 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 Programma Annuale di Audit.

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*.

Il Rapporto di Follow up 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.

10.1 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.

11. ARCHIVIAZIONE DELLA DOCUMENTAZIONE DI AUDIT

11.1 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 (Regolamento operativo, Piano annuale di audit, fascicoli degli audit, ecc.). Il materiale viene fascicolato e custodito all'interno di appositi armadi.

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.

11.1.1 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.

11.2 L'archivio informatico e il Sistema Informativo di Audit

L'archivio informatico è organizzato in sezioni o cartelle, secondo la seguente architettura:
- Regolamento 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 Programma 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 ai componenti del Gruppo Operativo aziendale IA.
La concessione di diritti di accesso ad eventuali altri soggetti deve essere valutata ed autorizzata da parte del Dirigente Responsabile della funzione di IA.