REGOLAMENTO DI INTERNAL AUDITING

ASL GALLURA

Luglio *2026*

INDICE

Premessa

La legge regionale n. 24 dell'11.9.2020, art. 3, comma 3, lett. e), attribuisce all'Azienda Regionale della Salute (Ares) la Funzione di omogeneizzazione della gestione dei bilanci e della contabilità delle singole aziende ivi compreso il sistema di Internal Auditing, il presente Regolamento di Internal Auditing per l'Asl Gallura si colloca nel quadro disciplinato dalla delibera della Giunta Regionale n. 31/16 del 13.10.2022 avente ad oggetto le "*Linee di indirizzo per l'avvio e l'espletamento della Funzione di Internal Auditing nel Sistema Sanitario della Regione Autonoma della Sardegna, in attuazione dell'art. 3 della L.R. 11.9.2020 n. 24"*, al quale mandato ha fatto seguito con delibera Ares n.276 del 07.12.2022 l'approvazione del *Regolamento di Internal Auditing del Sistema Sanitario della Regione Autonoma della Sardegna*, avente lo scopo di definire: i livelli, le metodologie e gli strumenti di controllo, nonché la ripartizione operativa delle competenze tra Ares e le altre aziende del SSR e le linee guida minime a cui gli enti del SSR devono conformarsi nello svolgimento della propria Funzione di IA.

Art. 1 Oggetto e finalità

Il presente regolamento disciplina il sistema di internal auditing dell'Azienda, quale strumento di supporto alla Direzione Strategica per: il miglioramento dei processi amministrativi, sanitari e tecnici, la verifica dell'efficacia, efficienza ed economicità della gestione, la prevenzione dei rischi, inclusi quelli corruttivi e il rafforzamento del sistema dei controlli interni.

L'attività di Internal Auditing (IA) rappresenta uno strumento essenziale per la valutazione e il miglioramento dei processi di governance, gestione del rischio e controllo dell'organizzazione, tramite un approccio sistematico, rigoroso e di *risk based*; nonché è di supporto al vertice e alla dirigenza, con responsabilità di monitoraggio e valutazione del sistema del controllo interno e, in generale, dei rischi relativi alle attività poste in essere dall'azienda nell'ottica di prevenire eventuali fatti pregiudizievoli rispetto al raggiungimento degli obiettivi istituzionali, con il fine di governare i rischi piuttosto che subirli.

Le **finalità** che si intendono perseguire attraverso il presente Regolamento sono le seguenti:

- definire i principi, le procedure e le metodologie utili allo svolgimento della Funzione di Internal Auditing (IA) per assistere la Direzione Aziendale nell'identificazione, mitigazione e monitoraggio dei rischi e dei relativi controlli;
- promuovere una consapevolezza condivisa che coinvolga oltre la Direzione Aziendale, anche tutte le strutture ed unità operative aziendali;
- individuare gli strumenti di lavoro della Funzione Internal Audit dell'ASL Gallura;
- armonizzare e standardizzare le fasi e le modalità operative nonché gli output dell'attività di Auditing;
- definire gli ambiti di collaborazione tra la Funzione Internal Audit, la Direzione Aziendale e le Unità Organizzative e le Strutture di Asl Gallura;
- definire le fasi e le tempistiche del processo di audit.

Il contenuto del presente regolamento, che ha l'obiettivo di fornire una guida pratica e un

riferimento metodologico per lo svolgimento delle attività di audit interno, può essere soggetto a revisioni nel caso di mutamento del contesto organizzativo e sulla base dei risultati annuali dell'attività di auditing. Le revisioni dovranno essere approvate seguendo l'iter procedurale previsto per l'approvazione del Regolamento stesso.

Art. 2 Ambito di applicazione

L'attività di internal auditing si applica a tutte le strutture aziendali (sanitarie, amministrative, tecniche); processi clinico-assistenziali, amministrativo-contabili e di supporto; progetti, programmi e utilizzo delle risorse.

Art. 3 Principi di riferimento

La Funzione di IA si deve conformare ai princìpi e alle regole di condotta emanate a livello internazionale dall'Institute of Internal Auditors (IIA) che rappresentano il cosiddetto International Professional Practices Framework (IPPF).

L'internal auditing si ispira ai seguenti principi:

- indipendenza e autonomia;
- obiettività e imparzialità;
- riservatezza;
- professionalità;
- approccio basato sul rischio (risk-based auditing).

Art. 4 Quadro normativo di riferimento

La Funzione di IA si deve conformare ai princìpi e alle regole di condotta emanate a livello internazionale dall'Institute of Internal Auditors (IIA) che rappresentano il cosiddetto International Professional Practices Framework (IPPF).

I nuovi Global Internal Audit Standards (GIAS), rilasciati dall'Institute of Internal Auditors (IIA) nel gennaio 2024 ed entrati in vigore il 9 gennaio 2025, riorganizzano e razionalizzano il framework operativo (ossia, lo schema che facilita lo sviluppo, l'interpretazione e l'applicazione delle conoscenze utili a una disciplina o a una professione) per l'Internal Auditing in modo sostanziale definendo i nuovi *Standards*.

Il documento dedica uno specifico approfondimento all'Internal Auditing nel settore pubblico, dettando una serie di linee guide e requisiti peculiari volti a garantire che le particolarità di questo settore siano adeguatamente considerate dagli Internal Auditors che vi operano.

Applicato alle aziende sanitarie, il proposito dei nuovi standard è quella di trasformare l'Internal Audit da semplice strumento di verifica formale a pilastro strategico per la governance, la gestione integrata dei rischi e la tutela della salute pubblica. Particolare attenzione è dedicata alla prevenzione e alla rilevazione delle frodi, sottolineando il contributo dell'Internal Audit nella protezione dell'integrità e della trasparenza dei processi aziendali.

L'applicazione dei GIAS nelle funzioni di IA del settore pubblico deve comunque tenere conto che esso opera in un ambiente politico, con strutture di governance, organizzative e di finanziamento differenti rispetto al settore privato, nonché in un quadro normativo che include leggi,

regolamenti, ordini e norme amministrative e altri tipi di requisiti governativi specifici per le giurisdizioni all'interno delle quali opera un'organizzazione.

Sulla base di tali indicazioni, le funzioni Internal Audit nel settore pubblico sono spesso chiamate a concentrare la propria attività nel:

- garantire la conformità a leggi e/o regolamenti;
- identificare le opportunità per migliorare l'efficienza, l'efficacia e l'economicità dei processi e dei programmi dell'amministrazione pubblica;
- determinare se le risorse pubbliche sono adeguatamente salvaguardate e utilizzate in modo appropriato per fornire servizi in base a principi di equità;
- valutare se le prestazioni di un'organizzazione sono in linea con le finalità e gli obiettivi strategici della stessa.

Art. 5 Funzione di Internal Auditing

L'Internal Auditing, secondo la definizione fornita dall'Associazione Italiana Internal Auditors (AIIA), è "*un'attività indipendente e obiettiva di assurance* (Valutazione Sistema di Controllo Interno e di Gestione dei Rischi (SCIGR)) *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 è esercitata nel rispetto del Codice Etico, dei Principi e delle Regole di condotta (Integrità, Obiettività, Riservatezza, Competenza, Diligenza professionale) cui gli auditor devono conformarsi.

La Funzione di IA per l'ASL Gallura si inserisce nel modello regionale di IA che prevede una ripartizione di compiti e competenze tra Ares e le altre aziende del SSR, come previsto nel *Regolamento di Internal Auditing del Sistema Sanitario della Regione Autonoma della Sardegna* di cui al precedente art.2.

Nel quadro del riparto delle competenze nello svolgimento delle funzioni di IA, si riepiloga quanto segue:

- **Ares**, a seguito della individuazione di un Responsabile, svolge una Funzione di IA di omogeneizzazione del sistema di IA per il SSR, definendo le linee guida minime, coordina l'attività di controllo interno, propone le linee guida di omogeneizzazione contabile, fornendo il supporto metodologico per la pianificazione, per lo svolgimento degli audit, per il reporting e la formazione;
- **Asl Gallura (come le altre aziende del SSR)**, svolge l'attività di IA conformandosi alle indicazioni del Responsabile della Funzione di IA in Ares.
  Oltre all'attività svolta nel quadro regionale, l'azienda è legittimata a svolgere attività di IA finalizzata al monitoraggio di ulteriori aspetti critici scaturiti nella fase di mappatura dei rischi aziendali.

Tenuto conto delle competenze di coordinamento funzionale, di supporto metodologico e di elaborazione delle linee guida per le funzioni di IA di tutto il SSR attribuite ad Ares, il presente

regolamento ha lo scopo di regolare l'attività della Funzione di IA dell'Asl Gallura, sia in coordinamento con la Funzione di IA esercitata da Ares, sia come Funzione propria, conformandosi ai principi ed alle regole di condotta emanate a livello internazionale *dall'Institute of Internal Auditors (IIA)* che rappresentano il cosiddetto *International Professional Practices Framework (IPPF)*, nonché ai nuovi *Global internal Audit Standards (GIAS o Standards)*.

Art.6 Funzione di Internal Auditing di Asl Gallura

La Funzione di Internal Auditing svolge un ruolo fondamentale nel migliorare la capacità di un'organizzazione di servire il pubblico interesse. Sebbene la Funzione principale dell'Internal Auditing sia quella di rafforzare la governance, il *risk management* e i processi di controllo, i suoi effetti si estendono ben oltre. L'Internal Auditing contribuisce infatti alla stabilità e alla sostenibilità complessive di un'organizzazione fornendo assurance sulla sua efficienza operativa, sull'affidabilità del reporting, sulla conformità a leggi e/o regolamenti, sulla salvaguardia delle risorse e sulle questioni etiche. Questo, a sua volta, favorisce la fiducia del pubblico nell'organizzazione e nei sistemi più ampi di cui fa parte.

Gli **obiettivi strategici** della Funzione di IA consistono nel:

- verificare il corretto funzionamento del sistema di controllo interno, volto a migliorare l'efficacia/efficienza dell'attività di controllo, razionalizzandola in Funzione dei rischi;
- nell'individuare i punti di debolezza dei processi aziendali;
- nel ridurre gli impatti economici dei rischi e nel validare i modelli interni.

Si premette che il *Risk Assessment (valutazione del rischio)* è l'insieme delle azioni volte a individuare e analizzare i rischi rilevanti per capirne gli impatti sul raggiungimento degli obiettivi di un'organizzazione.

Il *Regolamento di Internal Auditing del Sistema Sanitario della Regione Autonoma della Sardegna,* approvato con delibera Ares n.276 del 07.12.2022, chiarisce che il processo metodologico di *Risk Assessment* da utilizzare nell'ambito del SSR è di competenza di Ares.

Definito "*controllo" una qualsiasi azione intrapresa dal management, dal board o da altri soggetti per gestire i rischi ed aumentare le probabilità di conseguimento degli obiettivi stabiliti*, si asserisce che il *Sistema di Controllo Interno* dell'Azienda deve coinvolgere tutto il personale aziendale, seppur con diversi ruoli.

In particolare, la Funzione di Internal Audit, in quanto Funzione indipendente, svolge un *controllo di terzo livello*, focalizzandosi sulle attività di verifica (anche definite come controlli di secondo livello) poste in essere da altre funzioni aziendali. Inoltre, ha il compito di supervisionare i controlli di primo livello attuati dai referenti responsabili dei vari processi aziendali, ad ogni livello di operatività dell'Azienda.

Di seguito una sintesi della delle competenze attribuite ai vari livelli del Sistema di Controllo Interno:

Livello di controllo	Descrizione del controllo
I. Controlli di linea	Svolti sia da chi mette in atto una determinata attività, sia da chi ne ha la responsabilità di supervisione, generalmente nell'ambito della stessa unità organizzativa o Funzione (controlli procedurali, informatici, comportamentali, amministrativo-contabili, ecc.)
II. Monitoraggio e gestione rischi (Funzioni dedicate)	Verifiche di controllo periodiche effettuate da servizi preposti a individuare, valutare, gestire i rischi legati all'operatività, in coerenza rispetto agli obiettivi aziendali e secondo criteri che consentano un efficace monitoraggio (Risk Management, Controllo di gestione, ecc.)
III. Assurance (Internal Auditing)	Attività che deve fornire una generale assurance sul corretto funzionamento dei primi due livelli e sul complessivo disegno del Sistema di Controllo Interno, attraverso valutazioni indipendenti. Non deve deresponsabilizzare gli altri due livelli.

Resta fermo che l'attività di Internal Auditing non attenua le responsabilità in capo ai Direttori delle Unità Operative e delle funzioni aziendali, in merito all'istituzione ed al mantenimento di un idoneo controllo di primo livello, efficace e adeguato rispetto ai rischi connessi alla gestione. La Funzione di IA si configura pertanto come complementare e non succedanea rispetto ai controlli di secondo livello; questi ultimi permangono nella competenza esclusiva delle rispettive funzioni, che ne rispondono nei modi e nei termini concordati dall'Azienda.

Nel rispetto delle competenze attribuite dal *Regolamento di Internal Auditing del Sistema Sanitario della Regione Autonoma della Sardegna*, la Funzione di IA in ASL Gallura viene svolta in una duplice prospettiva:

Su coordinamento della Funzione Ares

La Funzione si configura nelle seguenti attività:

- applicazione del processo di *Risk Assessment* definito da Ares, quale strumento base di determinazione della Pianificazione Triennale da cui emergeranno le priorità dell'attività di IA;
- pianificazione Triennale della Funzione di IA Aziendale, definita sulla base delle, linee guida emanate da Ares;
- alimentazione periodica e costante dell'ambiente Cloud, consultabile e utilizzabile come archivio da tutte le funzioni di IA del SSR, ciascuna per la propria Azienda;
- partecipazione al piano di formazione, previsto per la funzione di IA di Ares e degli altri enti del SSR;
- partecipazione agli Audit sulle aree PAC, sulla base delle indicazioni del Responsabile della funzione di IA di Ares;
- supporto alla mappatura dei processi, quale attività propedeutica al corretto avvio della

funzione di IA su base regionale, con l'individuazione dell'owner di processo;

- supporto al Responsabile della funzione di IA su Ares in tutte le fasi del processo di analisi, misurazione e mappatura dei rischi, nella predisposizione del Piano Triennale di Audit e in tutte le fasi del processo di Audit.

Funzione di IA propria dell'Azienda Asl Gallura

La Funzione si configura nelle seguenti attività:

- pianificare e coordinare l'attività di audit all'interno della Asl;
- predisporre il piano triennale e il programma annuale di audit della Asl;
- eseguire gli audit programmati e i relativi follow up, oltreché eventualmente avviare e gestire degli audit su specifiche aree individuate della Direzione Aziendale, purché ulteriori rispetto a quelli individuati dal Responsabile della Funzione di IA su Ares;
- favorire la comprensione dell'importanza di un processo formale, documentato e collaborativo nel quale i responsabili dei processi auditati siano direttamente coinvolti nel giudicare e monitorare l'efficacia dei controlli svolti;
- svolgere attività consulenziale e di assurance, nei confronti della Direzione Aziendale e di tutti gli owner di processo sulla base delle risultanze degli audit condotti sul SSR;
- alimentare l'archivio cloud con le evidenze degli audit svolti;
- promozione della cultura del processo, dei rischi e dei controlli;

Art. 7 Coordinamento con altri organismi

L'Internal Audit opera in raccordo con:

- Organismo Indipendente di Valutazione (OIV);
- Responsabile Prevenzione Corruzione e Trasparenza (RPCT);
- Collegio Sindacale;

Art. 8 Struttura Organizzativa e Personale assegnato

La Funzione di Internal Auditing è svolta nell'ambito della SC Area Data Management ritenuta idonea sia in quanto Struttura di Staff alla Direzione Aziendale, svolgendo attività di supporto tecnico, sia per il *core* dell'attività di programmazione e controllo svolto sulla gestione aziendale.

La SC Area Data Management al fine di assicurare una gestione efficace dell'attività di IA, la comunicazione periodica alla Direzione Aziendale e alla struttura organizzativa di IA individuata da Ares individua all'interno della struttura un:

- Referente per la Funzione di Internal Auditing: partecipa a specifici corsi di formazione e/o aggiornamento definiti e individuati nel piano di formazione predisposto dalla struttura organizzativa di IA individuata da Ares.

Il personale assegnato allo svolgimento della Funzione di IA può svolgere ruoli e responsabilità addizionali purché la Direzione Aziendale nella fase di affidamento di tali ulteriori ruoli e responsabilità adotti le misure compensative di tutela del requisito dell'indipendenza.

Ciascun auditor assicura, per gli audit ai quali è designato a partecipare, l'insussistenza di conflitti d'interesse e qualora ritenga di trovarsi in una posizione di conflitto d'interesse seppur potenziale

deve tempestivamente segnalarlo al Direttore della SC Area Data Management che provvede alla sua immediata sostituzione.

Gli auditor non devono essere stati sottoposti nell'ultimo triennio a procedimenti di natura disciplinare. Nello svolgimento delle attività di IA il personale assegnato alla Funzione di IA non può prescindere dagli obblighi cui è tenuto il dipendente pubblico nell'ambito dell'attività lavorativa, obblighi che derivano dai principi costituzionali, quali l'imparzialità e il buon andamento dei processi svolti, nonché da disposizioni contenute nel codice civile, nelle norme nazionali sul pubblico impiego, nonché negli Standard professionali e del Codice Etico dell'Institute of Internal Auditors.

Qualora, nel corso dell'attività di audit emergano fatti che possano dar luogo a ipotesi di responsabilità civile, penale o amministrativa, il Referente della Funzione di IA è tenuto ad informare immediatamente il Direttore della SC Area Data Management che riferirà al Direttore Generale di Asl Gallura, quale rappresentante legale dell'Azienda per l'avvio di eventuali azioni di responsabilità e/o di denuncia qualora gli elementi raccolti siano concreti e attuali o per operare affinché il danno sia evitato.

Art. 9 Compiti e Responsabilità

La Funzione di Internal Audit di Asl Gallura è composta da:

- il Referente della Funzione di Internal Audit;
- il team di Audit, a supporto dell'attività svolta dal Referente di Internal Audit, se presente;
- eventuali esperti delle materie oggetto di audit per il supporto in ambito specialistico, se necessario.

<u>Le competenze del Referente IA sono:</u>

- predisposizione e invio al Responsabile della Funzione di IA di Ares entro il 30 settembre il *Piano Triennale di Audit* dell'Asl Gallura;
- recepimento, entro i tempi indicati dal Responsabile della Funzione di IA di Ares, le indicazioni del Responsabile della Funzione di IA di Ares;
- entro il 30 ottobre, conformarsi alle eventuali indicazioni del Responsabile della Funzione di IA di Ares e sottoporre all'esame e all'approvazione del Direttore Generale della Asl Gallura il *Piano Triennale di Audit*, che lo adotterà con delibera entro il 30 ottobre;
- riferire entro il 30 ottobre sui risultati, gli obiettivi e l'ambito di copertura dell'incarico mediante comunicazione formale alla propria Direzione e al Responsabile della Funzione di IA su Ares;
- trasmettere entro il 10 novembre il *Piano Triennale di Audit* deliberato al Responsabile della Funzione di IA di Ares;
- gestire efficacemente l'attività di IA al fine di assicurare che la stessa aggiunga valore all'organizzazione dell'Asl Gallura e del SSR;
- contribuire al miglioramento dei processi di *governance*, gestione del rischio e controllo dell'organizzazione presso l'Asl Gallura tramite un approccio sistematico, rigoroso e *risk based* sulla base di quanto stabilito nel piano suddetto;
- raccogliere, analizzare e valutare informazioni sufficienti e utili al fine di conseguire gli obiettivi

dell'incarico;

- comunicare periodicamente alla Direzione Aziendale dell'Asl Gallura e alla SSD IA individuata da Ares in merito allo stato di avanzamento del piano, comprensivo dei rischi significativi, dei problemi di controllo e *governance* e ogni altra questione che necessita di essere sottoposta all'attenzione della Direzione Aziendale e alla SSD IA individuata da Ares;
- definire un sistema di monitoraggio delle azioni intraprese a seguito dei risultati segnalati alla Direzione Aziendale e alla SSD IA individuata da Ares;
- conservare la documentazione dell'incarico sulla base dei criteri definiti dalla SSD IA individuata da Ares;
- supportare la SSD IA individuata da Ares nell'espletamento di attività pianificate nell'ambito di altre aziende sanitarie, consistente per lo più nel rendere disponile il personale dedicato alla Funzione a svolgere gli interventi di *audit* presso le altre aziende del SSR al fine di preservarne l'indipendenza e l'obiettività;
- partecipazione a specifici corsi di formazione e/o aggiornamento definiti e individuati nel piano di formazione predisposto dalla SSD IA individuata da Ares.

Il Referente di IA di Asl Gallura del SSR è autorizzato all'accesso ai dati, ai documenti, alla procedura SiSar-AMC e ai beni aziendali che risultano necessari per lo svolgimento degli incarichi.
L'ambito di copertura delle attività di IA riguarda tutti gli aspetti, i processi, le procedure, le attività ed i comportamenti che abbiano effetti riflessi o diretti sul Bilancio aziendale.

Competenze della Direzione Aziendale sono:

- adottare il regolamento di IA qui declinato e condividere e/o approvare le modifiche allo stesso;
- implementare la Funzione di IA, favorendo e verificando il rispetto del coordinamento funzionale in capo ad Ares e rendendo disponibile il proprio Referente di IA per lo svolgimento degli audit sul SSR avviati da Ares;
- fornire al Referente IA della propria azienda, in base a specifiche e motivate esigenze di controllo e monitoraggio di aree strategiche, indicazioni in merito al contenuto del *piano di audit*;
- assicurare il pieno accesso alle informazioni, documenti, sistemi e personale necessario allo svolgimento delle attività di audit;
- analizzare e prendere atto delle risultanze degli audit, comprese raccomandazioni e piani d'azione, promuovendone l'attuazione presso le strutture competenti;
- curare il dialogo con gli organi di controllo esterni;
- favorire la tempestiva implementazione delle azioni correttive indicate dalla Funzione di Internal Audit;
- promuovere una cultura organizzativa orientata al controllo, alla trasparenza e alla responsabilizzazione, valorizzando il ruolo dell'audit come leva di miglioramento;
- ricevere, entro il 30 ottobre, le risultanze dell'attività di IA svolta sull'Asl Gallura da parte del

Referente di IA;

- approvare, entro il 30 ottobre, il *Piano di Audit* Triennale dell'Asl Gallura.

Le Unità Organizzative e le Strutture di Asl Gallura auditate sono chiamate a collaborare con le attività della Funzione di auditing attraverso:

- messa a disposizione nei tempi concordati dei dati e delle informazioni richieste, su supporto cartaceo e/o informatico, anche in occasione di interviste;
- revisione delle procedure;
- elaborazione tempestiva di commenti e di azioni migliorative in risposta ai rilievi e suggerimenti elaborati dalla Funzione di Internal Audit;
- monitoraggio della effettiva esecuzione delle azioni di rimedio ad esse assegnate;
- informativa tempestiva in merito a riorganizzazioni e progetti speciali che comportino un cambiamento nel profilo dei rischi e del sistema di controllo interno a livello.

Art. 10 Tipologia di Rischi

Si definisce il "*rischio"* come *"un evento incerto che può influire positivamente o negativamente sul raggiungimento degli obiettivi dell'organizzazione (fonte GIAS)".* I rischi possono essere "interni", se derivanti da fattori interni all'azienda ed "esterni", se derivanti da fattori al di fuori del controllo diretto dell'azienda.

Le tipologie di rischio a cui può essere soggetta un'azienda nell'esercizio della sua attività sono di diverse:

TIPOLOGIE DI RISCHI		
Tipologia di rischio	**Codice**	**Descrizione**
Rischio di Compliance	**RC**	Rischi di non conformità a norme, regole standard, nonché a disposizioni e regolamenti, procedure interni alla azienda stessa.
Rischio Amministrativo Contabile	**RAC**	Rischi connessi al mancato rispetto delle norme, direttive, procedure e istruzioni operative dirette a garantire la correttezza e la tempestività di una informativa attendibile, in accordo con i principi contabili adottati dall'Azienda.
Rischio di Frode	**RF**	Rischi connessi alla possibilità che soggetti esterni o soggetti operanti all'interno della struttura aziendale, agiscano attraverso comportamenti fraudolenti pregiudicando l'attività o i risultati dell'Azienda.
Rischio Operativo	**RO**	Rischi connessi alla normale operatività dei processi, flessibilità, efficacia ed efficienza operativa, tutela del patrimonio e della reputazione aziendale.
Rischio di Reporting		Rischi relativi alla produzione veritiera e tempestiva della qualità dell'informazione, intesa sia come informazione interna che esterna.
Rischio Strategico	**RS**	Rischi derivanti dal manifestarsi di eventi che possono condizionare e/o modificare in modo rilevante le strategie e il raggiungimento degli obiettivi aziendali.

TIPOLOGIE DI RISCHI		
Tipologia di rischio	**Codice**	**Descrizione**
Rischio IT	**RIT**	Rischi correlati al verificarsi di situazioni, interne o esterne, che metterebbero a repentaglio la protezione dell'integrità, della disponibilità, della confidenzialità dell'informazione automatizzata e delle risorse usate per acquisire, memorizzare, elaborare e comunicare tale informazione. Tali situazioni possono essere causate anche dall'inadeguatezza e dall'obsolescenza degli strumenti informatici impiegati (hardware) e/o alla scarsa funzionalità dei software, in termini di architettura del sistema, rapidità nei tempi di elaborazione dei dati, facilità di utilizzo, ecc..

Art. 11 Definizione delle Metodologie e degli Strumenti

L'Internal Auditing (IA) è una Funzione indipendente e obiettiva che supporta la Direzione Aziendale nel valutare l'adeguatezza del Sistema di Controllo Interno (SCI). Adottando una metodologia basata sull'analisi dei processi, l'IA assiste il vertice aziendale identificando le aree di rischio, verificando la conformità alle normative e implementando adeguate misure di mitigazione.

Le metodologie e gli strumenti che verranno descritti sono adottati sia nella Funzione di IA svolta dal Referente aziendale quale membro del gruppo di Audit nominato dal Referente in Ares, sia nelle indagini di audit svolte dal Referente aziendale su indicazioni della Direzione Aziendale, a seguito di criticità specifiche emerse nel corso della fase di *Risk Assessment*.

Obiettivi e Indipendenza

L'attività di controllo dell'IA si concentra sui processi amministrativo-contabili e gestionali. Per garantire l'obiettivo primario dell'assurance e consulenza, la Funzione deve godere della massima autonomia:

- assenza di conflitti d'interesse individuali;
- piena libertà di accesso alle informazioni;
- assenza di limitazioni nel campo d'azione;
- indipendenza gerarchica rispetto ai soggetti verificati.

Fasi

Il lavoro dell'Internal Auditing si articola in un ciclo continuo composto da seguenti passaggi fondamentali:

1. **analisi e valutazione dei rischi:** mappatura delle aree più esposte e definizione dei controlli;
2. **pianificazione Triennale e Programmazione operativa:** definizione degli obiettivi di audit a medio e breve termine;
3. **esecuzione del lavoro**: applicazione delle procedure di verifica sul campo o documentali;
4. **reporting e comunicazione dei risultati:** stesura e condivisione dei rapporti di audit con gli stakeholder (ossia ciascun soggetto direttamente o indirettamente coinvolto dalla Funzione di auditing);
5. **follow-up audit**: monitoraggio dell'effettiva attuazione delle azioni correttive concordate;

6. **archiviazione** della documentazione cartacea ed informatica;
7. **formazione** idonea del personale addetto.

Tipologie di Verifiche

Le attività di verifica si dividono in due categorie principali, condotte in collaborazione con i referenti aziendali:

- **verifiche sul campo**: controlli in loco presso le strutture, che coinvolgono i responsabili di processo e gli operatori,
- **verifiche documentali**: analisi e riscontro dei dati e della documentazione fornita dalle unità organizzative.

Art.11.1 Fase 1) Metodologia di Identificazione e valutazione del rischio (*Risk Assessment*)

La prima fase dell'attività di I.A. è costituita dal *Risk Assessment*, ossia da un processo sistematico di identificazione e valutazione dei rischi per individuare le aree maggiormente esposte a rischio, che potrebbero pregiudicare il raggiungimento degli obbiettivi posti dal management.

Il *Risk Assessment* è l'insieme delle azioni volte a individuare e analizzare i rischi rilevanti per capirne gli impatti sul raggiungimento degli obiettivi di un'organizzazione; rappresenta l'analisi preliminare utile per la stesura del Piano di Audit e richiede la mappatura dei processi aziendali.

L'analisi dei rischi del Sistema Sanitario Regionale (SSR) individua le aree critiche che possono compromettere gli obiettivi aziendali, allineandosi alle 7 Aree di Intervento dei *Percorsi Attuativi di Certificabilità del Bilancio (PAC):*

- A - Generale
- B - Immobilizzazioni
- C - Rimanenze
- D - Crediti e Ricavi
- E - Disponibilità Liquide
- F - Patrimonio Netto
- G - Debiti e Costi.

Le aree di rischio sono ulteriormente identificate tramite il monitoraggio di fonti interne ed esterne:

- Verbali del Collegio Sindacale: analisi degli organi di controllo;
- Richieste Istituzionali: ispezioni della Corte dei Conti, dei Ministeri e della Regione;
- Input dell'Assessorato: direttive specifiche dell'Assessorato dell'Igiene e Sanità e dell'Assistenza Sociale.

Nella procedura di valutazione del rischio è necessario tenere conto dei vari livelli di rischio al fine di individuare il livello sul quale agire con la Funzione di IA.

Individuati i rischi oggetto di analisi segue la fase di valutazione, tenuto conto che:

- *Rischio inerente o potenziale* di ciascun processo aziendale è il livello di rischio valutato senza tener conto dell'esistenza e dell'effettiva operatività del Sistema di Controllo Interno e Gestione

del Rischio (SCIGR) implementato dall'azienda;

- *Rischio residuo* è il livello di rischio valutato tenendo conto dell'esistenza e dell'effettiva operatività del SCIGR. Pertanto è il rischio reale a cui l'azienda è esposta;
- *Risk appetite* è il livello di rischio che l'azienda è disponibile ad accettare.

Generalmente, nella fase di *Risk Assessment* finalizzata alla pianificazione degli interventi di *audit*, la valutazione dei rischi viene 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.

La significatività dei rischi viene generalmente valutata mediante una matrice che permette di valutare il rischio in termini di **probabilità**, intesa come la frequenza del manifestarsi del rischio, e di **impatto**, inteso come livello in cui il manifestarsi del rischio potrebbe influenzare il raggiungimento delle strategie e degli obiettivi, con una valutazione di tipo qualitativo.

MATRICE DI VALUTAZIONE DEL GRADO DI RISCHIO			
	B	**M**	**A**
C			
PR			
PO			
R			

GRADO DI RISCHIO = PROBABILITA' x IMPATTO

VALUTAZIONE DELLA PROBABILITA'		
CERTO	**C**	E' presumibile che l'evento si manifesti sistematicamente o ripetutamente nell'arco di un periodo definito
PROBABILE	**PR**	La probabilità di accadimento dell'evento è da considerarsi reale, superiore al 50%
POSSIBILE	**PO**	L'evento ha qualche probabilità di manifestarsi nel periodo e comunque inferiore al 50%
REMOTO	**R**	La probabilità di accadimento dell'evento è da considerarsi remota

VALUTAZIONE DELL'IMPATTO		
ALTO	**A**	Impatto rilevante sul raggiungimento degli obiettivi strategici
MEDIO	**M**	Impatto rilevante sulle attività operative dell'organizzazione
BASSO	**B**	Impatto contenuto sul raggiungimento degli obiettivi strategici dell'azienda; inefficienza o interruzioni nell'operatività, nei pagamenti, problemi temporanei di erogazione del servizio

Il *rischio residuo*, che è quello a cui l'organizzazione è effettivamente esposta, è quindi il risultato di un rischio inerente che è stato ridotto da un insieme di controlli ad un livello minore. La differenza è legata al grado di efficacia dei controlli.

MATRICE DI VALUTAZIONE DEL RISCHIO RESIDUO IN FUNZIONE DEL GRADO DI EFFICACIA DEI CONTROLLI						
	Rischio inerente o potenziale					
Efficacia del sistema di controllo interno		Basso	Medio-Basso	Medio	Medio-Alto	Alto
	Basso					
	Medio-Basso					
	Medio					
	Medio-Alto					
	Alto					

Art. 11.2 Fase 2) Pianificazione triennale e Programmazione Operativa annuale di audit

Il processo di *Risk Assessment* è lo strumento di determinazione della Pianificazione Triennale da cui emergono le priorità dell'attività di IA, quale attività della Funzione di IA svolta dall'azienda su coordinamento della Funzione di Ares.

Il Referente IA in Asl Gallura è tenuto a:

- predisporre e inviare al Responsabile della Funzione di IA di Ares entro il 30 settembre il *Piano Triennale di Audit* dell'Asl Gallura;
- recepire, entro i tempi indicati dal Responsabile della Funzione di IA di Ares, le indicazioni del Responsabile della Funzione di IA di Ares;
- entro il 30 ottobre, conformarsi alle eventuali indicazioni del Responsabile della Funzione di IA di Ares e sottoporre all'esame e all'approvazione del Direttore Generale della Asl Gallura il Piano Triennale di Audit, che lo adotterà con entro il 30 ottobre;
- riferire entro il 30 ottobre sui risultati, gli obiettivi e l'ambito di copertura dell'incarico mediante comunicazione formale alla propria Direzione e al Responsabile della Funzione di IA su Ares;
- trasmettere entro il 10 novembre il Piano Triennale di Audit deliberato al Responsabile della Funzione di IA di Ares;

Il Piano Triennale di Audit pianifica infatti le attività di audit sulla base dei rischi prioritari individuati e misurati con il *Risk Assessment*, evidenziando per ogni intervento di audit l'area PAC di riferimento, la tipologia di rischio che si vuole analizzare, il Responsabile del processo oggetto di analisi e la distribuzione degli interventi di audit nel triennio considerato.

Definita la pianificazione triennale, la fase di programmazione operativa rappresenta la risposta annuale ai rischi identificati nella Pianificazione Triennale.

Al fine di garantire l'indipendenza dell'attività svolta, il Referente della Funzione di IA dell'Asl Gallura è tenuto a redigere in maniera diretta il piano di audit della propria azienda nel rispetto delle indicazioni del Responsabile della struttura organizzativa di IA individuata da Ares, mentre **non può svolgere gli interventi di audit nell'azienda a cui appartiene ma solo nelle altre aziende del SSR**, come da convocazione e organizzazione del *Gruppo di Audit* che il Responsabile della struttura organizzativa di IA individuata da Ares determina in maniera dettagliata e specifica per ogni intervento di audit programmato nell'ambito del Piano di Audit del SSR, frutto del consolidamento dei piani di audit delle singole aziende del SSR e degli specifici Obiettivi di Audit individuati da Ares.

In particolare, il Responsabile della Funzione di IA di ARES forma, per ogni Azienda del SSR, un gruppo di auditor, avendo cura di individuarne anche un Responsabile/Referente e tenendo conto che il Referente della Funzione di IA di un'azienda non può svolgere gli interventi di audit nell'azienda alla quale appartiene, ma solo nelle altre aziende del SSR. Ciò al fin di preservarne il requisito dell'indipendenza.

Il Gruppo di Auditing individuato avvia quindi i lavori di preparazione della successiva fase di esecuzione del lavoro caratterizzata dall'*Osservazione sul Campo* (walkthrough).

In particolare, questa fase di programmazione operativa riguarda l'analisi e lo studio della normativa, dei regolamenti, delle procedure esistenti e delle regole di funzionamento del processo, dell'organizzazione dell'attività e si conclude con l'invio della "*lettera di comunicazione di avvio dell'Audit"* che il Responsabile della Funzione di IA di Ares invia:

- alla Direzione dell'Azienda sottoposta ad Audit;
- al gruppo di audit;
- al Responsabile del processo analizzato;
- al Direttore Generale di Ares per conoscenza.

Audit aziendali che esulano dalle indicazioni regionali

Il piano di Audit può includere anche interventi su aree specifiche individuate dalla Direzione Aziendale, purché ulteriori rispetto a quelli individuati dal Responsabile della funzione di IA di Ares, derivanti da obiettivi strategici della Direzione Aziendale, da segnalazioni di aree critiche da parte dei direttori delle unità operative, o comunque dall'attività di *Risk Assessment.*

Gli audit che derivano da criticità proprie che l'azienda intende analizzare sono svolte in autonomia dal proprio personale addetto alla Funzione di IA, nel rispetto degli obblighi di condotta previsti dagli Standard Internazionali dell'Institute of In Internal Auditors di indipendenza, riservatezza e competenza, lasciando facoltà di condivisione con il Responsabile della struttura organizzativa di IA individuata da Ares.

Per tali interventi di audit i requisiti minimi da indicare nel Piano di audit sono:

- il processo e/o procedura oggetto di audit,
- il tipo e obiettivo dell'audit,
- i criteri di valutazione,
- gli strumenti di supporto e di rilevazione,
- le modalità di comunicazione agli interessati del calendario e delle specifiche del singolo audit,
- il Responsabile e/ o Referente interno alle strutture interessate per la fase di istruttoria e verifica sul campo,
- le modalità di comunicazione dei risultati agli interessati e alla Direzione Generale.

Art.11.3 Fase 3) Esecuzione del lavoro

La fase di esecuzione dell'Audit, successiva alla programmazione, si articola nell'*osservazione diretta* (walkthrough) e nell'impiego di metodologie complementari. L'intero processo è volto a mappare le operazioni, rilevare i punti deboli, valutare i rischi e testare l'affidabilità dei controlli interni in

un'ottica di miglioramento aziendale continuo.

Strumenti e Metodologie di Esecuzione

Questionari o Check-list: Utilizzati per mappare le macro-fasi e le operazioni elementari, oggetto di domande specifiche e di un'analisi di dettaglio, è strutturato prevedendo un ventaglio di possibili risposte a sistema riduttivo (SI, NO, NA). Ad ogni domanda così creata viene associata la corrispondente tipologia di rischio, mentre in fase di intervista verranno raccolte eventuali ulteriori osservazioni;

Riunione di Apertura: Incontro preliminare obbligatorio tra auditor, responsabili e collaboratori per definire la struttura sottoposta a verifica, lo scopo e modalità operative sul campo;

Walkthrough: l'osservazione diretta prosegue con l'intervista rivolta ai principali attori del processo e il questionario, così strutturato, diventa uno strumento integrativo e fondamentale per condurla, utile sia per raccogliere dati e informazioni che per evitare errori e omissioni di fasi del processo nelle quali possono celarsi eventuali anomalie e irregolarità.

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

Workshop: Sessioni di gruppo per confrontare le posizioni dei vari funzionari coinvolti nelle diverse fasi di lavorazione;

Questionari Aperti/Chiusi: Strumenti di approfondimento somministrati previa notifica al Responsabile della struttura;

Azioni di Re-performance: Ripetizione pratica delle procedure di controllo da parte dell'auditor, alla presenza degli addetti ai lavori, per certificarne l'esito;

Campionamento: Verifica su un sottoinsieme rappresentativo della popolazione aziendale (casuale, mirato o sistematico) per trarre conclusioni sull'intero universo esaminato.

La fase appena descritta è rispettata sia in caso di partecipazione al Gruppo di Audit individuato dal Referente della Funzione IA in Ares, allo scopo di dare esecuzione alla Funzione di IA, così come programmata a livello regionale, sia nel caso di Funzione di audit avente ad oggetto obiettivi ritenuti strategici a livello aziendale.

Art.11.4 Fase 4) Reporting e Comunicazione dei Risultati

Conclusa la fase esecutiva, si procede con la predisposizione di un rapporto preliminare, che riassume le constatazioni formulate in fase di analisi del processo. Nell'incontro di chiusura del Gruppo di Audit vengono discusse tutte le constatazioni ed i rilievi emersi tramite l'attività Auditing e viene redatto il *Rapporto finale* che 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 sul sistema dei controlli di primo e secondo livello.

Il *Report finale* deve contenere almeno le seguenti informazioni:

- Data dell'Audit ed il periodo di tempo coperto dall'Audit;
- Identificazione dell'attività e del settore d'intervento sottoposti ad Auditing;
- Elenco dei partecipanti ai lavori;
- Obiettivi e criteri rispetto ai quali è stato condotto l'Audit;

- Documenti di riferimento per l'Audit;
- Rischi rilevati e gli adeguamenti raccomandati;
- Follow-up previsto.

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

È necessario produrre un *Report finale* anche nel caso di interventi di audit avente ad oggetto obiettivi ritenuti strategici a livello aziendale. Il report viene redatto dal Referente aziendale della Funzione di IA, e sintetizza in maniera rigorosa e dettagliata le evidenze raccolte durante l'analisi operativa. Il documento ha l'obiettivo di esporre i rilievi emersi, associando a ciascuno di essi un appropriato livello di rischio e proponendo raccomandazioni concrete finalizzate al miglioramento dei processi aziendali.

Il *Report finale*, sia in caso di Audit di rilievo regionale che in caso di audit riferito a rilievi critici aziendali, è condiviso non solo con l'Unità Operativa o la Funzione auditata, ma anche, laddove previsto, con l'Azienda oggetto di audit, in caso di Gruppo di Audit, affinché il documento possa essere oggetto di ulteriori valutazioni e, se necessario, di integrazioni o di commenti aggiuntivi da parte dei responsabili coinvolti dev'essere condiviso con il Responsabile del processo oggetto di audit e con il Direttore Generale.

Art.11.5 Fase 5) 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 della Funzione di IA di Ares 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.

Anche nel caso di audit specifici svolti nell'interesse di monitorare criticità specifiche dell'azienda, il monitoraggio e la verifica dell'implementazione delle azioni correttive rappresenta la chiusura dell'intero ciclo di audit. In tale contesto, il follow-up si configura come un processo sistematico volto a garantire che le misure adottate, in risposta alle criticità riscontrate, siano efficaci e realizzate nei tempi prestabiliti. Un'attenta verifica dell'efficacia delle azioni correttive consente, infatti, di confermare il raggiungimento degli obiettivi inizialmente prefissati o, eventualmente, di individuare ulteriori margini di miglioramento. Solo dopo aver accertato la completa risoluzione delle problematiche evidenziate si procede alla formale chiusura dell'audit, oppure si attivano eventuali

escalation per gestire nuove criticità, assicurando così un ciclo di controllo dinamico e orientato al costante miglioramento del sistema di gestione dei rischi.

Art.11.6 Fase 6) Archiviazione ed eventuale denuncia erariale

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.

Tutta la documentazione relativa all'attività di audit è conservata dal Responsabile/Referente del Gruppo di Audit. Il materiale viene fascicolato e custodito all'interno di apposito archivio informatico (area Cloud per tutte le aziende del SSR), che consenta di mantenere la segretezza degli atti e sia facilmente consultabile e reperibile dal Responsabile della Funzione di IA di Ares.

Qualora dall'attività di audit emergano fatti che possano dar luogo a responsabilità per danni causati alla finanza pubblica (responsabilità erariale) o venga acquisita notizia di un reato perseguibile penalmente, il Responsabile/Referente del Gruppo di Audit deve informare per iscritto il Direttore Generale dell'Azienda sottoposta ad Audit e per conoscenza il Responsabile della Funzione di IA di Ares.

L'obbligo di denuncia sussiste qualora il danno sia concreto e attuale e non quando i fatti abbiano solo una mera potenzialità lesiva.

Anche il Referente della Funzione IA, svolta a favore di obiettivi critici specifici dell'azienda Asl Gallura, quindi ulteriore rispetto all'attività configurata nel quadro regionale, è tenuto ad archiviare scrupolosamente tutta la documentazione relativa all'attività di Audit svolto. Il materiale, in formato elettronico, deve essere conservato in formato digitale in apposita area del sistema documentale aziendale. La documentazione per la quale non è possibile la conservazione digitale, viene fascicolata e custodita all'interno di apposito armadio che consenta di mantenere la segretezza degli atti facilmente consultabili e reperibili dal Team di Audit.

Anche in questo caso specifico, qualora dall'attività di Audit emergano elementi tali da far ipotizzare possibili profili di responsabilità di natura erariale o penale, il Referente della Funzione di IA ne dà riservata comunicazione alla Direzione Aziendale, affinché, valutata la rilevanza dei fatti, siano eventualmente attivate, nei modi e tempi ritenuti opportuni, le segnalazioni alle autorità competenti e agli organi preposti.

Art.11.7 Fase 7) Formazione e presentazione della Funzione di IA

II personale assegnato alla Funzione di IA, per svolgere il suo compito con la dovuta competenza deve seguire un percorso formativo adeguato, migliorando continuamente la propria preparazione professionale in materia.

È competenza di Ares, mediante la sua struttura di IA, nell'ottica di perseguire l'armonizzazione del sistema di IA del SSR, di curare la formazione continua.

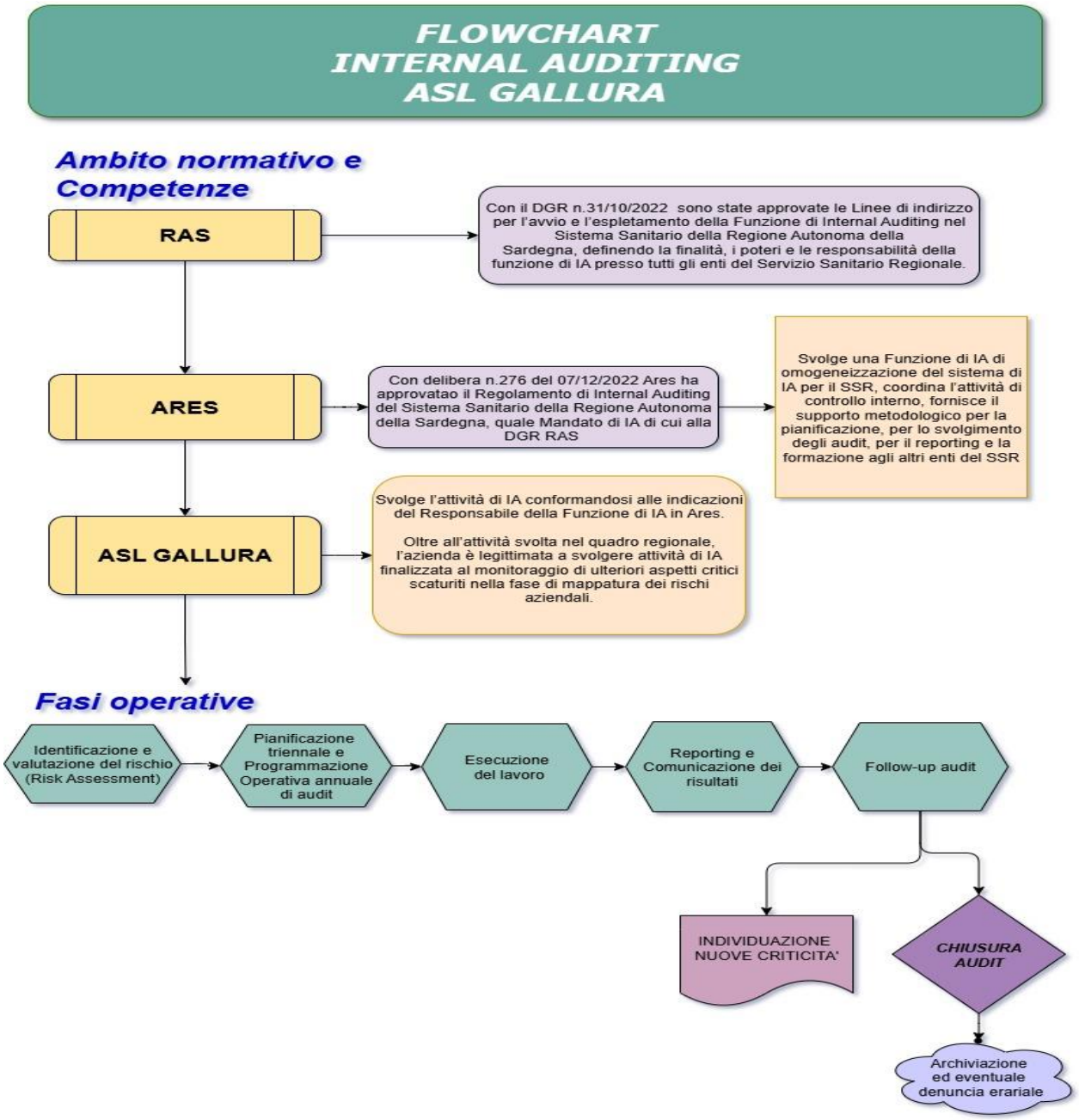
Permane in capo al Responsabile della Funzione di IA aziendale curare una formazione complementare a quella di cui al punto precedente, individuando l'istruzione da fornire al personale mediante formazione interna ed esterna.

La formazione del team IA deve svilupparsi su due direttrici: quella professionale (linee guida, normativa specifica, etc.) e quella generale di conoscenza dell'Azienda e dei suoi processi, con particolare riguardo all'organizzazione, alle sue regale, alle attività e ai controlli interni.

La formazione comprende anche l'esigenza di presentare la Funzione di IA, nei modi e nei tempi convenuti con la Direzione Aziendale, a tutte le strutture ed unità operative dell'azienda, per acquisire una partecipazione informata e condivisa in merito all'attività svolta, affinché l'intervento di IA sia efficace e costituisca un interesse comune dell'organizzazione.

Art. 12 Sintesi

Tutte le attività connesse al processo di l'Internal Audit e illustrate nel presente Regolamento sono sintetizzate nella seguente flowchart:



Art. 13 Definizioni e abbreviazioni

IA: Internal Auditing

SCI: Sistema di Controllo Interno

IIA: Institute of Internal Auditors

IPPF: International Professional Practices Framework

GIAS: Global Internal Audit Standards

Art. 14 Periodo di validità del documento

Il presente regolamento ha validità triennale in assenza di mutamenti normativi/legislativi, di variazioni organizzative o di necessità di modifica dei contenuti che determinino un aggiornamento anticipato dello stesso

Art. 15 Norma di rinvio

Per tutto ciò che risultasse necessario rispetto all'attività di l'Internal Audit, non compreso nel presente documento, si potrà fare riferimento alla delibera della Giunta Regionale n. 31/16 del 13.10.2022 avente ad oggetto le "*Linee di indirizzo per l'avvio e l'espletamento della Funzione di Internal Auditing nel Sistema Sanitario della Regione Autonoma della Sardegna, in attuazione dell'art. 3 della L.R. 11.9.2020 n. 24"*, e al *Regolamento di Internal Auditing del Sistema Sanitario della Regione Autonoma della Sardegna* di cui alla delibera Ares n.276 del 07.12.2022.