Sistema Socio Sanitario
Regione Lombardia
ATS Brianza

DIREZIONE GENERALE
Internal Auditing

Viale Elvezia 2, 20900 Monza
Tel. 0341/482225

**REGOLAMENTO**

# INTERNAL AUDITING

ID 02297

| rev | data di verifica | Descrizione delle modifiche | FIRMA DI REDAZIONE | FIRMA DI VERIFICA |
|---|---|---|---|---|
| | | | NOMINATIVO (FUNZIONE) | NOMINATIVO (FUNZIONE) |
| 0 | 08/11/2016 | prima emissione | Civillini Paolo<br>Responsabile IA | Civillini Paolo<br>Responsabile IA |
| | | | | |
| | | | | |

Approvato con deliberazione nr. 617 del 18 novembre 2016

**DOCUMENTO DI PROPRIETA' DELLA ATS DELLA BRIANZA**

# Sommario

## Premessa

Il presente regolamento recepisce le indicazioni contenute nella Legge Regionale 4 giugno 2014, n. 17 “Disciplina del sistema dei controlli interni ai sensi dell'articolo 58 dello Statuto d'autonomia”, con cui Regione Lombardia ha disciplinato nell’ambito dell’ordinamento regionale le finalità, le modalità, gli strumenti e le procedure che sovrintendono al sistema dei controlli interni, quale presidio di garanzia della correttezza dell’azione amministrativa della stessa Regione e dei soggetti appartenenti del Sistema Regionale (SiReg).

Il presente Regolamento ha lo scopo di definire le competenze dell’Internal Auditing (da ora IA) rispetto all’esistente sistema dei controlli interni dell’Agenzia Territoriale Sanitaria della Brianza (da ora denominata ATS) e di stabilire principi, regole e responsabilità per la sua applicazione.

Il Sistema di Controllo Interno (da ora SCI) dell’ATS è strutturato su tre livelli:

- **primo livello** (cd “controlli operativi di linea”) – ogni struttura organizzativa dell’ATS definisce e gestisce i controlli necessari per la corretta realizzazione dei propri processi produttivi e/o di supporto (da ora “processi”) e/o delle proprie singole operazioni; la responsabilità di tali controlli è tipica espressione della responsabilità dirigenziale e come tale appartiene ai responsabili delle strutture dell’ATS o, ove individuati, dei processi in esse attuati. Conseguentemente questa responsabilità è esplicitata nei contratti individuali di lavoro e specifico elemento di valutazione delle responsabilità di tipo gestionale;
- **secondo livello** (cd “controlli trasversali”) – le strutture dell’ATS responsabili delle funzioni di controllo di secondo livello (allegato 1) gestiscono, nel rispetto delle politiche e degli obiettivi aziendali, le predette funzioni e le esercitano su tutte le strutture dell’ATS comprese le proprie; la responsabilità di tali controlli appartiene ai responsabili preposti dall’ATS alle predette funzioni;
- **terzo livello** (cd “controlli aziendali”) – gli “organismi interni” (allegato 2) sono responsabili dei controlli stabiliti dalla normativa vigente. Tra essi l’Internal Auditing (da ora IA) verifica la completa strutturazione ed il corretto funzionamento del SCI.

I destinatari del presente regolamento sono il Responsabile dell’Internal Auditing (da ora RIA) la Direzione e tutte le strutture dell’ATS.

## Art. 1: Organizzazione della funzione

La funzione di IA è diretta dal RIA che opera, nello svolgimento delle proprie attività, in piena indipendenza organizzativa ed autonomia.
Il RIA per lo svolgimento delle proprie attività si avvale, dal momento della sua attivazione, di una struttura di supporto[1] individuata dal piano di organizzazione aziendale strategico (da ora POAS).

[1] attuale denominazione della struttura di supporto individuata dal POAS “governo attività amministrative”.

Il RIA inoltre promuove la realizzazione di un flusso informativo interno all'ATS di dati e informazioni necessarie per lo svolgimento delle proprie funzioni coinvolgendo, in tale attività, le strutture dell'ATS detentrici delle stesse.

## Art. 2: Funzioni dell'Internal Auditing

L'IA è la funzione dell'ATS preposta a verificare la completa strutturazione ed il corretto funzionamento del SCI attraverso un approccio sistematico orientato a:

1. valutare e migliorare:
   a) i *controlli trasversali* (allegato 1) previsti dal POAS e/o comunque attivati dalla ATS;
   b) i *controlli operativi di linea* esplicitamente richiesti dalla Regione Lombardia[2] (allegato 3) e/o comunque attivati dalla ATS sui processi e/o le singole operazioni realizzati nelle proprie strutture organizzative;
2. identificare i rischi di tipo giuridico amministrativo propri dei processi e/o delle singole operazioni al fine di monitorarli e mitigarli;
3. supportare la dirigenza e la Direzione Aziendale ad individuare idonee forme di controllo operativo di linea sui processi e/o sulle singole operazioni al fine di assicurare la conformità delle loro attività ai vincoli normativi e/o regolamentari.

Al fine di perseguire le predette funzioni l'IA svolge attività di controllo, di consulenza e partecipa alle attività svolte dal Coordinamento dei Controlli Interni di cui al successivo art. 5.

## Art. 3: Attività di controllo

L'attività di controllo dell'IA a diretta alla verifica:

1) delle attività di competenza delle strutture responsabili dei *controlli trasversali* (allegato 1) allo scopo di promuovere l'effettuazione dei controlli di loro competenza e di verificare che gli stessi siano effettuati in modo efficiente, efficace ed economico;
2) dei processi ritenuti "critici" e/o delle rispettive singole operazioni, delle strutture dell'ATS allo scopo di promuovere e verificarne l'effettività e l'efficacia dei necessari *controlli operativi di linea* in modo che gli stessi siano realizzati conformemente ai vincoli legislativi e ai regolamenti/procedure che stabiliscono standard di condotta;

in modo di fornire un giudizio professionale sull'esistenza, sul funzionamento e sulla affidabilità dei controlli e al fine di assicurare il miglioramento dell'organizzazione e dei suoi risultati.

L'IA non effettua controlli rispetto:

1) all'operato degli organismi "esterni" che effettuano attività di controllo sull'ATS;
2) all'operato degli organismi "interni" che effettuano i controlli aziendali (allegato 2);
3) agli atti sanitari e sociosanitari in sé, intesi come "atti professionali", se non esclusivamente per gli aspetti amministrativi propedeutici e di carattere istruttorio preliminari all'adozione di un provvedimento amministrativo.

[2] si veda DGR n. X/5113 del 29 aprile 2016 avente ad oggetto "Linee guida regionali per l'adozione dei piani di organizzazione aziendale strategici …".

## Art. 4: Attività di consulenza

L'IA inoltre svolge attività di consulenza, supporto e suggerimento ai Responsabili di tutte le strutture dell'ATS al fine di individuare idonee forme di controllo operativo di linea interno ai propri processi che possano assicurare la conformità delle loro attività rispetto ai vincoli legislativi e ai regolamenti dell'ATS.

## Art. 5: Coordinamento delle funzioni del servizio di controllo interno

Al fine di coordinare le funzioni/attività dell'IA con quelle delle strutture della ATS responsabili dei controlli trasversali (allegato1) il responsabile della struttura di supporto[3] della funzione di IA, individuata dal POAS, costituisce il "Coordinamento dei Controlli Interni" (da ora "CCI").

Al CCI partecipano tutti i responsabili delle strutture della ATS che svolgono controlli trasversali. Agli incontri del CCI possono essere invitati anche esperti per gli argomenti all'ordine del giorno.

Il Coordinatore del CCI è individuato nella figura del responsabile gestionale della struttura di supporto della funzione di IA, individuata dal POAS. Le funzioni di verbalizzazione sono assicurate dal personale della predetta struttura di supporto.

Il CCI, dal momento della sua costituzione:

- promuove l'effettuazione di una "analisi dei rischi" unica valevole per tutte le funzioni di controlli trasversali tenute alla sua effettuazione per quanto di loro competenza;
- effettua l'analisi dei rischi di cui al successivo art 7;
- predispone i "piani triennali e annuali delle verifiche" di cui al successivo art. 8;
- partecipa, con le modalità successivamente descritte all'art. 9, alla effettuazione delle verifiche.

## Art. 6: Principi di base dell'attività di controllo

L'attività di controllo, di cui al precedente art. 3, si conforma ai principi contenuti nel Codice Etico dell'Institute of Internal Auditors e agli Standard Internazionali Professionali di Indipendenza, Obiettività, Riservatezza e Competenza (allegato 4).

L'attività di controllo si articola in:

A. analisi e valutazione dei rischi;
B. pianificazione delle verifiche;
C. verifica (cd "audit").

[3] cfr nota 1.

Al RIA è assicurato l'accesso a tutti i dati, alle informazioni ed ai beni aziendali necessari allo svolgimento delle proprie attività senza alcuna intermediazione e/o restrizione da parte delle strutture detentrici.

Le verifiche possono consistere in:

- verifiche sul campo – verifiche effettuate presso le strutture dell'ATS alla presenza del responsabile della stessa, del responsabile – se individuato – del processo verificato e degli operatori coinvolti nelle diverse fasi e attività del processo;
- verifiche documentali – verifiche effettuate attraverso l'analisi di documenti e/o dati forniti dalle strutture della ATS.

Alle verifiche pianificate possono aggiungersi per particolari esigenze verifiche straordinarie.

## Art. 7: L'analisi dei rischi

L'analisi dei rischi è un processo sistematico, condotto dal CCI con periodicità annuale, diretto ad individuare i processi della ATS maggiormente esposti a rischio così come definiti dal precedente art. 2 comma 1 punto 2.

L'analisi dei rischi rappresenta l'attività preliminare alla formazione dei piani pluriennali ed annuali delle verifiche ed è condotta, nel secondo semestre di ogni anno, dal CCI e, per quanto riguarda le fasi 2 e 3 di cui al successivo comma, da tutte le strutture dell'ATS e, se individuati, dai responsabili dei processi.

Il processo di analisi dei rischi prevede:

1) la **definizione delle "aree a rischio" (universo di audit)** - in questa fase sono individuate le aree della ATS ritenute maggiormente critiche. Le aree possono consistere in funzioni/attività dell'ATS e/o nelle corrispondenti strutture.

   Ai fini della definizione delle aree possono essere considerati:
   - la rilevazione e catalogazione degli articoli/interventi apparsi sui mezzi di comunicazione (giornali, agenzie di stampa ecc) a livello locale, regionale e nazionale riguardanti possibili e/o acclarati illeciti di carattere amministrativo, penale, civile e/o contabile;
   - le eventuali indicazioni trasmesse dai livelli regionali (es funzione di Internal Auditing regionale);
   - le eventuali indicazioni proposte dalla Direzione della ATS;
   - le eventuali segnalazioni fornite dagli organismi dell'ATS preposti ai controlli aziendali (si veda allegato 2) e/o soggetti esterni all'ATS;
   - esiti di precedenti audit;
   - segnalazioni rilevate a livello aziendale.

2) l'**identificazione e la valutazione dei rischi dei processi aziendali** - in questa fase sono individuati i rischi potenziali in termini di probabilità di accadimento e impatto non considerando i controlli operativi di linea in essere nelle strutture dell'ATS nelle quali si attuano i processi oggetto delle verifiche;
3) l'**identificazione e valutazione dei controlli operativi di linea** - in questa fase sono rilevati i controlli operativi di linea previsti dai responsabili delle strutture dell'ATS per mitigare i rischi potenziali e si conclude con l'identificazione dei fattori interni ed esterni ai controlli operativi di linea che possono pregiudicare il raggiungimento degli obiettivi ad essi sottointesi.
   La valutazione delle attività di controllo operativo di linea è effettuata in funzione di due aspetti:
   - **effettività** nello svolgimento del controllo;
   - **efficacia** del controllo nel mitigare il rischio potenziale, ossia se il controllo è idoneo ad assicurare il contenimento del rischio nei limiti ritenuti accettabili.

Il processo di analisi dei rischi si conclude con l'elaborazione della "relazione dell'analisi dei rischi".

## Art. 8: La pianificazione delle attività

Il CCI predispone annualmente, in una logica di "scorrimento" il "piano delle verifiche". Il piano contempla la:

- **programmazione triennale –** questa programmazione identifica le strutture della ATS e/o i processi che saranno oggetto di verifica nel triennio. La programmazione è aggiornata annualmente sulla base degli esiti dell'attività di verifica svolta nell'anno precedente, dell'esito delle azioni correttive realizzate e dell'eventuale aggiornamento della valutazione dei rischi;
- **pianificazione annuale -** questo piano definisce le strutture della ATS e/o i processi che saranno verificati nell'anno di competenza.
  Per ogni verifica sono indicati:
  - la struttura e/o il processo oggetto della verifica;
  - il gruppo di verifica;
  - le risorse necessarie;
  - il crono-programma di massima delle attività.

Il piano delle verifiche (triennale e annuale) è approvato con delibera del Direttore Generale entro i termini stabiliti dal livello regionale o comunque entro il 31 dicembre di ogni anno, e comunicato alla Direzione dell'ATS e a tutte le strutture della ATS.
Con il provvedimento di approvazione del piano può essere delegata la possibilità di apportare in corso d'anno, per particolari esigenze nel frattempo intervenute, eventuali modifiche significative del piano stesso.

## Art. 9: Composizione dei gruppi di verifica

La verifica sui controlli trasversali è effettuata esclusivamente dal RIA

Ai gruppi di verifica dei controlli operativi di linea partecipano, come di regola il RIA (quale "responsabile" del gruppo di verifica"), il Responsabile della Prevenzione della Corruzione e Trasparenza dell'ATS (da ora RPCT) ed un verificatore indicato dal gruppo di coordinamento scelto tra i restanti componenti del coordinamento oppure tra i verificatori presenti nel "elenco dei verificatori aziendali" elaborato dalla struttura dell'ATS preposta ad assicurare la gestione della qualità dell'ATS, delle sue strutture organizzative e dei loro processi.

Nella composizione dei gruppi di verifica dei controlli operativi di linea accorre garantire il principio di indipendenza.

Il gruppo di verifica, nell'esercizio delle sue attività, si può avvalere di eventuali "esperti" e, se esterni all'ATS, preferibilmente scelti tra gli operatori del sistema sanitario regionale. Gli esperti potranno esprimere, su richiesta del gruppo di verifica, esclusivamente pareri specifici di natura tecnica.

Tutta l'attività del gruppo di verifica deve essere debitamente verbalizzata.

Per eventuali verifiche straordinarie la composizione del gruppo di verifica può essere limitata al solo RIA (quale "responsabile" e "verbalizzatore" del gruppo di verifica) e al RPCT dell'ATS.

## Art. 10: Le verifiche sul campo

Le verifiche sul campo devono rispettare le seguenti fasi:

- **La programmazione operativa**: il gruppo di verifica definisce:
  - Gli obiettivi dell'intervento di verifica;
  - L'ambito di copertura della verifica, ovvero: confini temporali che l'analisi deve coprire, i processi e le procedure da esaminare, le caratteristiche del campione da sottoporre a test, etc;
  - Il calendario di massima dei lavori;
- **L'analisi preliminare**: il gruppo di verifica raccoglie ed analizza la documentazione riguardante la struttura e/o processo da verificare necessaria per comprendere e/o approfondire i rischi e i controlli previsti e predispone una specifica lista di riscontro degli elementi da verificare**;**
- **Comunicazione dell'avvio**: il responsabile del gruppo di verifica avvia la verifica con comunicazione scritta alla struttura organizzativa coinvolta nella verifica e alla Direzione dell'ATS allo scopo:
  - di evidenziare:
    - ✓ gli obiettivi generali della verifica

- ✓ l'ambito di copertura della verifica;
- ✓ le eventuali limitazioni all'ampiezza della verifica;
- ✓ la previsione temporale di massima della verifica;
- ✓ la composizione del gruppo di verifica.

– richiedere, con indicazione della scadenza entro cui dovrà pervenire:
- ✓ il nominativo, se individuato, del responsabile del processo;
- ✓ l'assenso alla data di avvio;
- ✓ l'eventuale documentazione integrativa.

- **Riunione di apertura della verifica**: alla data concordata o, in assenza di accordo, alla data successivamente comunicata dal responsabile del gruppo di verifica, l'inizio delle attività avviene con una riunione di apertura. All'incontro deve obbligatoriamente partecipare il Responsabile della struttura oggetto di verifica e, se individuato, il Responsabile del processo verificato. Nell'incontro si devono chiarire: l'obiettivo e l'ambito della verifica, nonché le metodologie che saranno in essa seguite e le fasi operative della verifica sul campo.
- **Lavoro sul campo**: il lavoro sul campo consiste nell'acquisizione presso la struttura verificata delle evidenze necessarie per verificare l'effettività ed efficacia dei controlli operativi di linea esistenti.
  Fatto salvo l'obbligo per il responsabile del gruppo di verifica di richiedere preventivamente la disponibilità dei dati e/o di evidenze da verificare, il Responsabile della struttura verificata deve assicurare al gruppo di verifica l'accesso diretto a tutte le informazioni (documenti, dati) necessarie alla verifica.
- **Collaudo dei controlli**: questa fase è finalizzata a esprimere un giudizio circa l'esistenza effettiva ed efficace dei controlli presenti nel processo.
- **Comunicazione dei risultati**: conclusa la fase di esecuzione della verifica sul campo, il gruppo di verifica predispone e trasmette al Responsabile della struttura un rapporto preliminare sullo stato dei controlli interni riscontrati evidenziando, se esistenti, le criticità rilevate e chiedendo, entro un termine definito, al Responsabile della struttura verificata di formulare le proprie osservazioni e di ipotizzare le necessarie azioni di miglioramento.
- **Incontro di chiusura**: il rapporto preliminare, le osservazioni e le azioni di miglioramento proposte sono esaminati in un successivo incontro al quale, oltre al responsabile della strutture, possono partecipare tutti gli operatori che, a qualunque titolo, hanno partecipato al lavoro sul campo. L'incontro si conclude con la predisposizione di un **rapporto definitivo** contenente la sintesi di tutta l'attività svolta e dei risultati raggiunti.
  Il RIA trasmette il "rapporto definitivo" alla Direzione dell'ATS. Il rapporto definitivo è inoltre trasmesso, per conoscenza, al responsabile della struttura/processo verificato e, se prevede azioni di miglioramento, anche alla struttura dell'ATS[4] preposta al assicurare la gestione della qualità dell'ATS, delle sue strutture e dei loro processi.
- **Monitoraggio delle azioni di miglioramento:** la struttura dell'ATS di cui al precedente punto attiva l'apertura nelle necessarie "azioni correttive", assicura il monitoraggio del loro stato di realizzazione e aggiorna il RIA sugli esiti conseguiti**.**

[4] attuale denominazione della struttura individuata dal POAS "gestione qualità".

## Art. 11: Le verifiche documentali

Le verifiche documentali devono rispettare le seguenti fasi:

- **L'acquisizione delle informazioni**: il gruppo di verifica, se non già in possesso dei documenti, dati e/o informazioni necessari per l'effettuazione delle proprie analisi, le richiede alle strutture della ATS;
- **L'analisi preliminare**: il gruppo di verifica analizza le informazioni acquisite per comprendere e/o approfondire i rischi e i controlli previsti. In questa fase il gruppo di verifica può proporre domande scritte al Responsabile della struttura della ATS competente e può chiedere informazioni aggiuntive**;**
- **Collaudo dei controlli**: questa fase è finalizzata a esprimere un giudizio circa l'esistenza effettiva ed efficace dei controlli presenti nel processo;
- **Rapporto definitivo**: la sintesi di tutta l'attività svolta, il giudizio sui sistemi di controllo esaminati e le eventuali azioni di miglioramento proposte.
  Il RIA trasmette il "rapporto definitivo" alla Direzione dell'ATS. Il rapporto definitivo è inoltre trasmesso, per conoscenza, al responsabile della struttura/processo verificato e, se prevede azioni di miglioramento, anche alla struttura dell'ATS[5] preposta al assicurare la gestione della qualità dell'ATS, delle sue strutture e dei loro processi.
- **Monitoraggio delle azioni di miglioramento**: la struttura dell'ATS di cui al precedente punto attiva l'apertura nelle necessarie "azioni correttive", assicura il monitoraggio del loro stato di realizzazione e aggiorna il RIA sugli esiti conseguiti.

## Art. 12: Archiviazione dei documenti prodotti

Tutto il materiale prodotto e/o raccolto durante la verifica deve essere raccolto in un fascicolo debitamente codificato per verifica e custodito per 5 anni successivi all'anno di riferimento.

## Art. 13: Norma finale e transitoria.

Il presente regolamento entra in vigore dal 01 gennaio 2017.

Nell'ipotesi di non avvenuta attivazione della struttura di supporto[6] della funzione aziendale di IA le attività previste dall'art. 5, 7 e 8 sono svolte dal RIA.

Ai fini dell'art. 9 nell'ipotesi che l'ATS preveda la differenziazione tra Responsabile della Prevenzione della Trasparenza e Responsabile della Prevenzione della Corruzione ai gruppi di verifica partecipa obbligatoriamente solo il secondo.

[5] cfr nota 4.
[6] attuale denominazione della struttura di supporto individuata dal POAS "governo attività amministrative".

## Allegato 1: controlli interni di 2° livello – controlli trasversali

| denominazione delle funzioni | Strutture e/o *funzioni* (*) competenti |
|---|---|
| controllo di gestione | controllo di gestione<br>sviluppo operativo |
| performance | gestione qualità |
| privacy | affari generali e legali<br>servizi informativi aziendali |
| controllo della qualità | gestione qualità |
| controlli atti (regolarità amministrativa) | affari generali e legali |
| regolarità contabile | economico-finanziario |
| risk management | risk management (*) |
| servizio prevenzione e protezione | prevenzione e protezione dai rischi professionali (*) |
| trasparenza e anticorruzione | trasparenza e anticorruzione (*) |
| controlli interni | governo attività amministrative |
| diritto d'accesso | affari generali e legali |

*(*) l'asterisco indica le funzioni*

*L'elenco non è esaustivo di tutti i controlli trasversali attivati nella ATS*

## Allegato 2: controlli di 3° livello

| organismi interni |
|---|
| Collegio Sindacale |
| Internal Auditing |
| Nucleo di Valutazione |

## Allegato 3: controlli operativi di linea previsti esplicitamente dal POAS

| denominazione delle funzioni | Strutture e/o *funzioni* competenti |
|---|---|
| controllo presenza in servizio del personale dipendente | sviluppo risorse umane |
| procedimenti in materia di esercizio di attività extra istituzionale | sviluppo risorse umane |
| controllo sul rispetto della disciplina delle incompatibilità del personale dipendente | sviluppo risorse umane |
| controllo sul rispetto della disciplina delle incompatibilità del personale convenzionato | affari generali e legali |
| controllo sulle autocertificazioni | governo attività amministrative |

*L'elenco non è esaustivo di tutti i controlli operativi di linea attivati nella ATS*

## Allegato 4: codice etico

Introduzione

Lo scopo del Codice Etico dell'Institute of Internal Auditors è di promuovere la cultura etica nell'esercizio della professione di internal auditing.
L'internal auditing è un'attività indipendente ed obiettiva di assurance e consulenza, finalizzata al miglioramento dell'efficacia e dell'efficienza dell'organizzazione.
Assiste l'organizzazione nel perseguimento dei propri obiettivi tramite un approccio professionale sistematico, che genera valore aggiunto in quanto finalizzato a valutare e migliorare i processi di gestione dei rischi, di controllo e di governance.
Il codice etico è uno strumento necessario ed appropriato per l'esercizio dell'attività professionale di internal audit, che è fondata sulla fiducia indiscussa nell'obiettività dei suoi servizi di assurance riguardanti la governance, la gestione dei rischi e il controllo.
Il Codice Etico dell'Institute of Internal Auditors si estende oltre la Definizione di Internal Auditing per includere due componenti essenziali.

- I Principi, fondamentali per la professione e la pratica dell'internal auditing.
- Le Regole di Condotta, che descrivono le norme comportamentali che gli internal auditor sono tenuti ad osservare.

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

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

## Principi

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

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

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

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

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

## Regole di Condotta

*1. Integrità*

L'internal auditor:

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

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

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

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

*2. Obiettività*

L'internal auditor:

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

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

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

*3. Riservatezza*

L'internal auditor:

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

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

*4. Competenza*

L'internal auditor:

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

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

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

## DEFINIZIONE DI INTERNAL AUDITING

L'Internal Auditing è un'attività indipendente ed obiettiva di assurance e consulenza, finalizzata al miglioramento dell'efficacia e dell'efficienza dell'organizzazione.

Assiste l'organizzazione nel perseguimento dei propri obiettivi tramite un approccio professionale sistematico, che genera valore aggiunto in quanto finalizzato a valutare e migliorare i processi di gestione dei rischi, di controllo e di governance.

## STANDARD DI CONNOTAZIONE

*1000 – Finalità, poteri e responsabilità*

Le finalità, i poteri e le responsabilità dell'attività di internal audit devono essere formalmente definiti in un Mandato di internal audit, coerente con la Definizione di Internal Auditing, il Codice Etico e gli Standard. Il responsabile internal auditing deve verificare periodicamente il Mandato e sottoporlo all'approvazione del senior management e del board.

*Interpretazione:*

Il Mandato dell'internal audit è un documento formale che definisce finalità, poteri e responsabilità dell'attività di internal audit. Il Mandato stabilisce la posizione dell'attività di internal audit nell'organizzazione, precisando la natura del riporto funzionale del responsabile internal auditing al board; autorizza l'accesso ai dati, alle persone e ai beni aziendali che sono necessari per lo svolgimento degli incarichi di audit e definisce l'ambito di copertura delle attività di internal audit.

L'approvazione finale del Mandato di internal audit è una responsabilità del board.

*1000.A1 –* La natura dei servizi di assurance forniti all'organizzazione deve essere definita nel Mandato di internal audit.
Anche nel caso in cui i servizi di assurance sono forniti a soggetti esterni all'organizzazione, la natura di tali servizi deve essere dichiarata nel Mandato di internal audit.
*1000.C1 –* La natura dei servizi di consulenza deve essere definita nel Mandato di internal audit.

*1010 – Riconoscimento della Definizione di Internal Auditing, del Codice Etico e degli Standard nel Mandato di internal audit*
Il carattere vincolante della Definizione di Internal Auditing, del Codice Etico e degli Standard deve essere rispecchiato nel Mandato di internal audit. Il responsabile internal auditing dovrebbe discutere la Definizione di Internal Auditing, il Codice Etico e gli Standard con il senior management e il board.

*1100 – Indipendenza e obiettività*
L'attività di internal audit deve essere indipendente e gli internal auditor devono essere obiettivi nell'esecuzione del loro lavoro.

*Interpretazione:*
Indipendenza è la libertà da condizionamenti che minaccino la capacità dell'attività di internal audit di adempiere senza pregiudizio alle proprie responsabilità. Per raggiungere il livello di indipendenza necessario per esercitare in modo efficace le responsabilità dell'attività di internal audit, il responsabile internal auditing ha diretto e libero accesso al senior management e al board.
Ciò può essere conseguito tramite un duplice riporto organizzativo.
Casi di limitazione all'indipendenza devono essere gestiti a livello di singolo auditor, di incarico, funzionale e organizzativo.
Obiettività è l'attitudine mentale di imparzialità che consente agli internal auditor di svolgere i propri incarichi in un modo che consenta loro di credere nella validità del lavoro svolto e nell'assenza di compromessi sulla qualità. In materia di audit, l'obiettività richiede che gli internal auditor non subordinino il proprio giudizio professionale a quello di altri.
Eventuali ostacoli all'obiettività devono essere gestiti a livello di singolo auditor, di incarico, funzionale e organizzativo.

*1110 – Indipendenza organizzativa*
Il responsabile internal auditing deve riportare ad un livello dell'organizzazione che consenta all'attività di internal audit il pieno adempimento delle proprie responsabilità. Il responsabile internal auditing deve confermare al board, almeno una volta l'anno, lo stato di indipendenza organizzativa dell'attività di internal audit.

*Interpretazione:*
Si realizza un'indipendenza organizzativa efficace quando il responsabile internal auditing riferisce funzionalmente al board.
Esempi di riporto funzionale al board comportano che il board di attività basato sulla valutazione dei rischi;

- approvi il budget e il piano delle risorse dell'attività di internal audit;
- riceva comunicazioni dal responsabile internal auditing in merito ai risultati dell'attività di internal audit rispetto al piano e ad altre questioni;
- approvi le decisioni relative alla nomina e all'esonero del responsabile internal auditing;
- approvi il compenso spettante al responsabile internal auditing;
- effettui opportune verifiche con il management e il responsabile internal auditing per stabilire se sono presenti limitazioni non appropriate dell'ambito di copertura e delle risorse.

*1110.A1 –* L'attività di internal audit deve essere libera da interferenze nella definizione dell'ambito di copertura, nell'esecuzione del lavoro e nella comunicazione dei risultati.

*1111 – Comunicazione con il board*
Il responsabile internal auditing deve poter comunicare e interagire direttamente con il board.

*1120 – Obiettività individuale*
Gli internal auditor devono avere un atteggiamento imparziale e senza pregiudizi; devono inoltre evitare qualsiasi conflitto di interesse.

*Interpretazione:*
Conflitto di interessi è una situazione nella quale gli internal auditor, che godono di una posizione di fiducia, si trovano ad avere un interesse personale o professionale contrario agli interessi dell'organizzazione. Un simile contrasto con l'organizzazione rende difficile l'adempimento dei compiti dell'internal auditor con imparzialità. Un conflitto di interessi può sussistere anche quando non dà luogo a comportamenti non etici o comunque impropri. L'esistenza di un conflitto di interessi può dare l'impressione che vi siano comportamenti scorretti, con il risultato di compromettere la fiducia verso gli internal auditor, l'attività di internal audit e la professione. Il conflitto di interessi può pregiudicare la capacità individuale di svolgere con obiettività i propri compiti e responsabilità.

*1130 – Condizionamenti dell'indipendenza o dell'obiettività*
Se indipendenza od obiettività sono compromesse o appaiono tali, le circostanze dei condizionamenti devono essere riferite a un livello appropriato. La natura dell'informativa dipende dal tipo di condizionamento.

*Interpretazione:*
Tra i fattori che possono condizionare l'indipendenza organizzativa e l'obiettività individuale si possono annoverare conflitti di interesse individuali, limitazioni del campo di azione, restrizioni dell'accesso a dati, persone e beni aziendali e vincoli di risorse, tra cui quelle finanziarie.
La determinazione del livello più appropriato al quale dovrebbero essere riferite le circostanze di pregiudizio all'indipendenza o all'obiettività dipende dalle aspettative dell'attività di internal audit, dai doveri del responsabile internal auditing verso il senior management e il board, definiti nel Mandato di internal audit, e dalla natura dei condizionamenti stessi.

> *1130.A1 –* Gli internal auditor devono evitare di effettuare attività di audit in ambiti in cui ricoprivano una precedente responsabilità. Si presume che l'obiettività sia condizionata se un internal auditor effettua un servizio di assurance sulle attività di cui è stato responsabile nell'anno precedente.
> *1130.A2 –* Gli incarichi di assurance per attività che rientrano nella gestione del responsabile internal auditing devono essere supervisionati da soggetti esterni alla Struttura di internal audit.
> *1130.C1 –* Gli internal auditor possono fornire servizi di consulenza anche per quelle attività operative delle quali siano stati precedentemente responsabili.
> *1130.C2 –* Se gli internal auditor, a fronte di prospettati servizi di consulenza, si trovano in una situazione di potenziale condizionamento della propria indipendenza od obiettività, devono segnalarlo al cliente prima di accettare l'incarico.

*1200 – Competenza e diligenza professionale*
Gli incarichi devono essere effettuati con la dovuta competenza e diligenza professionale.

*1210 – Competenza*
Gli internal auditor devono possedere le conoscenze, capacità e altre competenze necessarie all'adempimento delle loro responsabilità individuali. L'attività di internal audit nel suo insieme deve possedere o dotarsi delle conoscenze, capacità e altre competenze necessarie all'esercizio delle proprie responsabilità.

*Interpretazione*: internal auditor per adempiere efficacemente alle proprie responsabilità professionali. Gli internal auditor sono incoraggiati a dimostrare la propria competenza conseguendo le opportune certificazioni e qualifiche professionali, come quella di "Certified Internal Auditor" e altre certificazioni rilasciate dal "The Institute of Internal Auditors" e da altri organismi professionali riconosciuti.

> *1210.A1* – Il responsabile internal auditing deve dotarsi di opportuna assistenza e consulenza se gli internal

auditor non possiedono le conoscenze, le capacità o altre competenze necessarie per lo svolgimento di tutto o di parte dell'incarico.
*1210.A2* – Gli internal auditor devono possedere conoscenze sufficienti per valutare i rischi di frode e il modo in cui l'organizzazione li gestisce, senza aspettarsi che essi abbiano le competenze proprie di chi ha come responsabilità primaria quella di individuare e investigare frodi.
*1210.A3* – Gli internal auditor devono possedere una sufficiente conoscenza dei rischi e dei controlli chiave dell'Information Technology, nonché degli strumenti informatici di supporto all'attività di audit per svolgere gli incarichi assegnati. Tuttavia, non è richiesto che tutti gli internal auditor posseggano le competenze di chi ha come responsabilità primaria quella dell'Information Technology auditing.
*1210.C1* – Il responsabile internal auditing deve rifiutare l'incarico di consulenza, oppure dotarsi di valido supporto e assistenza nel caso in cui gli internal auditor non posseggano le conoscenze, le capacità o le altre competenze necessarie per lo svolgimento di tutto o di parte dell'incarico.

*1220 – Diligenza professionale*
Gli internal auditor devono applicare la diligenza e le capacità che ci si attende da un internal auditor ragionevolmente prudente e competente. Diligenza professionale non implica infallibilità.

*1220.A1* – L'internal auditor deve esercitare la diligenza professionale tenendo in considerazione:
- l'ampiezza del lavoro necessario per raggiungere gli obiettivi dell'incarico;
- la complessità, importanza o la significatività delle attività oggetto di assurance;
- l'adeguatezza e l'efficacia dei processi di governance, di gestione del rischio e di controllo;
- la probabilità della presenza di errori, frodi o non conformità significativi;
- il costo dell'assurance in relazione ai suoi potenziali benefici.

*1220.A2* – Per svolgere l'attività di audit con diligenza professionale, gli internal auditor devono considerare l'utilizzo di strumenti informatici di supporto e di altre tecniche di analisi dei dati.
*1220.A3* – Gli internal auditor devono prestare attenzione ai rischi significativi che possono incidere su obiettivi, attività o risorse. Comunque, le sole procedure di assurance, anche quando effettuate con la dovuta diligenza professionale, non garantiscono che tutti i rischi significativi vengano individuati.
*1220.C1* – Nel corso di un incarico di consulenza, gli internal auditor devono esercitare la dovuta diligenza professionale, tenendo in considerazione:
- le esigenze e le aspettative dei clienti, inclusa la natura, i tempi e le forme di comunicazione dei risultati dell'incarico;
- la complessità e l'ampiezza del lavoro necessario per raggiungere gli obiettivi dell'incarico;
- il costo dell'incarico di consulenza in relazione ai suoi potenziali benefici.

*1230 – Aggiornamento professionale continuo*
Gli internal auditor devono migliorare le proprie conoscenze, capacità e altre competenze attraverso un aggiornamento professionale continuo.

*1300 – Programma di assurance e miglioramento della qualità*
Il responsabile internal auditing deve sviluppare e sostenere un programma di assurance e miglioramento della qualità che copra tutti gli aspetti dell'attività di internal audit.

*Interpretazione:*
L'elaborazione di un programma di assurance e miglioramento della qualità permette una valutazione di conformità dell'attività di internal audit alla Definizione di Internal Auditing e agli Standard e consente di verificare se gli internal auditor rispettano il Codice Etico.
Il programma valuta inoltre l'efficienza e l'efficacia dell'attività di internal audit e identifica opportunità per il suo miglioramento.

*1310 – Requisiti del programma di assurance e miglioramento della qualità*
Il programma di assurance e miglioramento della qualità deve includere valutazioni sia interne che esterne.

*1311 – Valutazioni interne*

Le valutazioni interne devono includere:
il monitoraggio continuo della prestazione dell'attività di internal auditing;
periodiche auto-valutazioni o valutazioni condotte da altre persone interne all'organizzazione che abbiano conoscenze adeguate delle metodologie di internal audit.

Interpretazione: Il monitoraggio continuo costituisce parte integrante dell'attività quotidiana di supervisione, verifica e misurazione dell'attività di internal audit. Il monitoraggio continuo è incorporato nelle procedure utilizzate di norma per gestire l'attività di internal audit e viene svolto utilizzando processi, strumenti e informazioni necessari per valutare la conformità alla Definizione di Internal Auditing, al Codice Etico e agli Standard.
Le valutazioni periodiche sono effettuate con l'obiettivo specifico di valutare la conformità alla Definizione di Internal Auditing, al Codice Etico e agli Standard.
La comprensione di tutti gli elementi dell'International Professional Practices Framework è necessaria per una adeguata conoscenza della metodologia di internal audit.

*1312 – Valutazioni esterne*

Le valutazioni esterne devono essere effettuate almeno una volta ogni cinque anni da parte di un valutatore, o di un team di valutatori, qualificato e indipendente, esterno all'organizzazione. Il responsabile internal auditing deve discutere con il board:

- la modalità e la frequenza della valutazione esterna;
- le qualifiche e l'indipendenza del valutatore o del team di valutatori esterni, inclusa l'esistenza di qualsiasi possibile situazione di conflitto di interessi.

*Interpretazione:*

Le valutazioni esterne possono essere costituite da valutazioni esterne complete oppure essere condotte sotto forma di autovalutazione con convalida esterna indipendente.
Un valutatore o un team di valutatori qualificati devono dimostrare di essere competenti in due ambiti: la pratica professionale dell'internal auditing e il processo di valutazione esterna.
La competenza può essere dimostrata attraverso una combinazione di esperienza e conoscenze teoriche. L'esperienza acquisita presso organizzazioni analoghe per dimensioni, complessità, settore o comparto e specializzazione tecnica è più significativa di un'esperienza meno specifica.
Nei team di valutatori, non è necessario che tutti i componenti del team posseggano tutte le competenze, in quanto è il team nel suo insieme a risultare idoneo. Nel determinare se un valutatore o un team di valutatori dimostrino competenza sufficiente per essere ritenuti idonei, il responsabile internal auditing applica un giudizio professionale.
Il valutatore o il team di valutatori sono indipendenti quando non hanno alcun reale o apparente conflitto di interessi e non fanno parte né sono sotto il controllo dell'organizzazione alla quale appartiene l'attività di internal audit oggetto di valutazione esterna.

*1320 – Comunicazione del programma di assurance e miglioramento della qualità*

Il responsabile internal auditing deve comunicare i risultati del programma di assurance e miglioramento della qualità al senior management e al board.

*Interpretazione:*

La forma, il contenuto e la periodicità della comunicazione dei risultati del programma di assurance e miglioramento della qualità vanno concordati con il senior management e il board, considerando le responsabilità dell'attività di internal audit e del responsabile internal auditing definite nel Mandato.
Per dimostrare la conformità alla Definizione di Internal Auditing, al Codice Etico e agli Standard, i risultati delle valutazioni periodiche esterne e interne vanno comunicati al termine del processo di valutazione, mentre i risultati del monitoraggio continuo vanno comunicati almeno una volta l'anno. I risultati devono includere la valutazione del valutatore o del team di valutatori sul livello di conformità.

*1321 – Uso della dizione "Conforme agli Standard Internazionali per la Pratica Professionale dell'Attività di Internal Auditing"*

Il responsabile internal auditing può dichiarare che l'attività di internal audit è conforme agli Standard Internazionali per la Pratica Professionale dell'Attività di Internal Auditing solo se le risultanze del programma di assurance e miglioramento della qualità avvalorano tale affermazione.

Interpretazione: L'attività di internal audit risulta conforme agli Standard quando raggiunge i risultati descritti nella Definizione di Internal Auditing, nel Codice Etico e negli Standard. I risultati del programma di assurance e miglioramento della qualità comprendono i risultati delle valutazioni interne ed esterne. Tutte le attività di internal audit devono essere oggetto di valutazioni interne, mentre le attività di internal audit che operano da almeno cinque anni devono essere oggetto anche di valutazioni esterne.

*1322 – Comunicazione di non conformità*
In presenza di non conformità alla Definizione di Internal Auditing, al Codice Etico o agli Standard che influiscano in modo significativo sull'ambito complessivo di copertura o sull'operatività dell'attività di internal audit, il responsabile internal auditing deve comunicare le non conformità e il relativo impatto al senior management e al board.

## STANDARD DI PRESTAZIONE

*2000 – Gestione dell'attività di internal audit*
Il responsabile internal auditing deve gestire in modo efficace l'attività al fine di assicurare che essa apporti valore aggiunto all'organizzazione.

*Interpretazione:*
L'attività di internal audit è gestita efficacemente quando:
- i risultati del lavoro dell'attività di internal audit permettono di raggiungere le finalità e le responsabilità indicate nel Mandato di internal audit;
- l'attività di internal audit è conforme alla Definizione di Internal Auditing e agli Standard;
- coloro che svolgono l'attività di internal audit dimostrano di operare in conformità al Codice Etico e agli Standard.

L'attività di internal audit aggiunge valore all'organizzazione (e ai suoi stakeholder) quando fornisce assurance obiettiva e pertinente e quando contribuisce all'efficacia e all'efficienza dei processi di governance, gestione del rischio e controllo.

*2010 – Piano delle attività di internal audit*
Il responsabile internal auditing deve predisporre un piano delle attività, basato sulla valutazione dei rischi, al fine di determinarne le priorità in linea con gli obiettivi dell'organizzazione.

*Interpretazione:*
Il responsabile internal auditing deve predisporre un piano, basato sulla valutazione dei rischi, tenendo conto dei processi aziendali di gestione del rischio e dei limiti di accettabilità dello stesso stabiliti dal management per le diverse attività o parti dell'organizzazione. Se non esiste un modello di riferimento, il responsabile internal auditing esprimerà un proprio giudizio sui rischi, sulla base delle indicazioni fornite dal senior management e dal board. Il responsabile internal auditing deve rivedere e adeguare opportunamente il piano, in risposta ai cambiamenti intervenuti a livello di attività, rischi, operatività,programmi, sistemi e controllo dell'organizzazione.

> *2010.A1* – Il piano delle attività di internal audit deve basarsi su una documentata valutazione del rischio, effettuata almeno una volta l'anno. Le indicazioni del senior management e del board devono essere tenute in debita considerazione nella formulazione del piano.
> *2010.A2* – Il responsabile internal auditing deve individuare e considerare le aspettative del senior management, del board e degli altri stakeholder verso i giudizi dell'internal audit e le altre conclusioni.

*2010.C1* – Il responsabile internal auditing deve decidere se accettare un incarico di consulenza, sulla base delle possibilità di miglioramento della gestione dei rischi, delle possibilità di aggiungere valore e di migliorare l'operatività dell'organizzazione. Gli incarichi accettati devono essere inclusi nel piano di audit

*2020 – Comunicazione e approvazione del piano*
Il responsabile internal auditing deve sottoporre il piano delle attività di internal audit e delle risorse necessarie, incluse eventuali variazioni significative intervenute, al senior management e al board per il relativo esame e approvazione. Il responsabile internal auditing deve, inoltre, segnalare l'impatto di un'eventuale carenza di risorse.

*2030 – Gestione delle risorse*
Il responsabile internal auditing deve assicurare che le risorse disponibili siano adeguate, sufficienti ed efficacemente impiegate per l'esecuzione del piano approvato.

*Interpretazione:*
Il termine "adeguate" è riferito all'insieme di conoscenze, capacità e altre competenze necessarie per dare esecuzione al piano.
Il termine "sufficienti" è riferito alla quantità di risorse necessarie per portare a termine il piano.
Le risorse sono efficacemente impiegate quando vengono utilizzate in modo da ottimizzare il raggiungimento del piano approvato.

*2040 – Direttive e procedure*
Il responsabile internal auditing deve definire direttive e procedure per lo svolgimento dell'attività.

*Interpretazione:*
La forma e il contenuto di direttive e procedure dipende dalla Struttura e dalle dimensioni dell'attività di internal audit, nonché dalla complessità dei suoi compiti.

*2050 – Coordinamento delle attività*
Il responsabile internal auditing dovrebbe condividere le informazioni e coordinare le diverse attività con i diversi prestatori, esterni e interni, di servizi di assurance e consulenza, al fine di assicurare un'adeguata copertura e di minimizzare le possibili duplicazioni.

*2060 – Informazione periodica al senior management e al board*
Il responsabile internal auditing deve informare periodicamente il senior management e il board in merito a finalità, poteri e responsabilità dell'attività di internal audit, nonché comunicare lo stato di avanzamento del piano. Tale comunicazione deve comprendere inoltre i rischi significativi, inclusi quelli di frode, i problemi di controllo, i problemi di governance e ogni altra informazione necessaria o richiesta dal senior management e dal board.

*Interpretazione:*
Frequenza e contenuto dell'attività di comunicazione sono definiti di concerto con il senior management e il board e variano a seconda della rilevanza delle informazioni che devono essere comunicate e dell'urgenza dei relativi provvedimenti che competono al senior management e al board.

*2070 – Prestatore esterno di servizi e responsabilità organizzativa sull'internal auditing*
Quando l'attività di internal audit è affidata a un prestatore esterno di servizi, quest'ultimo deve fare in modo che l'organizzazione sia consapevole di avere la responsabilità di mantenere un'attività di internal audit efficace.

*Interpretazione*
Questa responsabilità si dimostra attraverso il programma di assurance e miglioramento della qualità, che valuta la conformità alla Definizione di Internal Auditing, al Codice Etico e agli Standard.

*2100 – Natura dell'attività*
L'attività di internal audit deve valutare e contribuire al miglioramento dei processi di governance, gestione del rischio e di controllo, tramite un approccio professionale e sistematico.

*2110 – Governance*
L'attività di internal audit deve valutare e fornire appropriati suggerimenti volti a migliorare il processo di governance nel raggiungimento dei seguenti obiettivi:

- favorire lo sviluppo di appropriati valori e principi etici nell'organizzazione;
- garantire l'efficace gestione dell'organizzazione e l'accountability;
- comunicare informazioni su rischi e controllo alle relative funzioni dell'organizzazione;
- coordinare le attività e il processo di scambio di informazioni tra il board, i revisori esterni, gli internal auditor e il management.

*2110.A1* – L'attività di internal audit deve valutare l'architettura, l'attuazione e l'efficacia degli obiettivi, dei programmi e delle attività dell'organizzazione in materia di etica.

*2110.A2* – L'attività di internal audit deve valutare se il processo di governance dei sistemi informativi aziendali aiuta le strategie e gli obiettivi dell'organizzazione stessa.

*2120 – Gestione del rischio*
L'attività di internal audit deve valutare l'efficacia e contribuire al miglioramento dei processi di gestione del rischio.

*Interpretazione:* Determinare se i processi di gestione del rischio siano efficaci è un giudizio che l'internal auditor esprime in base alla propria valutazione dei seguenti aspetti:

- che gli obiettivi aziendali supportino e siano coerenti con la "mission" aziendale;
- che i rischi significativi siano identificati e valutati;
- che vengano individuate opportune azioni di risposta ai rischi, al fine di ricondurli entro i limiti di accettabilità per l'azienda;
- che le informazioni sui rischi vengano raccolte e diffuse tempestivamente all'interno dell'organizzazione, consentendo al personale, al management e al board di adempiere alle rispettive responsabilità.

L'attività di internal audit può raccogliere le informazioni necessarie per questa valutazione attraverso molteplici incarichi.
I risultati di questi incarichi, visti nel complesso, permettono di capire i processi di gestione del rischio dell'organizzazione e la loro efficacia.
I processi di gestione del rischio sono monitorati attraverso la gestione manageriale continua, specifiche valutazioni, o entrambi.

*2120.A1* – L'attività di internal audit deve valutare l'esposizione al rischio che attiene alla governance, all'operatività e ai sistemi informativi dell'organizzazione, in termini di:

- raggiungimento degli obiettivi strategici dell'organizzazione;
- affidabilità e integrità delle informazioni contabili, finanziarie e operative;
- efficacia ed efficienza delle operazioni e dei programmi;
- salvaguardia del patrimonio;
- conformità a leggi, regolamenti, direttive, procedure e contratti.

*2120.A2* – L'attività di internal audit deve valutare la potenziale presenza di casi di frode e come l'organizzazione gestisce tali rischi.
*2120.C1* – Nello svolgimento di incarichi di consulenza, gli internal auditor devono tenere conto degli eventi di rischio attinenti agli obiettivi dell'incarico e prestare attenzione a qualsiasi altro rischio significativo.
*2120.C2* – Nella valutazione dei processi di gestione del rischio, gli internal auditor devono tenere conto anche delle conoscenze dei rischi dell'organizzazione, acquisite nel corso di incarichi di consulenza.
*2120.C3* – Quando assistono il management nella implementazione o nel miglioramento dei processi di gestione del rischio, gli internal auditor devono evitare di gestire direttamente i rischi, perché verrebbero così ad assumere responsabilità manageriali.

*2130 – Controllo*

L'attività di internal audit deve assistere l'organizzazione nel garantire la validità dei controlli attraverso la valutazione della loro efficacia ed efficienza e attraverso la promozione di un continuo miglioramento.

*2130.A1* – L'attività di internal audit deve valutare l'adeguatezza e l'efficacia dei controlli introdotti in risposta ai rischi riguardanti la governance, le operazioni e i sistemi informativi dell'organizzazione, relativamente a:

- raggiungimento degli obiettivi strategici dell'organizzazione;
- affidabilità e integrità delle informazioni contabili, finanziarie e operative;
- efficacia ed efficienza delle operazioni e dei programmi;
- salvaguardia del patrimonio;
- conformità a leggi, regolamenti, direttive, procedure e contratti.

*2130.C1* – Nella valutazione dei processi di controllo dell'organizzazione, gli internal auditor devono tenere conto anche delle conoscenze in materia di controllo acquisite nel corso di incarichi di consulenza

*2200 – Pianificazione dell'incarico*

Per ciascun incarico gli internal auditor devono predisporre e documentare un piano che comprenda gli obiettivi dell'incarico, l'ambito di copertura, la tempistica e l'assegnazione delle risorse.

*2201 – Elementi della pianificazione*

Nel pianificare l'incarico, gli internal auditor devono considerare:

- gli obiettivi e le modalità di controllo dell'andamento dell'attività oggetto di audit;
- i rischi significativi dell'attività, i propri obiettivi, risorse e operazioni, nonché le modalità di contenimento dei rischi entro i livelli di accettabilità;
- l'adeguatezza e l'efficacia dei processi di governance, di gestione dei rischi e di controllo dell'attività oggetto di audit, in riferimento a un quadro o modello di riferimento riconosciuto;
- le possibilità di apportare significativi miglioramenti ai processi di governance, di gestione dei rischi e di controllo dell'attività oggetto di audit.

*2201.A1* – Nel pianificare un incarico per conto di terze parti esterne all'organizzazione, gli internal auditor devono definire con queste un accordo scritto che chiarisca obiettivi, ambito di copertura, rispettive responsabilità ed eventuali aspettative e che stabilisca restrizioni alla diffusione dei risultati dell'incarico e all'accesso alla relativa documentazione.

*2201.C1* – Gli internal auditor devono concordare con i clienti di un incarico di consulenza gli obiettivi, l'ambito di copertura, le rispettive responsabilità e ciò che di ulteriore ci si attende. Per gli incarichi di maggiore rilevanza, tale accordo deve essere formalizzato in un documento scritto.

*2210 – Obiettivi dell'incarico*

Per ciascun incarico devono essere fissati obiettivi specifici.

*2210.A1* – Gli internal auditor devono effettuare una valutazione preliminare dei rischi afferenti l'attività oggetto di audit.

Gli obiettivi dell'incarico devono rispecchiare i risultati di tale valutazione.

*2210.A2* – Al momento della definizione degli obiettivi dell'incarico, gli internal auditor devono considerare il grado di probabilità che esistano errori significativi, frodi, non conformità e altre situazioni pregiudizievoli.

*2210.A3* – Per valutare la governance, la gestione dei rischi e dei controlli, sono necessari criteri adeguati. Gli internal auditor devono accertare che il management e/o il board abbiano stabilito criteri adeguati per valutare il raggiungimento di obiettivi e traguardi. Se tali criteri sono adeguati, gli internal auditor devono utilizzarli nell'effettuare la propria valutazione. In caso contrario, devono collaborare con il management e/o il board allo sviluppo di opportuni criteri di valutazione.

*2210.C1* – Gli obiettivi degli incarichi di consulenza devono riguardare processi di governance, di gestione dei rischi e di controllo, nella misura concordata con il cliente.

*2210.C2* – Gli obiettivi degli incarichi di consulenza devono essere coerenti con i valori, le strategie e gli obiettivi dell'organizzazione.

*2220 – Ambito di copertura dell'incarico*

L'ambito di copertura definito, deve essere sufficiente per consentire il raggiungimento degli obiettivi dell'incarico

*2220.A1* – L'ambito di copertura dell'incarico deve tenere conto dei sistemi informativi, delle registrazioni, del personale e dei beni patrimoniali, compresi quelli sotto il controllo di terze parti esterne.

*2220.A2* – Qualora, nel corso di un incarico di assurance, emergano opportunità significative di incarichi di consulenza, si dovrebbe stipulare uno specifico accordo scritto su obiettivi, ambito di copertura, rispettive responsabilità e su ciò che di ulteriore ci si attenda. I risultati raggiunti vanno comunicati secondo gli standard vigenti per gli incarichi di consulenza.

*2220.C1* – Nello svolgimento di un incarico di consulenza, gli internal auditor devono assicurarsi che l'ambito di copertura dell'incarico sia sufficientemente ampio per conseguire gli obiettivi concordati. Se, nel corso dell'incarico, gli internal auditor ritengono di ridefinire l'ambito di copertura, ne devono discutere con il cliente, per decidere se sia opportuno proseguire.

*2220.C2* – Nel corso degli incarichi di consulenza, gli internal auditor devono analizzare i controlli in coerenza con gli obiettivi dell'incarico ed essere attenti all'eventuale presenza di problematiche di controllo significative.

*2230 – Assegnazione delle risorse*

Gli internal auditor devono determinare le risorse necessarie e sufficienti per conseguire gli obiettivi dell'incarico in base alla valutazione della natura e complessità dello stesso, dei vincoli temporali e delle risorse a disposizione.

*2240 – Programma di lavoro*

Gli internal auditor devono sviluppare e documentare programmi di lavoro che permettano di conseguire gli obiettivi dell'incarico.

*2240.A1* – I programmi di lavoro devono includere le procedure per raccogliere, analizzare, valutare e documentare le informazioni durante lo svolgimento dell'incarico. I programmi di lavoro devono essere approvati prima della loro utilizzazione e ogni successiva modifica deve essere prontamente approvata.

*2240.C1* – I programmi di lavoro per gli incarichi di consulenza possono variare nella forma e nel contenuto, secondo la natura dell'incarico.

*2300 – Svolgimento dell'incarico*

Gli internal auditor devono raccogliere, analizzare, valutare e documentare informazioni sufficienti al raggiungimento degli obiettivi dell'incarico.

*2310 – Raccolta delle informazioni*

Gli internal auditor devono raccogliere informazioni sufficienti, affidabili, pertinenti e utili per conseguire gli obiettivi dell'incarico.

*Interpretazione:*

Le informazioni sono sufficienti quando sono concrete, adeguate e convincenti, così che, in base a esse, qualunque persona prudente e informata giungerebbe alle stesse conclusioni dell'auditor. Le informazioni sono affidabili quando sono fondate e sono le migliori ottenibili attraverso l'uso di tecniche adeguate all'incarico. Le informazioni sono pertinenti quando sono coerenti con gli obiettivi dell'incarico e danno fondamento ai rilievi e alle raccomandazioni. Le informazioni sono utili quando possono aiutare l'organizzazione a raggiungere le proprie finalità.

*2320 – Analisi e valutazione*

Gli internal auditor devono pervenire alle conclusioni e ai risultati dell'incarico sulla base di analisi e valutazioni appropriate.

*2330 – Documentazione delle informazioni*

Gli internal auditor devono documentare le informazioni atte a supportare le conclusioni e i risultati dell'incarico.

*2330.A1* – Il responsabile internal auditing deve controllare l'accesso alla documentazione dell'incarico. Prima di distribuire tale documentazione a parti terze, il responsabile internal auditing deve ottenere l'approvazione del senior management e/o, secondo le circostanze, il parere dell'ufficio legale.
*2330.A2* – Il responsabile internal auditing deve definire i criteri di conservazione delle carte di lavoro, indipendentemente dalle modalità di archiviazione. Tali criteri devono essere conformi alle linee guida dell'organizzazione, alla regolamentazione vigente in materia o a disposizioni di altro genere
*2330.C1* – Il responsabile internal auditing deve definire le direttive concernenti la custodia e l'archiviazione della documentazione relativa agli incarichi di consulenza, nonché la sua distribuzione all'interno e all'esterno dell'organizzazione.
Tali direttive devono essere conformi alle linee guida dell'organizzazione, alla regolamentazione vigente in materia o a disposizioni di altro genere.

*2340 – Supervisione dell'incarico*
Gli incarichi devono essere sottoposti a opportuna supervisione al fine di garantire che gli obiettivi vengano raggiunti, che la qualità sia assicurata e che il personale possa crescere professionalmente.

*Interpretazione:*
Il grado di supervisione richiesta dipende dalla professionalità e dall'esperienza degli internal auditor, nonché dalla complessità dell'incarico. Il responsabile internal auditing ha la completa responsabilità della supervisione dell'incarico, anche nel caso in cui questo sia svolto per conto dell'internal audit. Il responsabile internal auditing può delegare tale supervisione a internal auditor di provata esperienza.
Evidenza dell'avvenuta supervisione deve essere documentata e opportunamente conservata.

*2400 – Comunicazione dei risultati*
Gli internal auditor devono comunicare i risultati degli incarichi.

*2410 – Modalità di comunicazione*
La comunicazione deve includere gli obiettivi e l'estensione dell'incarico, così come le pertinenti conclusioni, raccomandazioni e piani d'azione.

*2410.A1* – Laddove appropriato, la comunicazione finale dei risultati deve contenere il giudizio o le conclusioni degli internal auditor. Quando espressi, il giudizio o la conclusione devono tenere in considerazione le aspettative del senior management, del board e degli altri stakeholder e devono essere corroborati da informazioni sufficienti, affidabili, pertinenti e utili.
Interpretazione:
I giudizi espressi a livello d'incarico possono essere valutazioni, conclusioni o altre descrizioni dei risultati. In questi casi, l'incarico può riguardare il controllo su un processo, un rischio o una business unit specifici.
Per formulare questi giudizi è necessario considerare i risultati dell'incarico e il loro significato.
*2410.A2* – Nelle comunicazioni relative all'incarico, gli internal auditor sono incoraggiati a dare atto delle operazioni svolte in modo adeguato dall'organizzazione.
*2410.A3* – In caso d'invio a terze parti esterne all'organizzazione, la comunicazione dei risultati deve prevedere espressamente limiti di utilizzo e di distribuzione.
*2410.C1* – Le comunicazioni relative allo stato di avanzamento e ai risultati finali degli incarichi di consulenza possono variare, nella forma e nei contenuti, in funzione della natura dell'incarico e delle esigenze del cliente.

*2420 – Qualità della comunicazione*
La comunicazione deve essere accurata, obiettiva, chiara, concisa, costruttiva, completa e tempestiva.

*Interpretazione:*

Una comunicazione accurata non presenta errori né distorsioni ed è fedele ai fatti rilevati. Una comunicazione obiettiva è corretta, imparziale e scevra da pregiudizi ed è il risultato di una valutazione imparziale ed equilibrata di tutti i fatti e le circostanze rilevanti.
Una comunicazione chiara ha senso logico ed è facilmente comprensibile. La chiarezza può essere migliorata limitando l'uso di termini tecnici e fornendo sufficienti informazioni di supporto.
Una comunicazione concisa è essenziale, evita formulazioni non necessarie, dettagli superflui, ridondanze e prolissità.

Una comunicazione costruttiva è utile al committente dell'incarico e all'organizzazione e induce miglioramenti laddove necessari.
Una comunicazione completa contiene tutti gli elementi informativi essenziali per i destinatari, nonché tutte le informazioni e le osservazioni significative atte a corroborare raccomandazioni e conclusioni.
Una comunicazione tempestiva è puntuale e opportuna nei tempi, in funzione della portata del problema, consentendo al management di intraprendere appropriate azioni correttive.

*2421 – Errori e omissioni nella comunicazione*
Se la comunicazione finale dei risultati contiene significativi errori od omissioni, il responsabile internal auditing deve inviare rettifiche e correzioni a tutti coloro che hanno ricevuto la comunicazione originale.
Gli internal auditor possono indicare che i loro incarichi sono "effettuati in conformità agli Standard Internazionali per la Pratica".

*2430 – Uso della dizione "Effettuato in accordo con gli Standard Internazionali per la Pratica Professionale dell'Internal Auditing"*
Gli internal auditor possono indicare che i loro incarichi sono "effettuati in conformità agli Standard Internazionali per la Pratica Professionale dell'Internal Auditing" solo se le risultanze del programma di assurance e miglioramento della qualità avvalorano tale affermazione.

*2431 – Comunicazione di non conformità di uno specifico incarico*
Nel caso di non conformità al Codice Etico o agli Standard che incidano negativamente su uno specifico incarico, la comunicazione dei risultati dell'incarico deve riportare:

- il principio o la regola di condotta del Codice Etico oppure lo Standard che non è stato pienamente rispettato;
- le ragioni della non conformità;
- le conseguenze della non conformità sull'incarico e sulla comunicazione dei relativi risultati.

*2440 – Divulgazione dei risultati*
Il responsabile internal auditing deve comunicare i risultati agli opportuni destinatari.
Interpretazione:
Il responsabile internal auditing, è tenuto a verificare ed approvare sia la comunicazione finale dei risultati dell'incarico prima dell'emissione degli stessi, sia la lista di distribuzione che la modalità di divulgazione. Laddove il responsabile internal auditing deleghi queste funzioni, egli ne rimane comunque totalmente responsabile.

*2440.A1* – Il responsabile internal auditing ha la responsabilità di comunicare i risultati finali dell'incarico ai soggetti dell'organizzazione in grado di assicurarne un seguito adeguato.

*2440.A2* – Se non diversamente prescritto da leggi, normative o regolamenti, prima di comunicare i risultati a terze parti esterne all'organizzazione, il responsabile internal auditing deve:

- valutare i potenziali rischi per l'organizzazione;
- consultare il senior management e/o l'ufficio legale a seconda delle circostanze;
- controllare la divulgazione, disponendo limitazioni sull'utilizzo dei risultati.

*2440.C1* – Il responsabile internal auditing è responsabile della comunicazione ai clienti dei risultati finali dell'incarico di consulenza.

*2440.C2* – Nel corso di incarichi di consulenza è possibile che vengano rilevate criticità concernenti la governance, la gestione dei rischi e il controllo. Se tali criticità sono significative per l'organizzazione, esse devono essere segnalate al senior management e al board.

*2450 – Giudizi complessivi*

Quando si esprime un giudizio complessivo, questo deve tenere in considerazione le aspettative del senior management, del board e degli altri stakeholder e deve essere corroborato da informazioni sufficienti, affidabili, pertinenti e utili.

Interpretazione: La comunicazione deve precisare:

- l'ambito di copertura, specificando il periodo di tempo cui si riferisce il giudizio;
- le limitazioni dell'ambito di copertura;
- tutti i progetti connessi che sono stati presi in considerazione, indicando l'eventuale ricorso ad altri fornitori di assurance;
- il modello di rischio o di controllo o gli altri criteri usati come fondamento per esprimere il giudizio complessivo;
- il parere, il giudizio o la conclusione complessivi formulati.

È necessario specificare i motivi dell'eventuale giudizio complessivo sfavorevole.

*2500 – Monitoraggio delle azioni correttive*

Il responsabile internal auditing deve stabilire e mantenere un sistema di monitoraggio delle azioni intraprese a seguito dei risultati segnalati al management.

> *2500.A1* – Il responsabile internal auditing deve impostare un processo di follow- up per monitorare e assicurare che le azioni correttive siano state effettivamente attuate dal management oppure che il senior management abbia accettato il rischio di non intraprendere alcuna azione.
> *2500.C1* – L'attività di internal audit deve monitorare le azioni intraprese a seguito di incarichi di consulenza nella misura concordata con il cliente.

*2600 – Comunicazione dell'accettazione del rischio*

Qualora il responsabile internal auditing concluda che il management abbia accettato un livello di rischio che potrebbe essere inaccettabile per l'organizzazione, ne deve discutere con il senior management. Se il responsabile internal auditing ritiene che la problematica non sia stata risolta, deve informarne il board.
È possibile identificare il rischio accettato dal management o attraverso un incarico di assurance o di consulenza che permetta di monitorare lo stato di implementazione delle azioni intraprese dal management in risposta a incarichi precedenti, oppure in altri modi. Il responsabile internal auditing non è responsabile per la gestione del rischio.

## GLOSSARIO

*Adeguato controllo*

Un controllo è adeguato se viene pianificato e organizzato (progettato) dal management in modo da dare ragionevole sicurezza che i rischi dell'organizzazione siano stati gestiti efficacemente e che le finalità e gli obiettivi dell'organizzazione saranno raggiunti in modo efficiente ed economico.

*Ambiente di controllo*

È costituito dagli atteggiamenti e dalle azioni del board e del management rispetto all'importanza del controllo all'interno dell'organizzazione. Esso fornisce la disciplina e l'organizzazione per il raggiungimento degli obiettivi primari del sistema di controllo interno. Gli elementi costitutivi dell'ambiente di controllo sono i seguenti:

- integrità e valori etici;
- filosofia e stile di direzione;
- Struttura organizzativa;
- attribuzione di poteri e responsabilità;
- politiche e prassi di gestione del personale;
- competenze del personale.

*Attività di internal audit*
Reparto, divisione, team di consulenti o di altri professionisti che forniscono servizi indipendenti e obiettivi di assurance e di consulenza, concepiti per aggiungere valore e migliorare l'operatività di un'organizzazione. L'attività di internal audit assiste un'organizzazione nel perseguimento dei propri obiettivi, tramite un approccio professionale sistematico finalizzato a valutare e migliorare l'efficacia dei processi di governance, di gestione dei rischi e di controllo

*Board*
Per board si intende il massimo organo di governo, che ha la responsabilità di indirizzare e/o di sorvegliare le attività e la gestione dell'organizzazione. In genere, il board è costituito da un gruppo indipendente di amministratori (per esempio, consiglio di amministrazione, consiglio di sorveglianza, consiglio dei governatori o dei trustee).
Nei casi in cui questo gruppo non è presente, per "board" si può intendere la persona a capo dell'organizzazione. Il termine "board" può anche designare un Audit Committee al quale l'organo di governo abbia delegato determinate funzioni

*Codice Etico (o Codice Deontologico)*
Il Codice Etico dell'Institute of Internal Auditors (IIA) è composto da Principi, fondamentali per la professione e la pratica dell'attività di internal audit, e da Regole di Condotta, che descrivono le norme comportamentali che gli auditor sono tenuti a osservare. Esso si applica sia alle singole persone sia agli enti che forniscono servizi di internal audit. Scopo del Codice Etico è quello di promuovere una cultura etica in tutti gli ambiti della professione di internal auditor.

*Condizionamenti*
Condizionamenti all'indipendenza organizzativa e all'obiettività individuale possono comprendere conflitti di interesse personali, limitazioni del campo di azione, restrizioni dell'accesso a dati, persone e beni aziendali e vincoli sulle risorse (come quelle finanziarie).

*Conflitto di interessi*
Qualsiasi relazione tra persone e/o organizzazioni che sia o appaia essere contraria agli interessi dell'organizzazione. Il conflitto di interessi pregiudica la capacità individuale di svolgere i propri compiti e responsabilità con obiettività.

*Conformità*
L'aderenza a direttive, piani, procedure, leggi, regolamenti, contratti o altri requisiti.

*Controlli IT (Information Technology)*
Controlli che supportano la gestione del business e la governance prevedendo controlli generali e specifici sulle infrastrutture informatiche quali sistemi applicativi, informazioni, infrastrutture e persone.

*Controllo*
Qualsiasi azione intrapresa dal management, dal board o da altri soggetti per gestire i rischi e aumentare le possibilità di conseguimento degli obiettivi e dei traguardi stabiliti. Il management pianifica, organizza e dirige l'esecuzione di iniziative in grado di fornire una ragionevole sicurezza sul raggiungimento di obiettivi e traguardi.

*Deve (devono)*
Gli Standard utilizzano la dizione "deve (devono)" per indicare un requisito la cui conformità è vincolante.

*Dovrebbe (dovrebbero)*
Gli Standard utilizzano la dizione "dovrebbe (dovrebbero)" per indicare un requisito la cui conformità è vincolante a meno di circostanze ed eventi che, sottoposti a un giudizio professionale, ne giustifichino l'inosservanza.

*Frode*
Qualsiasi atto illegale caratterizzato da falsità, dissimulazione e abuso di fiducia. Tali atti non sono legati a minacce di ricorso alla violenza o alla forza fisica. Le frodi sono perpetrate da persone e organizzazioni per ottenere denaro, beni o servizi, per evitare il pagamento o la perdita di servizi o per procurarsi vantaggi personali o commerciali.

*Gestione del rischio*
Processo teso a identificare, valutare, gestire e controllare possibili eventi o situazioni negativi, al fine di fornire una ragionevole assicurazione in merito al raggiungimento degli obiettivi dell'organizzazione

*Giudizio complessivo*
Valutazione, conclusione e/o altra descrizione dei risultati presentata dal responsabile internal auditing; essa verte, in termini generali, sui processi di governance, di gestione dei rischi e/o di controllo dell'organizzazione. Per giudizio complessivo si intende il giudizio professionale del responsabile internal auditing, basato sui risultati di una serie di incarichi
individuali e di altre attività per un determinato periodo di tempo.

*Giudizio dell'incarico*
Valutazione, conclusione e/o altra descrizione dei risultati di un incarico di internal audit, con riferimento agli obiettivi e all'ambito di copertura dell'incarico.

*Governance*
Insieme dei procedimenti e delle strutture messi in atto dall'organo di governo dell'organizzazione per informare, indirizzare, gestire e controllare le attività dell'organizzazione nel raggiungimento dei suoi obiettivi.

*Governance dei sistemi informativi*
Consiste nella guida, nelle strutture organizzative e nei processi finalizzati ad assicurare che la tecnologia informatica dell'azienda (IT) supporti le strategie e gli obiettivi dell'organizzazione.

*Incarico*
È la specifica assegnazione di un audit, compito o attività di verifica, siano essi un incarico di internal audit, una verifica di control self-assessment, una investigazione per frode o una consulenza. Un incarico può includere più compiti o attività, concepiti per raggiungere un insieme specifico di obiettivi interrelati.

*Indipendenza*
Libertà dai condizionamenti che minacciano la capacità dell'attività di internal audit di assolvere alle responsabilità di internal audit senza pregiudizi.

*International Professional Practices Framework (IPPF)*
Schema concettuale che definisce come deve essere Strutturato l'insieme delle disposizioni normative (authoritative guidance) emanate dall'IIA (The Institute of Internal Auditors) che si suddividono in due categorie: (1) disposizioni vincolanti e (2) disposizioni fortemente raccomandate.

*Livello di accettazione del rischio (risk appetite)*
Il livello di rischio che un'organizzazione è disposta a sostenere.

*Mandato di internal audit*
Il Mandato di internal audit è un documento formale che definisce finalità, poteri e responsabilità dell'attività di internal audit.
Il Mandato deve determinare la posizione dell'internal auditing nell'organizzazione, autorizzare l'accesso ai dati, alle persone e ai beni aziendali necessari per lo svolgimento degli incarichi di audit, nonché definire l'ambito di copertura delle

attività di audit.

*Obiettivi dell'incarico*
Enunciazioni di carattere generale che definiscono gli obiettivi attesi dell'incarico.

*Prestatore esterno di servizi*
Persona o società esterna all'organizzazione, munita di particolari conoscenze, competenze ed esperienze in una disciplina specifica.

*Processi di controllo*
Le politiche, le procedure (manuali e automatizzate) e le attività che fanno parte di un modello di controllo, progettato e gestito per assicurare che i rischi siano contenuti entro il livello che l'organizzazione è disposta a sostenere.

*Responsabile internal auditing (CAE – Chief Audit Executive)*
Il responsabile internal auditing è la persona con ruolo direttivo che ha la responsabilità di gestire in modo efficace l'attività di internal audit, in conformità al Mandato di internal audit e alla Definizione di Internal Auditing, al Codice Etico e agli Standard. Il responsabile internal auditing o i collaboratori che riferiscono a lui sono in possesso delle opportune qualifiche e certificazioni professionali. La designazione specifica del responsabile internal auditing può variare nelle diverse organizzazioni.

*Rischio*
Possibilità che si verifichi un evento che possa avere un effetto sul raggiungimento degli obiettivi. Il rischio si misura in termini di impatto e di probabilità.

*Servizi di assurance*
Consistono in un esame obiettivo delle evidenze, allo scopo di ottenere una valutazione indipendente dei processi di governance, di gestione del rischio e di controllo dell'organizzazione. Tra gli esempi si possono citare incarichi di tipo finanziario, di tipo operativo, di conformità, di sicurezza informatica e di due diligence.

*Servizi di consulenza*
Servizi di supporto e assistenza al cliente, la cui natura ed estensione vengano concordate con il cliente, tesi a fornire valore aggiunto e a migliorare i processi di governance, gestione del rischio e controllo di un'organizzazione, senza che l'internal auditor assuma responsabilità manageriali a riguardo. Tra i possibili esempi figurano consulenza, assistenza specialistica, facilitazione e formazione.

*Significatività*
Importanza relativa di un fatto, nell'ambito del contesto nel quale è considerato. Include fattori quantitativi e qualitativi quali la grandezza, la natura, le conseguenze, la rilevanza e l'impatto. Agli internal auditor è richiesto un giudizio professionale quando valutano la significatività dei fatti collocati nell'ambito degli obiettivi considerati.

*Standard*
Un enunciato professionale emanato dall'Internal Audit Standards Board che definisce le condizioni richieste per svolgere una vasta gamma di attività di internal audit e per la valutazione delle prestazioni dell'internal audit.

*Strumenti informatici di supporto all'audit*
Strumenti di audit automatizzati, quali software generici di audit, generatori dati di test, programmi informatici di audit e computer- assisted audit techniques (CAAT).

*Valore aggiunto*
L'attività di internal audit aggiunge valore all'organizzazione (e ai suoi stakeholder) quando fornisce un'assurance obiettiva e pertinente e quando contribuisce all'efficacia e all'efficienza dei processi di governance, di gestione del

rischio e di controllo.

## Allegato 5: tabella degli acronomi/abbreviazioni

Di seguito sono riportati gli acronimi – abbreviazioni utilizzati nel testo del presente regolamento:

| ACRONIMO - ABBREVIAZIONE | DESCRIZIONE |
|---|---|
| SiReg | Sistema Regionale |
| ATS | Agenzia Territoriale Sanitaria della Brianza |
| SCI | Sistema di Controllo Interno |
| IA | Internal Auditing |
| RIA | Responsabile Internal Auditing |
| POAS | Piano di Organizzazione Aziendale Strategico |
| CCI | Coordinamento dei Controlli Interni |