2017

Dispensa sull'internal auditing

VENTIN GIULIA

1 SOMMARIO

2 DISCIPLINA PROFESSIONALE

The Institute of Internal Auditors (The IIA) emana l'International Professional Practices Framework (IPPF) per guidare la pratica professionale dell'internal audit e assicurare elevati standard qualitativi nei risultati dell'attività di internal audit nei vari contesti di riferimento.
L'IPPF è costituito da:

- Missione;
- Principi fondamentali per la pratica professionale dell'internal auditing;
- Definizione di internal auditing;
- Codice etico;
- Gli Standard internazionali per la pratica professionale dell'Internal Auditing (detti anche Standard);
- Guide attuative;
- Guide supplementary.

I primi quattro elementi fanno parte della guida obbligatoria.
Gli Standard sono una guida obbligatoria basata su principi. Alcuni Standard includono "interpretazioni", cioè testi che spiegano meglio il contenuto della guida.
Gli Standard adottano termini che hanno significati specifici. Il libro rosso degli IPPF contiene un Glossario degli Standard.
Ci sono tre tipi di Standard:

- di connotazione;
- di prestazione;
- di implementazione.

Questi ultimi dettagliano gli Standard di connotazione e di prestazione fornendo separate indicazioni (obbligatorie) per gli interventi di Assurance (A) o di Consulenza (C).

Servizi di Assurance: valutazione obiettiva delle evidenze di audit finalizzata a fornire un'opinione o una conclusione indipendente circa le operazioni, funzioni, processi, sistemi, ecc., di un'entità. Generalmente sono tre i soggetti coinvolti: (1) il responsabile del processo auditato; (2) l'internal auditor; (3) l'utilizzatore del risultato

Servizi di Consulenza: hanno natura consultiva e sono generalmente svolti a fronte di una specifica richiesta del cliente. La natura e l'ambito dell'intervento di consulenza sono soggetti ad accordo con il cliente. Generalmente sono due i soggetti coinvolti: (1) l'internal auditor; (2) il cliente. Nello svolgimento di servizi di consulenza l'internal auditor deve mantenere l'obiettività e non deve assumere responsabilità manageriali.

Nel caso in cui leggi o regole impediscano agli internal auditor di attenersi a certe parti degli Standard, deve esserne data adeguata informazione. Gli internal auditor devono attenersi a tutte le altre parti degli Standard.

Le Guide attuative aiutano gli internal auditor a tradurre in pratica gli Standard obbligatori. Indicano l'approccio, la metodologia e considerazioni, non individuano processi e procedure dettagliati.

Le Guide supplementari forniscono una guida dettagliata per condurre attività di internal audit e includono processi e procedure dettagliate, come strumenti e tecniche, programmi, approcci step-by-step, compresi esempi di deliverables.

Gli internal auditor svolgono valutazioni interne ininterrotte della qualità e devono sottoporsi a una valutazione esterna indipendente della qualità per validare la conformità agli Standard (Quality Assurance & Improvement Program).

2.1 MISSIONE DELL'INTERNAL AUDITING

La Missione dell'Internal Auditing, inserita nel nuovo IPPF, ha l'obiettivo di rafforzare e supportare l'intero framework al fine di fornire una chiara e concisa descrizione di ciò che l'Internal Auditing aspira a conseguire all'interno delle organizzazioni:

"Proteggere ed accrescere il valore dell'organizzazione, fornendo assurance obiettiva e risk based, consulenza e competenza."

2.2 PRINCIPI FONDAMENTALI PER LA PRATICA PROFESSIONALE DELL'INTERNAL AUDITING

I Principi Fondamentali, nel loro insieme, caratterizzano un efficace internal auditing. Per considerare efficace una funzione internal audit, tutti i 10 Principi devono essere presenti ed applicati in modo ottimale. Il modo in cui i singoli internal auditor, o le funzioni internal audit, riescono a dimostrare la coerenza con tutti i Principi può essere molto diverso da un'organizzazione all'altra. Il mancato rispetto di uno o più Principi potrebbe lasciare intendere che l'attività di internal auditing non è efficace come invece dovrebbe essere nel compimento della propria Missione.

1. *Agire con manifesta integrità.*
2. *Dimostrare competenza e diligenza professionale.*
3. *Mantenere obiettività ed indipendenza di giudizio (libera da indebiti condizionamenti).*
4. *Operare in coerenza con le strategie, gli obiettivi e i rischi dell'organizzazione.*
5. *Avere un appropriato posizionamento organizzativo e risorse adeguate al ruolo.*
6. *Dimostrare elevati standard qualitativi ed essere orientati al miglioramento continuo.*
7. *Comunicare con efficacia.*
8. *Fornire una risk based assurance.*
9. *Operare con un approccio propositivo, proattivo e lungimirante.*
10. *Favorire il miglioramento dell'organizzazione.*

2.3 DEFINIZIONE DI INTERNAL AUDITING

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

2.4 CODICE ETICO

Introduzione

Scopo del Codice Etico dell'Institute of Internal Auditors è di promuovere la cultura etica nell'esercizio della professione di internal auditing. Il codice etico è uno strumento necessario e appropriato per l'esercizio dell'attività professionale di Internal Audit, che è fondata sulla fiducia indiscussa nell'obiettività dei suoi servizi di assurance riguardanti la governance, la gestione dei rischi e il controllo. Il Codice Etico dell'Institute of Internal Auditors si estende oltre la Definizione di Internal Auditing per includere due componenti essenziali.

1) I Principi, fondamentali per la professione e la pratica dell'internal auditing.
2) Le Regole di Condotta, che descrivono le norme comportamentali che gli internal auditor sono tenuti a osservare. Queste regole sono un aiuto per orientare l'applicazione pratica dei Principi e intendono fornire agli internal auditor una guida di comportamento professionale.

Il termine internal auditor si riferisce ai membri dell'Institute of Internal Auditors, ai detentori delle certificazioni professionali rilasciate dall'Institute, a coloro che si candidano a riceverle e a tutti coloro che svolgono attività di internal audit secondo la Definizione di Internal Auditing.

Applicabilità e attuazione

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

Principi

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

***1) Integrità -** L'integrità dell'internal auditor permette lo stabilirsi di un rapporto fiduciario e quindi costituisce il fondamento dell'affidabilità del suo giudizio professionale.*
***2) Obiettività -** Nel raccogliere, valutare e comunicare le informazioni attinenti l'attività o il processo in esame, l'internal auditor deve manifestare il massimo livello di obiettività professionale. L'internal auditor deve valutare in modo equilibrato tutti i fatti rilevanti, senza venire indebitamente influenzato da altre persone o da interessi personali nella formulazione dei propri giudizi.*
***3) Riservatezza -** L'internal auditor deve rispettare il valore e la proprietà delle informazioni che riceve ed è tenuto a non divulgarle senza autorizzazione, salvo che lo impongano motivi di ordine legale o deontologico.*
***4) Competenza -**Nell'esercizio dei propri servizi professionali, l'internal auditor utilizza il bagaglio più appropriato di conoscenze, competenze ed esperienze..*

Regole di condotta

***1) Integrità -** L'internal auditor:*
1.1 Deve operare con onestà, diligenza e senso di responsabilità.
1.2 Deve rispettare la legge e divulgare all'esterno solo se richiesto dalla legge e dai principi della professione.
1.3 Non deve essere consapevolmente coinvolto in nessuna attività illegale, né intraprendere azioni che possano indurre discredito per la professione o per l'organizzazione per cui opera.
1.4 Deve rispettare e favorire il conseguimento degli obiettivi dell'organizzazione per cui opera, quando etici e legittimi.
***2) Obiettività -** L'internal auditor:*

2.1 Non deve partecipare ad alcuna attività o avere relazioni che pregiudichino o appaiano pregiudicare l'imparzialità della sua valutazione. In tale novero vanno incluse quelle attività o relazioni che possano essere in conflitto con gli interessi dell'organizzazione.
2.2 Non deve accettare nulla che pregiudichi o appaia pregiudicare l'imparzialità della sua valutazione.
2.3 Deve riferire tutti i fatti significativi a lui noti, la cui omissione possa fornire un quadro alterato delle attività analizzate.
***3) Riservatezza -** L'internal auditor:*
3.1 Deve acquisire la dovuta cautela nell'uso e nella protezione delle informazioni acquisite nel corso dell'incarico.
3.2 Non deve usare le informazioni ottenute né per vantaggio personale, né secondo modalità che siano contrarie alla legge o di nocumento agli obiettivi etici e legittimi dell'organizzazione.
***4) Competenza -** L'internal auditor:*
4.1 Deve effettuare solo prestazioni per le quali abbia la necessaria conoscenza, competenza ed esperienza.
4.2 Deve prestare i propri servizi in pieno accordo con gli Standard internazionali per la Pratica Professionale dell'Internal Auditing
4.3 Deve continuamente migliorare la propria preparazione professionale nonché l'efficacia e la qualità dei propri servizi.

2.5 STANDARD INTERNAZIONALI PER LA PRATICA PROFESSIONALE DELL'INTERNAL AUDITING

Standard di Connotazione

1000 Finalità, poteri e responsabilità
1010 Riconoscimento delle Guidance vincolanti nel Mandato di internal audit
1100 Indipendenza e obiettività
1110 Indipendenza organizzativa
1111 Interazione diretta con il board
1112 Ruoli addizionali del responsabile internal auditing
1120 Obiettività individuale
1130 Condizionamenti dell'indipendenza o dell'obiettività
1200 Competenza e diligenza professionale
1210 Competenza
1220 Diligenza professionale
1230 Aggiornamento professionale continuo
1300 Programma di assurance e miglioramento della qualità
1310 Requisiti del programma di assurance e miglioramento della qualità
1311 Valutazioni interne
1312 Valutazioni esterne
1320 Comunicazione del programma di assurance e miglioramento della qualità
1321 Uso della dizione "Conforme agli Standard Internazionali per la pratica professionale dell'internal auditing"
1322 Comunicazione di non conformità

Standard di prestazione

2000 Gestione dell'attività di internal audit
2010 Pianificazione
2020 Comunicazione e approvazione
2030 Gestione delle risorse
2040 Direttive e procedure

Standard di Connotazione

2050 Coordinamento e affidamento
2060 Comunicazione al senior management e al board
2070 Prestatore esterno di servizi e responsabilità organizzativa dell'internal auditing
2100 Natura dell'attività
2110 Governance
2120 Gestione del rischio
2130 Controllo
2200 Pianificazione dell'incarico
2201 Elementi della pianificazione
2210 Obiettivi dell'incarico
2220 Ambito di copertura dell'incarico
2230 Assegnazione delle risorse per l'incarico
2240 Programma di lavoro dell'incarico
2300 Svolgimento dell'incarico
2310 Raccolta delle informazioni
2320 Analisi e valutazioni
2330 Documentazione delle informazioni
2340 Supervisione dell'incarico
2400 Comunicazione dei risultati
2410 Modalità di comunicazione
2420 Qualità della comunicazione
2421 Errori e omissioni
2430 Uso della dizione "Effettuato in accordo con gli Standard Internazionali per la pratica professionale dell'internal auditing"
2431 Comunicazione di non conformità dell'incarico
2440 Divulgazione dei risultati
2450 Giudizi complessivi
2500 Monitoraggio delle azioni correttive
2600 Comunicazione dell'accettazione del rischio

2.5.1 Standard di connotazione

Standard 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 Mission dell'Internal Auditing e con gli elementi vincolanti dell'International Professional Practices Framework (i Principi fondamentali per la pratica professionale dell'internal auditing, il Codice Etico, gli Standard e la Definizione di Internal Auditing). Il responsabile internal auditing deve verificare periodicamente il Mandato di internal audit e sottoporlo all'approvazione del senior management e del board.

Interpretazione:

Il Mandato di 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 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 siano 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.*

Standard 1010 - Riconoscimento delle guidance vincolanti nel Mandato di internal audit

Il carattere vincolante dei Principi fondamentali per la pratica professionale dell'internal auditing, del Codice Etico, degli Standard e della Definizione di Internal Auditing deve essere specificato nel Mandato di internal audit. Il responsabile internal auditing dovrebbe discutere la Mission dell'internal auditing e gli elementi vincolanti dell'International Professional Practices Framework con il senior management e il board.

Il Mandato deve essere allineato con gli Standard e, se vi sono parti degli IPPF che non possoo essere applicati per motivi di legge, il Mandato le deve specificare.
Elementi tipici del Mandato sono:

- *missione e ampiezza del lavoro*
- *responsabilità del RIA nei confronti del management e del Consiglio di Amministrazione/Audit Committee*
- *indipendenza della funzione Internal Audit*
- *livello di responsabilità del RIA e dello staff di Internal Audit*
- *livello di autorità del RIA e dello staff di internal audit*
- *standard della pratica di internal audit da applicare o da superare*
- *necessità di un accesso senza restrizioni a informazioni, persone e sistemi.*

Il Mandato deve essere adattato a ciascuna attività di internal audit e alle regole di governo di ciascuna organizzazione.

Standard 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 alle proprie responsabilità senza pregiudizi. Per raggiungere il livello di indipendenza necessario per adempiere efficacemente alle 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. I casi di limitazione all'indipendenza devono essere gestiti a livello di singolo auditor, di incarico, funzione e organizzazione.
Obiettività è l'attitudine mentale di imparzialità che consente agli internal auditor di svolgere gli 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 loro giudizio a quello di altri. Eventuali ostacoli all'obiettività devono essere gestiti a livello di singolo auditor, di incarico, funzionale e organizzativo.

Standard 1110 – Indipendenza organizzativa

Il responsabile internal auditing deve riportare a 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:

L'indipendenza organizzativa si realizza con efficacia quando il responsabile internal auditing riferisce funzionalmente al board. Ad esempio, il riporto funzionale al board comporta che il board:

- *approvi il Mandato di internal audit;*
- *approvi il piano di internal audit 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 alla revoca del responsabile internal auditing;*
- *approvi il compenso spettante al responsabile internal auditing;*
- *effettui opportune verifiche con il management e con 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 delle attività di internal auditing, nell'esecuzione del lavoro e nella comunicazione dei risultati. Il responsabile internal auditing deve comunicare eventuali interferenze al board e discuterne le implicazioni.*

Standard 1111 – Interazione diretta con il board

Il responsabile internal auditing deve comunicare e interagire direttamente con il board.

Standard 1112 - Ruoli addizionali del responsabile internal auditing

Laddove il responsabile internal auditing abbia, o si prevede abbia, ruoli e/o responsabilità che esulano dall'internal auditing, devono essere poste in essere opportune misure di tutela atte a limitare i condizionamenti all'indipendenza o all'obiettività.

Interpretazione:

Al responsabile internal auditing possono essere richiesti ruoli e responsabilità addizionali che esulano dall'internal auditing, come ad esempio la responsabilità per attività di Compliance o Risk Management. Tali ruoli e responsabilità possono condizionare, anche solo apparentemente, l'indipendenza organizzativa dell'attività di internal audit o l'obiettività individuale dell'internal auditor. Le misure di tutela sono quelle attività di supervisione, spesso intraprese dal board, atte a indirizzare questi potenziali condizionamenti e possono comprendere attività come la valutazione periodica delle linee di riporto e delle responsabilità e lo sviluppo di processi alternativi per ottenere l'assurance sulle aree di responsabilità addizionali.

Standard 1120 – Obiettività Individuale

Gli internal auditor devono avere un atteggiamento imparziale e senza pregiudizi ed evitare qualsiasi conflitto di interessi.

Interpretazione:

Il conflitto di interessi è una situazione nella quale un internal auditor, che gode di una posizione di fiducia, si trova ad avere un interesse personale o professionale contrario agli interessi dell'organizzazione. Un simile interesse contrario rende difficile per l'internal auditor assolvere ai propri compiti con imparzialità. Un conflitto di interessi sussiste anche quando non dà luogo a comportamenti non etici o 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 l'internal auditor, l'attività di internal audit e la professione. Il conflitto di interessi può pregiudicare la capacità individuale di assolvere con obiettività i propri compiti e responsabilità.

Standard 1130 - Condizionamenti dell'Indipendenza o dell'Obiettività

Se indipendenza od obiettività sono compromesse o appaiono tali, le circostanze dei condizionamenti devono essere rese note ad appropriati interlocutori. 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 a titolo unicamente esemplificativo conflitti di interessi personali, limitazioni del campo di azione, restrizioni dell'accesso a dati, persone e beni e vincoli di risorse, tra cui quelle finanziarie. L'individuazione degli interlocutori più appropriati al quale devono essere rese note le circostanze del condizionamento all'indipendenza o all'obiettività dipende dalle aspettative relative aspettative all'attività relative all'attività di internal audit e dalle responsabilità del responsabile internal auditing nei confronti del senior management e del board definite nel Mandato di internal audit, nonché dalla natura del condizionamento stesso.

***1130.A1** – Gli internal auditor devono astenersi dal valutare specifiche attività per le quali sono stati in precedenza responsabili. Si presume che l'obiettività sia condizionata se un internal auditor effettua un servizio di assurance per un'attività di cui è stato responsabile nell'anno precedente.*

***1130.A2** – Gli incarichi di assurance per funzioni che ricadono sotto la responsabilità del responsabile internal auditing devono essere supervisionati da soggetti esterni all'attività di internal audit.*

***1130.A3 NEW!!** – L'attività di internal audit può fornire servizi di assurance anche per quelle aree dove ha in precedenza svolto servizi di consulenza, a patto che la natura della consulenza non condizioni l'obiettività e che, nell'assegnazione delle risorse all'incarico, l'obiettività individuale sia salvaguardata.*

***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.*

Standard 1200 – Competenza e diligenza professionale

Gli incarichi devono essere effettuati con la dovuta competenza e diligenza professionale.

Standard 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:

Il termine competenza si riferisce complessivamente alle conoscenze, capacità e altre caratteristiche richieste agli internal auditor per adempiere efficacemente alle proprie responsabilità professionali. Questo include la valutazione della situazione attuale, dei trend e delle tematiche emergenti, allo scopo di consentire la formulazione di pareri e raccomandazioni pertinenti. 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 da "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 le modalità con cui l'organizzazione li gestisce; tuttavia non è richiesto 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 a livello di Information Technology, nonché avere a disposizione degli strumenti informatici di supporto all'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*

Standard 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 dovuta diligenza professionale tenendo in considerazione:*
• l'ampiezza del lavoro necessario per raggiungere gli obiettivi dell'incarico;
• la complessità, importanza o 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 di eventi di non conformità significativi;
• il costo dell'assurance in relazione ai suoi potenziali benefici.

***1220.A2** – Nell'esercizio dell'opportuna diligenza professionale, gli internal auditor devono considerare l'utilizzo di strumenti informatici di supporto all'audit 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. In ogni caso, 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 la 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.

Standard 1230 – Aggiornamento professionale continuo

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

Standard 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:

Il programma di assurance e miglioramento della qualità è disegnato per permettere una valutazione di conformità dell'attività di internal audit agli Standard e per consentire 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. Il responsabile internal auditing dovrebbe incoraggiare il board a supervisionare il programma di assurance e miglioramento della qualità.

Standard 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.

Standard 1311 – Valutazioni interne
Le valutazioni interne devono includere:

- *il monitoraggio continuo della prestazione dell'attività di internal audit;*
- *periodiche auto-valutazioni o valutazioni condotte da altre persone interne all'organizzazione che abbiano conoscenze adeguate della pratica professionale 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 considerati necessari per valutare la conformità al Codice Etico e agli Standard.
Le valutazioni periodiche sono effettuate con l'obiettivo di valutare la conformità al Codice Etico e agli Standard. L'adeguata conoscenza delle metodologie di internal audit presuppone perlomeno l'adeguata comprensione di tutti gli elementi dell'International Professional Practices Framework.

Standard 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 potenziali conflitti di interessi.*

Interpretazione:

Le valutazioni esterne possono essere effettuate con una valutazione interamente esterna oppure tramite un'autovalutazione con convalida esterna indipendente. Il valutatore esterno deve esprimere le proprie conclusioni in merito alla conformità al Codice Etico e agli Standard; la valutazione esterna può altresì comprendere osservazioni operative o strategiche.

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. Per quanto attiene ai 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 il proprio 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. Il responsabile internal auditing dovrebbe adoperarsi affinché il board supervisioni la valutazione esterna allo scopo di ridurre i conflitti di interessi percepiti o potenziali.

Standard 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. La comunicazione dovrebbero comprendere:

- *l'ambito e la frequenza delle valutazioni interne ed esterne;*
- *le qualifiche e l'indipendenza del(i) valutatore(i) o del team di valutatori, inclusa l'esistenza di potenziali conflitti di interessi;*
- *le conclusioni dei valutatori;*
- *le azioni correttive.*

Interpretazione:

La forma, il contenuto e la periodicità della comunicazione dei risultati del programma di assurance e miglioramento della qualità vengono concordati con il senior management e il board, considerando le responsabilità dell'attività di internal audit e del responsabile internal auditing definite nel Mandato di internal audit. Per dimostrare la conformità al Codice Etico e agli Standard, i risultati delle valutazioni periodiche esterne e interne vengono

comunicati al termine del processo di valutazione, mentre i risultati del monitoraggio continuo vengono comunicati almeno una volta l'anno. I risultati includono la valutazione del valutatore o del team di valutatori sul livello di conformità.

Standard 1321 - Uso della dizione "Conforme agli Standard Internazionali per la pratica professionale dell'internal auditing"

È consentito indicare che l'attività di internal audit risulta conforme agli Standard internazionali per la pratica professionale dell'internal auditing unicamente se i risultati del programma di assurance e miglioramento della qualità avvalorano tale affermazione.

Interpretazione:

L'attività di internal audit risulta conforme al Codice Etico e agli Standard quando raggiunge i risultati in essi descritti. 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. Le strutture di internal audit che operano da almeno cinque anni devono essere oggetto anche di valutazioni esterne.

Standard 1322 – Comunicazione di non conformità

In presenza di non conformità al Codice Etico o agli Standard che influiscano 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.

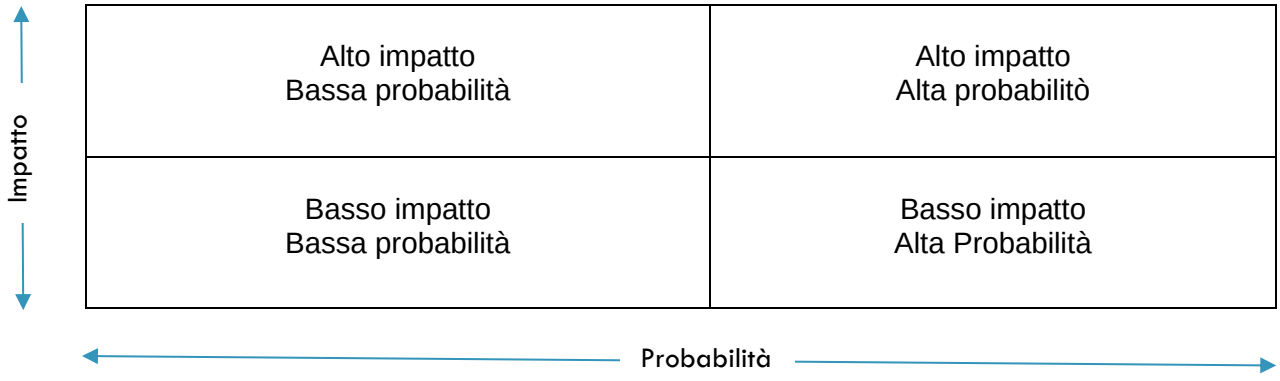
3 CONTROLLO INTERNO E RISCHIO

3.1 MISURAZIONE DEL RISCHIO

Rischio:

- interente: rischio in assenza di trattamento del rischio;
- residuo: rischio che residua dopo che è stata elaborata una risposta al rischio.

Misurazione del rischio: Probabilità (P) * Impatto (I)



3.2 TIPI DI CONTROLLO E SUOI REQUISITI

Standard 2130 – Controllo

L'attività di internal audit deve assistere l'organizzazione nel mantenere controlli efficaci attraverso la valutazione della loro efficacia ed efficienza e promuovendo il miglioramento continuo.

***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 attività e i sistemi informativi dell'organizzazione, relativamente a:*

- *raggiungimento degli obiettivi strategici dell'organizzazione;*
- *affidabilità e integrità delle informazioni 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 delle conoscenze in materia di controllo acquisite in occasione di incarichi di consulenza.*

Il management è responsabile dell'implementazione e del mantenimento di un sistema di controllo interno nell'organizzazione.

Controllo è "qualsiasi azione intrapresa dal management, dal Consiglio 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." (Glossario IPPF).
Strutture, attività, processi e sistemi che aiutano il management a mitigare efficacemente il rischio sono esempi di controlli interni.

Si riportano di seguito alcune classificazioni dei controlli.

I controlli possono essere classificati in:

- entity-level: si applicano all'intera organizzazione e sono disegnati sia per assicurare che gli obiettivi organizzativi siano raggiunti sia per mitigare i rischi che minacciano l'organizzazione nel suo complesso:
    - governance: stabiliscono la cultura del controllo e chiarificano le aspettative dell'organizzazione (ad es.: istituzione della supervisione dell'audit committee sui controlli; comunicare il risk appetite del Consiglio e del top management; atteggiamento nei confronti della redazione del bilancio), e includono direttive e procedure (ad es.: codice etico; direttive di conformità; direttive IT; procedure di management come ad esempio l'utilizzo dell'entrprise risk management) valide per l'organizzazione nel suo complesso;
    - management oversight: sono controlli posti a livello di unità organizzativa, diretti al raggiungimento degli obiettivi delle unità organizzative e alla mitigazione dei relativi rischi (ad es.: controlli period-end; controlli di tipo IT general);
- process-level: stabiliti da un process owner per assicurare che gli obiettivi del processo siano raggiunti e che i rischi a livello di processo siano fronteggiati (ad es.: supervisione; monitoraggio; risk assessment a livello di processo; valutazione delle performance; riconciliazione di conti chiave, ricognizione inventariale);
- transaction-level: sono specifici della singola transazione. Esistono per assicurare che gli obiettivi della transazione siano raggiunti e che i relativi rischi siano fronteggiati (ad es.: requisiti della documentazione, segregazioni dei compiti, autorizzazioni, controlli di tipo IT application).

I controlli possono essere classificati anche in base alla loro importanza:

- key control: controllo che deve operare efficacemente per ridurre un rischio significativo a un livello accettabile;
- secondary control: controllo che aiuta il processo a operare correttamente ma non è essenziale; esistono per mitigare un rischio non significativo o operano come controllo ridondante per un rischio significativo già fronteggiato da un key control.

Un'altra classificazione si basa sulle funzioni dei controlli:

- preveventive: controlli proattivi che impediscono a determinati eventi indesiderati di manifestarsi;
- detective: sono reattivi e rilevano eventi indesiderati che si sono manifestati;
- corrective: sono reattivi e sono disegnati per consentire una correzione manuale o automatica delle irregolarità rilevate;
- directive: controlli proattivi che stimolano l'accadimento di eventi desiderabili (ad es.: linee guida; programmi di formazione; piani di incentivazione);
- mitigating: riducono il potenziale impatto degli eventi rischiosi (ad es.: assicurazione);
- compensating: compensano l'assenza dei controlli attesi (ad es.: una stretta supervisione può compensare per una mancata segregazione dei compiti);
- redundant o backup: duplica un controllo e può operare come secondario se il key control fallisce.

Dal punto di vista dell'operatore:

- attivo o manuale: prevede l'intervento umano (ad es.: review di una transazione da parte del manager);
- passivo o automatico: opera senza l'intervento umano (ad es.: termostato).

Un'altra classificazione significativa è la seguente:

- hard control: quantitativi e oggettivi (direttive e procedure; struttura organizzativa; burocrazia; processi rigidamente formalizzati; accentramento decisionale);
- soft control: qualitativi e soggettivi, sono indicativi della cultura dell'organizzazione (competenza; fiducia; valori condivisi; leadership forte; alte aspettative; apertura; alti standard etici).

I controlli IT possono essere classificati in:

- IT general: sono controlli entity-level che si applicano ai processi IT generali. Sono di livello governance (ad es.: privacy policy) e management oversight (ad es.: standard di test, segregazione di compiti IT);
- application o technical: sono process o transaction level e possono essere di tipo:
    - Input: verificano l'integrità dei dati in ingresso (manualmente o in modo automatico);
    - Processing: controllano che il data processing sia accurato, completo e valido;
    - Output: verificano che i dati di output siano accurati, completi e validi.

Il controllo deve:

- essere disegnato in maniera efficace;
- operare efficacemente.

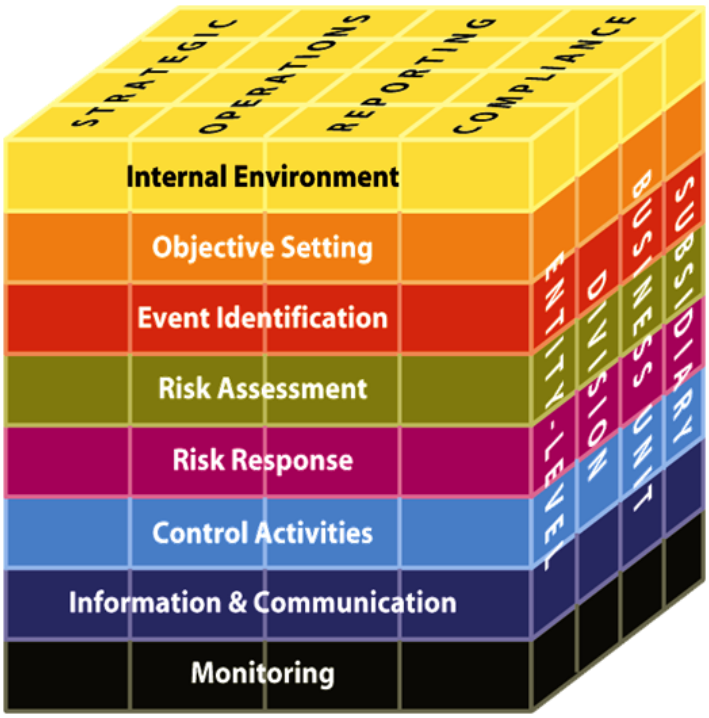
3.3 FRAMEWORK DI CONTROLLO INTERNO

Un control framework è un sistema riconosciuto di concetti che ricomprendono tutti gli elementi del controllo interno.

COSO's Internal Control – Integrated Framework

Componente	Descrizione
Control environment	Fissa il tono dell'organizzazione, influenzando la coscienza di controllo di tutto il personale. E' il fondamento di tutte le altre componenti del controllo interno. Si esprime nei seguenti fattori: - integrità e valori etici; - commitment alla competenza; - CdA o audit committee; - filosofia e stile del management; - struttura organizzativa; - assegnazione di autorità e responsbilità; - direttive e pratiche HR.
Risk assessment	Identificazione e analisi dei rischi rilevanti, costituisce la base per determinare come i rischi dovrebbero essere gestiti.
Control activities	Direttive e procedure. Assicurano che siano assunte le decisioni necessarie per fronteggiare i rischi al fine di consentire il raggiungimento degli obiettivi.
Information and communication	Informazioni pertinenti devono essere identificate, raccolte e comunicate in modo da consentire al personale di prendersi carico delle proprie responsabilità.
Monitoring	I sistemi di controllo interno devono essere monitorati attraverso attività di monitoraggio continuo, valutazioni distinte o una combinazione delle due.

COSO's ERM – Enterprise Risk Management



Componente	Descrizione
Internal environment	L'ambiente interno comprende il tono dell'organizzazione e definisce le basi per capire come il rischio è visto e gestito dal personale, compresa la filosofia di risk management e il risk appetite, l'integrità e i valori etici, e l'ambiente in cui operano.
Objective setting	Il management deve avere implementato un processo di definizione degli obiettivi che devono essere allineati con la missione e con il risk appetite.
Event identification	Devono essere identificati gli eventi interni e esterni che influenzano il raggiungimento degli obiettivi e devono essere distinti in rischi e opportunità.
Risk assessment	I rischi sono analizzati, considerando probabilità e impatto, per determinare come dovrebbero essere gestiti. I rischi sono valutati sia in quanto inerenti sia in quanto residui, dopo che è intervenuto il relativo trattamento..
Risk response	Il ranagement sceglie la risposta al rischio (avoiding, accepting, reducing, sharing), sviluppando un set di azioni che allineino i rischi con la risk tolerance e il risk appetite dell'ente.
Control activities	Direttive e procedure sono definite e implementate per assicurare che la risposta al rischio sia effettivamente posta in atto.
Information and communication	Informazioni pertinenti devono essere identificate, raccolte e comunicate in modo da consentire al personale di prendersi carico delle proprie responsabilità.
Monitoring	L'enterprise risk management viene monitorato nella sua interezza e sono introdotte modifiche ove necessario. Il monitoraggio è attuato attraverso attività di monitoraggio continuo, valutazioni distinte o una combinazione delle due.

3.4 CONSAPEVOLEZZA DEL RISCHIO DI FRODE

***1210.A2** – Gli internal auditor devono possedere conoscenze sufficienti per valutare i rischi di frode e le modalità con cui l'organizzazione li gestisce; tuttavia non è richiesto che essi abbiano le competenze proprie di chi ha come responsabilità primaria quella di individuare e investigare frodi.*

Tipi di frode:
- frode a beneficio di un individuo e a spese dell'organizzazione;
- frode a beneficio dell'organizzazione (falso in bilancio, evasione fiscale, ecc.).

Altra classificazione:
- frode commessa da un interno;
- frode commessa all'esterno dell'organizzazione.

Ancora:
- on-book;
- off-book.

Un'ultima classificazione riguarda il ciclo di business in cui si verifica.

Vi è un set di tre condizioni che, se presenti nella giusta proporzione, suggeriscono la possibilità di frode (red flags):
- opportunità: il controllo fallisce o è mal disegnato o assente; persone in posizione di autorità possono creare opportunità per l'evasione dei controlli esistenti, in quanto i collaboratori o gli scarsi controlli possono consentirgli di bypassare le regole;
- motivazione o incentivo o pressione: il potere è un forte motivatore; un altro è la gratificazione di un desiderio o la pressione;
- razionalizzazione: rubare a un'azienda non è "male" (depersonalizzazione), le regole non hanno senso, prendo il denaro solo in prestito, neanche i dirigenti rispettano le regole, ecc.

4 PIANO DI AUDIT RISK BASED

Standard 2010 – Pianificazione

Il responsabile internal auditing deve predisporre un piano basato sulla valutazione dei rischi al fine di determinare le priorità dell'attività di internal audit in linea con gli obiettivi dell'organizzazione.

Interpretazione:

Per predisporre il piano risk based, il responsabile internal auditing si consulta con il senior management e il board per comprendere le strategie, i principali obiettivi di business, i rischi associati e i processi di gestione del rischio dell'organizzazione. Il responsabile internal auditing deve rivedere e adeguare opportunamente il piano, in risposta ad eventuali cambiamenti intervenuti a livello di attività, rischi, operatività, programmi, sistemi e controlli dell'organizzazione.

***2010.A1** – Il piano degli incarichi dell'attività di internal audit deve basarsi su una documentata valutazione del rischio, effettuata almeno una volta l'anno. Tale processo deve tenere in considerazione le indicazioni del senior management e del board.*

***2010.A2** – Il responsabile internal auditing deve individuare e considerare le aspettative del senior management, del board e degli altri stakeholder per quanto attiene ai giudizi e alle conclusioni dell'internal audit.*

***2010.C1** – Il responsabile internal auditing dovrebbe 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.*

Gli internal auditor non possono valutare tutti i possibili rischi di un'organizzazione. E' necessario un uso efficiente di risorse di internal audit limitate. Per far questo l'internal audit ricorre a un risk assessment framework (ad es.: COSO's ERM).
Nella fase di identificazione dei rischi di distinguono:

- rischi strategici;
- rischi di progetto/programma/processo;
- rischi operativi.

Alla fase di identificazione dei rischi segue la misurazione, quindi la definizione delle priorità di intervento che confluiscono nel Piano di Audit.

Standard 2020 – Comunicazione e approvazione

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

Standard 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 temine "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.

E' responsabilità del RIA comunicare al senior management e al Consiglio quali risorse sono disponibili e se vi è qualche limitazione nelle risorse che può incidere negativamente sull'ampiezza degli interventi proposti o sull'esecuzione del programma degli interventi. In questi casi, il corso di azioni meno desiderabile è quello di eliminare alcuni interventi programmati. Il RIA dovrebbe considerare delle alternative come il co-sourcing per acquisire risorse temporanee.

5 TIPI DI INTERVENTI DI AUDIT

Tipo	Servizi di Assurance	Servizi di Consulenza
Definizione	Esame obiettivo delle evidenze col proposito di fornire una valutazione indipendente sui processi di governance, di risk management e di controllo dell'organizzazione.	Consultiva e di servizio al cliente, la cui natura e ambito sono concordate con il cliente e che mirano ad aggiungere valore e migliorare i processi di governance, di risk management e di controllo dell'organizzazione, senza che l'internal auditor assuma responsabilità gestionali.
Soggetti coinvolti	Tipicamente tre:	Tipicamente due:

	- il process owner; - l'internal auditor; - l'utilizzatore dei risultati.	- l'internal auditor; - il cliente.
Ambito di intervento	La natura e l'ambito dell'intervento sono definiti dall'internal auditor	La natura e l'ambito dell'intervento sono definiti dal cliente, in accordo con l'internal auditor
Deliverable	Comunica una valutazione, opinione o conclusione sui risultati dell'intervento	Consiglia, assiste e aggiunge valore ai processi di governance, di risk management e di controllo dell'organizzazione.

Tipologie di interventi di assurance:

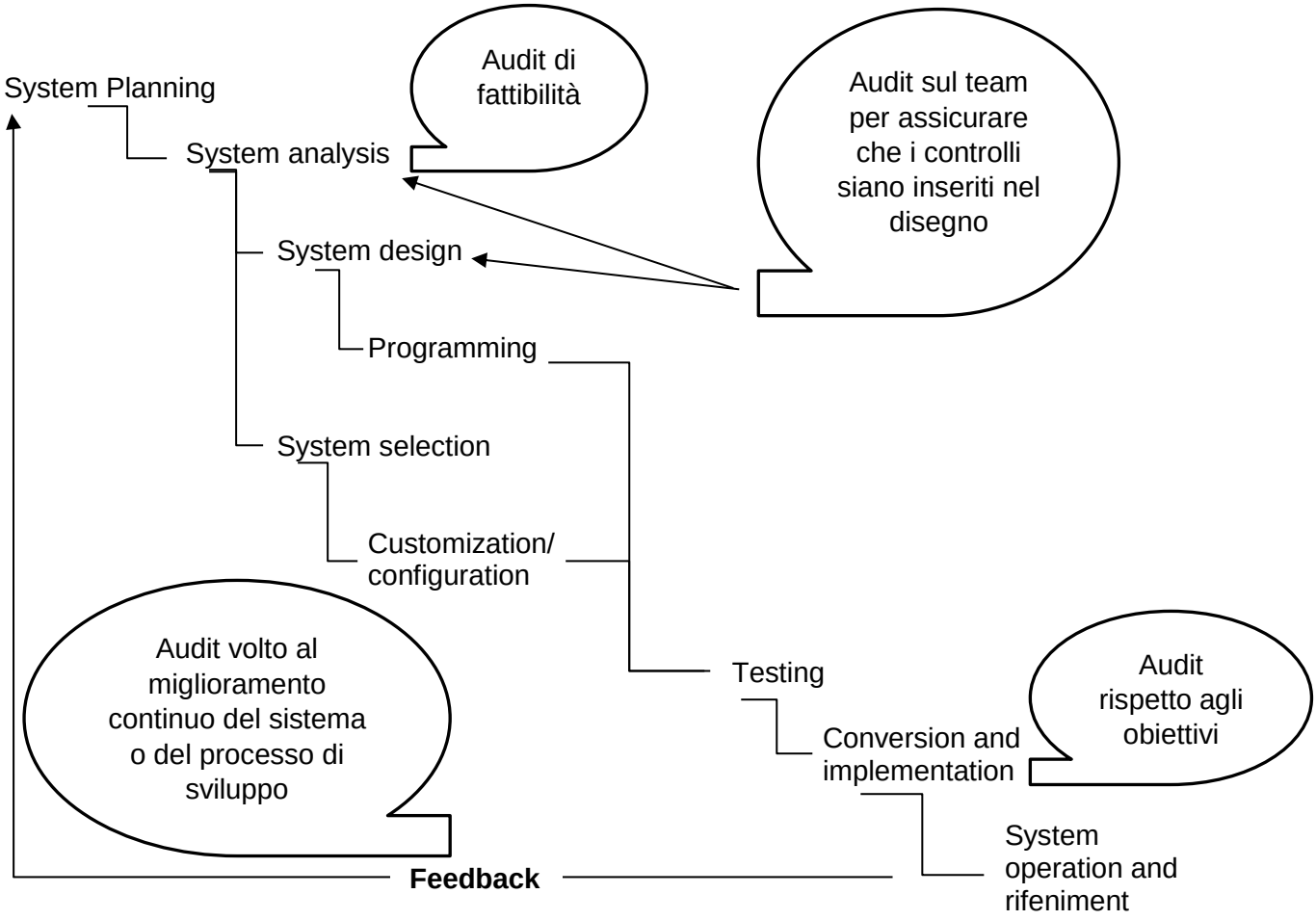
Tipo di intervento	Descrizione
CSA (Control self-assessment) o CRSA (Control/risk self assessment)	Il ruolo dell'internal auditor varia tra due estremi: - coinvolgimento intenso, con l'internal auditor fortemente coinvolto nelle dinamiche del processo, con un ruolo di formatore e un forte ruolo di facilitazione e coordinamento; - coinvolgimento minimo, in cui l'internal auditor ha il ruolo di parte interessata, consulente, e verificatore delle valutazioni del team. In entrambi i casi l'internal auditor deve mantenere la propria obiettività e evitare ogni forma di conflitto di interessi. Modalità di svolgimento: - workshop; - questionario; - analisi autoprodotte dal management.
EBR (External Business Relationship) o Contract	Può avere ad oggetto un partner in una joint venture, produttori di servizi in out-sourcing, agenti, fornitori, ecc.
Quality	Può assumere la forma di una conformità a un sistema di qualità organizzato come ad esempio la gestione della qualità totale. I costi della qualità possono essere così riassunti: - prevention: sostenuti per eliminare prodotti difettosi prima della loro produzione; - appraisal: sostenuti per identificare i prodotti difettosi prima della spedizione. O altrimenti: - internal failure: sostenuti per identificare i prodotti difettosi prima della spedizione; - external failure; sostenuti quando il cliente riceve i prodotti difettosi.
Due diligence	E' il processo di investigazione di una persona, un business, una transazione finanziaria per stabilire il valore di un'entità, di una transazioe e il costo di ogni passività associata. I tipi più comuni sono: - finanziario; - immobiliare; - proprietà intellettuale. Normalmente sono coinvolti tre tipi di soggetti: - internal auditors;

	- avvocati; - revisori esterni. Possono essere svolte: - pre-acquisizione: prospettiva del compratore o del venditore; - post acquisizione.
Security	Si concentra sulla valutazione dei rischi, dei controlli e della governance in relazione alla salvaguardia delle attività e alla affidabilità e integrità delle informazioni.
Privacy	L'internal auditor lavora qui con i legali interni, con specialisti IT e con esperti di privacy.
Performance	Si valuta il processo di gestione delle performance, che rappresenta la chiave per un management di successo.
Operational	Fornisce assurance sulla governance, il risk management e I controlli per quanto concerne l'efficacia e l'efficienza delle operazioni.
Financial	Si concentra sui controlli interni dell'organizzazione, in ambito finanziario. Utilizza indici di bilancio: di attività, di liquidità, di leva finanziaria e di profittabilità.
Compliance	L'organizzazione dovrebbe stabilire standard e procedure di compliance in grado di ridurre il rischio di condotte illegittime.

Tipologie di interventi di consulenza:

Tipo di intervento	Descrizione
Business Process Mapping	E' spesso usato negli interventi di consulenza come un equivalente dell'intervento di audit operativo. Utilizza strumenti quali: - walk through; - flowcharting.
Benchmarking	Ci sono diversi tipi di benchmarking: - interno: confronto all'interno del processo o dell'ente; - competitivo: confonto con i competitori diretti; - di settore: confronto con processi simili nel settore; - funzionale: confronto con funzioni collegate in altri settori; - generico: confronto con processi dalle caratteristiche analoghe in altri settori; - best-in-class: confronto che organizzazioni che sono best-in-class nella funzione.
Systems development life cycle review	Gli internal auditor possono essere coinvolti nella revisione del disegno in diversi punti del ciclo di sviluppo del Sistema: - system analysis: audit sulla fattibilità; - system design e system selection: audit sul team per assicurare che i controlli siano inseriti nel disegno; - system conversion e system implementation: audit rispetto agli obiettivi;

	- feedback: audit volto al miglioramento continuo del sistema o del processo di sviluppo.



6 CONDUZIONE DEGLI INTERVENTI DI AUDIT

6.1 PIANIFICAZIONE DELL'INCARICO

Durante la fase di pianificazione, si svolge in primo luogo un'analisi preliminare. Durante questa fase, si esaminano i precedenti rapporti di audit e altra documentazione rilevante per l'intervento. Inoltre vengono elaborate checklist o questionari di controllo interno. Infine, vengono condotte interviste e walk-through.

Segue lo svolgimento di un risk assessment per l'intervento in corso con l'identificazione dei rischi e dei controlli chiave.

Può anche essere elaborata una Matrice Rischi-Controlli.

Obiettivi	Rischi	Probabilità/Impatto	Controlli	Val.ne disegno	Val.ne operatività	Valutazione finale

Possono inoltre essere utilizzati strumenti di process mapping, tra cui i flowchart, per comprendere pienamente i processi operativi di riferimento.

Da ciò, viene sviluppato un audit program, che deve essere approvato per iscritto dal RIA o da un collaboratore da lui designato.

Si determina quindi il livello di staff e risorse necessarie per l'intervento e si elabora un diagramma di Gantt.

Segue la selezione dei campioni che possono essere di tipo statistico o non statistico.

Una volta elaborata la bozza di audit program, è necessario informare il management sull'intervento in partenza. Costituiscono oggetto dell'incontro iniziale con il cliente, detto kick off meeting:

- l'identificazione dei contatti chiave e relativa disponibilità;
- canali preferiti di comunicazione;
- documenti e record necessari;
- complessità delle operazioni da esaminare;
- accesso alle sedi;
- autorizzazioni;
- ecc.

6.2 VALUTAZIONE DELLE EVIDENZE

Tipi di evidenze:

- fisica;
- documentale;
- testimoniale (la forma più debole di evidenza);
- analitica.

Evidenze provenienti da terze parti sono più affidabili di quelle provenienti dall'ente auditato.

Standard 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 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 aiutano l'organizzazione a raggiungere le proprie finalità.

Le modalità di acquisizione delle evidenze sono:

-

Procedure	Descrizione	Esempi
Inchiesta	Porre domande al personale auditato o a terze parti e ottenere la loro risposta orale o scritta. Produce evidenza indiretta, che raramente da sola è persuasiva.	• Fare circolare un questionario tra i dirigenti chiedendo loro di identificare i principali 10 rischi che minacciano l'organizzazione; • Chiedere al consulente legale esterno dell'organizzazione di fornire informazioni su cause, richieste di risarcimento e o pratiche contro l'organizzazione.
Osservazione	Osservare persone, procedure o processi. Generalmente considearta più persuasiva dell'inchiesta in quanto l'internal auditor ottiene evidenze dirette.	• Giro dello stabilimento per comprendere le operazioni quotidiane; • Osservare con attenzione le operazioni di conta durante l'inventario di fine anno
Ispezione	Studiare documenti e registrazioni e esaminare fisicamente le risorse tangibili. L'ispezione di documenti e record fornisce evidenza diretta del loro contenuto. L'esame fisico delle risorse tangibili (ad es., un edificio o un'attrezzatura) fornisce all'internal auditor una conoscenza personale dell'esistenza e della condizione fisica della risorsa.	• Visionare i verbali del Consiglio per verificare l'autorizzazione di eventi significativi (ad es., l'acquisizione di un'altra azienda); • Ispezionare determinate rimanenze per valutare la loro condizione e vendibilità.
Vouching	Tracciare informazioni all'indietro da un documento o record a un documento o record precedentemente preparato. Serve a verificare la validità di informazioni documentate o registrate.	• Vouching di un campione di rimanenze dai record contabili al magazzino per verificare che la rimanenze esistano; • Vouching di un campione di fatture di vendita ai corrispondenti documenti di trasporto per verificare che la specizione sia avvenuta.
Tracing	racciare informazioni in avanti da un documento o record a un documento o record preparato successivamente. Serve a verificare la completezza di informazioni documentate o registrate.	• Tracing dei conteggi delle rimanenze dell'internal auditor ai record di compilazione delle rimanenze di magazzino del cliente per verificare che i conteggi siano stati inclusi nella compilazione; • Tracing degli assegni datati in un periodo di alcuni giorni prima e dopo fine anno ai record contabili per assicurare che gli assegni siano stati registrati nell'anno corrretto.
Re-performance	Rifare attività di controllo o altre procedure; rifare calcoli per	• Ricalcolare l'ammortamento per verificare che sia corretto;

	verificare se i calcoli del cliente sono corretti.	• Valutare indipendentemente i fondi rischi per assicurare la ragionevolezza delle stime del settore contabilità.
Analytical procedure	Valutare informazioni che prevedono comparazioni delle informazioni con stime identificate o sviluppate dall'internal auditor. Alcune relazioni tra diversi pezzi di informazioni ci si aspetta rimangano costanti in assenza di condizioni note che sostengano il contrario.	• Analisi di bilancio (indici di composizione); • Benchmarking interno e esterno.
Richiesta di conferme esterne	Ottenere verifica (positiva o negativa) scritta diretta dell'accuratezza dell'informazione da una terza parte indipendente.	• Conferma del saldo dei crediti verso clienti; • Conferma del saldo del conto banca.

6.3 Analisi e interpretazione dei dati

A volte i programmi di internal audit lavorano in collegamento con il programma gestionale consentendo a volte di monitorare le transazioni in tempo reale.

In generale, si utilizzano i GAS - General Audit Software, tra cui molto comune è MS Access. I GAS consentono di:

- leggere i file digitali;
- esaminare particolari record in base a criteri definiti dall'auditor;
- fare verifiche sui calcoli o fare calcoli autonomi;
- analizzare, riassumere o modificare la sequenza dei dati;
- verificare l'efficacia dei controlli.

Le carte di lavoro possono essere quindi anche elettroniche, non sempre cartacee.

Molto diffuso è l'uso di fogli di calcolo tipo MS Excel, che pongono diversi problemi di affidabilità in particolare quando sono strumenti di lavoro del cliente, e vanno quindi accuratamente verificati.

I dati raccolti sono frequentemente oggetto di analisi statistiche.
Inoltre, i dati possono essere elaborati attraverso teniche analitiche, tra cui:

- test di ragionevolezza;
- analisi di varianza;
- analisi di trend;
- analisi basata su indici (finanziari e non);
- regressione;
- diagrammi di causa ed effetto;
- analisi di Pareto: si basa sulla regola dell'80/20 per cui l'80% degli effetti è causata dal 20% delle possibili cause;
- comparazione tra periodi;
- comparazione con budget, preconsuntivi e informazioni economiche;
- comparazione con fattori indipendenti casuali o collegati.

6.4 DOCUMENTAZIONE/CARTE DI LAVORO

Standard 2330 – Documentazione delle informazioni

Gli internal auditor devono documentare informazioni sufficienti, affidabili, pertinenti e utili per supportare i risultati e le conclusioni dell'incarico.

***2330.A1** – Il responsabile internal auditing deve controllare l'accesso alla documentazione dell'incarico. Prima di rilasciare tale documentazione a parti terze, il responsabile internal auditing deve ottenere l'approvazione del senior management e/o del consulente legale, secondo le circostanze.*

***2330.A2** – Il responsabile internal auditing deve definire i criteri di conservazione della documentazione dell'incarico, indipendentemente dalle modalità di archiviazione. Tali criteri devono essere conformi alle linee guida dell'organizzazione e ai requisiti normativi o di altra natura in materia.*

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 e ai requisiti normativi o di altra natura in materia.

Le carte di lavoro comprendono tutta la documentazione di un intervento di audit, dalla fase di pianificazione al rapporto finale.

Le carte di lavoro devono essere:
- comprensibili: concise e chiare;
- rilevanti: per gli obiettivi dell'incarico;
- uniformi: stessa misura, organizzate in raccoglitori, ecc.;
- economiche: utilizzare una stessa carta di lavoro per più test, utilizzare lo stesso campione per più test, usare i documenti degli audit precedenti, non porre domande non necessarie;
- complete: non devono lasciare domande rilevanti prive di risposte;
- scritte in maniera semplice: evitare gerghi tecnici, inserire spiegazioni chiare;
- organizzate in maniera logica: organizzate in segmenti, con una spiegazione narrativa all'inizio di ogni segmento e una conclusione alla fine, che supporti l'opinione complessiva.

Sotto il profilo formale devono contenere:
- il riferimento all'intervento di audit, descrivere il contenuto o lo scopo della carta di lavoro;
- la firma o sigla dell'auditor che l'ha preparata e la data;
- un indice o un numero di riferimento;
- i simboli di verifica (tick mark) dovrebbero essere spiegati e mantenuti uniformi nel corso dell'intervento;
- le fonti dei dati dovrebbero essere chiaramente identificate.

Possono essere cartacee o in formato elettronico.

Al termine dell'intervento, le carte di lavoro vengono riviste e vengono conservate solo le versioni finali. Normalmente le carte di lavoro vengono conservate per 7 anni in un luogo sicuro con restrizione nell'accesso.

6.5 SUPERVISIONE DELL'INCARICO

Il RIA o un collaboratore da lui designato deve supervisionare i singoli interventi di audit.

Standard 2340 – Supervisione dell'incarico

Gli incarichi devono essere opportunamente supervisionati al fine di garantire che gli obiettivi siano 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 e dalla complessità dell'incarico. Il responsabile internal auditing ha la responsabilità generale di supervisionare l'incarico, sia esso svolto da o per conto dell'internal audit. Il responsabile internal auditing può delegare tale supervisione a membri dell'attività di internal audit di provata esperienza. Evidenza dell'avvenuta supervisione deve essere documentata e conservata.

La supervisione inizia nella fase di pianificazione e continua durante tutto l'intervento di audit. Il processo include:

- assicurare che gli auditors posseggano collettivamente le conoscenze, capacità e altre competenze richieste per svolgere l'incarico;
- fornire appropriate istruzioni durante la fase di pianificazione e approvare l'audit program;
- assicurare che l'audit program approvato sia completato a meno che cambiamenti non siano stati giustificati e autorizzati;
- assicurare che le carte di lavoro supportino adeguatamente le osservazioni, conclusioni e raccomandazioni;
- assicurare che le comunicazioni dell'intervento siano accurate, oggettive, chiare, concise, costruttive e tempestive;
- assicurare che siano raggiunti gli obiettivi dell'incarico;
- fornire opportunità per lo sviluppo delle conoscenze, capacità e altre competenze degli internal auditor.

Include inoltre:

- promuovere una relazione cooperativa tra il team di audit e il personale dell'area soggetta a audit;
- coordinare i lavori assegnati ai membri del team in modo da evitare duplicazione e da assicurare che tutti gli aspetti dell'audit program siano coperti (prevedendo, as esempio, degli incontri periodici del team di audit);
- rivedere le carte di lavoro per verificare che supportino adeguatmente le conclusioni e le raccomandazioni;
- condurre l'exit meeting con l'obiettivo di:
    - discutere conclusioni e raccomandazioni;
    - risolvere eventuali incomprensioni o differenze di interpretazione;
    - trovare un accordo su possibili soluzioni;
    - ringraziare i partecipanti per la collaborazione e le informazioni fornite;
- completare la valutazione dello staff del team di audit:
    - risultati di survey sull'efficacia dell'internal audit valutata dal cliente;
    - valutazioni dell'auditor incaricato dell'intervento;
    - valutazione annuale del RIA.

6.6 COMUNICAZIONE

La prima comunicazione con il cliente avviene durante il kick off meeting.

L'ambito e gli obiettivi degli interventi sono tipicamente comunicati:

- nella fase di pianificazione dell'incarico;

- nel corso dell'intervento, se vi sono deviazioni rispetto all'ambito e agli obiettivi pianificati dell'intervento;
- al termine dell'intervento.

Standard 2400 – Comunicazione dei Risultati

Gli internal auditor devono comunicare i risultati degli incarichi.

Standard 2410 – Modalità di comunicazione

La comunicazione deve includere gli obiettivi, l'ambito di copertura e i risultati dell'incarico.

2410.A1 *– La comunicazione finale dei risultati dell'incarico deve contenere le relative conclusioni e raccomandazioni e/o piani d'azione. Laddove appropriato, dovrebbe essere fornito il giudizio dell'internal auditor. Il giudizio deve tenere in considerazione le aspettative del senior management, del board e degli altri stakeholder e deve essere avvalorato da informazioni sufficienti, affidabili, pertinenti e utili.*

Interpretazione:
I giudizi espressi a livello di incarico possono consistere in 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 la loro rilevanza.

2410.A2 *– Nelle comunicazioni relative all'incarico, gli internal auditor sono incoraggiati a dare atto delle operazioni svolte in modo adeguato.*

2410.A3 *– In caso di invio a terze parti esterne all'organizzazione, la comunicazione dei risultati deve espressamente prevedere limiti di utilizzo e distribuzione.*

2410.C1 *– Le comunicazioni relative allo stato di avanzamento e ai risultati degli incarichi di consulenza possono variare, nella forma e nei contenuti, in funzione della natura dell'incarico e delle esigenze del cliente.*

Standard 2420 – Qualità della comunicazione

La comunicazione deve essere accurata, obiettiva, chiara, concisa, costruttiva, completa e tempestiva.

Interpretazione:

Una comunicazione accurata non presenta errori e distorsioni ed è fedele ai fatti rilevati. Una comunicazione obiettiva è corretta, imparziale e scevra da pregiudizi ed è il risultato di una valutazione bilanciata ed equilibrata di tutti i fatti e le circostanze rilevanti. Una comunicazione chiara ha senso logico ed è facilmente comprensibile, evita l'uso di termini tecnici non necessari e fornisce tutte le informazioni significative e pertinenti. 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 essenziali per i destinatari, nonché tutte le informazioni e le osservazioni significative atte ad avvalorare raccomandazioni e conclusioni. Una comunicazione tempestiva è puntuale e opportuna nei tempi, in funzione della significatività del problema, e consente al management di intraprendere opportune azioni correttive.

Il rapporto di internal audit deve contenere almeno i seguenti elementi:
- scopo;
- ambito di intervento;
- risultati.

Normalmente si sviluppa nelle seguenti sezioni:

- scopo;
- ambito di intervento: individua le attività auditate;
- metodi di audit: costituisce una sezione autonoma se sono utilizzate nuove metodologie o tecnnologie o se si utilizza il lavoro di altri organismi interni o esterni. Altrimenti questi aspetti sono trattati nella sezione riservata alle osservazioni;
- risultati: includono osservazioni, conclusioni, opinioni, raccomandazioni e piani di azione. Osservazioni minori possono essere collocate in una sezione separata;
- raccomandazioni: può costituire una sezione a parte se le raccomandazioni sono generali e non riferite alle singole osservazioni.

Le raccomandazioni devono aderire al principio SMART:

- S – specifiche: devono sottolineare esattamente quello che l'organizzazione dovrebbe ottenere;
- M – misurabili: si deve poter valutare se sono state implementate;
- A – orientate all'azione: devono essere specificate le azioni che l'organizzazione deve intraprendere;
- R – rilevanti: devono essere in linea con la natura dell'organizzazione ed essere raggiungibili;
- T – tempestive: devono specificare l'orizzonte temporale per la loro implementazione.

Prima dell'approvazione del rapporto, le osservazioni, le conclusioni e le raccomandazioni sono discusse con il management nel corso dell'Exit meeting con il cliente.
In questa occasione, vengono chiariti fraintendimenti e viene acquisito il punto di vista del cliente.

Alcuni suggerimenti in termini di "soft skills" per la redazione del rapporto:
- assumere che l'auditor e il cliente siano dalla stessa parte e ricerchino le vie migliori per raggiungere gli obiettivi dell'organizzazione;
- iniziare a livello generale mostrando di aver compreso la natura e lo scopo dell'operazione;
- inserire per primi i finding positivi;
- presentare i rilievi come opportunità di miglioramento;
- enfatizzare gli effetti dei finding;
- concludere: riassumere i risultati brevemente con enfasi sull'azioni che il cliente può porre in atto. Concludere con una nota positiva.

Il rapporto deve essere rivisto e approvato dal RIA o da un collaboratore da lui designato.

Standard 2440 – Divulgazione dei risultati

Il responsabile internal auditing deve comunicare i risultati agli opportuni destinatari.

Interpretazione:

Il responsabile internal auditing è tenuto a verificare e approvare la comunicazione finale dei risultati dell'incarico prima dell'emissione degli stessi e a determinare la lista dei destinatari e le modalità della divulgazione. Laddove il responsabile internal auditing deleghi queste funzioni, ne rimarrà in ogni caso pienamente responsabile.

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

***2440.A2** – Se non diversamente prescritto da requisiti di legge o normativi, 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 ha la responsabilità di comunicare i risultati finali degli incarichi di consulenza ai clienti.*

***2440.C2** – Nel corso degli 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.*

La comunicazione può anche essere diretta al Consiglio, ai revisori esterni o ad altri soggetti interessati o coinvolti.

Il RIA può distribuire solo il riassunto generale del rapporto di internal audit al senior management e al Consiglio, che è più interessato ai risultati che non agli aspetti metodologici. Sono ipotizzabili anche riassunti multi-report che riassumono i risultati di più interventi di audit.

6.7 MONITORAGGIO DEI RISULTATI DELL'INTERVENTO

Standard 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.*

Può essere opportuno un vero e proprio intervento di follow up. Per raccomandazioni meno critiche, può essere sufficiente un questionario o una conversazione di follow up.

I risultati dell'attività di follow up confluiscono nei report trimenstrali sull'attività di internal audit diretti al senior management e al Consiglio. I report possono evedenziare la necessità di continuare nel monitoraggio (in quanto le raccomandazioni non sono state pienamente implementate o sono state implementate in una maniera non corretta o perché la raccomandazione non ha risulto il problema osservato) oppure la possibilità di interrompere il monitoraggio in quanto il problema è stato risolto. Il monitoraggio può essere interrotto quando la raccomandazione è implementata con successo.

Un'osservazione che rappresenta un rischio significativo per l'organizzazione richiede una risposta del management pronta e efficace. Se il RIA ritiene che il management non stia rispondendo o stia rispondendo in modo inadeguato a fronte del rischio osservato e non dimostri intenzione di assoggettare il rischio a controllo, allora il RIA è professionalmente obbligato a riportare la questione al senior management e, se questo non risponde, al Consiglio.

7 MANTENERE UN EFFICACE SISTEMA DI QA&IP – QUALITY ASSURANCE & IMPROVEMENT PROGRAM

Standard 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.

Standard 1311 – Valutazioni interne

Le valutazioni interne devono includere:

- *il monitoraggio continuo della prestazione dell'attività di internal audit;*
- *periodiche auto-valutazioni o valutazioni condotte da altre persone interne all'organizzazione che abbiano conoscenze adeguate della pratica professionale 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 considerati necessari per valutare la conformità al Codice Etico e agli Standard.
Le valutazioni periodiche sono effettuate con l'obiettivo di valutare la conformità al Codice Etico e agli Standard. L'adeguata conoscenza delle metodologie di internal audit presuppone perlomeno l'adeguata comprensione di tutti gli elementi dell'International Professional Practices Framework.

Standard 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 potenziali conflitti di interessi.*

Interpretazione:

Le valutazioni esterne possono essere effettuate con una valutazione interamente esterna oppure tramite un'autovalutazione con convalida esterna indipendente. Il valutatore esterno deve esprimere le proprie conclusioni in merito alla conformità al Codice Etico e agli Standard; la valutazione esterna può altresì comprendere osservazioni operative o strategiche.

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. Per quanto attiene ai 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 il proprio 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. Il responsabile internal auditing dovrebbe adoperarsi affinché il board supervisioni la valutazione esterna allo scopo di ridurre i conflitti di interessi percepiti o potenziali.

Standard 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. La comunicazione dovrebbero comprendere:

- *l'ambito e la frequenza delle valutazioni interne ed esterne;*
- *le qualifiche e l'indipendenza del(i) valutatore(i) o del team di valutatori, inclusa l'esistenza di potenziali conflitti di interessi;*
- *le conclusioni dei valutatori;*
- *le azioni correttive.*

Interpretazione:

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

Standard 1321 - Uso della dizione "Conforme agli Standard Internazionali per la pratica professionale dell'internal auditing"

È consentito indicare che l'attività di internal audit risulta conforme agli Standard internazionali per la pratica professionale dell'internal auditing unicamente se i risultati del programma di assurance e miglioramento della qualità avvalorano tale affermazione.

Interpretazione:

L'attività di internal audit risulta conforme al Codice Etico e agli Standard quando raggiunge i risultati in essi descritti. 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. Le strutture di internal audit che operano da almeno cinque anni devono essere oggetto anche di valutazioni esterne.

Standard 1322 – Comunicazione di non conformità

In presenza di non conformità al Codice Etico o agli Standard che influiscano 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.

Anche un ufficio di internal audit che ricorre ad un out-sourcing completo richiede un QA&IP.
Le valutazioni interne continuative sono pratiche messe in atto dal RIA per svolgere valutazioni di routine delle pratiche e delle direttive nello svolgimento dei singoli interventi di audit. Le conclusioni dovrebbero essere sviluppate mano a mano in via continuativa, e dovrebbero essere intraprese azioni appropriate per migliorare la qualità delle attività in corso.
Le valutazioni interne periodiche sono di tipo self-assessment. Molte organizzazioni utilizzano questo tipo di analisi per autovalutarsi in vista di una valutazione della qualità esterna.
I soggetti che svolgono valutazioni interne continuative o periodiche dovrebbero far capo al RIA nella fase di valutazione e dovrebbero poi rendicontare i risultati direttamente al RIA.

La valutazione esterna della qualità può essere svolta da:

- un team totalmente indipendente dall'organizzazione;
- autovalutazione con validazione indipendente di un certificatore indipendente;
- team di peer review composto da membri di almeno tre differenti organizzazioni.

8 CERTIFICAZIONI PROFESSIONALI

Si riportano di seguito i principali tipi di certificazione:

CERTIFIED INTERNAL AUDITOR	CERTIFICATION IN CONTROL SELF-ASSESSMENT
CERTIFIED FINANCIAL SERVICES AUDITOR	CERTIFICATION IN RISK MANAGEMENT ASSURANCE

Le certificazioni conferiscono dei «patentini» internazionali che rappresentano, per la professione di internal auditor, un simbolo di eccellenza riconosciuto in tutto il mondo.
L'AIIA è l'unica istituzione italiana autorizzata a rilasciare, attraverso l'IIA, le certificazioni.

I requisiti per la certificazione CIA (la più diffusa) sono:

- formazione: il candidato deve aver conseguito un titolo universitario, almeno triennale, in qualunque disciplina, o un titolo a esso equivalente, rilasciato da un istituto di livello universitario riconosciuto. (vi sono però delle eccezioni …);
- esperienze professionali: il candidato deve aver maturato un'esperienza di due anni nell'internal auditing o in un'attività correlata. Per attività correlata si intende l'esperienza di lavoro in discipline di auditing/valutazione, come Revisione Esterna, Certificazione della Qualità, Ispettorato, Compliance o Controllo interno. Una laurea di almeno 4 anni anziché 3, o un'esperienza di lavoro in attività professionali collegate (ad es., contabilità, legge o finanza) possono avere la validità di un anno di esperienza in Internal Auditing;
- Referenze personali: il candidato deve sottoscrivere il codice etico dell'IIA e presentare un documento (modulo) contenente le referenze personali di un suo referente.

Gli studenti universitari possono accedere al programma di certificazione ed iniziare a sostenere gli esami. L'attestato di Certificazione verrà però rilasciato solo dopo il conseguimento della laurea e dopo aver maturato l'esperienza professionale richiesta.

La certificazione CIA è organizzata su tre moduli d'esame:

- CIA I;
- CIA II;
- CIA III.

Il candidato è libero di scegliere l'ordine in cui sostenere le parti d'esame. Il mancato superamento di una parte non comporta l'impossibilità di sostenere la successiva.

Per accedere al percorso di certificazione, è necessario inviare ad AIIA la modulistica necessaria per la verifica dei requisiti. Quindi, è necessario iscriversi online all'esame.
Per ogni domanda di iscrizione online, dopo circa 20 gg, il candidato riceve, via email, una lettera di autorizzazione.
A partire dalla data di autorizzazione dell'IIA (ca. 10 gg prima della ricezione della stessa da parte del candidato) decorrono i 180 gg di tempo a disposizione del candidato per sostenere l'esame.
E' possibile ottenere una proroga di 30, 60 o 90 gg del periodo utile per il sostenimento dell'esame.

La certificazione deve essere conseguita entro un arco temporale di 4 anni dal momento della prima autorizzazione. Scaduto tale termine, le parti d'esame già superate sono considerate perse e dunque da ripetere.

Al fine del mantenimento della certificazione, il candidato dovrà dimostrare, a partire dal terzo anno di conseguimento della certificazione, di seguire costantemente iniziative di aggiornamento professionale (tra le quali, ad esempio, i corsi ed eventi AIIA…), presentando all'IIA, secondo le modalità descritte nel Programma CPE, i crediti necessari.
Al fine di mantenere lo status di "certificato", è necessario che il professionista segua costantemente corsi di approfondimento e aggiornamento.
La partecipazione a iniziative di audit, ove segnalato, dà diritto a tanti punti CPE quante sono le ore della durata dell'incontro e dell'effettiva presenza del professionista.
La presentazione dei punti CPE avviene tramite la compilazione di un modulo di autocertificazione, a partire dal terzo anno di conseguimento della certificazione.
La documentazione a supporto dell'ottenimento dei punti CPE, deve essere conservata per almeno tre anni in quanto l'IIA si riserva il diritto di effettuare controlli a campione.
In caso di inadempienza, il certificato viene automaticamente considerato "inattivo" e non potrà più avvalersi di tale qualifica.

È "praticante" il CIA che opera con continuità come internal auditor.

È "non praticante" il CIA che NON opera con continuità come internal auditor: può usare la designazione di CIA ma non praticare la professione. Gode di requisiti CPE ridotti.

I CPE richiesti per mantenere la certificazione CIA sono:
- 40 ore all'anno (se praticante);
- 20 ore all'anno (se non praticante).

Le attività che danno diritto alle ore CPE sono suddivise nelle seguenti aree tematiche:
- formazione;
- pubblicazioni;
- traduzioni;
- presentazioni;
- partecipazioni a meeting specifici;
- external quality assessment.