La figura professionale dell'*Internal Auditor* (IA) e le fasi della sua attività

6

di Alberto Oliva, Patrizia Riva

SOMMARIO

6.1 Il sistema di controllo interno e la funzione di *Internal Audit*

Il sistema di controllo interno (SCI) e di gestione dei rischi (nella versione più attuale e completa quindi SCI-GR) è costituito dall'insieme delle regole, delle procedure e delle strutture organizzative volte a consentire l'identificazione, la misurazione, la gestione e il monitoraggio dei principali rischi aziendali.

Come per ogni fenomeno umano, il significato e l'ampiezza del concetto di controllo varia in relazione all'ambiente di riferimento ed è frutto di uno sviluppo storico legato al più complesso ambito della storia economica. Nella dottrina economico-aziendale italiana fino ai primi del Novecento l'idea di controllo è intesa come verifica, ossia come un'azione volta a individuare e reprimere comportamenti illeciti negativi per la produzione e la difesa della ricchezza dell'imprenditore. Nel 1922 Fabio Besta, con la sua opera "La Ragioneria"[1], estende questo concetto introducendo il controllo sia come attività ispettiva sia come elemento determinante per raggiungere gli obiettivi aziendali. Il controllo non è più solo un deterrente per evitare perdite ma diventa in parte elemento che contribuisce a guidare le scelte aziendali.

Quale elemento di guida dell'azienda verso il raggiungimento dei propri obiettivi, esso viene sviluppato in particolare da Robert Anthony a partire dagli anni Sessanta[2]. L'autore, partecipe della scuola di Harvard, ebbe un ruolo prioritario nella definizione degli elementi di un modello di riferimento. Tra questi, prioritario il concetto di approccio sistemico ossia l'equilibrio complessivo che si crea fra le singole parti che lo costituiscono nella consapevolezza che l'insieme è un qualcosa di diverso della mera somma delle parti.[3] Secondo la schematizzazione dell'autore, il controllo segue il flusso del top-down, che parte dagli obiettivi strategici pianificati per poi scomporli in sotto-obiettivi.

Tali lavori vengono in seguito arricchiti dai contributi forniti dagli approcci comportamentalistici (Hopwood)[4] e strategici (Mintzberg)[5]: il primo di

[1] F. Besta, *La ragioneria*, Milano, Vallardi, Vol. I., 1922.

[2] N.R. Anthony, *Planning and Control Systems: A Framework for Analysis*, Division of Research, Graduate School of Business Administration, Harvard University, Boston, 1965.

[3] La prima definizione di "sistema" come elemento astratto generale con proprie caratteristiche e dignità di analisi è dovuta agli studi di Ludwig von Bertalanffy nella sua opera "Teoria generale dei sistemi". L. von Bertalanffy, *General System Theory*, George Braziller, New York, 1968.

[4] G. A. Hopwood, *Accounting and Human Behaviour*, Englewood Cliffs, Prentice Hall Inc., 1976. In questo lavoro si evidenzia come l'informazione derivante dalla analisi contabile possa influenzare il comportamento degli individui su un duplice piano: da una parte il comportamento degli individui sarà influenzato dalla conoscenza del dato e dall'altra chi produce il dato sarà influenzato dal risultato che vorrà avere sul comportamento di chi ne è destinatario.

[5] Tra questi il più significativo è il lavoro di H. Mintzberg, *La progettazione dell'organizzazione aziendale*, Il Mulino, Bologna, 1996.

questi approcci mette in discussione l'eccessiva razionalità e meccanicità del modello cibernetico della scuola di Harvard e si sposta sul riconoscimento dell'elemento comportamentale come agente determinante dell'efficacia dei sistemi di controllo; il secondo approccio, quello strategico, sviluppa la funzione di indirizzo del controllo volto ad una più efficace attività di governo strategico dell'impresa.

6.1.1 Il CoSO (Committee of Sponsoring Organizations) Report

Il flusso di studi normativo-descrittivi, qui presentati solo in sintesi estrema, si scontrarono duramente con la realtà economica a partire dalla metà degli anni Ottanta a seguito della presenza nel mercato statunitense di importanti procedure fallimentari ad alto impatto sul sistema economico. Ciò fece emergere, anche a livello della opinione pubblica, la presenza di inefficienze nei controlli interni così come erano allora strutturati. La *National Commission on Fraudolent Financial Reporting*, nota anche come *Treadway Commission*, propose una nuova chiave di lettura del sistema dei controlli interni in grado di far emergere i difetti discendenti dalla visione fino ad allora utilizzata. La *Treadway Commission* diede successivamente vita a un apposito sottogruppo di lavoro, denominato *Committee of Sponsoring Organizations of the Treadway Commission* (***CoSO***) con la collaborazione di Coopers & Lybrand (oggi PricewaterhouseCoopers) avente il compito di realizzare uno studio sulla dottrina esistente in tema di controlli interni, in vista della definizione di un modello di riferimento innovativo e utile per il management aziendale.

Il risultato dello studio, pubblicato nel 1992 e **denominato CoSO (Committee of Sponsoring Organizations) Report**, rappresenta tutt'ora il modello di riferimento per il controllo interno utilizzato sia dai codici di autodisciplina, sia dalla normativa nazionale ed internazionale in materia di *Corporate Governance*. A titolo di esempio, il modello di riferimento definito dal Comitato di Basilea per il sistema di controllo interno nelle banche è basato sugli stessi componenti definiti nel *CoSO Report*, mentre il Codice di Corporate Governance per le società quotate in Borsa riprende esplicitamente, riassumendola, la definizione di sistema di controllo e le caratteristiche del controllo interno evidenziate nel *CoSO Report*.

Secondo questo modello il controllo interno è costituito generalmente da cinque componenti:

1. l'ambiente di controllo (**Control Environment**), che si riferisce essenzialmente ai valori etici e alla filosofia di gestione del *management*, inclusa l'assegnazione di ruoli e responsabilità. Fa riferimento al contesto organizzativo nel quale si effettuano i controlli finalizzati al raggiungimento degli obiettivi;
2. il processo per la valutazione del rischio (**Risk Assessment**) adottato

dall'impresa finalizzato a identificare e rispondere ai rischi connessi alle attività ed ai risultati che ne conseguono. L'incremento del valore economico di un'impresa per gli azionisti deriva soprattutto dalla capacità di individuare e valutare i rischi, unitamente a un adeguato SCI. Dal punto di vista operativo è necessario:

a) identificare e valutare i rischi, in conformità agli obiettivi di business definiti per l'azienda nel suo complesso e per le singole aree di attività (c.d. *Risk assestment*);
b) gestire i rischi in ottica strategica, producendo un idoneo flusso informativo di specifici indicatori di rischio per diversi livelli di management;
c) monitorare i rischi con un adeguato e tempestivo sistema di reporting da indirizzare a tutti i livelli di management. Nei fatti il modello descrive una realtà dotata di sensori in grado di comprendere e segnalare le opportunità e – soprattutto – le minacce.

3. le attività di controllo (**Control Activities**), costituite dall'insieme delle politiche e delle procedure che garantiscono che le direttive del management siano eseguite. Esse si estendono all'intera organizzazione aziendale e si attuano a tutti i suoi livelli, con l'obiettivo primario di adottare i provvedimenti necessari a fronteggiare i rischi che potrebbero pregiudicare la realizzazione degli obiettivi aziendali;
4. il sistema informativo (**Information & Communication**), rilevante per l'informativa economico finanziaria e per la comunicazione. Un sistema di controllo IT (Information Technology) è adeguato se:
   – vi è sufficiente protezione fisica dei dati (compresi gli aspetti legati ai rischi geografici) e logica all'accesso non autorizzato al sistema;
   – vi sono adeguate misure che garantiscono che il sistema sia operativo e funzionante nei tempi e nelle modalità richieste dai processi aziendali, fondamentale in questo senso la continuità nella disponibilità delle informazioni;
   – vi sono corrette metodologie di sviluppo e di manutenzione dei sistemi applicativi che assicurino che le funzioni di elaborazione di questi ultimi siano sempre quelle attese dagli utenti;
5. il monitoraggio dei controlli (**Monitoring Activities**): al fine di valutare la qualità del funzionamento del controllo interno nel tempo e l'adeguatezza alla specifica organizzazione, è necessario monitorare i sistemi di controllo mediante verifiche periodiche e continuative insieme alle opportune azioni di follow up.

6.1.2 L'Enterprise Risk Management (ERM) Framework

L'inclusione del concetto di rischio in queste analisi diventa quantomai necessario considerando che il rischio è un elemento che caratterizza ogni

attività imprenditoriale e che, qualora non esplicitato e affrontato in modo consapevole e dinamico, potrebbe aumentare le probabilità di crisi.

Per focalizzare il concetto di rischio e declinarlo a livello dell'intera operatività aziendale nel 2004 il **Committee of Sponsoring Organizations of the Treadway Commission** ha pubblicato un modello di riferimento, l'**Enterprise Risk Management (ERM) Framework**. Di fatto l'**ERM** rappresenta un'evoluzione, per incorporazione, del **CoSO Report**.

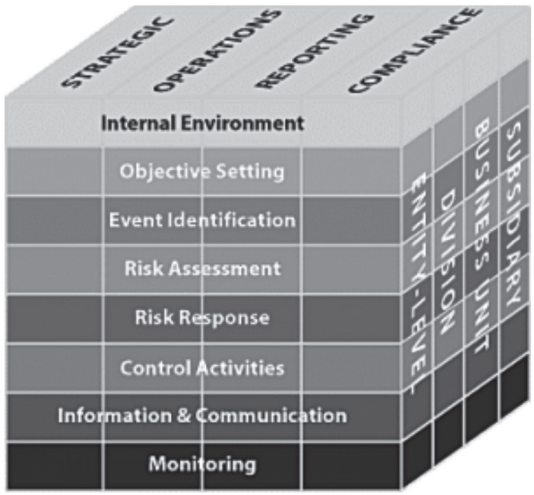
L'**ERM** è quindi:

i. un processo continuo che coinvolge tutta l'organizzazione e si concretizza in una sequenza di attività che devono essere pervasive e integrate nell'ambito del sistema di *management* esistente, allo scopo di evitare l'aggiunta di procedure parallele che comporterebbero costi ulteriori;
ii. svolto da persone che a tutti i livelli della struttura organizzativa aziendale occupano posizioni che influenzano l'efficacia del processo e che a loro volta ne sono condizionate.

L'*Enterprise Risk Management* è costituito da otto componenti interconnesse e non sequenziali che derivano dal modo (soggettivo) in cui il *management* gestisce l'azienda e che sono integrate con i processi operativi. Come per il *CoSO Report*, anche l'*ERM* è solitamente rappresentato graficamente con la figura cubica riportata di seguito.

Vale la pena evidenziare che il modello *ERM* di gestione del rischio aziendale si differenzia dal *CoSO Report* in quanto incorpora il controllo interno fornendo al management uno strumento più completo; nello specifico:

Figura 6.1 – L'Enterprise Risk Management



– l'*ERM* è utilizzato per identificare e gestire i rischi che circondano e minacciano un'organizzazione;
– il *CoSO Report* è utilizzato per comprendere e gestire i controlli interni quale parte integrante dell'operatività aziendale.

La rappresentazione grafica del sistema *ERM* può ulteriormente aiutare a chiarire questo concetto, in quanto consente di analizzare le componenti che costituiscono il processo di *risk management* scorporandole da quelle, invece, caratteristiche anche dei sistemi di controllo che rivestono un ruolo di supporto nell'ambito del contesto.

L'*ERM* è alimentato dal processo di pianificazione strategica, che definisce la missione e gli obiettivi aziendali e trova supporto nel processo di gestione dei rischi e nell'ambiente interno, nelle attività di controllo, nei sistemi di informazione e comunicazione e nelle attività di monitoraggio continuo sull'adeguatezza del sistema.

In questo schema, il processo di *risk management* si articola in tre fasi:
a. identificazione degli eventi,
b. valutazione del rischio,
c. risposta al rischio.

Nel caso in cui quest'ultima sia orientata a evitare o a ridurre il rischio, occorrerà valutare l'adeguatezza e l'efficacia del Sistema di Controllo Interno, che deve fornire ragionevole sicurezza sul raggiungimento degli obiettivi aziendali.

6.1.3 Analisi comparata del CoSO Report e dell'ERM

L'analisi comparata del *CoSO Report* e dell'*ERM*, porta a identificare una serie di differenze.

1) Una prima differenza risulta relativa agli obiettivi di *reporting* perseguiti dal Sistema di Controllo Interno:
   – il *CoSO* si focalizza sull'affidabilità della reportistica economico-finanziaria;
   – l'*ERM* fa riferimento a tutte le informazioni gestionali e finanziarie diffuse sia internamente sia esternamente all'impresa.

2) Una seconda distinzione è relativa all'introduzione nel modello *ERM* della categoria degli "obiettivi strategici", tra cui sono da ricomprendersi obiettivi operativi, di bilancio e di conformità.

3) Un terzo elemento di distinzione è relativo alla valutazione dei rischi: entrambi i modelli evidenziano la necessità di valutare i rischi in modo strutturato, ma l'*ERM* introduce concetti importanti nell'attività di assun-

zione dei rischi, riconoscendo anche quelli con un impatto positivo che rappresentano quindi un elemento di opportunità che l'organizzazione può gestire e volgere a proprio vantaggio. In sostanza il concetto è esprimibile mediante la differenza tra:
- *rischio inerente*, ovvero il rischio esistente in assenza di azioni da parte del *management* tese a limitarne gli effetti; e
- *rischio residuo*, ovvero il rischio che rimane dopo che sono state effettivamente implementate azioni del *management* tese alla mitigazione del rischio inerente.

Tali concetti verranno esaminati anche nel seguito di questa trattazione.

È utile richiamare le quattro tipologie di azioni identificate nell'ERM framework che il management può decidere di attuare nei confronti del rischio:

i. evitarlo, eliminando un prodotto o un'attività;
ii. ridurlo, implementando azioni capaci di ridurre l'incidenza di probabilità o impatto;
iii. condividerlo, attuando azioni di trasferimento del rischio quali le polizze assicurative;
iv. accettarlo, decidendo di non intraprendere alcuna misura di contenimento.

4) Con riferimento al sistema informativo, l'ERM amplia i concetti espressi dal CoSO Report evidenziando la necessità di raccolta e diffusione anche dei dati previsionali, fondamentali anche per monitorare adeguatamente l'insorgenza di situazioni di squilibrio che possono generare incertezza sul presupposto della continuità aziendale.

5) Un'ultima differenza che assume rilevanza è relativa all'impostazione di fondo del sistema:
- nel CoSO il controllo e la massimizzazione della sua efficacia rappresentano l'obiettivo a cui tendere e la valutazione del rischio lo strumento per raggiungerlo;
- nell'ERM il controllo diventa lo strumento da utilizzare per garantire l'obiettivo ultimo, ovvero contenere il rischio nei limiti dell'accettabilità e della tolleranza definite, tenendo conto della propensione al rischio.

6.1.4 La definizione di Sistema di Controllo Interno (SCI) e il ruolo dell'*Internal Auditor* (IA) nel Codice di Corporate Governance

Nel panorama italiano, un autorevole ambito di trattazione delle caratteristiche fondanti del Sistema di Controllo Interno *(SCI)* è rappresentato dal Codice di Corporate Governance (delle società quotate) che all'art. 6 contiene le indicazioni per le buone prassi di governo di impresa, condivise

anche a livello internazionale[6]. Non a caso in questo articolo denominato "Sistema di controllo interno e di gestione dei rischi" si tratta anche della figura e dei compiti dell'*Internal Auditor (IA)*. Ci troviamo pertanto di fronte ad un *benchmark* di riferimento, che opportunamente declinato, può essere utilmente considerato anche per le imprese di minori dimensioni.

Secondo la Raccomandazione 32 il sistema di controllo interno e di gestione dei rischi coinvolge una molteplicità di attori, evidenziandone cosi la pervasività. Come anticipato in un precedente capitolo, questi attori sono costituiti da un elemento principale rappresentato dall'Organo di Amministrazione, il quale ha interesse a basare le proprie decisioni su dati robusti, il Chief Executive Officer, incaricato dell'istituzione e del mantenimento del sistema di controllo interno e di gestione dei rischi ed un Comitato controllo e rischi (ove presente) formato da amministratori indipendenti (*AI*) e non esecutivi con il compito di supportare, con un'adeguata attività istruttoria, le valutazioni e le decisioni del Consiglio di Amministrazione relative al sistema. È prevista poi la presenza di un Responsabile della funzione di *Internal Audit* (*IA*), che opera in *staff* al Consiglio di Amministrazione ed è incaricato di verificare che il *SCI* sia funzionante, adeguato e che la contabilità sia completa e attendibile e di eventuali altri ruoli e funzioni aziendali con specifici compiti in tema di controllo interno e gestione dei rischi, articolati in relazione a dimensioni, complessità e profilo di rischio dell'impresa (ad esempio *Risk manager* e *Compliance officer*), oltre ovviamente al Collegio Sindacale, che vigila sulla adeguatezza degli assetti organizzativi e quindi sull'efficacia del *SCI* interfacciandosi con il Consiglio di Amministrazione e con l'*Internal Auditor.*

In sostanza il Sistema di Controllo Interno (*SCI*) è un processo attuato dal Consiglio di Amministrazione, dai dirigenti e da altri soggetti della struttura aziendale finalizzato a fornire una ragionevole sicurezza sul conseguimento degli obiettivi rientranti nelle seguenti categorie:
– efficacia ed efficienza delle attività operative;
– attendibilità delle informazioni di bilancio;
– conformità alle leggi e ai regolamenti in vigore.

Un'efficace *corporate governance* si basa sull'integrazione dei sistemi di gestione dei rischi e di controllo interno.

In questo panorama, talvolta complesso e affollato, emerge l'importanza di una chiara definizione dei tre livelli di controllo in cui si articola il *SCI*,

[6] Borsa Italiana, Codice di Corporate Governance – Comitato per la Corporate Governance, edizione gennaio 2020.

in sostanza, come è stato detto, per passare dalla mera "sommatoria dei controlli" ad un "sistema olistico di controllo[7]":

1. il primo livello definisce e gestisce i controlli cosiddetti di linea insiti nei processi operativi (ad esempio il *back office* e in parte lo stesso responsabile del reparto/ufficio);
2. il secondo livello presidia il processo di gestione e controllo dei rischi garantendone la coerenza rispetto agli obiettivi aziendali e rispondendo a criteri di segregazione organizzativa in modo sufficiente per consentire un efficace monitoraggio (es. *Compliance*, *Risk manager*, Dirigente Preposto, Responsabile qualità, Responsabile funzione antiriciclaggio, ecc.);
3. il terzo livello fornisce un'*assurance* indipendente sul disegno e sul funzionamento del complessivo Sistema di Controllo Interno (*Internal Audit*).

Se da una parte si deve quindi progettare un SCI che eviti l'*overlapping* dei controlli – per l'esame del quale si rinvia infra al Capitolo 11 – è necessario, dall'altra, che si definiscano correttamente la dimensione e l'ampiezza dello stesso. Abbiamo visto che nel complesso sistema del controllo interno (o revisione interna, temine in uso nella normativa e regolamentazione dei soggetti vigilati finanziari) il ruolo affidato all'*Internal Audit* (IA) è collocato al cosiddetto terzo livello[8]. Il citato Codice di Corporate Governance per le società quotate in Borsa attribuisce esplicitamente alla funzione di *Internal Audit* (IA) una posizione centrale tra le funzioni aziendali coinvolte nel governo del sistema dei controlli. Ulteriormente "alla funzione di *Internal Audit* viene riconosciuta una spiccata indipendenza, che si esplica sia con l'attribuzione di autonomi poteri di iniziativa nella predisposizione del piano di Audit e nell'attivazione dei singoli interventi, sia con le modalità stabilite per la nomina, revoca e remunerazione del suo responsabile. I poteri riservati al Consiglio di Amministrazione in questa materia denotano l'esistenza di un vero e proprio rapporto gerarchico nei confronti del responsabile della

[7] L'aggettivo "olistico" deriva dal greco "olos" cioè "tutto, intero, totale" e si riferisce alla teoria dell'olismo, paradigma filosofico secondo cui le proprietà di un dato sistema non possono essere determinate dalla somma delle sue componenti, bensì è il sistema in generale che determina il comportamento delle parti. In altre parole il tutto non è riducibile alla somma delle parti di cui è composto, poiché il tutto è più (o comunque qualcosa di diverso) della somma di queste.

[8] Dato l'alto rischio di impatto delle crisi aziendali degli enti finanziari, anche in termini di possibili contagi ad altri settori economici, la sensibilità alla strutturazione di un robusto SCI in questi enti è molto più evidente e maggiormente storicizzato rispetto ad altri settori. Gli schemi più complessi, frutto anche di una normativa, sia comunitaria (i.e. MiFID), che nazionale (i.e. TUB), che regolamentare (ampissima in tal senso la produzione regolamentare a vari livelli di Banca d'Italia), si trovano appunto in tale ambito.

funzione di *Internal Audit*. In ogni caso, è necessario che le decisioni sulle materie di cui sopra siano assunte con il parere favorevole del comitato controllo e rischi (o, in alternativa, limitatamente alle proposte relative al trattamento economico, del comitato per la remunerazione) e sentito il Collegio Sindacale"[9]. Il posizionamento gerarchico considerato più corretto nella migliore pratica è quello alle dipendenze del Consiglio di Amministrazione ed in stretto contatto, anche operativo, con il Comitato Controllo e Rischi e con il Collegio Sindacale[10]. Queste indicazioni, sono valide anche per le società non quotate o di minori dimensioni in cui sempre più spesso si assiste all'introduzione della figura dell'*Internal Auditor*, seppure, secondo le specifiche esigenze e risorse aziendali, con mansioni alquanto variabili.

6.1.5 Le origini della professione di *Internal Auditor* (IA)

Come vedremo nel successivo paragrafo, l'*auditing* ha assunto in Italia un grande peso solo negli ultimi vent'anni, ma è importante evidenziare che non si tratta di una professione solo contemporanea. L'*auditing*, nelle sue forme primordiali, esisteva fin dall'inizio della civiltà umana. Già nel 4000 a.C., gli storici ritengono che i primi sistemi formali di conservazione della documentazione fossero stati istituiti da imprese e governi mediorientali per dissipare le loro preoccupazioni sulla corretta contabilizzazione delle entrate e delle uscite e sulla riscossione delle imposte. Sistemi similari furono attivati durante la dinastia Zhao in Cina (1122 – 256 a.C.). Durante il regno di Calif Omar bin Al Khattab (VII secolo d.C.) si implementò una attività di controllo interno nelle città che erano sotto il suo dominio per evitare il rischio che i funzionari di alto grado potessero utilizzare la loro posizione per ottenere ingiusti benefici.

In seguito tutte forme di governo si sono concentrate, tra gli altri obiettivi, sulla riduzione degli errori contabili e sull'accuratezza dei dati. Pertanto, nel corso dei secoli, il concetto di controllo ha iniziato a svilupparsi a fianco della evoluzione delle stesse pratiche contabili.

Il concetto di *auditing interno* ha iniziato ad acquisire importanza all'inizio del XX secolo, quando le attività commerciali cominciarono a crescere in termini di dimensioni e portata, e si avvertì l'esigenza di una funzione aziendale che fosse in grado di sorvegliare la produzione di documenti contabili per il processo decisionale. Ovviamente queste esigenze erano maggiormente

[9] Codice di Corporate Governance – *op. cit.*, pag. 18.

[10] Si rimanda al Capitolo 4 per approfondimenti in merito alla relazioni fra *Internal audit* e Consiglio di Amministrazione e i suoi Comitati.

manifeste laddove le dimensioni economiche erano più consistenti ed avanzate ossia gli Stati Uniti. L'anno 1941 segnò un importante punto di svolta. Victor Z. Brink diede alle stampe il primo vero libro sull'*Auditing Interno*[11]. Allo stesso tempo, John B. Thurston, *Internal Auditor* della *North American Company di New York*, e il suo ex collega Robert B. Milne stavano pensando di creare un'organizzazione che si occupasse proprio delle attività e delle problematiche dell'*Internal Audit*. Quando il libro di Brink giunse all'attenzione di Thurston, i tre si riunirono e decisero di avviare una collaborazione basata sui coincidenti interessi professionali. Il comitato organizzatore contattò un piccolo gruppo di professionisti dell'*Audit* interno in tutti gli Stati Uniti. Il certificato di costituzione del **"The Institute of Internal Auditors"**, in sigla **IIA**, fu depositato il 17 novembre **1941**. Ciononostante, nei primi anni successivi all'istituzione dell'*IIA*, l'*Audit* interno era ancora percepito come un'estensione strettamente correlata al lavoro dei revisori esterni: essi venivano spesso consultati per assistere revisori esterni nelle revisioni di bilanci o nelle funzioni relative allo svolgimento di attività connesse, come ad esempio le riconciliazioni bancarie[12].

Nel **1978**, l'*IIA* approvò gli **Standard per la pratica professionale di *Internal Auditing***. Gli *Standard*, norme professionali di organizzazione, svolgimento e comunicazione del lavoro di *Audit* interno, erano il frutto delle pionieristiche attività di revisione che venivano ora messe a sistema, coordinate e assunte come riferimento professionale. Da quel momento la professione di *Internal Auditor* (*IA*) assunse una dimensione completa il cui divenire e il cui affinarsi è frutto di una incessante attività di sintesi delle migliori esperienze internazionali in settori sempre più estesi ed è sempre più diffusa.

6.2 L'evoluzione dell'*Internal Audit* in Italia e l'inquadramento normativo e regolamentare

In Italia opera l'**AIIA**, **Associazione Italiana Internal Auditors** – associazione senza fini di lucro, costituita nel 1972 come affiliazione italiana dell'**IIA** – per migliorare i sistemi di governo, gestione del rischio e controllo delle organizzazioni mediante la valorizzazione della funzione di *Internal Audit*, che conta circa 4.000 professionisti associati in rappresentanza di oltre 900 tra gruppi e imprese. Nonostante la data di fondazione dell'AIIA, associazione di categoria italiana, risalga al 1972, il processo di diffusione

[11] Z. V. Brink, *Internal Auditing*, New York, Ronald Press, 1941.

[12] S. Ramamoorti, *Chapter 1.Internal Auditing: History, Evolution, and Prospects*, in Andrew Bailey; A. Gramling, S. Ramamoorti, *Research Opportunities in Internal Auditing*, Altamonte Springs, The Institute of *Internal Auditors* Research Foundation, 2003, pagg. 2-23.

dell'*Internal Auditing* in Italia inizia effettivamente solo a partire dagli anni '90. Emblematica è stata ad esempio, a partire dalla seconda metà di quel decennio, la trasformazione delle funzioni bancarie precedentemente esistenti, denominate sovente "ispettorato", in funzioni di "*Internal Audit*" (poi diventate "revisione interna"). Tale mutamento riflette l'evoluzione, anche concettuale, degli scopi della attività di *Audit* il cui raggio d'azione si è spostato da verifiche circoscritte agli aspetti di conformità normativa e procedurale ad attività di maggiore ampiezza e valore aggiunto nell'ambito dell'*assurance* e della consulenza in merito al controllo sistemico, alla gestione dei rischi ed alla corporate governance. In sostanza un processo di passaggio, tuttora in corso, da un ruolo di "*Assurance Provider*" ad uno di "*Trusted Advisor*"[13].

L'ultima revisione degli *Standard* della professione ha cercato di fare propri tali mutamenti, mediante alcune modifiche con riferimento ad eventuali ruoli addizionali assunti dal responsabile dell'*Internal Audit*, al coordinamento con altri prestatori di servizi di *Assurance* e consulenza interni ed esterni all'organizzazione, al programma di miglioramento della qualità ed alla comunicazione e *reporting* verso il Consiglio di Amministrazione e il *senior management*.

È opportuno evidenziare in proposito che anche l'informativa fornita al mercato in merito alle effettive pratiche di *governance* e, più in generale, su elementi di carattere non strettamente finanziario e contabile, può senz'altro diventare elemento di creazione del valore dell'impresa e per tale ragione è diventato meritevole di attività di *Audit*. Giova ricordare che, se non correttamente monitorati, anche i rischi apparentemente a minore impatto possono rappresentare delle significative fonti di crisi e di danno economico. Tra questi è di particolare importanza, nell'attuale sistema sociale che riserva una spasmodica attenzione alle strategie comunicative ed ai suoi effetti, la gestione dei rischi reputazionali[14].

In Italia, ancorché richiesta per gli emittenti di titoli quotati a seguito della adozione delle previsioni del Codice di Corporate Governance[15], la

[13] PWC, *State of the Internal Audit Profession Study*, 2018.

[14] A. Oliva, S. Bocchino, *L'internal auditor e il sistema di controllo interno*, in "I nuovi compiti degli organi sociali" a cura di P. Riva, Collana "Crisi d'impresa", Milano, Il Sole 24 ore, 2019.

[15] Il Codice è redatto sulla base del modello "comply or explain"; ciò significa che il Codice non deve essere necessariamente implementato dalle società quotate aderenti, tuttavia la loro mancata adesione, anche se soltanto parziale, deve necessariamente essere adeguatamente motivata da parte di ciascuna società nella relazione annuale sul governo societario ai sensi dell'art. 123-bis, comma 2, lett. a) del D.Lgs. 24 febbraio 1998, n. 58.

costituzione di una struttura di *Internal Audit* non è ad oggi normativamente obbligatoria ad eccezione di alcuni **settori regolamentati** come il settore finanziario e assicurativo, per quanto si assista via via ad una sua progressiva diffusione anche in realtà di minori dimensioni nel settore manifatturiero e terziario. Per le società non quotate la crescente diffusione della figura dell'*Internal Auditor* è spesso ricollegabile alla adozione del decreto legislativo 231/2001[16]. Come anticipato, i settori regolamentati, detti anche vigilati in quanto soggiacenti alla vigilanza di apposite Autorità come la Banca d'Italia, la Consob o IVASS, rispettivamente per il settore bancario e finanziario, per le società quotate ed emittenti titoli diffusi e per le assicurazioni, sono quelli che presentano storicamente una più antica tradizione e attitudine a complessi sistemi di controllo interno e quindi alla presenza di adeguate strutture di *audit* interno. La ragione è ovviamente evidente, il grande peso che questi enti rivestono negli equilibri economici nazionali e la tutela del pubblico risparmio richiedono un maggior grado di garanzie rispetto ad entità più semplici. Parimenti l'ordinamento in questo ambito passa da un livello di previsioni di opportunità, quando anche fortemente sostenute mediante la produzione di codici di autodisciplina, a previsioni normative cogenti di vario livello. Si va dalla regolamentazione prodotta dalle Autorità di vigilanza, spesso anche derivanti da lettere roneate, manuali, circolari, disposizioni e regolamenti, fino a norme vere e proprie.

Nel primo gruppo (regolamentare) si segnalano in particolare il "Regolamento in materia di organizzazione e procedure degli intermediari che prestano servizi di investimento o di gestione collettiva del risparmio" emanato da CONSOB congiuntamente a Banca d'Italia il 29 ottobre 2007 e successive modifiche e le "Disposizioni di vigilanza per gli intermediari finanziari" (Circolare Banca d'Italia n. 288 del 3 aprile 2015) ed il Regolamento n. 38 IVASS del 3 luglio 2018. Tali normative di vigilanza recepiscono i principi guida sulla materia pubblicati nel 2005 dal Comitato di Basilea[17].

Nel secondo gruppo (normativo) si segnalano in particolare la Legge 28 dicembre 2005, n. 262, Disposizioni per la tutela del risparmio e la disciplina dei mercati finanziari; il decreto legislativo 24 febbraio 1998, n. 58, Testo unico delle disposizioni in materia di intermediazione finanziaria TUF (Testo Unico della Finanza); il decreto legislativo 1° settembre 1993, n. 385,

[16] Per approfondimenti in tema di D.Lgs. 231/2001 si rinvia infra al Capitolo 9. Si veda anche: N. Pecchiari, S. Beretta, *Analisi e valutazione del sistema di controllo interno. Metodi e tecniche*, Milano, Il Sole 24 Ore, 2007.

[17] Basel Committee on Banking Supervision, *Enhancing corporate governance for banking organisations*, 2005.

cioè il Testo unico delle leggi in materia bancaria e creditizia, ossia il TUB (Testo Unico Bancario).

Se le società sono quotate in mercati esteri vanno ovviamente rispettate le norme locali; ad esempio le aziende italiane quotate al NYSE devono rispettare tra l'altro la SOX – Sarbanes-Oxley Act. Si rinvia per un approfondimento su quest'ultima specifica e rilevante normativa al Capitolo 8.

6.3 Definizione e tipologie di *Internal Auditing*

Secondo la definizione dell'AIIA del 1999:

> "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."

Dall'analisi della definizione ufficiale si ottengono molteplici e significativi concetti chiave, ovvero di:

- **attività**, che non necessariamente è una funzione aziendale della struttura, ma prescinde dalla collocazione di chi la esercita e quindi può anche essere svolta in *outsourcing*, come meglio dettagliato al paragrafo 8;
- **indipendenza**, ossia il responsabile dell'IA deve possedere una neutralità '*super partes*', ma è al contempo fondamentale uno spirito di empatia ed accettazione delle forme di coinvolgimento ai generali obiettivi dell'entità. Decisamente scorretta e improduttiva è la contrapposizione aprioristica con le risorse auditate. Il più possibile va valorizzato lo sforzo non di una correzione a posteriori degli errori, ma di una partecipazione della definizione delle attività. L'indipendenza è anche organizzativa ovvero l'attività deve essere libera da ogni interferenza nella definizione dell'ambito di copertura delle verifiche, nell'esecuzione del lavoro e nella comunicazione dei risultati;
- **obiettività**, quale atteggiamento mentale e operativo fondato esclusivamente sulla competenza tecnica relativa al singolo caso, evitando giudizi aprioristici e conflitti di interessi;
- **di assurance e di consulenza**, due anime della attività di *audit* interno, sintesi del citato recente processo di evoluzione della professione. La prima consiste sostanzialmente di una attività di esame delle evidenze allo scopo di ottenere una valutazione indipendente dei processi di gestione o di *governance*. La seconda è riferibile soprattutto di servizi di supporto e assistenza intesi a fornire suggerimenti per migliorare gli stessi processi di gestione e le attività di *governance, risk management* e controllo;

- **assistenza all'organizzazione**, funzione di *staff* all'organo gestorio o di comitati in esso presenti, mentre la responsabilità finale delle *operations* permane in capo al *management*;
- **approccio professionale sistematico**, come valorizzazione del metodo, delle competenze e degli strumenti propri dell'*IA* nel condurre le analisi;
- **generazione di valore aggiunto**, intesa come realizzazione di benefici derivanti dallo svolgimento dell'attività superiori ai costi prodotti. Appare evidente, ma sorprendentemente non sempre correttamente applicato, che se una attività di verifica consta di un onere maggiore al danno evitabile, tale attività è diseconomica e di per sé priva di senso (può averlo solo in taluni casi in cui l'attività di verifica ha anche motivazioni di tipo educativo e stimolo alle buone prassi).

Tenendo conto dell'oggetto di verifica si individuano le seguenti tipologie di *Audit interno*:

i. **financial auditing**: verifica dei controlli a garanzia della veridicità delle rilevazioni contabili;
ii. **management auditing**: indagine all'interno dell'entità allo scopo di accertare se si è realizzata una coerente politica direzionale volta a creare efficaci rapporti con l'esterno e di efficiente gestione al suo interno;
iii. **operational auditing**: analisi dei meccanismi operativi dei processi gestionali allo scopo di assicurare la compatibilità e la coerenza tra i risultati raggiunti da un'entità e gli obiettivi ad essa assegnati.

Altre tipologie di *audit interne* possono essere:

iv. *fraud audit* (finalizzato all'identificazione ed alla quantificazione delle frodi subite dall'entità);
v. *IT audit* (processo di verifica, condotto da personale esperto, sui sistemi informativi di una entità e sulla conformità a quanto previsto da norme, regolamenti o politiche interne);
vi. *audit sui progetti* (volto ad identificare i rischi dei propri progetti e le strategie per ridurli o eliminarli ed anche a migliorare la capacità di effettuare analisi di causa-effetto);

e, infine,

vii. *audit etico* (avente come area di analisi la governance etica dell'impresa).

Più in generale, altre classificazioni utilizzano la categoria "*audit*" per le attività più strettamente legate a una analisi di tipo contabile, mentre le altre di tipologie di verifica rientrano nella macrocategoria di attività di "*assurance*".

6.4 Il concetto di proporzionalità e di *risk appetite*

Nel primo paragrafo abbiamo appurato come il concetto di rischio sia fondamentale nella definizione dei modelli più attuali di analisi del Sistema di Controllo Interno (SCI) che, appunto, nelle ultime versioni del Codice di Corporate Governance è ora definito *SCI-GR*, aggiungendo proprio l'acronimo *GR* di Gestione dei Rischi per evidenziarne l'imprescindibile valutazione. Ci guidano in tale compito due concetti molto importanti:

- la **proporzionalità**; e,
- il ***risk appetite***.

In base al principio di **proporzionalità** la strutturazione e il dimensionamento del *SCI*[18], anche in termini di complessità e di risorse destinate, devono essere proporzionati alla natura, alla dimensione e alla complessità dell'attività svolta, nonché, in particolare per i soggetti finanziari, alla tipologia e alla gamma dei servizi prestati. Abbiamo già incontrato questo concetto nella analisi della definizione stessa di *Internal Audit*, laddove si prevede che la sua azione generi per l'entità un valore aggiunto (positivo). Dal principio di proporzionalità si passa al principio dell'approccio basato sul rischio (*risk based approach*) che ne è una declinazione operativa. Infatti, una volta compresi i rischi connessi allo svolgimento dell'attività dell'entità, è logica conseguenza il passaggio alla definizione delle misure di mitigazione da adottare di volta in volta per il loro contenimento. La strategia *risk based approach* trova la sua più esplicita trattazione nell'ambito del sistema normativo italiano in ambito di antiriciclaggio[19], ma essendo questo concetto di primaria importanza, esso risulta estendibile ad ogni valutazione relativa al più generale *SCI-GR*.

[18] Il principio di proporzionalità è notoriamente uno dei più importanti principi generali del diritto comunitario, secondo il quale l'azione comunitaria deve limitarsi allo stretto necessario per il raggiungimento dell'obiettivo prefissato. Altri esempi sono riscontrabili nella produzione normativa di vario livello sia amministrativa che finanziaria. Il principio di proporzionalità gioca però ruolo fondamentale anche a livello dell'organizzazione societaria; si ricordi in tal senso la connessione di questo concetto con quello di adeguatezza previsto nell'art. 2381 c.c.

[19] Banca d'Italia, Disposizioni in materia di organizzazione, procedure e controlli interni volti a prevenire l'utilizzo degli intermediari a fini di riciclaggio e di finanziamento del terrorismo del26/03/2019 Parte I – Sezione II: recita: "In applicazione dell'approccio basato sul rischio (c.d. risk based approach), i destinatari si dotano di un assetto organizzativo, di procedure operative e di controllo, nonché di sistemi informativi idonei a garantire l'osservanza delle norme di legge e regolamentari in materia antiriciclaggio, tenendo conto della natura, della dimensione e della complessità dell'attività svolta nonché della tipologia e della gamma dei servizi prestati".

Il **Risk Appetite Framerwork-RAF** (o sistema degli obiettivi di rischio) è il quadro di riferimento che definisce – in coerenza con il massimo rischio assumibile, il *business model* e il piano strategico – la propensione al rischio, le soglie di tolleranza, i limiti di rischio, le politiche di governo dei rischi, i processi di riferimento necessari per definirli e attuarli.

I due concetti sono a ben vedere strettamente correlati, e consentono di definire, dopo una attenta e consapevole analisi costi-benefici, quale sia il livello di rischio che l'impresa intende accettare in relazione ai suoi obiettivi complessivi e con quali risorse intenda far fronte al livello di rischio accettato (ossia al proprio *risk appetite*)**,** ottimizzando la complessa funzione di "costo del controllo", anche in relazione alle dimensioni (e quindi ragionevolmente anche alle possibilità) dell'entità stessa. Dalla risoluzione di questa "equazione" dipende l'individuazione degli obiettivi che l'entità è in grado di sostenere nel medio periodo, e quindi la definizione degli strumenti necessari per controllarli e delle modalità per evitare e monitorare i rischi, nonché l'individuazione delle risorse disponibili a tale fine. Questo complesso processo di ricerca dell'equilibrio consente, se svolto in modo continuo e consapevole, di limitare al massimo la deriva verso la crisi d'impresa prima e l'insolvenza poi[20]. Come si vedrà diffusamente *infra* nel Capitolo 14, la segnalazione di una situazione anche solo di crisi comporta, tra l'altro, alla luce della nuova disciplina del nuovo CCI che ha sostituito la legge fallimentare, un impatto rilevantissimo proprio sulla *governance* aziendale sia quanto a soggetti coinvolti sia quanto a poteri dagli stessi esercitabili.

In questo contesto si collocano lo sviluppo e la diffusione in ambito internazionale di modelli teorici relativi al Sistema di Controllo Interno che forniscono riferimenti concettuali alle componenti degli stessi di facile comprensione e condivisione, definizioni di generale applicabilità che prescindono dai confini settoriali e geografici. La **tassonomia dei rischi** ne individua le seguenti tipologie principali, variamente presenti e con un diverso grado di magnitudo a seconda della azienda e del settore in cui opera:

- *rischio di mercato*: perdita di valore dovuta a fluttuazioni del valore di mercato degli strumenti finanziari o al mutamento nell'esito commerciale dei prodotti o servizi ceduti;

[20] Questi concetti sono stati definiti proprio nell'art. 2 del nuovo Codice della crisi e dell'insolvenza nei termini seguenti: a) «crisi»: lo stato di difficoltà economico-finanziaria che rende probabile l'insolvenza del debitore, e che per le imprese si manifesta come inadeguatezza dei flussi di cassa prospettici a far fronte regolarmente alle obbligazioni pianificate; b) «insolvenza»: lo stato del debitore che si manifesta con inadempimenti od altri fatti esteriori, i quali dimostrino che il debitore non è più in grado di soddisfare regolarmente le proprie obbligazioni.

- *rischio di credito*: perdita di valore dovuta al depauperamento del capitale investito nell'operazione per insolvenza della controparte;
- *rischio operativo*: perdite dovute a inefficienze nei processi di operatività degli soggetti coinvolti;
- *rischio reputazionale*: è importante ricordare che anche i rischi apparentemente di minore impatto possono rappresentare delle significative fonti di crisi e di danno economico se non correttamente monitorati. Tra questi è di particolare importanza, nell'attuale sistema sociale che riserva una spasmodica attenzione alle strategie comunicative ed ai suoi effetti, la gestione dei rischi reputazionali. A seguito di banali errori di comunicazione o di veicolazione delle informazioni sui propri prodotti e servizi, così come ad esempio sulla gestione delle risorse umane o delle relazioni con la clientela, si può incorrere in un rilevante *social-shame* che può produrre nel giro di pochissimo tempo rilevanti danni economici;
- *altri rischi*: possono presentarsi rischi di tipo legale, rischi legati a fattori macro-economici, demografici e simili.

In stretta connessione al **Risk Appetite** viene definita la **Risk tolerance**, ossia il perimetro entro il quale il parametro può variare senza che sia necessario decidere di implementare ulteriori azioni di intervento a mitigazione. A seconda del settore di appartenenza, le aziende decidono quale può essere la soglia di rischio accettabile. Superata tale soglia scatta un *warning* e si rende necessario un intervento a mitigazione del probabile evento dannoso. Diventa quindi di fondamentale importanza la misurazione di diverse variabili

Figura 6.2 – Risk Appetite e Risk tolerance

Fonte: Calpers 2017.

aziendali connesse alla definizione del limite di rischio accettato. La Figura 6.2 rappresenta questi concetti in modo sintetico ed efficace.

Naturalmente a seconda del settore e dell'azienda vi sarà un diverso approccio al rischio. Rischi prioritari per una entità del settore finanziario potranno essere di minore attenzione per una azienda di servizi ben capitalizzata, così come quelli di una entità che lavora nel settore *fashion* saranno diversi da una azienda di costruzioni di infrastrutture. La definizione del *Risk Appetite* deve essere preceduta da una accurata mappatura dei rischi che abbia come orizzonte primario proprio le peculiarità della azienda analizzata nel concreto. La prassi oziosa di "calare dall'alto" mappature standard, utilizzate per molteplici realtà, solo apparentemente semplifica il lavoro in quanto tale attività rimane estranea a chi operativamente in azienda svolge i compiti considerati nella mappatura e nelle correlate attività di definizione di KPI (Key Performance Indicators) di rischio e di monitoraggio degli stessi. Si genera quindi paradossalmente un **ulteriore rischio**, molto spesso sottovalutato o ignorato, ossia che tutta questa attività sia considerata un corpo estraneo all'interno della azienda e sia vissuta come un onere periodico inutile e fastidioso, quando non anche ignorato. Regola aurea è quindi quella di fare partecipare al massimo i *key user* nella definizione della mappatura dei rischi mediante colloqui individuali, tavole rotonde, *brainstorming* spiegando esattamente gli obiettivi, condividendo materiali e metodologie in uso e raccogliendo il più possibile, dopo ovviamente una attività di filtraggio e sistemizzazione, i suggerimenti dei vari partecipanti. Un'altra buona regola è quella di semplificare il più possibile la documentazione di *output* di tale lavoro, la produzione di schemi di analisi molto strutturati e la definizione di KPI complessi e ponderosi è sicuramente suggestiva dal punto di vista grafico e porta a pensare all'esistenza di un grande lavoro; spesso è così, ma, come detto, ha il grande rischio di essere un organismo a vita propria che mal si collega alla dinamica esistenza gestionale di una azienda.

6.5 Il piano di *Internal Audit*

Una volta definita la mappatura dei rischi e considerate le risorse, sia temporali sia economiche, a disposizione della funzione di IA diventa imprescindibile la definizione di un piano di *audit* che rappresenti le scelte operative susseguenti a tali valutazioni. La redazione di questo piano, in genere annuale (nelle realtà più grandi sono talvolta presenti anche piani pluriennali più generali detti anche piani delle priorità), non ha solo una valenza operativa e ottimizzatrice, serve anche a garantire il più possibile quei requisiti di indipendenza e obiettività che abbiamo già visto nella definizione di *Internal Audit*. Sforzarsi, per quanto possibile, di rendere oggettivi e tracciabili i cri-

teri di scelta permette di evitare ogni possibile rischio o malizia di controlli "*ad personam*". L'importanza del piano di *audit* è rintracciabile anche nella Raccomandazione 33 – c) del Codice di Corporate Governance la quale stabilisce che il Consiglio di Amministrazione, previo parere del Comitato controllo e rischi, approva, con cadenza almeno annuale, il piano di lavoro predisposto dal responsabile della funzione di *IA*, sentiti l'organo di controllo e il Chief Executive Officer. Il piano di *audit* è quindi posto all'approvazione del massimo organo gestorio. Ulteriormente la Raccomandazione 36 – a) prevede che il responsabile della funzione di *Internal Audit* verifichi, sia in via continuativa, sia in relazione a specifiche necessità e nel rispetto degli standard internazionali, l'operatività e l'idoneità del sistema di controllo interno e di gestione dei rischi, mediante un piano di *Audit*, approvato dall'organo di amministrazione, basato su un processo strutturato di analisi e prioritizzazione dei principali rischi. In questa previsione si indica quindi come l'attività di *Audit* debba avere come guida il piano e come questo debba essere basato sulla analisi e valutazione dei rischi, concetti che abbiamo prima analizzato. Il piano di *Audit* non deve però diventare uno strumento limitativo, a seguito della inaspettata emersione di una specifica criticità, della urgenza di effettuare verifiche per evitare o limitare danni imminenti o anche solo per comprendere un fenomeno che al momento non risulta adeguatamente intellegibile. Il Consiglio di Amministrazione, il Comitato controllo e rischi, l'Amministratore Delegato (o il Chief Executive Officer), la Direzione generale, il Collegio Sindacale o l'Organismo di Vigilanza possono, anche in collaborazione tra loro (verifiche congiunte), chiedere di attivarsi per svolgere specifici *audit*, dandone adeguata motivazione. L'attività *Auditing* si presenta come una sequenza coordinata di attività finalizzate all'ottenimento di uno specifico risultato, è quindi essa stessa un processo. Oggetto dell'*audit* interno possono essere, come detto, i processi gestionali o i rischi aziendali.

6.6 Le principali fasi dell'attività di *Internal Audit*

Ripercorrendo gli standard professionali si possono individuare le seguenti fasi principali nella attività di audit:

a. **pianificazione dell'incarico (2200-2240)** – Per ogni 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. Il piano sarà conforme alle strategie e gli obiettivi dell'entità e ai rischi attinenti l'incarico;
b. **svolgimento dell'incarico (2300-2340)** – Questa fase fa riferimento a tutte le operazioni compiute dall'Internal Auditor per raccogliere la documentazione necessaria a supportare le proprie conclusioni. Le "carte

di lavoro" dell'Internal Auditor devono documentare i fatti che hanno indotto le conclusioni raggiunte e consentire di svolgere un adeguato lavoro di supervisione sul metodo seguito e sulla bontà delle soluzioni eventualmente suggerite al *management*;

c. **comunicazione dei risultati (2400-2450)** – Il rapporto di internal audit è il documento che conclude e riepiloga l'attività di *audit*. In esso quindi sono segnalate ai destinatari le principali criticità emerse e le raccomandazioni circa l'esecuzione di adeguate azioni di remediation;
d. **monitoraggio delle azioni correttive (2500)** – L'Internal Auditor deve stabilire e mantenere un sistema di monitoraggio delle azioni intraprese a seguito dei risultati segnalati al management. L'attività cosiddetta di *follow-up* è una parte fondamentale della attività di *audit*, finalizzata a verificare che i piani di miglioramento suggeriti siano stati effettivamente adottati in modo adeguato, efficace e tempestivo, riducendo il rischio ad un livello accettabile per l'entità (compresa l'accettazione integrale del rischio qualora rientri nella determinazione del *risk appetite*);
e. **comunicazione dell'accettazione del rischio (2600)** – Secondo lo standard 2600 qualora l'Internal Auditor concluda che il *management* abbia accettato un livello di rischio che potrebbe essere inaccettabile per l'entità, ne deve discutere con l'alta direzione. Se egli crede che la problematica permanga deve segnalarlo al Consiglio di Amministrazione (e/o al Comitato controllo e rischi o al Collegio Sindacale).

6.7 Le relazioni con gli altri organi di governance

Come abbiamo detto nel primo paragrafo, nell'ambito del SCI si possono individuare, soprattutto nelle realtà più organizzate, molteplici soggetti con compiti riferiti all'area dei controlli.

In tale contesto, occorre essere consapevoli che alcune aree sono di «comune interesse». Si segnala, ad esempio, la rilevanza dell'area amministrativo-contabile (e del relativo sottosistema di controllo interno) per i seguenti attori:

- Dirigente preposto alla redazione dei documenti contabili societari (o nel caso di non quotate il CFO);
- Collegio Sindacale;
- Società di Revisione;
- Organismo di Vigilanza ex D.Lgs. 231/2001.

In tale scenario, risulta evidente l'opportunità/la necessità di disegnare la *governance* e il sistema di controllo interno secondo criteri di adeguatezza ed efficienza, assicurando il mantenimento nel tempo di tali requisiti; prevedere gli opportuni meccanismi di coordinamento tra gli attori del sistema dei controlli e implementare gli opportuni flussi informativi tra tali attori.

Anche il Codice di Corporate Governance reputa fondamentale l'esigenza di coordinamento tra i diversi soggetti coinvolti al fine di massimizzare l'efficienza del sistema di controllo interno e di gestione dei rischi e di ridurre le duplicazioni di attività[21]. L'*Internal Auditor* avrà necessariamente relazioni con il Consiglio di Amministrazione e con il Comitato controllo e rischi (il secondo come supporto al primo, per le valutazioni e le decisioni relative al *SCI-GR* e all'approvazione delle relazioni finanziarie periodiche). In tema di flussi informativi generati dalla funzione di *Internal Audit*, il Codice stabilisce che gli esiti delle verifiche effettuate dovrebbero essere resi noti, di norma in modo contestuale, ai Presidenti dell'Organo di controllo, del Comitato controllo e rischi e dell'Organo di amministrazione, nonché al Chief Executive Officer, salvo i casi in cui l'oggetto di tali relazioni riguardi specificamente l'attività di tali soggetti. In un ottica più propriamente di scambio di informazioni i soggetti d'elezione sono la Società di revisione (o il revisore unico) e l'Organismo di Vigilanza, oltre, in certi ambiti, lo stesso Collegio Sindacale (denominato sia nel CCI sia nel Codice di CG "Organo di controllo societario"). La collaborazione si rivela particolarmente auspicabile, sia al fine di ottimizzare le risorse, sia per condividere e diffondere metodologie, approcci e punti di vista differenti.

Necessariamente l'*Internal Auditor* avrà contatti diretti con ogni funzione aziendale ad ogni livello, non certo e non solo con l'alta direzione, nell'ambito dello svolgimento delle proprie verifiche. Data la potenziale molteplicità di referenti con diverse attitudini, formazione, grado di istruzione, finanche diversi linguaggi in caso di gruppi multinazionali, gli sono richieste elevate capacità comunicative ed empatiche per poter entrare in efficace relazione con questa notevole diversità di risorse.

Rispetto all'inquadramento come funzione interna all'entità (dipendente) in alternativa al ricorso a professionalità esterne (qui l'aggettivo "*Internal*" non deve trarre in inganno). È lo stesso Codice di Corporate Governance a proporre il suo punto di vista: "Qualora (la società) decida di affidare la funzione di internal audit, nel suo complesso o per segmenti di operatività, a un soggetto esterno alla società, assicura che esso sia dotato di adeguati requisiti di professionalità, indipendenza e organizzazione e fornisce adeguata motivazione di tale scelta nella relazione sul governo societario..."[22].

[21] Codice di Corporate Governance – *op. cit.*, Principio XX.

[22] Codice di Corporate Governance – *op. cit.*, Raccomandazione 33 – b).Analogo commento era presente nella precedente versione del Codice 2018 all'articolo 7, Criteri applicativi 6. Si noti che nella versione del Codice del gennaio 2020 non sono più presenti le sezioni "commento" e "criteri operativi" al fine di renderlo più snello secondo una delle quattro linee d'azione a cui si ispira il nuovo Codice: sostenibilità, *engagement*, proporzionalità e,

Non esiste una soluzione unica a questa scelta e tutto dipende dalla tipologia dell'entità, dalle sue risorse, dalla sua organizzazione e dal suo ambiente culturale. Tra gli aspetti positivi del ricorrere all'outsourcing si rileva una maggiore indipendenza, flessibilità, risparmio di costi e talvolta migliore qualità, frutto di diverse esperienze e diverse realtà nel tempo affrontate. Dall'altro lato, però, gli svantaggi legati alla scelta di esternalizzare queste attività comprendono la perdita di fedeltà, data dalla possibilità che la stessa azienda di servizi operi anche per altri operatori del medesimo settore e la minore conoscenza del business in cui opera l'entità. Negli ultimi anni sembra prevalere la scelta di non ricorrere all' *outsourcing* o *co-sourcing* principalmente per il timore di rivelare a soggetti esterni informazioni chiave dell'entità e per la percezione che una funzione di *internal audit in-house* possa avere una maggiore dimestichezza con i meccanismi formali e informali in atto nell'organizzazione stessa[23]. È comunque innegabile che il disporre internamente di una funzione così strategica possa garantire il permanere nella entità delle conoscenze via via acquisite nel corso della attività. Si possono poi manifestare anche situazioni ibride, in particolare, spesso avviene nel caso di *IT audit*, quando la struttura interna non dispone delle specifiche competenze richieste e fa ricorso a professionalità esterne a supporto.

6.8 Lo stato dell'*Internal Audit* in Italia

Nel 2018 al fine di rilevare le effettive pratiche di governo societario riscontrabili negli emittenti quotati *PricewaterhouseCoopers Advisory* ha condotto l'indagine intitolata "*Internal Auditing* nelle società quotate – Approfondimenti sull'informativa fornita al mercato". A tal fine sono state analizzate le Relazioni sul governo societario e gli assetti proprietari delle società quotate sul Mercato Telematico Azionario gestito da Borsa Italiana. Dall'analisi dei dati si osserva un'accelerazione al percorso evolutivo della funzione *Internal Audit*, che vede il suo raggio d'azione spostarsi da verifiche circoscritte agli aspetti di conformità normativa e procedurale ad attività di maggiore ampiezza e valore aggiunto nell'ambito dell'*assurance* e della consulenza in merito al controllo sistemico, alla gestione dei rischi ed alla *corporate governance*. Lo

appunto, semplificazione. Al posto dei commenti, accanto ai principi e alle raccomandazioni, saranno introdotte Q&A, da aggiornare periodicamente, per rendere più agevole l'adesione al codice, cosi come affermato da Patrizia Grieco, Presidente del Comitato italiano per la corporate governance. In questo senso: L. Serafini, *Pmi, dal nuovo Codice di Corporate Governance una spinta alla Borsa*, Sole 24 ore del 3 febbraio 2020.

[23] G. D'Onza, *L'internal auditing*, G. Giappichelli Editore, Torino, 2013.

studio evidenzia alcune interessanti informazioni. L'istituzione di una funzione di *IA* nelle società quotate rappresenta ormai una prassi consolidata ed ampiamente diffusa essendo presente in circa il 95% degli emittenti. Chi ne è sprovvisto ne attribuisce i motivi a ragioni prevalentemente dimensionali. Riguardo alla configurazione organizzativa, gli emittenti scelgono in larga maggioranza (72%) soluzioni interne (*in house*); in caso di esternalizzazione della funzione (*outsourcing*), la scelta risulta ricadere tipicamente su società di consulenza, revisione o professionisti esterni, oppure è affidata a strutture presenti nell'ambito del Gruppo di appartenenza. Tra le motivazioni addotte in merito all'esternalizzazione della funzione rientrano valutazioni di maggior efficienza in termini di costi e competenze, oltre alla necessità di garantire indipendenza, autonomia e professionalità. Con riferimento alla collocazione organizzativa, il riporto gerarchico verso il Consiglio di Amministrazione è esplicitamente confermato nel 64% dei casi. In caso di indicazione di soggetti differenti, è comunque indicato il riporto a figure di *governance* di primo livello (Amministratore Delegato, Presidente del Consiglio di Amministrazione). Il processo di nomina appare pienamente allineato a quanto atteso dal Codice di Corporate Governance nel 48% dei casi, mentre i restanti casi emergono parziali disallineamenti o non sono disponibili informazioni.

La necessità di una appropriata valorizzazione delle attività di *Internal Audit* si collega necessariamente all'ineluttabile evoluzione della professione per effetto dei significativi cambiamenti del contesto di riferimento in cui operano le organizzazioni e dei correlati nuovi scenari di rischio. Le funzioni di *Internal Audit* sono chiamate a supportare l'entità al fine di garantire che i processi e i controlli siano efficaci, senza rallentare il ritmo dell'innovazione e tenendo conto degli impatti dirompenti dei rapidi ed incessanti cambiamenti nel contesto di riferimento in cui operano le aziende. Cambiando i rischi delle organizzazioni, cambiano di conseguenza le competenze necessarie per comprendere, analizzare e valutare tali rischi. In tale panorama l'impatto pervasivo della tecnologia espone le entità a nuovi significativi rischi di cui è fondamentale avere piena consapevolezza e impone di dotarsi di adeguati strumenti efficaci per la loro relativa gestione. Ne consegue la necessità per l'*Internal Auditor* di acquisire differenti competenze, metodologie e strumenti di lavoro.

Bibliografia

Anthony N. R., *Planning and Control Systems: A Framework for Analysis*, Boston, Division of Research, Graduate School of Business Administration, Harvard University, 1965

Associazione Italiana Internal Auditors, *Manuale di Internal Auditing*, 1989

Banca d'Italia, *Disposizioni in materia di organizzazione, procedure e controlli*

interni volti a prevenire l'utilizzo degli intermediari a fini di riciclaggio e di finanziamento del terrorismo del 26/03/2019 Parte I – Sezione II
Basel Committee on Banking Supervision, *Enhancing corporate governance for banking organisations*, 2005
Bertalanffy von L., *General System Theory*, New York, George Braziller, 1968
Besta F., *La ragioneria*, Milano, Vallardi, Vol. I, 1922
Borsa Italiana, Comitato Corporate Governance, Codice di Corporate Governance, gennaio 2020
Brink Z. V., *Internal Auditing*, New York, Ronald Press, 1941
Comoli M., *I sistemi di controllo interno nella corporate governance*, Egea, 2002
Dittmeier C., *Internal Auditing. Chiave per la Corporate Governance*, Egea, 2011
D'Onza G., *L'internal auditing*, Torino, G. Giappichelli Editore, 2013
Hopwood G., *Accounting and Human Behaviour*, Englewood Cliffs, Prentice Hall Inc., 1976
Messier W., *Auditing*, McGraw-Hill, 2000
Mintzberg H., *La progettazione dell'organizzazione aziendale*, Bologna, Il Mulino, 1996
Oliva A., Bocchino S., *L'internal auditor e il sistema di controllo interno*, in Fascicolo VI "I nuovi compiti degli organi sociali" a cura di Riva P., nella Collana "Crisi d'impresa", Milano, Il Sole 24 Ore, 2019
Pecchiari N., Beretta S., *Analisi e valutazione del sistema di controllo interno. Metodi e tecniche*, Milano, Il Sole 24 Ore, 2007
PWC, *State of the Internal Audit Profession Study*, 2018
Ramamoorti S., *Chapter 1. Internal Auditing: History, Evolution, and Prospects*, in Bailey A., Ramamoorti S., Audrey G., *Research Opportunities in Internal Auditing*, Altamonte Springs, The Institute of Internal Auditors Research Foundation, 2003
Serafini L., *Pmi, dal nuovo Codice di Autodisciplina una spinta alla Borsa*, Sole 24 Ore, 3 febbraio 2020
Tettamanzi P., *Internal auditing. Evoluzione storica, stato dell'arte e tendenze di sviluppo*, Egea, 2004