UNIVERSITÀ POLITECNICA DELLE MARCHE

FACOLTÀ DI ECONOMIA "GIORGIO FUÀ"

Corso di Laurea triennale in Economia e Commercio

Revisione legale e IT Audit

Financial auditing and IT audit

Relatore:

Prof. Giuliani Marco

Rapporto Finale di:

Federico Pieroni

Anno Accademico 2018/2019

Indice

Introduzione

Nell'ambito della disciplina di revisione aziendale, l'analisi dei sistemi informativi, con l'avvento delle nuove e più efficienti tecnologie informatiche, è divenuta sempre più complessa ed importante verificare la veridicità e correttezza dei dati presenti in questi sistemi è infatti fondamentale per esercitare un'adeguata ed efficace attività di revisione. L'attività in parola spesso necessita anche di specifiche conoscenze informatiche e, quindi, porta sovente ad avvalersi di un esperto.

Il sistema informativo è una componente importante del sistema di controllo interno (SCI).Il SCIha come obiettivo il governo dell'azienda stessa attraverso l'individuazione, valutazione, monitoraggio, misurazione e mitigazione/gestione di tutti i rischi d'impresa, coerentemente con il livello di rischio scelto/accettato dal vertice aziendale. Il SCI si basa sempre di più sulle tecnologie informatiche onde averepiù efficacia ed efficienza.

L'obiettivo di questo lavoro è quello di andare a presentare le metodologie, con cui si effettua l'attività di revisione del sistema di controllo interno approfondendo i sistemi informativi attualmente più utilizzati dalle imprese, al fine di cogliere la rilevanza che questo aspetto riveste sia nelle procedure di revisione sia nella prassi aziendale.

Per comprendere meglio come le imprese effettuano i controlli interni e di conseguenza come approcciarsi dal punto di vista del revisore, inoltre verranno anche trattati alcuni aspetti più legati al settore tecnologico riguardanti ad esempio le infrastrutture IT che le imprese adottano.

Il presente lavoro sarà quindi strutturato in tre capitoli predisposti con l'obiettivo di far comprendere il perché l'attività di revisione del SCI è così importante e come viene effettuata.

Il capitolo 1 illustra le caratteristiche dei sistemi informativi, le loro strutture e tecnologie utilizzate e come si rapportano in relazione all'attività aziendale e a quella di revisione.

Il capitolo 2 si propone di analizzare il sistema di controllo interno, i vari gradi di complessità che esso può raggiungere e come si relaziona ai sistemi informativi precedentemente enunciati.

Il terzo ed ultimo capitolo, infine, affronta le procedure e metodologie utilizzate per effettuare la revisione del sistema del SCI informativo, con l'obiettivo di comprenderne al meglio il funzionamento e l'importanza che esse rivestono nell'ambito più generale dell'intera attività di revisione.

Capitolo 1: I Sistemi Informativi

1.1 Componenti e scopo dei sistemi informativi

“Un sistema informativo aziendale può essere definito come quell'infrastruttura di una organizzazione aziendale deputata alla raccolta e gestione delle informazioni e quindi è composto da elementi che raccolgono, catalogano, ricercano, memorizzano e distinguono i dati trasformandoli in informazioni utili per supportare le attività decisionali e di controllo di un’azienda.” [1]

In un ambiente dinamico come quello odierno, le imprese si trovano quindi in una situazione di grande complessità gestionale e nell'esigenza di gestire quantità sempre maggiori di informazioni in modo sempre più efficace, efficiente e tempestivo per poter così rispondere ai continui cambiamenti del mercato e delle sue esigenze; prendere decisioni velocemente richiede infatti la possibilità di disporre di tutte le informazioni necessarie in tempi rapidi, il che è possibile solo se l'impresa è dotata di un sistema informativo in grado di rendere disponibili queste informazioni in tempo reale. Le tecnologie informatiche offrono a questo scopo grandi potenzialità poiché consentono alle aziende di controllare, pianificare e gestire in modo integrato tutte le attività, nonché di elaborare velocemente una maggiore quantità di dati ed informazioni di quanto fosse possibile in passato.

La parte del sistema informativo composta dai calcolatori, dalle reti informatiche, dalle procedure per la memorizzazione e la trasmissione elettronica delle informazioni prende

[1]Kenneth C. Laudon,Jane P. Laudon,Vincenzo Morabito,Ferdinando Pennarola,"Management dei sistemi informativi", 2006, Pearson

il nome di sistema informatico. Infatti, i concetti fondamentali alla base di un sistema informativo sono dati, informazioni e processi, i quali di per sé non presuppongono l'utilizzo di tecnologie informatiche. Ciononostante, anche se l'esistenza del sistema informativo è indipendente dalla sua automazione, il relativo sistema informatico ricorre quasi sempre all'utilizzo di uno o più database per l'archiviazione e il reperimento delle informazioni, e ad appositi moduli software per l'inserimento e la gestione.

Come dice la parola stessa, un sistema informativo è un "insieme" di elementi (o informazioni) uniti in un unico agglomerato. Si può quindi dare una prima classificazione delle caratteristiche essenziali che connotano questo tipo di sistemi[2]:

1. Dati: sono la componente essenziale del sistema, ma dal momento che non sono ancora stati elaborati, si presentano in uno stato primitivo.
2. Informazioni: insieme di dati già elaborati, strettamente collegati tra di loro con un fine preciso.
3. Persone: coloro che si occupano di raccogliere e catalogare i dati di interesse (opportunamente registrati), affinché possano essere poi elaborati dalle strutture competenti. Sono anche i destinatari delle informazioni già manipolate.
4. Strumenti: è l'insieme delle attrezzature che sono in grado di far viaggiare le informazioni tra fornitore e acquirenti, tra diverse aziende, e in genere tra punti diversi di un'azienda. Si possono anche inserire in questa categoria tutte quelle infrastrutture in grado di trasformare i dati in informazioni. Ovviamente al giorno d'oggi si tratta principalmente di mezzi altamente tecnologici.
5. Procedimenti: sono l'insieme delle procedure che permettono di capire in che maniera vengono raccolti ed elaborati i dati. Per ogni singola finalità, le persone

[2]Kenneth C. Laudon,Jane P. Laudon,Vincenzo Morabito,Ferdinando Pennarola,"Management dei sistemi informativi", 2006, Pearson

di competenza devono scegliere la modalità per elaborare i dati, dal momento che ogni azienda ha una propria esigenza da soddisfare.

Lo scopo quindi di un sistema informativo è svolgere principalmente 3 funzioni[3]:

1. Acquisizione dei dati (processo di input)
2. Trasformazione dei dati (processo di elaborazione)
3. Restituzione di informazioni (processo di output)

Le operazioni sopra elencate devono essere svolte dai sistemi cercando di massimizzare l'efficienza (capacità di raggiungere il miglior risultato con le risorse a disposizione) e l'efficacia (rapporto tra risultato ottenuto ed obiettivo prefissato) e ciò avviene quando il sistema è selettivo (produce solo le informazioni utili e necessarie per poter prendere le decisioni), tempestivo (produce le informazioni necessarie al destinatario nel minor tempo possibile ed è in grado di riprodurle nel tempo con la medesima celerità), affidabile (produce informazioni corrette ed esenti da errori migliorando l'accuratezza dei dati), flessibile (capace di assecondare le esigenze dell'azienda e strutturato sulla base delle stesse, adattandosi alle loro modificazioni) ed infine accettabile (cioè il grado di difficoltà di comprensione che il sistema presenta che deve essere appunto accettabile).[4]

L'esecuzione di questi passaggi è affidata come in precedenza accennato sempre più alle tecnologie informatiche, infatti si parla di CBIS (Computer Based Information

[3]Kenneth C. Laudon,Jane P. Laudon,Vincenzo Morabito,Ferdinando Pennarola,"Management dei sistemi informativi", 2006, Pearson

[4] V.Zwass, "Management Information Systems", 1993, Brown (William C.)

Systems). In base alla natura delle operazioni nel quale vengono utilizzati o all'ambito aziendale, possono essere classificati in senso gerarchico nel seguente modo: alla base troviamo i TPS (Transaction Processing System), destinati alla gestione delle transazioni e che quindi tengono traccia di tutte le informazioni di routine nelle organizzazioni alimentate dal processo degli ordini, delle spedizioni e così via. Questi sistemi di gestione delle transazioni sono spesso centrali per le imprese in quanto pur riguardando aspetti basilari dell'attività aziendale, costituiscono la base informativa sulla quale si basano i livelli successivi di informazioni. Ad un livello superiore sono collocati i MIS (Management Information Systems) che sono sistemi che acquisiscono i dati dai TPS e consentono una rappresentazione periodicamente strutturata delle situazione delle operazioni aziendali, alimentando report utili per il management aziendale.Al fianco dei MIS si collocano come sistemi di supporto alle decisioni i DSS (Decision Support Systems) che permettono al management di valutare situazioni non di routine o di formulare ipotesi circa l'impatto di un'operazione sui parametri aziendali anche avvalendosi di fonti esterne quali tassi di mercato, prezzi delle materie prime e così via. Infine come sistemi di vertice si hanno gli ESS (Executive Information System) che vengono utilizzati dal Management per prendere decisioni strategiche e valutare complessivamente l'andamento aziendale sotto tutti i punti di vista basandosi sulle informazioni e sui dati raccolti ed elaborati dagli altri sistemi gerarchicamente inferiori.[5]

[5]Kenneth C. Laudon, Jane P. Laudon, Vincenzo Morabito, Ferdinando Pennarola, "Management dei sistemi informativi", 2006, Pearson

1.2 Le tipologie di sistemi informativi

Per quanto riguarda la classificazione in base all'ambito aziendale nel quale i sistemi trovano applicazionesi hanno[6] gli ERP (Enterprise Resource Planning) che sono sistemi che raccolgono e classificano tutti i dati provenienti delle varie aree funzionali (ad esempio il ciclo attivo o quello passivo), al fine di fornire all'amministrazione, finanza e controllo dell'impresa informazioni utili, i CRM (Customer Relationship Management) che sono sistemi dedicati alla gestione delle relazioni con il cliente e presidiano tutta l'area commerciale, sia a livello di marketing , sia a livello di attività pre e post vendita, molto utilizzati per la formulazione e la valutazione dei piani di marketing ed infine i SCM (Supply Chain Management) che si occupano della gestione del processo produttivo, dal reperimento delle risorse , passando per il processo di trasformazione fino all' attività logistica.

Per quanto riguarda il rapporto dei sistemi informativi con il processo di revisione e più nello specifico la revisione del SCI, oltre alle varie classificazioni e tipologie di sistemi informativi, è fondamentale conoscere i tipi dei controlli dei sistemi informativi e le relativepolitiche di valutazione dei rischi e della sicurezza che l'azienda pratica, in maniera tale che il revisore possa meglio individuare le aree più rischiose, quelle più suscettibili di frodi o manipolazioni e il grado di affidabilità del SCI che condizionerà poi le procedure che adotterà .

[6]Kenneth C. Laudon, Jane P. Laudon, Vincenzo Morabito, Ferdinando Pennarola, "Management dei sistemi informativi", 2006, Pearson

Per quanto concerne i controlli[7], questi possono essere sia manuali che automatici sia di tipo generale che relativi alle applicazioni, ma spesso accade che ci sia una combinazione di controlli generali e controlli delle applicazioni.

I controlli generali riguardano la progettazione, la sicurezza e l'uso dei programmi per computer e la sicurezza dei file di dati in generale nell'infrastruttura IT dell'azienda, infatti includono controlli sul software, sull' hardware, sul funzionamento dei terminali, sulla sicurezza dati, controlli amministrativi e così via.

I controlli per le applicazioni sono invece controlli specifici per ciascuna applicazione in esecuzione sui terminali, come ad esempio il libro paghe o il programma di elaborazione ordini, possono essere suddivisi in tre categorie:

1. Controlli di input: verificano la precisione e la completezza dei dati introdotti nel sistema.
2. Controlli di elaborazione: garantiscono che i dati siano completi e precisi durante gli aggiornamenti di questi ultimi, utilizzando verifiche dei totali, dei calcoli e procedure affini.
3. Controlli di output: sono controlli che assicurano che i risultati dell'elaborazione siano precisi, completi e correttamente archiviati.

Per quanto riguarda l'estensione e la profondità e precisone dei controlli che monitorano i sistemi informativi, e che confluiranno nel sistema di controllo interno che poi il revisore dovrà analizzare, questi dipendono dalla valutazione dei rischi che l'azienda ha effettuato in sede di progettazione dei sistemi, in base alle procedure e informazioni chiave di cui si devono occupare.

[7]Kenneth C. Laudon, Jane P. Laudon, Vincenzo Morabito, Ferdinando Pennarola, "Management dei sistemi informativi", 2006, Pearson

A seguito dei rischi individuati le aziende tendono spesso a sviluppare politiche di sicurezza al fine di proteggere i propri asset e al tempo stesso ridurre il costo derivante da eventuali errori in termini di sanzioni o inefficienze produttive.

Una politica di sicurezza è costituita da dichiarazioni che classificano i rischi per le informazioni, identificano gli obiettivi accettabili per la sicurezza e i meccanismi per ottenere questi risultati.

Solitamente vengono messe a punto due tipologie di politiche spesso conniventi: le politiche di uso accettabile e quelle di autorizzazione[8].

La prima tipologia si occupa di definire gli usi accettabili delle informazioni e delle attrezzature informatiche dell'azienda, chiarendo i criteri adottati in materia di privacy, responsabilità degli utenti, e uso personale delle attrezzature e reti aziendali, specificando anche le conseguenze per la mancata adesione a questi criteri.

La seconda tipologia e cioè le politiche di autorizzazione, stabilisce diversi livelli di accesso alle informazioni accoppiati a diversi livelli di utenza differente (cioè il grado gerarchico necessario per accedere a determinate informazioni) al fine di consentire a ciascun utente di accedere solo ad alcune parti del sistema in base alle informazioni stabilite da un insieme di regole di accesso.

Inoltre, le imprese che intendono testare l'affidabilità dei propri sistemi informativi, possono disporre un sistema di ampie e sistematiche attività di auditing denominato MIS auditing (Management Information System auditing); queste procedure serviranno all'azienda per analizzare tecnologie, sicurezza, procedure, documentazione e così via, se molto accurato addirittura la risposta dei sistemi ad attacchi o disastri, al fine di individuare ed elencare tutti i punti deboli dei controlli e stimare la probabilità che si

[8]Kenneth C. Laudon, Jane P. Laudon, Vincenzo Morabito, Ferdinando Pennarola, "Management dei sistemi informativi", 2006, Pearson

verifichino falle o la facilità di manomissione, fornendo così utili indicazioni al management.[9]

Tutti questi aspetti, ove presenti, sono di grande rilevanza per l'attività di revisione, in quanto se i sistemi informativi risultano affidabili e tanto più lo sono, il revisore, coadiuvato da un esperto informatico, potrà agevolmente rilevare le criticità che si potranno presentare nell'auditing del SCI e concentrare i propri sforzi sugli aspetti più rischiosi e sulle opportunità manipolative che potranno emergere nel caso di sistemi informativi aziendali complessi.

[9]Kenneth C. Laudon, Jane P. Laudon, Vincenzo Morabito, Ferdinando Pennarola, "Management dei sistemi informativi", 2006, Pearson "

Capitolo 2: Il Sistema di Controllo Interno(SCI)

2.1 Definizione del sistema di controllo interno

Il sistema di controllo interno può essere definito come l'insieme dei processi attuati dagli organi aziendali (CdA, Management, personale, ecc...) finalizzato a fornire una ragionevole sicurezza sul conseguimento degli obiettivi di efficacia ed efficienza delle attività operative, attendibilità delle informazioni contabili ed extracontabili sia rivolte ai terzi sia a fini interni e di conformità (compliance) alle leggi , regolamenti , norme e politiche interne.[10]

Di fatto l'obiettivo principale del SCI è quello di mettere in pratica dei processi e delle procedure che possano permettere all'impresa di eliminare o ridurre considerevolmentei rischi a cui è esposta la gestione aziendale.

Inoltre, è bene ricordare che con il termine "controllo" si indica non solo ciò che tradizionalmente è l'attività di accertamento o di assicurazione dell'esattezza, della regolarità e della rispondenza di un dato elemento a determinati criteri e parametri di riferimento, ma anche l'attività di "guida e governo" dell'attività aziendale verso il conseguimento di obiettivi prestabiliti.

In riferimento all'accezione tradizionale di "controllo" questa può essere intesa come l'insieme delle attività di ispezione, verifica e vigilanza ("Contre-role"); con riguardo invece alla seconda accezione che riguarda "la guida e il governo" è concepito come sistema basato sul principio della delega ("To control").

[10] L.Marchi, "Revisione aziendale e sistemi di controllo interno", 2012, Giuffrè

Si è dunque arrivati nel tempo alla "ridefinizione" di sistema di controllo interno, evoluta verso un'accezione moderna, di strumento di gestione integrata del rischio d'impresa associata ai processi di risk assessment e di risk management e da ultimo, con l'adozione dell'approccio risk-based in sede di progettazione e valutazione dei controlli interni.[11]

2.2. Breve cronistoria del processo evolutivo del SCI

Fino agli anni '40, il controllo interno era, per lo più, concepito come un aspetto incidentale della revisione contabile.

Solo un decennio dopo la nozione di controllo interno includerà i controlli amministrativi e controlli contabili: gli uni concernenti l'efficienza operativa e l'aderenza alle politiche gestionali; gli altri relativi alla salvaguardia dei beni aziendali e alla affidabilità dei documenti finanziari (Statement on Auditing Procedure No. 29, Committee on Auditing Procedure dell'American Institute of CertifiedPublic Accountants (AICPA)), ma in quegli anni l'attività di controllo era esercitata prevalentemente attraverso autonome attività ispettive, condotte a cadenze regolari da appartenenti all'amministrazione societaria, investiti di un incarico ad hoc su presupposti di integrità e indipendenza.

Intorno alla metà degli anni '80 la National Commission on Fraudolent Financial Reporting (più nota come Treadway Commission) propose una nuova chiave di lettura

[11] G.Leonardi, "Risk Management"

del sistema dei controlli interni, in grado di far emergere i difetti discendenti dalla concezione del controllo fino ad allora applicata. La Treadway Commission diede successivamente vita a un apposito sottogruppo di lavoro, denominato Committee of Sponsoring Organizations of the Treadway Commission (CoSO), con 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.La soluzione raccomandata prevedeva l'adozione di un'apposita politica di risk management, diretta a individuare ex ante le aree aziendali maggiormente esposte al rischio (effettuando una cosiddetta "mappatura dei rischi") e a rafforzare le aree più "deboli" attraverso l'introduzione di opportuni aggiustamenti organizzativi, anche nella forma di protocolli comportamentali. Il Treadway Report rivolse, inoltre, una serie di raccomandazioni ai soggetti coinvolti, a vario titolo, nei processi di predisposizione e controllo dell'informativa economico-finanziaria segnalando l'importanza dell'ambiente di controllo, dei codici di comportamento, della competenza e dell'operatività dei comitati di auditing, nonché della presenza di una funzione di revisione interna attiva e obiettiva.[12]

Prese vita così nel 1992, il rapporto finale intitolato "Internal Control: Integrated Framework", più noto come CoSO Report, oggi nell'aggiornamento 2013, che dopo aver rilevato che l'assenza di una univoca definizione di controllo interno aveva determinato confusione e malintesi tra i vari soggetti interessati alle relative procedure, ne delineò per la prima volta le caratteristiche fondamentali, in vista della creazione di un modello di riferimento per imprese e altre organizzazioni complesse.

[12] G.Gasparri, "I controlli interni nelle società quotate", 2013

Il controllo interno, in base alla definizione proposta dal CoSO, è un processo (che coinvolge CdA, dirigenti e altri operatori dell'organizzazione aziendale) finalizzato a fornire ragionevole garanzia circa il perseguimento degli obiettivi aziendali in relazione ai seguenti aspetti[13]:

1. Conformità a leggi, normative e contratti;
2. Affidabilità e integrità del bilancio e delle informazioni;
3. Salvaguardia del patrimonio;
4. Efficacia ed efficienza delle operazioni

In modo non dissimile, Bankitalia definisce il sistema dei controlli interni come l'insieme delle regole, delle funzioni, delle strutture, delle risorse, dei processi e delle procedure che mirano ad assicurare il conseguimento delle seguenti finalità[14]:

1. Verifica dell'attuazione delle strategie e delle politiche aziendali;
2. Contenimento del rischio (Risk Appetite Framework "RAF")
3. Salvaguardia del valore delle attività e protezione dalle perdite;
4. Efficacia ed efficienza dei processi aziendali;
5. Affidabilità e sicurezza delle informazioni aziendali e delle procedure informatiche;
6. Prevenzione del rischio di commissione e coinvolgimento, anche involontariamente, in attività illecite;
7. Conformità delle operazioni con la legge, nonché con le politiche, i regolamenti e le procedure interne.

[13] L.Marchi, "Revisione aziendale e sistemi di controllo interno", 2012, Giuffrè

[14] L.Marchi, "Revisione aziendale e sistemi di controllo interno", 2012, Giuffrè

Il SCI è dunque uno strumento utilizzato nella gestione, costruito ed implementato "nell'impresa" e non "sull'impresa".

2.3.L'analisi del SCI

Il sistema di controllo interno può essere analizzato prendendo i considerazione diversi aspetti che lo caratterizzano, ovvero:

1. Gli elementi di struttura (ambiente di controllo e processi informativi e di comunicazione);
2. Gli elementi di processo (valutazione dei rischi, interni ed esterni, economici o extra-economici), e definizione delle attività di controllo e monitoraggio);
3. L'aspetto oggettivo dato dall'analisi delle metodologie applicate dagli organi di controllo interno per la valutazione dei rischi, la definizione delle attività di controllo e dall'audit del SCI attraverso i processi di monitoraggio;
4. L'aspetto, detto soggettivo,che riguarda l'esame degli organi interni all'azienda e delle funzioni ad essi attribuite in relazione ai controlli interni e comprende anche l'esame degli organi esterni deputati a valutare e vigilare sulla correttezza di comportamento e sull'efficacia dei processi adottati dagli organi di controllo interno.

Approfondendo l'analisi delle componenti del SCI in modo più specifico, esse si possono raggruppare in 5 elementi interdipendenti ed implementati l'uno con l'altro, che sono:

1. L’ambiente di controllo, costituito dal contesto aziendale e dai soggetti che operano nell’organizzazione con i loro valori, le loro competenze e la loro integrità, concorrendo così a dare affidamento all’organizzazione dell’azienda.
2. L’informazione e la comunicazione, fondamentali per avere una corretta gestione dell’informazione al fine di una corretta attività operativa e di controllo aziendale.
3. L’identificazione e valutazione dei rischi, al fine di individuare le attività di controllo sulla base del processo di gestione dei rischi riscontrato.
4. L’attività di controllo, che concerne le politiche e le procedure che vengono elaborate ed applicate con lo scopo di garantire l’efficace attivazione dei provvedimenti ritenuti necessari dal management per ridurre i rischi connessi al raggiungimento degli obiettivi.
5. Il monitoraggio, il quale rappresenta l’attività di verifica posta in essere per testare il corretto funzionamento del SCI, al fine di reagire prontamente alle sollecitazioni che il contesto competitivo presenta.[15]

Nella valutazione complessiva di queste componenti rientra anche l’analisi del sistema informativo aziendale, in quanto esso costituisce sia un elemento oggetto di controllo, sia uno strumento per il controllo stesso attraverso le numerose attività che possono essere effettuate mediante il suo coretto utilizzo.Il sistema di controllo interno deve essere ispirato a dei principi di controllo che assumono valenza generale e sono utili per impostare un efficace e solido SCI. Il primo principio attiene alla verifica della coerenza, della congruità e tracciabilità delle operazioni che devono essere accompagnate ognuna da un adeguato supporto documentale su cui si possa procedere

[15] L.Marchi, "Revisione aziendale e sistemi di controllo interno", 2012, Giuffrè

in ogni momento all'effettuazione di controlli che attestino le caratteristiche e le motivazioni dell'operazione ed individuino i responsabili di autorizzazioni, registrazioni e verifiche riguardanti le operazioni stesse.

Il secondo principio riguarda la separazione dei compiti, infatti un processo non deve essere sotto il controllo e la responsabilità di un unico soggetto. Lo svolgimento delle attività richiede un controllo preventivo, l'esecuzione della stessa ed eventualmente un controllo successivo, e tutte queste attività di controllo devono essere eseguite da soggetti differenti. Per fare sì che ciò avvenga e quindi che il principio di separazione dei compiti funzioni correttamente, è necessario che le autorizzazioni all'effettuazione delle operazioni siano sotto la responsabilità di soggetti differenti rispetto a chi si occupa degli aspetti contabili, esegue operativamente o controlla l'operazione stessa, e che i poteri e le responsabilità siano chiaramente definite e conosciute all'interno dell'organizzazione e coerenti con le responsabilità organizzative assegnate.

Il terzo principio necessario al buon funzionamento del SCI è che quest'ultimo deve documentare l'effettuazione dei controlli, anche quelli di supervisione, affinchési possa sempre rilevare i responsabili dei controlli e anche eventuali responsabilità riguardanti la sottovalutazione di alcuni rischi eventualmente emersi (Ovviamente i controlli dipendono fortemente dalle specificità e dall'ambiente peculiari di ogni singola azienda).L'ultimo principio da prendere in considerazione è che deve essere presente una corretta definizione dei flussi di comunicazione tra i diversi soggetti, prevedendo una corretta distribuzione delle informazioni tra i soggetti che svolgono le diverse attività e per quanto riguarda la definizione di quali comunicare e con quali modalità farlo.

Per quanto riguarda le dimensioni del sistema di controllo interno si possono distinguere due dimensioni, una cosiddetta "informativa" e un'altra definita "organizzativa"[16]. La prima riguarda l'adeguata documentazione a supporto dei controlli, i controlli di dettaglio (volti ad individuare incongruenze tra i dati, confrontando informazioni elementari ed individuando eventuali eccezioni) e controlli di coerenza (effettuati dal confronti tra aggregati di informazioni e coerenza con le aspettative di risultato prefissate). Considerando invece la dimensione "organizzativa" quest'ultima interessa la suddivisione dei compiti (ovviamente nel rispetto del principio di separazione), i processi di comunicazione, che devono essere conformi ai bisogni degli utenti ed alla tempistica preventivata, e infine l'ambiente organizzativo, che comprende tutto l'aspetto concernente le responsabilità, le deleghe, lo stile di leadership e così via.Volendo quindi riassumere quelli che sono gli aspetti della gestione aziendale che più riguardano il SCI si possono indicare[17]:

1. Organizzazione aziendale e delega delle responsabilità
2. Disegno dei processi aziendali e relativo quadro normativo
3. Pianificazione della strategia aziendale
4. Programmazioneoperativa e Budgeting
5. Controllo di gestione e sistema valutativo
6. Bilancio e contabilità
7. Sistema informatico e comunicazionale (che è una componente del più ampio sistema informativo)

[16] L.Marchi, "Revisione aziendale e sistemi di controllo interno", 2012, Giuffrè

[17] L.Marchi, "Revisione aziendale e sistemi di controllo interno", 2012, Giuffrè

8. Sistema di sicurezza fisica e logica (anchequest'ultimo aspetto può ricadere nell'ambito del sistema informativo)
9. Risk management

Infine, si può concludere l'analisi del SCI verificando chi sono i soggetti principalmente coinvolti nel processo, sia esterni che interni e vedendo le forme che il suddetto sistema può assumere.Tra i soggetti coinvolti a livello interno si possono trovare i vertici aziendali per i controlli di vertice, il CdA e l'amministratore delegato sempre per quanto riguarda i controlli che coinvolgono gli aspetti chiave della gestione, il collegio sindacale e il revisore interno, ove presente, per quanto riguarda la compliance e gli aspetti contabili e infine ove presente il comitato per i controlli interni e rischi. A livello di soggetti esterni troviamo gli enti di vigilanza e il revisore legale o le società di revisione.In ultima analisi, trattando ora delle forme che il SCI può assumere, nelle fattispecie aziendali più comuni si rilevano tre tipologie che sono adottate a seconda della dimensione aziendale: il SCI informale, dato da controlli blandi e non molto strutturati, con scarse procedure presenti soprattutto nelle imprese di minori dimensioni, il SCI di tipo formale manuale, dato cioè da un insieme di controlli e procedure standardizzati ma senza l'ausilio di un adeguato sistema informativo, perciò si rinvengono spesso in aziende di dimensioni superiori a quelle che adottano un sistema informale oppure in aziende che mirano a crescere ma che ancora non hanno sufficiente capacita economia per approntare un sistema informatico adeguato. L'ultima tipologia di SCI è quello cosiddetto formale informatico, che presenta un sistema di controlli ben definiti, strutturati ed organizzati coadiuvati (a differenza della precedente forma) da un sistema informativo che supporta e irrobustisce l'affidabilità, efficacia e l'efficienza di

tutto il sistema, rendendo così questa forma quella tipicamente adottata dalla grande impresa.

Capitolo 3: Audit del Sistema di Controllo InternoInformativo

3.1. I rischi ed obiettivi dell'audit

Il processo di revisione del sistema di controllo interno è uno degli aspetti fondamentali nell'ambito delle attività svolte dal revisore o dalle società di revisione, in quanto sedal lato delle imprese un efficace SCI permette all'azienda stessa di fornire valide assurances durante la revisione , per chi effettua la revisione invece permette , pur verificandone sempre il corretto funzionamento, di avere un valido supporto di dati ed informazioni utili per eseguire al meglio e nel minor tempo possibile tutte le procedure previste per il processo di revisione. Come emerge dai precedenti capitoli, poiché si è avuta una progressiva estensione del sistema informativo a quasi tutti i processi aziendali, quest'ultimo è una componente fondamentale del sistema di controllo interno. Il sistema informativo aziendale, diventa quindi il depositario di tutte le informazioni gestite dall'azienda. Alla luce di tutto questo, è inevitabile per il revisore, nella fase di esame del sistema di controllo interno, procedere con la raccolta di informazioni su quest'ultimo. Pertanto nel processo di revisione si dovranno effettuare opportuni controlli volti a verificarne il corretto funzionamento (presupposto necessario qualora il revisore intenda fare affidamento anche su questa risorsa) al fine di poter esprimere in giudizio adeguato in merito al SCI.

In conformità a quanto previsto dal principio di revisione nr. 400 "la valutazione del rischio il sistema di controllo interno", il revisore deve "...valutare l'ambiente

informatico nel pianificare le procedure di revisione al fine di ridurre i rischi ad un livello accettabile".

Infatti numerose caratteristiche peculiari dei sistemi informativi influiscono fortemente sull'attività di audit del sistema di controllo interno, questo perché se la maggiore affidabilità di tali sistemi riduce infatti la frequenza di manifestazione dei rischi, è però necessario considerare che l'impatto dell'eventuale manifestazione di tali rischi può essere estremamente gravosa, proprio in considerazione dell'integrazione del sistema informativo nei vari processi aziendali.L'automazione e l'integrazione propria di questi sistemi infatti comporta numerosi effetti sui processi aziendali che non possono essere trascurati nell'analisi e nella revisione del SCI. In particolare il sistema informativo assume il ruolo di "integratore" delle diverse attività che concretizzano i processi.[18]

Come conseguenze di questa integrazione si hanno il sorgere di nuovi rischi ma anche la presenza di elementi che rafforzano l'efficacia del sistema di controllo interno. Per quanto riguarda i rischi, L'analisi del rischio consiste nella valutazione sistematica di tutti i fattori di rischio individuati

Normalmente la modalità più diffusa consiste nell'attribuzione di un coefficiente qualitativo (alto, medio, basso), che classifica l'importanza di ogni fattore e di ogni classe di fattori. Il revisore verifica il grado di correttezza con cui determinate informazioni forniscono adeguata rappresentazione di una specifica realtà aziendale. Un'informazione può considerarsi attendibile qualora, dal suo confronto con altri dati rappresentativi della medesima realtà, emerga una sostanziale, precisa e univoca concordanza.

[18]F.Bava, "L'audit del sistema di controllo interno", 2004, Giuffrè

Il giudizio di attendibilità del sistema informativo è spesso un giudizio probabilistico.

Infatti la numerosità di sistemi di rilevazione non garantisce la qualità delle informazioni ottenute in mancanza di un'adeguata suddivisione organizzativa del lavoro tale per cui i diversi sistemi di rilevazione siano gestiti da operatori sostanzialmente differenti. Lo strumento principale è la separazione dei ruoli, rappresentata dal ciclo autorizzazione – esecuzione – controllo.

Lo scopo del lavoro di rilevazione del sistema IT aziendale è quello di fornire una review ad alto livello del sistema informativo dell'azienda, evidenziando i cambiamenti avvenuti in corso di attuazione.

I principali rischi sono: la possibile alterazione dei programmi o dei dati, la scorretta applicazione del principio di separazione dei compiti, un'eccessiva delega ai tecnici informatici potrebbe far sì che si attribuiscano ad essi anche compiti no pertinenti alle loro competenze e responsabilità ed anche la possibilità che eventuali errori di digitazione abbiano un forte impatto economico a causa dell'integrazione.Nelle aziende caratterizzate da un intenso utilizzo dei sistemi informativi quindi è necessario poter riporre la massima fiducia nel personale tecnico che può accedere ai dati, al fin di ridurre il rischio di comportamenti scorretti; perciò l'integrazione del sistema informativo procura sul sistema di controllo degli effetti riguardanti le procedure da adottare, come ad esempio le autorizzazioni, che in genere sono concesse tramite dei codici. Il rischio in questo caso è dato dalla possibilità che soggetti non autorizzati si procurino i codici necessari. Per evitare e ridurre rischi di questo tipo è importante che il sistema sia implementato in maniera corretta, perché se così è, genera importanti benefici al sistema di controllo interno, consentendo di eliminare numerose attività di inserimento di medesimi dati grazie alle procedure di condivisione delle basi dati e

collocare le attività di rilevazione nel momento in cui i relativi dati nascono riducendo così gli errori.Inoltre ulteriori rischi per i sistemi di controllo interno che sorgono dall'integrazione con i sistemi informativi sono dati da tutti quegli aspetti che oltre ad essere internamente integrati in un sistema sono anche integrati con sistemi esterni(web) come i vari processi di Customer Relationship Management o la Supply Chain Management o ancora le vendite tramite E-commerce. In tutti questi ambiti, il rischio principale cui deve far fronte il SCI è dato dalla adeguata gestione della sicurezza dei sistemi adottati; anche qui però di contro si hanno importanti benefici se il sistema è approntato correttamente come ad esempio la riduzione di errori di trascrizione dei dati degliacquirenti (che nel caso di vendite tramite e-commerce inseriscono autonomamente) o la possibilità di essere sempre in contatto con clienti e fornitori per qualsiasi tipo di esigenza organizzativa.A seguito di questo processo di integrazione interna ed esterna dei sistemi informativi, l'Institute of Internal Auditor ha messo a punto un modello denominato eSAC (Electronic Systems Assurance and Control), che ha indicato gli obiettivi del sistema di controllo interno nei contesti aziendali caratterizzati dall'e-business e dall'uso di sistemi informativi strutturati, che principalmente deve verificare:

1. La garanzia della disponibilità delle informazioni.
2. La capacità del sistema di portare a temine le transazioni (Operatività).
3. La capacità del sistema non soltanto di elaborazione ma anche di facilità d'uso ed efficacia della comunicazione sistema-utente (Funzionalità).
4. La protezione del sistema informativo e cioè dei dati, del software e dell'hardware (Proteggibilità)

5. La capacità di identificare ed autenticare i soggetti che attivano le transazioni (Accountability e Auditability).

Per quanto concerne il processo di audit del sistema di controllo interno informativo aziendale, si deve specificare che il sistema è spesso esposto a numerosi rischi che come precedentemente esposto principalmente riguardano i malfunzionamenti e le violazioni di sicurezza. Perciò le attività di controllo dei sistemi informativi, che si devono effettuare in fase di revisione, sono generalmente distinte in due tipologie: controlli generali (o di struttura) e controlli applicativi (o di processo).[19]I controlli generali riguardano l'ambiente di elaborazione delle informazioni, l'architettura del sistema informativo e le risorse dedicate, mentre i controlli applicativi riguardano le transazioni poste in essere dal sistema. Tra i controlli generali è possibile considerare anche i controlli finalizzati a garantire la sicurezza fisica del sistema informativo.

3.2.I controlli generali

I controlli generali catalogabili in quattro categorie:

1. Controlli organizzativi: come nel tradizionale sistema di controllo senza utilizzo di sistemi infirmativi l'organizzazione delle mansioni e dei compiti deve prevedere una separazione di questi ultimi, definendo bene le responsabilità e i ruoli degli operatori, dei tecnici e dei vari sistemi che si integrano; a livello operativo ciò è possibile tramite la predisposizione di profili di accesso e password dedicate.

[19]F.Bava, "L'audit del sistema di controllo interno", 2004, Giuffrè

2. Controlli sullo sviluppo e modifica dei sistemi: nello sviluppo dei diversi programmi, deve essere predisposta un'adeguata documentazione per consentire di essere verificati. Ovviamente tra questa tipologia di controlli ci sono anchequelli volti a verificare che gli sviluppi o le modifiche siano state correttamente autorizzate. Inoltre nel caso di sviluppo o modifica di software questi devono essere testati in un apposito ambiente di testing prima di essere inseriti nel sistema aziendale.
3. Controlli dell'hardware e del software di sistema: in questo caso di solito le procedure di verifica del corretto funzionamento del sistema informativo sono predefinite dalle case produttrici dell'hardware e dei software operativi. Però "i controlli che vengono effettuati servono a garantire che l'azienda esegua le istruzioni di programma in modo appropriato e corretto."[20] Queste verifiche possono essere operativamente svolte analizzando il "log", cioè i file che contengono le informazioni sulle diverse attività svolte dal sistema.
4. Controlli sulla sicurezza e sulle procedure: va precisato che le minacce al sistema informativo possono derivare da fattori umani o naturali. Tra i primi si possono ricomprendere gli eventi accidentali da quelli volontari, quelli interni da quelli esterni. La tendenza negli ultimi anni è di un graduale aumento degli attacchi esterni grazie alla maggiore interconnessione dei sistemi rispetto agli atti di sabotaggio interni, denotando così un'inversione di tenenza rispetto al passato. Le minacce naturali sono rappresentate da varie eventi catastrofici come alluvioni, terremoti e così via che possono danneggiare o distruggere le componenti fisiche del sistema informativo oltre che compromettere la

[20]F.Bava, "L'audit del sistema di controllo interno", 2004, Giuffrè

continuità dell'attività aziendale stessa. In concreto proteggere le informazioni significa definire tre tipologie di rischi che riguardano il livello ritenuto accettabileche un soggetto non autorizzato riesca ad accedere al sistema (Riservatezza), il livello di rischi accettabile di perdita o modificazione delle informazioni (Integrità) e infine il livello accettabile di inaccessibilità alle informazioni o ai dati causato da cause esterne come blackout, attacchi hacker, ecc…(Disponibilità). Una volta definiti i livelli accettabili di rischio, l'impresa deve pianificare gli interventi volti a ridurre o mantenere sotto tale soglia i rischi, tenendo in considerazione i costi, il decadimento fisiologico delle prestazioni del sistema e l'eventuale aumento della "burocrazia" necessario per gestireunsistema di controllo più complesso. Inoltre l'azienda deve garantire un sistema di protezione fisica e un'infrastruttura adeguate per evitare accessi indesiderati, ridurre i danni da eventi naturali ed evitare accessi fisici non autorizzati nei locali ospitanti l'hardware del sistema informativo. Tra le procedure che è possibile adottare si possono annoverare, a titolo di esempio, il blocco degli accessi dopo un certo numero di tentativi falliti, l'adozione di procedure di backup adeguate, i firewall, o predisporre test di vulnerabilità al fine di verificare la resistenza e la solidità del sistema informativo approntato. Il revisore deve accertare i livelli di rischio e verificare che le procedure attuate dall'impresa siano adeguate e conformi al sistema informativo adottato ed eventualmente per gli aspetti di carattere più tecnico avvalersi del supporto di un esperto competente in materia.

3.3. I controlli applicativi

A differenza dei controlli generali, questa tipologia di controlli riguarda l'attività svolta dal sistema informativo. Tali controlli si propongono infatti di contribuire ad assicurare che le diverse transazioni siano autorizzate, correttamente classificate, processate e oggetto di reporting. Al revisore spetterà poi il compito di valutare l'adeguatezza di questi controlli che l'azienda pone in essere (ove presenti) ed eventualmente rieseguirli, in modo da formarsi un giudizio in merito all'affidabilità del sistema informativo e quindi del sistema di controllo in generale, ove questo sia gestito principalmente da quello informativo.

Riprendendo e approfondendo la trattazione già accennata nel capitolo sui sistemi informativi, si possono individuare tre tipi di controlli che solitamente si effettuano:

1. Controlli sugli input: questi controlli riguardano l'immissione dei dati o dei documenti nel sistema informativo. La validità delle transazioni deve essere accertata attraverso la verifica della presenza delle autorizzazioni, che consistono nella richiesta di una password conosciuta solo dagli autorizzati. La corretta immissione può essere verificata confrontando i documenti originali dai quali si traggono i dati con i tabulati dell'immissione stessa o predisponendo un software che segnali le deviazioni dallo standard per quella tipologia di dati.
2. Controlli sul trattamento/elaborazione dei dati:sono finalizzati ad assicurare la corretta elaborazione dei dati. Possono consistere in diverse attività utilizzate anche nel trattamento manuale dei dati, come controlli incrociati, riconciliazioni e verifica della presenza dei segni di ricevuta. Infatti un adeguato sistema di

controllo prevede che il sistema informativo sia in grado di generare documenti di audit che descrivano tutte le operazioni effettate nella fase di elaborazione dei dati in modo da consentire la verifica del percorso nelle singole transazioni.

3. Controlli sull'output: prima di procedere nel merito dei controlli, va precisato che l'output può consistere o in un documento cartaceo o in uno elettronico (file) e la verifica della correttezza e delle autorizzazioni è ovviamente necessaria in entrambi i casi. I controlli consistono della verifica che il documento prodotto sia rispondente a quelli richiesti e che i dati che vi sono inseriti siano effettivamente quelli che vi dovevano essere.

3.4. I controlli specifici

I controlli specifici sono quei controlli predisposti nell'ambito delle singole procedure informativo-contabili, al fine di fornire una ragionevole sicurezza che la registrazione dei dati e la produzione dei risultati siano correttamente eseguite.[21]

Questi controlli riguardano direttamente il processo di formazione di una singola voce di bilancio e possono essere raggruppati in rapporto agli aspetti di elaborazione automatica dei dati:[22]

[21]F.Bava, "L'audit del sistema di controllo interno"

[22] Si veda in merito il documento n. 3.2 dei principi di revisione statuiti dai Consigli nazionali dei dottori commercialisti e dei ragionieri.

1. Controlli sui dati in entrata,che vengono adottati per fornire una ragionevole sicurezza che i dati ricevuti per essere elaborati siano preventivamente autorizzati, siano correttamente convertiti e non siano eliminati o alterati.
2. Controlli sulle elaborazioni,i qualivengono invece adottati per avere una ragionevole sicurezza che l'elaborazione avvenga correttamente e conformemente alle procedure approvate.
3. Controlli sui risultati,che servono per fornire una ragionevole sicurezza che i risultati prodotti siano corretti e coerenti con i precedenti che vengono consegnati solo al personale autorizzato.

Per esprimere un giudizio sul sistema gestionale (che appunto è la componente informativo-contabile del più generale sistema informativo), il revisore deve verificare i diversi aspetti dell'accuratezza ed efficienza nel trattamento dei dati e dell'efficacia del sistema informativo in rapporto alle possibili utilizzazioni gestionali. Per fare ciò il revisore verifica tutto il processo, dalla rilevazione iniziale e quello della utilizzazione finale, valutando la natura e l'estensione dei controlli posti in essere, nonché della loro tipologia, con un occhio di riguardo per le procedure di immissione dei dati, di segnalazione e correzione degli errori, perché sono due delle fasi più critiche per quanto attiene al controllo interno. Oltre alla verifica poi dei processi messi in atto, il revisore deve anchestimare l'affidabilità ed efficacia del sistema di controllo interno informativo, andando a valutare:

1. Rilevanza: relativa alla significatività del dato in rapporto alla gestione completiva della redazione ad esempio della contabilità o di altri processi aziendali.
2. Selettività: il sistema deve fornire e selezionare solamente i dati utili per i vari centri decisionali e operativi.
3. Integrazione: raggruppamento dei dati contabili in serie o gruppi significativi (ad esempio per processi produttivi o intervalli temporali) e comparazione dei dati consuntivi con quelli preventivi.
4. Tempestività: capacità del sistema di fornire le informazioni necessarie in tempo utile in relazione alla loro natura ed al livello decisionale interessato con lo scopo di permettere un'adeguata organizzazione e pianificazione e controllo dei fenomeni aziendali.
5. Flessibilità: capacità del sistema di adattarsi rapidamente al mutare delle esigenze informative e delle tecniche di produzione e distribuzione delle informazioni.
6. Accuratezza: grado di approssimazione dei dati forniti ritenuto accettabile.
7. Verificabilità: capacità del sistema di essere verificabile in rapporto all'accuratezza dei dati ed all'affidabilità delle funzioni di raccolta, selezione, classificazione, elaborazione, memorizzazione e utilizzazione dei dati.
8. Accettabilità: capacità del sistema di garantire l'accettabilità del sistema di controllo interno, nelle sue procedure e flussi infirmativi, da parte di tutti i soggetti coinvolti nel trattamento e nella comunicazione dei dati,

prevendendo tutte le possibili reazioni e rimuovendo gli ostruzionismi e i meccanismi di resistenza passiva; per fare ciò è necessario che siano chiariti compiti, responsabilità e ruoli all'interno dell'organizzazione.

Conclusione

Il grado di affidabilità del sistema interno di controlli delle aziende, e quindi anche del sistema informativo che supporta tale sistema, ha un notevole impatto sull'ampiezza e sul livello di approfondimento della revisione dei conti. Se per le imprese di grandi dimensioni solitamente l'affidabilità è maggiormente garantita in virtù della maggiore articolazione organizzativa che esse possiedono, più complicata è la situazione per le piccole e medie imprese, dove l'attività di controllo non è formalizzata. In entrambi i casi, un sistema giudicato affidabile dal revisore riduce l'attività di controllo legale dei conti.Le imprese di grandi dimensioni infatti dispongono, per loro natura, di un articolato e strutturato sistema di controllo interno indispensabile per supportare lo sviluppo aziendale, permettendo l'esame delle minacce e delle opportunità provenienti dall'ambiente esterno nonché l'analisi del mercato di riferimento e il confronto con i competitor.Le relazioni tra revisione legale dei conti e attività di controllo interno assumono particolare rilevanza nel caso delle piccole e medie imprese e ancora di più nelle micro-imprese. Infatti se da una parte si è rilevato come l'attività di revisione legale dei conti possa essere agevolata e migliorata in termini di fluidità delle procedure e dei processi nelle ipotesi in cui vi sia un affidabile sistema di raccolta, elaborazione e rappresentazione delle operazioni di gestione, si pongono consistenti problemi nell'ipotesi in cui, invece, le procedure non siano ritenute dal revisore fluide, articolate ed affidabili. Qualora il revisore ritenga che i processi siano affidabili, le procedure di analisi delle informazioni aziendali possono essere ridotte mentre, al contrario, quando le procedure sono ritenute caratterizzate da carenze, il professionista dovrà ampliare l'operatività della propria azione oltre a confrontarsi con la direzione aziendale per

evidenziare tali eventuali carenze operative e di natura procedurale e per le quali non vi era consapevolezza da parte della struttura aziendale.Nel caso in cui i controlli e le procedure interne siano ritenuti inefficaci oppure nell'ipotesi in cui questi non siano applicati o applicati correttamente, il revisore illustra alla direzione le criticità riscontrate ed i punti di intervento formalizzandole, nelle realtà di maggiore dimensione nella lettera di suggerimenti (management letter). Con questo processo di influenza reciproca tra l'attività di revisione e quella di controllo interno, l'attività di controllo legale dei conti contribuisce al miglioramento delle performance aziendali. Nell'ambito di questo processo il revisore inoltre completa la propria conoscenza dei processi interni e conclude l'acquisizione delle informazioni aziendali.Le relazioni tra revisione dei conti e sistema di controllo interno si presentano con maggiore e più ampia delicatezza nelle piccole e medie imprese all'interno delle quali il sistema di controllo interno non è formalizzato oppure ci si trova in contesti in cui tutte le funzioni di natura gestionale e manageriale sono concentrate nelle mani dell'imprenditore che spesso non possiede le opportune competenze per poter creare e gestire un sistema di controllo interno.Anche per le piccole e medie imprese è indispensabile adottare un approccio alla pianificazione e al controllo dei risultati programmando le azioni da intraprendere per raggiungere determinati obiettivi di economicità e redditività. Quanto sopra evidenziato trova, però, nel contesto delle PMI alcuni fattori che ne limitano la diffusione. Le PMI dispongono, infatti, di minori risorse umane da dedicare a tali attività dimenticando che la mancata destinazione di tali risorse a tale attività crea una potenziale forma di rischio che rende più complicato e rischioso il compito del revisore.Con l'ampliamento degli obblighi di revisione anche alle società a responsabilità limitata di minore dimensione è difficile immaginare che "nelle realtà in cui il volume dei ricavi sia, ad esempio, di poco

superiore ai due milioni di euro si possa pensare che ci sia un articolato ed efficace sistema di controllo interno a supporto della gestione aziendale e anche delle attività di revisione." [23]La disponibilità di strumenti di controllo interno contribuisce, dunque, a ridurre il rischio di revisione e si riflette, ulteriormente, sul miglioramento della gestione aziendale e dei risultati in termini di maggiore consapevolezza circa gli effetti benefici che si possono ottenere da un efficace ed efficiente sistema di controlli dei risultati e delle performance aziendali.La revisione legale dei conti può, dunque, rappresentare un ulteriore motore di cambiamento della realtà aziendale e di adeguamento verso un mutato contesto operativo settoriale e di mercato favorendo la sensibilità circa i benefici che il sistema gestione dei controlli ed il supporto di un adeguato sistema informativo produce sui risultati complessivi aziendali. Un sistema di controllo interno ritenuto affidabile dal revisore contribuisce a ridurre e a semplificare l'attività di controllo legale dei conti e contemporaneamente, l'attività di revisione calata nel contesto aziendale, concorre a innescare un sistema positivo a favore dei sistemi di pianificazione e controllo grazie alla visione esterna che il revisore può offrire in termini di adeguatezza degli stessi. Tutto ciò assume un'esponenziale valenza strategica nel caso specifico delle PMI, per le quali i sistemi di programmazione e controllo, laddove presenti, assumono caratteri basilari di estrema semplicità e articolazione.

[23]Fabio Sansalvadore, membro del Cda della Fondazione Centro Studi UNGDC

Bibliografia:

- Kenneth C. Laudon, Jane P. Laudon, Vincenzo Morabito, Ferdinando Pennarola, “Management dei sistemi informativi", 2006, Pearson
- L.Marchi, "Revisione aziendale e sistemi di controllo interno", 2012, Giuffrè
- F.Bava, "L'audit del sistema di controllo interno", 2004, Giuffrè

Ringraziamenti

Eccomi giunto alla fine di questo percorso: sono tante le conoscenze che ho fatto, le amicizie che ho coltivato ed i rapporti che ho stretto. È stato un periodo di profondo apprendimento, non solo a livello scientifico, ma anche personale. Vorrei dedicare queste ultime pagine per ringraziare tutte le persone che mi hanno sempre sostenuto, aiutato e che hanno sempre creduto in me durante questo periodo.

In primis vorrei ringraziare il prof. Marco Giuliani, relatore di questa tesi di laurea, oltre che per l'aiuto fornitomi in tutto questo periodo e la grande conoscenza che mi ha donato, per la disponibilità, precisione, competenza e professionalità dimostratemi durante tutto il periodo di stesura e che senza le quali non sarebbe stato possibile completare questo lavoro. La ringrazio.

Vorrei ringraziare la mia famiglia, i miei genitori, mia sorella Chiara, i nonni, gli zii ed i cugini, in particolare Paolo, Francesco e Samuele. Grazie per i loro saggi consigli e la loro capacità di ascoltarmi, oltre che a fornirmi il sostegno morale necessario per arrivare fino a questo traguardo. Sono sempre stati al mio fianco e so che continueranno ad esserci. Vi voglio bene. Grazie.

Un ringraziamento va a lei,Champa, la mia meravigliosa ragazza, perché ha sempre creduto in me, mi ha supportato e sopportato durante tutti questi anni, e ha saputo farlo sempre nel migliore dei modi, donandomi sempre tempo, parole, amore, sorrisi e abbracci e voglia di sognarequando ne avevo bisogno e senza i quali non avrei mai raggiunto questo traguardo. Grazie amore.

Per ultimi ma certamente non meno importanti, ringrazio di cuore anche i miei amici. Gli amici di sempre, Giovi, Piglio ed Ale, che ci sono sempre stati in ogni momento, dal passare una serata in compagnia al condividere e confidarsi le cose più intime e so che ci sarete sempre.Vi voglio bene ragazzi. Grazie.

Ringrazio i compagniconosciuti durante questo percorso, ormai diventati amici, Nico, Riccà, Nobbi, Simo, Stecco e Cristian, che hanno reso piacevole ogni giornata, anche quelle con le lezioni più noiose. Grazie.

Ringrazio anche inuovi amici Davide, Nicola, Gianna, Maila, Lorè, Somy ed Emily, che ho conosciuto grazie a quella straordinaria famiglia che è il coro di Sant'Agostino, che ogni giovedì sera mi hanno fatto divertire e staccare la spina dallo studio e che si sono rivelate persone meravigliose e che sono contento di chiamare amici. Grazie Fishpallas.

Grazie alla famiglia del Follerau, in particolare a tutti i ragazzi e tutti i volontari. Mi avete dato forza e donato serenità anche nei periodi più stressanti e difficili. Grazie ai volontari perché ci sono sempre nei momenti del bisogno e grazie ai ragazzi, perché sanno sempre come rendere felice una persona, con la lorosemplicità, i loro sorrisi e i loro abbracci. Ringrazio in particolare Leo,amico e compagno di mille sfide ad Uno, ti voglio bene. Vorrei anche ringraziare tre stelle che brillano sopra al cielo, Gianluca, Elisa ed Emilio, angeli che sono andati via troppo presto e che mi hanno insegnato tanto grazie ai loro esempi. Grazie.

Ringrazio anche i ragazzi del gruppo Tourette, perché vedendoli ogni sabato, mi hanno fatto capire che credendo nei propri sogni, anche a volte con la spensieratezza di un ragazzino, si possono raggiungere grandi traguardi e questa tappa che ho raggiunto è

anche merito loro. Grazie inoltre anche a Ross che oltre ad essere una grande persona mi ha dimostrato come, se ci si crede veramente, ci si può sempre mettere in gioco. Grazie.

Grazie anche a tutti quelli che fanno parte della mia vita che in un modo o nell'altro mi sono stati vicini durante questo periodo o che comunque mi hanno reso in parte quello che sono ora, nello specifico, volevo ringraziare Pietro, Fra,Enrico e Riccardo, che seppur, per motivi diversi, ultimamente non li abbia frequentati moltissimo, con ognunodi loro conservo ancora un rapporto speciale e anche questo ha contribuito al raggiungimento di questo percorso. Grazie.

Grazie a tutti, perché ci siamo sempre sostenuti a vicenda, nella buona e nella cattiva sorte, sia durante le fatiche e lo sconforto che hanno caratterizzato questo percorso, che nei momenti di gioia e soddisfazione. Ringrazio tutti perogni momento bello che mi hanno donato e che spero continueranno a donarmi, e li ringrazio per tutti i momenti brutti che mi aiuteranno a superare, questo traguardo è anche, se non soprattutto, merito loro. Vi voglio bene!!!

Federico Pieroni

30/09/19