La revisione legale

Gestione del Rischio e Controllo Interno

Marco Saraceno

Revisore legale

7 giugno 2023

Agenda

Gestione del Rischio e Controllo Interno

- Caratteristiche e definizioni del sistema di controllo interno
- Principali tecniche ed analisi e la valutazione del sistema di controllo interno con particolare focus su piccole e medie imprese («SME»)
- Il controllo interno nei sistemi informatici

Caratteristiche e definizioni del sistema di controllo interno

Riferimenti

- Codice di autodisciplina delle società Quotate in Borsa
- Enterprise Risk Management – Integrated Framework (ERM) del *Committee of Sponsoring Organizations of the Treadway Commission* (COSO)
- Internal Control over External Financial Reporting 2013 del *Committee of Sponsoring Organizations of the Treadway Commission* (COSO)
- Principio di revisione internazionale (Isa Italia) 315 Revised - L'identificazione e la valutazione dei rischi di errori significativi mediante la comprensione dell'impresa e del contesto in cui opera
- Principio di revisione internazionale (Isa Italia) 265 - Comunicazione delle carenze nel controllo interno ai responsabili delle attività di governance ed alla direzione (PdR n. 265)
- Altri Principi di revisione
- Monografia COSO Framework: Guida alla lettura - Assirevi

Quadro definitorio – Il Codice di autodisciplina delle società quotate in borsa

La normativa primaria non fornisce una definizione di sistemi di gestione dei rischi e di controllo interno.
Il quadro definitorio è dato:

- A livello nazionale dal Codice di autodisciplina delle società quotate in borsa;
- A livello internazionale dal COSO nonché dalle *best practice* esistenti.

Le due definizioni non sono in conflitto tra di loro pur osservandosi che il COSO dà maggior enfasi al fatto che il sistema di controllo sia innanzitutto un processo, ovvero un'azione orientata a un fine, mentre il Codice di autodisciplina delle società quotate in borsa attribuisce maggior rilievo alle regole e alla formalizzazione delle procedure.

Quadro definitorio – Il Codice di autodisciplina delle società quotate in borsa

Art. 7 – Principio applicativo 7.P.1

"Ogni emittente si dota di un sistema di controllo interno e di gestione dei rischi costituito dall'insieme delle regole, delle procedure e delle strutture organizzative volte a consentire l'identificazione, la misurazione, la gestione e il monitoraggio dei rischi.

Tale sistema è integrato nei più generali assetti organizzativi e di governo societario adottati dall'emittente e tiene in adeguate considerazione i modelli di riferimento e le best practices esistenti in ambito nazionale e internazionale".

Codice di autodisciplina

Quadro definitorio – Il COSO (1/3)

Nel 2013 il COSO ha pubblicato *Enterprise Risk Management – Integrated Framework (ERM)* e nel 2013 ha aggiornato il *Internal Control over External Financial Reporting* che accresce la capacità dell'azienda di generale valore, consentendo alla Direzione aziendale di affrontare efficacemente le incertezze e i conseguenti rischi e opportunità.

L'ERM è

"un processo, posti in essere dal Consiglio di Amministrazione e dalla Direzione aziendale utilizzato per individuare eventi potenziali che possano influire sul raggiungimento degli obiettivi aziendali per gestire il rischio entro limiti accettabili"

Quadro definitorio – Il COSO (2/3)

Internal control – integrated fram1992)

Il sistema di controllo interno è *"il processo che si prefigge di fornire una ragionevole sicurezza sulla realizzazione degli obiettivi di:*

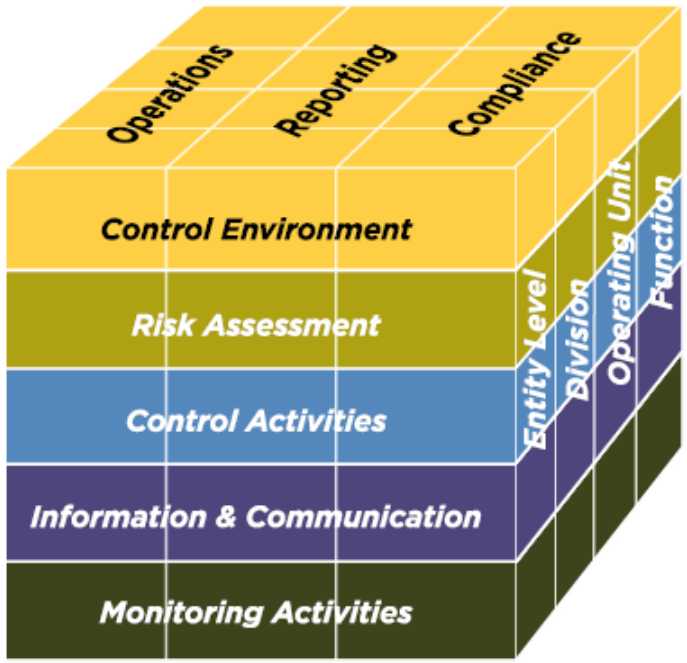
- ***efficacia ed efficienza delle attività operative;***
- ***attendibilità dell'informativa di bilancio;***
- ***conformità alle leggi."***

COSO

Imprese di piccole dimensioni

Sono previste delle indicazioni anche per le imprese di minori dimensioni.

Quadro definitorio – Il COSO (3/3)



LE 5 COMPOENTI DEL COSO

1. • Control Enviroment
   - Definizione dei valori, competenze e responsabilità
2. • Risk Assessment:
   - Identificazione dei rischi e delle opportunità
3. • Control Activities
   - identificazione dei presidi di contenimento e di contrasto dei rischi entro i limiti considerati accettabili.
4. • Information and Communication
   - identificazione dei flussi informativi e comunicativi rilevanti
5. • Monitoring
   - monitoraggio del processo con l'obiettivo di valutare eventuali modifiche/correzioni.

Quadro definitorio - *Best practice* esistenti

Secondo la *best practice* internazionale, gli obiettivi attribuiti al sistema di controllo interno aziendale sono riconducibili ai seguenti presidi:

1. **Economicità** (efficacia ed efficienza) delle operazioni aziendali in conformità alle strategie, obiettivi e politiche aziendali, ai fini anche della salvaguardia del patrimonio aziendale.
2. **Attendibilità** del sistema informativo aziendale, sia per le sue componenti finalizzate alla predisposizione del bilancio destinato alla pubblicazione, sia per quelle finalizzate alla predisposizione del reporting gestionale.
3. **Rispetto della normativa** applicabile all'attività dell'impresa.

Tali obiettivi individuano i seguenti ambiti del sistema di controllo aziendale:

1. Controllo di gestione
2. Controllo amministrativo contabile
3. Controlli di conformità alle leggi

Principali tecniche ed analisi e la valutazione del sistema di controllo interno

Le 5 componenti del controllo interno dell'impresa

Le 5 COMPONENTI del controllo interno dell'impresa sono:

- Ambiente di controllo

- Valutazione del rischio

- Informazioni e comunicazione

- Attività di controllo

- Monitoraggio

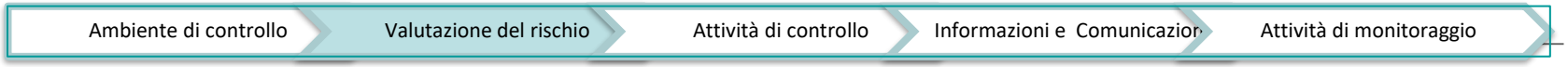
Ambiente di controllo – 1/2

- L'ambiente di controllo fornisce un **fondamento generale per l'operatività delle altre componenti** del sistema di controllo interno.
- L'ambiente di controllo non previene, ne individua e corregge direttamente gli errori. Può tuttavia influenzare l'efficacia dei controlli nelle altre componenti del sistema di controllo interno. Trattasi prevalentemente di **controlli indiretti**.
- Gli elementi probativi per la comprensione della valutazione del rischio da parte del revisore possono essere acquisiti mediante una combinazione di indagine, osservazione ed ispezione di documenti. **Le sole indagini presso il personale dell'impresa non sono tuttavia sufficienti** al fine di valutare che i controlli siano adeguatamente configurati e messi in atto.

Ambiente di controllo – 2/2

- Nelle imprese meno complesse, gli elementi probativi relativi ai diversi aspetti dell'ambiente di controllo possono non essere disponibili in forma documentale, specie laddove **la comunicazione tra direzione e personale sia informale**, ma gli elementi probativi possono tuttavia essere appropriatamente pertinenti e attendibili nelle circostanze.
- Se l'attività di governance e svolta direttamente dal proprietario-amministratore, il revisore può stabilire che l'indipendenza dei responsabili delle attività di governance non sia rilevante.
- E' possibile che le imprese meno complesse non dispongano di un codice di comportamento scritto, ma sviluppino, invece, una cultura aziendale che evidenzi l'importanza dell'integrità e di comportamenti eticamente corretti attraverso la comunicazione verbale e l'esempio della direzione. Gli atteggiamenti, a consapevolezza e le azioni della direzione o del proprietario-amministratore rivestono particolare importanza per la comprensione da parte del revisore dell'ambiente di controllo di un'impresa meno complessa.

Valutazione del rischio – 1/2



→ Gli aspetti che il revisore può considerare nel comprendere le modalità con cui la direzione abbia identificato **i rischi di business rilevanti ai fini della redazione del bilancio** includono le modalità con cui la direzione abbia:

- ✓ specificato gli obiettivi dell'impresa con precisione e chiarezza sufficienti a consentire l'identificazione e la valutazione dei rischi relativi agli obiettivi;
- ✓ identificato i rischi legati al raggiungimento degli obiettivi dell'impresa e analizzato gli stessi per stabilire in che modo dovrebbero essere gestiti;
- ✓ tenuto conto della possibilità di frode nel considerare i rischi legati al raggiungimento degli obbiettivi dell'impresa.

→ Gli elementi probativi per la comprensione della valutazione del rischio da parte del revisore possono essere acquisiti mediante una combinazione di indagine, osservazione ed ispezione di documenti. **Le sole indagini presso il personale dell'impresa non sono tuttavia sufficienti** al fine di valutare che i controlli siano adeguatamente configurati e messi in atto.

Valutazione del rischio – 2/2

→ In alcune imprese meno complesse, ed in particolare nelle imprese gestite dal proprietario-amministratore, una appropriata **valutazione del rischio può essere effettuata mediante il coinvolgimento diretto della direzione** o del proprietario-amministratore (ad esempio, la direzione o il proprietario-amministratore può regolarmente dedicare del tempo a monitorare le attività dei concorrenti e altri sviluppi sul mercato per identificare i rischi emergenti di business).

Ambiente di controllo

→ L'evidenza che tale valutazione del rischio venga effettuata in questa tipologia di imprese spesso non è formalmente documentata, ma **può risultare evidente dalle discussioni che il revisore ha con la direzione** sul fatto che la stessa stia in effetti svolgendo procedure di valutazione del rischio.

Informazione e comunicazione e Attività di controllo – 1/2

- I controlli relativi alle componenti “sistema informativo e comunicazione” e “attività di controllo” sono principalmente controlli diretti (ossia controlli che sono sufficientemente mirati per prevenire, individuare o correggere errori a livello di asserzioni). A tal scopo il revisore è tenuto a:
  - ✓ a **valutare la configurazione**; e
  - ✓ stabilire se **i controlli siano stati messi in atto**.
- La comprensione del «sistema informativo» da parte del revisore include la comprensione delle direttive che definiscono i flussi delle informazioni rilevanti per l’informativa finanziaria. Nell’acquisire una comprensione del modo in cui le informazioni confluiscono, attraversano e fuoriescono dal «sistema informativo» dell’impresa, il revisore può identificare i controlli relativi alla componente “attività di controllo” che e necessario identificare.
- **Quanto più alto è valutato un rischio nello spettro del rischio intrinseco, tanto più persuasivi è necessario siano gli elementi probativi** che possono comprende indagine, osservazione ed ispezione documentale.

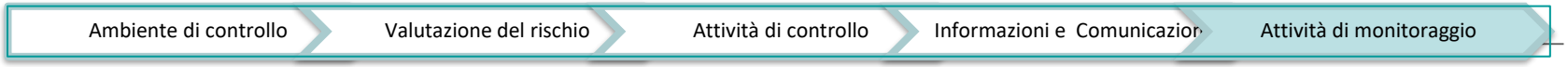
Informazione e comunicazione e Attività di controllo – 2/2

- I **controlli possono essere manuali o nell'ambito dell'ambiente IT**, possono avere diversi obiettivi ed essere applicati a vari livelli organizzativi e funzionali.
- Esempi di controlli nella componente "attività di controllo" includono
  - ✓ le autorizzazioni e approvazioni,
  - ✓ le riconciliazioni,
  - ✓ le verifiche (quali verifiche automatizzate in fase di modifica dei dati o riguardo la validità dei dati o calcoli automatizzati),
  - ✓ la separazione delle funzioni, e
  - ✓ i controlli fisici o logici, inclusi quelli che riguardano la salvaguardia dei beni
- Gli elementi probativi per la comprensione della valutazione del rischio da parte del revisore possono essere acquisiti mediante una combinazione di indagine, osservazione ed ispezione di documenti. **Le sole indagini presso il personale dell'impresa non sono tuttavia sufficienti** al fine di valutare che i controlli siano adeguatamente configurati e messi in atto.

Informazione e comunicazione e Attività di controllo – 3/3

- **I controlli nella componente "attività di controllo" nelle imprese meno complesse sono spesso simili a quelli delle imprese di dimensioni maggiori**, ma la forma con cui operano può variare. Inoltre è probabile che un numero maggiore di controlli sia eseguito direttamente dalla direzione;
- Il sistema informativo e i processi di business correlati sono spesso meno sofisticati ed è probabile che implichino un ambiente IT meno complesso, ma non di meno il sistema informativo potrebbe rivestire la stessa importanza.
- Stabilire la separazione delle funzioni nelle imprese meno complesse che hanno pochi dipendenti può essere meno attuabile. Tuttavia, in un'impresa gestita dal **proprietario-amministratore**, quest'ultimo **può essere in grado di esercitare una supervisione più efficace** mediante il coinvolgimento diretto rispetto ad un'impresa di dimensioni maggiori.
- Nella revisione di un impresa meno complessa, dove il sistema informativo risulta semplice, il revisore può valutare che non sono stati identificati controlli specifici sulle scritture contabili.

Monitoraggio – 1/2



Gli aspetti rilevanti che il revisore può considerare nel comprendere in che modo l'impresa monitora il proprio sistema di controllo interno includono:

- la configurazione delle attività di monitoraggio, per esempio se si tratti di un monitoraggio periodico o continuativo;
- lo svolgimento e la frequenza delle attività di monitoraggio;
- la valutazione tempestiva dei risultati delle attività di monitoraggio per stabilire se i controlli siano stati efficaci;
- in che modo le carenze identificate siano state affrontate mediante azioni correttive appropriate, inclusa la comunicazione tempestiva di tali carenze a chi ha la responsabilità di intraprendere le azioni correttive.

Le indagini presso le persone appropriate nell'ambito della funzione di revisione interna lo aiutano ad acquisire una comprensione della natura delle responsabilità di tale funzione. Gli elementi probativi possono essere acquisiti mediante una combinazione di indagine, osservazione ed ispezione di documenti. **Le sole indagini presso il personale dell'impresa non sono tuttavia sufficienti.**

Monitoraggio – 2/2

- Nelle imprese meno complesse, ed in particolare nelle imprese gestite dal proprietario - amministratore, la comprensione da parte del revisore del processo adottato dall'impresa per monitorare il sistema di controllo interno si focalizza spesso sulle modalità con cui la direzione o il proprietario-amministratore sono direttamente coinvolti nelle attività operative, in quanto possono non esserci altre attività di monitoraggio.

- Per le imprese in cui non esiste alcun processo formale di monitoraggio del sistema di controllo interno, la comprensione di tale processo può includere la comprensione dei riesami periodici delle informazioni gestionali che sono configurati per contribuire a prevenire o a individuare gli errori.

ODCEC m@ster

ORDINE DEI DOTTORI COMMERCIALISTI E DEGLI ESPERTI CONTABILI
MILANO

FONDAZIONE COMMERCIALISTI ODCEC di MILANO

Il controllo interno nei sistemi informatici

Comprensione sistema IT

- Il sistema informativo dell'impresa può comportare l'utilizzo di elementi manuali ed automatizzati, che influenza altresì il modo in cui le operazioni sono rilevate, registrate, elaborate e riportate. In particolare, le procedure per rilevare, registrare, elaborare e riportare le operazioni possono essere rafforzate mediante le applicazioni IT utilizzate dall'impresa e le modalità con cui l'impresa le ha configurate. Inoltre, gli archivi in formato digitale possono sostituire o integrare quelli cartacei;
- La comprensione del sistema informativo da parte del revisore include **l'ambiente IT rilevante per i flussi di operazioni e l'elaborazione di informazioni nel sistema informativo dell'impresa poiché l'uso di applicazioni IT da parte dell'impresa o altri aspetti nell'ambiente IT possono generare rischi derivanti dall'utilizzo dell'IT**.

Comprensione sistema IT

→ La comprensione dei rischi derivanti dall'utilizzo dell'IT e dei controlli generali IT messi in atto dall'impresa per fronteggiarli, può influenzare:

- ✓ la decisione del revisore se verificare o meno l'efficacia operativa dei controlli per fronteggiare i rischi di errori significativi a livello di asserzione;
- ✓ la valutazione del rischio di controllo a livello di asserzione;
- ✓ la strategia del revisore per la verifica delle informazioni prodotte dall'impresa che siano a loro volta prodotte da sue applicazioni IT, o che comportino l'utilizzo di informazioni tratte da tali applicazioni;
- ✓ la definizione delle procedure di revisione conseguenti.;

Elementi IT rilevanti - 1/2

- Al fine di identificare gli elementi IT rilevanti, è necessario innanzitutto **comprendere le applicazioni IT sulle quali la direzione fa leva** nello svolgimento dei controlli rilevanti identificati dal revisore, poiché tali controlli possono:
  - ✓ fare affidamento su automatismi (c.d. controlli automatici)
  - ✓ su report generati dall'applicazione;
  - ✓ sull'integrità delle informazioni gestite e mantenute dall'applicazione IT.
- Gli altri aspetti dell'ambiente IT che possono essere soggetti a rischi derivanti dall'utilizzo dell'IT includono l'infrastruttura, i sistemi operativi e i database e, in alcune circostanze, le interfacce tra applicazioni IT.
- **Quando il revisore non identifica applicazioni IT rilevanti, non sono generalmente identificati altri aspetti dell'ambiente IT.**
- Quando il revisore ha identificato applicazioni IT soggette a rischi derivanti dall'utilizzo dell'IT e probabile che siano identificati altri aspetti dell'ambiente IT in quanto sono di supporto e interagiscono con le applicazioni IT identificate.

Identificazione dei rischi associati all'IT – 1/2

- Nel processo di identificazione dei rischi derivanti dall'utilizzo dell'IT, il revisore considera attentamente la natura delle applicazioni IT e gli altri aspetti dell'ambiente IT, nonché le motivazioni che li rendono soggetti a rischi.
- Tra i rischi identificabili, figurano tipicamente i rischi correlabili a:
  - ✓ ccessi non autorizzati,
  - ✓ modifiche non autorizzate ai programmi e
  - ✓ modifiche non appropriate ai dati, inclusi i rischi di manipolazione diretta delle informazioni o accesso diretto al database.
- Inoltre, vengono valutati i rischi relativi alla cybersecurity.
- Tali rischi devono essere valutati a prescindere che gli elementi IT siano gestiti internamente o esternalizzati a fornitori esterni.
- L'intensificarsi del volume e della complessità dei controlli automatizzati aumenta i rischi connessi all'uso dell'IT da parte dell'azienda.

Identificazione dei rischi associati all'IT – 2/2

- E improbabile che un'impresa che utilizza un software commerciale e non ha accesso al codice sorgente per effettuare eventuali cambiamenti ai programmi abbia in essere una procedura per i cambiamenti ai programmi, ma può avere un processo o procedure per configurare un software (ad esempio, il piano dei conti, parametri o soglie di reportistica).
- Inoltre, anche le imprese più piccole possono avere un processo o procedure per gestire l'accesso all'applicazione (ad esempio, un individuo designato che abbia accesso al software commerciale in qualità di amministratore). In tali circostanze, e improbabile che l'impresa abbia in essere controlli generali IT formalizzati o abbia la necessita di averli.
- Quando la direzione non fa affidamento sui controlli automatizzati o sui controlli generali IT per elaborare operazioni o mantenere i dati, e il revisore non ha identificato alcun controllo automatizzato, il revisore può pianificare di verificare direttamente eventuali informazioni che coinvolgono l'IT ed e possibile che non identifichi alcuna applicazione IT soggetta a rischi derivanti dall'utilizzo dell'IT.

Controlli generali IT

- I controlli che mitigano i rischi associati all'IT sono definiti Controlli Generali IT e sono ricompresi nella componete «Control Activities» del COSO framework;
- Nella valutazione dei controlli generali IT, la valutazione della loro configurazione mira a determinare se sono in grado di prevenire o individuare errori significativi;
- È importante verificare che i controlli identificati siano effettivamente messi in atto dall'azienda.
- Le procedure di valutazione possono includere
  - ✓ indagini,
  - ✓ osservazioni, e
  - ✓ ispezioni di documenti.
- Le sole indagini presso il personale dell'impresa non sono tuttavia sufficienti al fine di valutare che i controlli siano adeguatamente configurati e messi in atto.

Domande