Il Sarbanes Oxley Act (SOX): la rilevanza dell'indipendenza dei controlli. Il contesto internazionale

8

di Vincenzo Capaccio, Patrizia Riva

SOMMARIO

8.1 Il Sarbanes Oxley Act

8.1.1 Brevi cenni storici

La Sarbanes-Oxley Act, conosciuta anche con il nome di *Public Company Accounting Reform and Investor Protection Act of 2002* e comunemente chiamata Sarbanes-Oxley (o anche SarBox o SOX), è una legge federale emanata nel luglio 2002 dal governo degli Stati Uniti d'America a seguito di diversi scandali contabili che hanno coinvolto importanti aziende americane. Tali scandali suscitarono grande sfiducia da parte degli investitori nei confronti dei mercati, sollevando altresì diversi dubbi circa le loro politiche di sicurezza.

Si trattava, in origine, di due diversi disegni di legge proposti dal deputato Mike Oxley (repubblicano, eletto nell'Ohio) e dal senatore Paul Sarbanes (democratico eletto nel Maryland): i due disegni furono unificati da una commissione bicamerale nell'atto finale approvato il 24 luglio 2002 con grandissima maggioranza in entrambe le Camere, e firmato dal presidente George W. Bush il 30 luglio 2002.

La legge mira ad intervenire per colmare alcune lacune nella legislazione, al fine di migliorare la corporate governance e garantire la trasparenza delle scritture contabili, agendo tuttavia anche dal lato penale, con l'incremento della pena nei casi di falso in bilancio. Viene inoltre aumentata la responsabilità degli *auditors* all'atto della revisione contabile.

Le regole della Sarbanes-Oxley Act del 2002 hanno modificato o integrato le leggi esistenti in materia di regolamentazione della sicurezza, tra cui il *Securities Exchange Act* del 1934 e altre leggi applicate dalla *Securities and Exchange Commission* (SEC).

Le Sezioni 302 e 906 del Sarbanes Oxley Act dispongono, rispettivamente con valenza civilistica e penale, il rilascio da parte dei vertici aziendali di certificazioni contenenti il "giuramento" sulla correttezza e completezza dell'informativa di bilancio. Per le imprese che godono dello stato di "*foreign private issuers*" le norme in esame si applicano al *Form 20-F* e ad ogni eventuale modifica ("bilancio"). Le disposizioni della Sezione 302 sono state rese operative dalla *Security and Exchange Commission* ("SEC") il 29 agosto 2002 mediante l'adozione delle Rule "*Certification of disclosure in companies' quarterly and annual reports*" ("*Rule SEC*"), mentre le indicazioni della Sezione 906 (cd. "*criminal certification*") sono in vigore dal 30 luglio 2002, data di approvazione del Sarbanes-Oxley Act.

Il combinato disposto della Sezione 302 del Sarbanes-Oxley Act e delle *Rule* emanate dalla SEC stabilisce che l'Amministratore Delegato (*principal executive officier* – CEO) e il responsabile dell'Area Amministrazione, Finanza e Controllo (*principal financial officie*r CFO), certifichino: 1) che

hanno analizzato il bilancio; 2) che (i) da un lato non vi sono indicazioni false riguardanti fatti di rilievo e omissioni di fatti rilevanti necessari a rendere ingannevoli le dichiarazioni rese; e (ii) dall'altro il bilancio e le altre informazioni finanziarie contenute nel documento rappresentano correttamente, sotto tutti gli aspetti rilevanti, la situazione patrimoniale-finanziaria, il risultato dell'impresa e i flussi di cassa dell'emittente; 3) che sono responsabili dell'istituzione e del monitoraggio delle procedure e dei controlli destinati ad assicurare il rispetto degli obblighi informativi (c.d. "*disclosure controls and procedures*"); 4) che hanno comunicato al revisore e all'*audit committee*: (i) ogni significativa carenza nella progettazione o nell'esecuzione dei controlli interni, (ii) le frodi anche non significative, poste in essere dal *management* o da dipendenti con ruoli rilevanti nel sistema di controllo interno; 5) hanno illustrato nel bilancio la presenza di cambiamenti significativi nel sistema di controllo interno.

8.1.2 Il ruolo del *Public Company Accounting Oversight Board* (PCAOB)

Oltre a ridefinire i compiti della SEC, la legge ha istituito il *Public Company Accounting Oversight Board*, ovvero il Consiglio di vigilanza sui bilanci delle aziende quotate. I punti su cui la legge focalizza la sua attenzione sono i seguenti: (i) è richiesta maggiore responsabilità per il *management* per quanto concerne l'accuratezza delle informazioni contabili sui bilanci e le relazioni finanziarie; (ii) viene creata una nuova autorità di controllo sui revisori esterni; (iii) vengono aumentate le pene per i crimini contabili e illeciti fiscali; (iv) si conferisce più potere alla minoranza.

8.1.3 Gli *Audit Standard* emessi dal PCAOB

Gli *Audit Standard* emessi dal PCAOB non sono "principi di revisione" in senso stretto (in altri termini non devono essere confusi con gli *ISA* ossia con gli *International Standard of Auditing*), ma sono principi per l'*oversight* sull'attività di revisione dei bilanci delle società US quotate e degli intermediari finanziari US.

8.1.4 L'indipendenza della società di revisione e i servizi vietati

La società di revisione, prima di accettare o proseguire un incarico di revisione, deve valutare e documentare: a) il possesso dei requisiti di indipendenza ed obiettività; b) l'eventuale presenza di rischi per la sua indipendenza e, nel caso, se siano state adottate idonee misure per mitigarli; c) la disponibilità di personale professionale competente, tempo e risorse necessari per svolgere in modo adeguato l'incarico di revisione.

Box 8.1 – Audit Standard

General Auditing Standards
1000 General Principles and Responsibilities
AS 1001: Responsibilities and Functions of the Independent Auditor
AS 1005: Independence
AS 1010: Training and Proficiency of the Independent Auditor
AS 1015: Due Professional Care in the Performance of Work
1100 General Concepts
AS 1101: Audit Risk
AS 1105: Audit Evidence
AS 1110: Relationship of Auditing Standards to Quality Control Standards
1200 General Activities
AS 1201: Supervision of the Audit Engagement
AS 1205: Part of the Audit Performed by Other Independent Auditors
AS 1210: Using the Work of a Specialist
AS 1215: Audit Documentation
AS 1220: Engagement Quality Review
1300 Auditor Communications
AS 1301: Communications with Audit Committees
AS 1305: Communications About Control Deficiencies in an Audit of Financial Statements
Audit Procedures
2100 Audit Planning and Risk Assessment
AS 2101: Audit Planning
AS 2105: Consideration of Materiality in Planning and Performing an Audit
AS 2110: Identifying and Assessing Risks of Material Misstatement
2200 Auditing Internal Control Over Financial Reporting
AS 2201: An Audit of Internal Control Over Financial Reporting That Is Integrated with An Audit of Financial Statements
2300 Audit Procedures in Response to Risks—Nature, Timing, and Extent
AS 2301: The Auditor's Responses to the Risks of Material Misstatement
AS 2305: Substantive Analytical Procedures
AS 2310: The Confirmation Process
AS 2315: Audit Sampling
2400 Audit Procedures for Specific Aspects of the Audit
AS 2401: Consideration of Fraud in a Financial Statement Audit
AS 2405: Illegal Acts by Clients
AS 2410: Related Parties
AS 2415: Consideration of an Entity's Ability to Continue as a Going Concern
2500 Audit Procedures for Certain Accounts or Disclosures
AS 2501: Auditing Accounting Estimates
AS 2502: Auditing Fair Value Measurements and Disclosures
AS 2503: Auditing Derivative Instruments, Hedging Activities, and Investments in Securities
AS 2505: Inquiry of a Client's Lawyer Concerning Litigation, Claims, and Assessments
AS 2510: Auditing Inventories
2600 Special Topics
AS 2601: Consideration of an Entity's Use of a Service Organization
AS 2605: Consideration of the Internal Audit Function
AS 2610: Initial Audits—Communications Between Predecessor and Successor Auditors
2700 Auditor's Responsibilities Regarding Supplemental and Other Information

AS 2701: Auditing Supplemental Information Accompanying Audited Financial Statements
AS 2705: Required Supplementary Information
AS 2710: Other Information in Documents Containing Audited Financial Statements
2800 Concluding Audit Procedures
AS 2801: Subsequent Events
AS 2805: Management Representations
AS 2810: Evaluating Audit Results
AS 2815: The Meaning of "Present Fairly in Conformity with Generally Accepted Accounting Principles"
AS 2820: Evaluating Consistency of Financial Statements
2900 Post-Audit Matters
AS 2901: Consideration of Omitted Procedures After the Report Date
AS 2905: Subsequent Discovery of Facts Existing at the Date of the Auditor's Report
Auditor Reporting
3100 Reporting on Audits of Financial Statements
AS 3101: The Auditor's Report on an Audit of Financial Statements When the Auditor Expresses an Unqualified Opinion
AS 3105: Departures from Unqualified Opinions and Other Reporting Circumstances
AS 3110: Dating of the Independent Auditor's Report
3300 Other Reporting Topics
AS 3305: Special Reports
AS 3310: Special Reports on Regulated Companies
AS 3315: Reporting on Condensed Financial Statements and Selected Financial Data
AS 3320: Association with Financial Statements
Matters Relating to Filings Under Federal Securities Laws
AS 4101: Responsibilities Regarding Filings Under Federal Securities Statutes
AS 4105: Reviews of Interim Financial Information
Other Matters Associated with Audits
AS 6101: Letters for Underwriters and Certain Other Requesting Parties
AS 6105: Reports on the Application of Accounting Principles
AS 6110: Compliance Auditing Considerations in Audits of Recipients of Governmental Financial Assistance
AS 6115: Reporting on Whether a Previously Reported Material Weakness Continues to Exist

Il requisito di indipendenza deve sussistere durante il periodo cui si riferiscono i bilanci da sottoporre a revisione e durante il periodo in cui viene eseguita la revisione stessa. Le leggi statunitensi in materia di titoli vietano alla società di revisione incaricata per la revsione contabile del bilancio e al proprio network di svolgere i seguenti servizi:

i. *bookkeeping services*;
ii. *financial information system design and implementation*;
iii. *internal audit outsourcing services*;
iv. *actuarial work*;
v. *appraisal, valuation, fairness opinions, or contribution-in-kind report*;
vi. *legal services*;
vii. *broker/dealer, investment adviser, or investment banking services*;

viii. *management functions or human resources, tax services for persons in financial reporting oversight roles*;
ix. *and expert services.*

La legge statunitense prevede inoltre per le società quotate che l'*Audit Committee* approvi in via preliminare tutti i servizi professionali che la società di revisione incaricata e le altre società appartenenti al proprio *network* dovranno svolgere sull'emittente e sulle sue controllate. Le società di revisione di grandi dimensioni hanno implementato procedure informatiche su piattaforma internet per la verifica della propria indipendenza sia a livello locale che a livello internazionale.

8.1.5 Il nuovo Codice di Corporate Governance 2020. La professionalità e l'indipendenza degli amministratori

Come già richiamato nei precedenti capitoli, il Codice di Corporate Governance 2020, che ha sostituito il precedente Codice di Autodisciplina 2018, si rivolge a tutte le società con azioni quotate sul Mercato Telematico Azionario ("MTA") gestito da Borsa Italiana e le società che adottano il Codice lo applicano a partire dal primo esercizio che inizi successivamente al 31 dicembre 2020. Si crede importante richiamare sinteticamente in questo capitolo dedicato al tema dell'indipendenza alcuni contenuti rilevanti del Codice di CG 2020, rinviando per gli approfondimenti ai singoli capitoli dedicati alle singole funzioni di governance. L'organo di amministrazione è composto da amministratori esecutivi e amministratori non esecutivi, tutti dotati di professionalità e di competenze adeguate ai compiti loro affidati. Il numero e le competenze degli amministratori non esecutivi devono essere tali da assicurare loro un peso significativo nell'assunzione delle delibere consiliari e da garantire un efficace monitoraggio della gestione. Come previsto dall'art. 6 del Codice, l'organo di amministrazione valuta l'indipendenza di ciascun amministratore non esecutivo dopo la nomina nonché durante il corso del mandato al ricorrere di circostanze rilevanti ai fini dell'indipendenza e comunque con cadenza almeno annuale. Le circostanze che compromettono, o appaiono compromettere, l'indipendenza di un amministatore sono descritte al punto 7 dell'art. 2 del Codice. Il sistema di controllo interno e dei rischi, trattato all'art. 6 del Codice, è costituito dall'insieme delle regole, procedure e strutture organizzative finalizzate ad una effettiva ed efficace identificazione, misurazione, gestione e monitoraggio dei principali rischi, al fine di contribuire al successo sostenibile della società. L'organizzazione del sistema del controllo interno e di gestione dei rischi descritto nella *Raccomandazione 32* dell'articolo 6 del Codice coinvolge, ciascuno per le proprie competenze: a) l'organo di amministrazione, che

svolge un ruolo di indirizzo e di valutazione sull'adeguatezza del sistema; b) il *chief executive officier*, incaricato dell'istituzione e del mantenimento del sistema di controllo interno e di gestione dei rischi; c) il Comitato controllo e rischi, istituito all'interno dell'organo di amministrazione, con il compito di supportare le valutazioni e le decisionidell'organo di amministrazione relative al sistema di controllo interno; d) il responsabile della funzione di *Internal audit*, incaricato di verificare che il sistema di controllo interno e di gestione dei rischi sia funzionante e coerente con le linee di indirizzo definite dall'organo di amministrazione; e) le altre funzioni aziendali coinvolte nei controlli quali le funzioni di *risk management* e di presidio del rischio legale e di non conformità; f) l'organo di controllo, che vigila sull'efficacia del sistema di controllo interno e di gestione dei rischi.

8.2 La responsabilità del management aziendale

8.2.1 Il *Management Report*

La Section 404 della Sarbanes-Oxley Act si compone di due parti, A) e B):

LA PARTE A) prescrive la responsabilità del management per la strutturazione e il mantenimento in esercizio di un adeguato sistema di controllo interno in ambito amministrativo e contabile "*Internal Control over Financial Reporting*" *ICFR*. Inoltre, descrive come la responsabilità del *management* si estenda anche alla valutazione periodica dell'efficacia di tale sistema, da rendere pubblica mediante una relazione od attestazione incluse nell' "*Annual Report*". In tale attestazione il *management* deve riferire, se del caso, l'esistenza nei processi di *ICFR* di*:*

1. insufficienze significative, "*Significant Deficiencies*", qualora siano ravvisabili una o una combinazione di carenze nei controlli tali da rendere "più probabile che remota" la possibilità che esistano conseguenti e verosibilmente non trascurabili errori nel bilancio e nell'informativa di bilancio non prevenuti o scoperti.
2. lacune sostanziali, "*Material Weaknesses*", qualora siano ravvisabili una o una combinazione di più carenze significative tali da rendere "più probabile che remota" la possibiltà che esistano errori sostanziali, "*Material Missatements*", nel bilancio e nell'informativa di bilancio non prevenuti o scoperti.

LA PARTE B) prescrive la responsabilità della società di revisione incaricata della revisione del bilancio, quale parte integrante del proprio incarico, di attestare o di emettere una relazione circa la valutazione di efficacia effettuata dal *management*.

In punti chiave della responsabilità del *management* sono:

1. Valutazione del rischio di errori materiali (rischio intrinseco e fraudolento);
2. Identificazione dei controlli a livello aziendale;
3. Identificazione di conti significativi e le informazioni;
4. Identificazione delle asserzioni delle voci di bilancio pertinenti;
5. Identificazione di processi significativi;
6. Identificazione delle sedi e/o delle business unit;
7. Documentazione della progettazione dei controlli;
8. Valutazione dell'efficacia progettuale dei controlli;
9. Test e documentazione dell'efficacia operativa dei controlli;
10. Valutazione delle carenze di controllo interno ed espressione di conclusioni sulla sua efficacia complessiva;
11. Comunicazione dei risultati al comitato di audit e al revisore;
12. Documentazione del processo di valutazione dei controlli interni.

1. Valutazione del rischio di errori materiali

La valutazione del controllo interno da parte della direzione dovrebbe iniziare con una valutazione del rischio di errore materiale. Questo rischio ha due componenti: Rischio intrinseco e Rischio di frode.

Tali rischi dovrebbero essere valutati dalla direzione sia a livello di bilancio globale sia a livello di asserzione delle singole voci di bilancio.

2. Identificazione dei controlli a livello aziendale ("Company Level Controls")

Sono i controlli messi in atto per, monitorare le operazioni e supervisionare l'ambiente di controllo nel processo di valutazione dei rischi a livello aziendale complessivo, nonché presso le singole sedi o unità aziendali.

Hanno spesso un impatto pervasivo sul controllo a livello di processo, transazione o applicazione, e la direzione è tenuta a valutare se siano adeguati a livello aziendale e documentarli.

I controlli a livello aziendale includono:

- ambiente di controllo, assegnazione di autorità e responsabilità, politiche e procedure coerenti e programmi a livello aziendale (ad es. codice di condotta) che si applicano a tutte le sedi e business unit;
- processo di valutazione dei rischi;
- elaborazione e controlli centralizzati;
- monitoraggio dei risultati delle operazioni;
- monitoraggio dei controlli (compresa la funzione di *audit* interno);
- processo di formazione del bilancio a fine periodo;
- politiche approvate dal Consiglio di Amministrazione indirizzate al controllo e gestione dei rischi.

3. Identificazione di conti significativi e le informazioni
La direzione deve identificare i conti significativi che formano il bilancio e fornire un'informativa esaustiva sul loro contenuto.

4. Identificazione delle asserzioni rilevanti per le voci di bilancio
La direzione deve identificare per ciascun conto significativo del bilancio le asserzioni più rilevanti ovvero quelle che incidono in modo significativo sulla corretta valutazione della voce di bilancio. Per asserzioni si intendono rispetto alla voce di bilancio: la completezza, l'accuratezza, la presentazione, l'esistenza e la valutazione.

5. Identificazione di processi significativi
È necessario identificare tutti i processi significativi su ogni classe di transazioni che impattano significativamente sul bilancio. A causa dei diversi livelli di rischio intrinseco ad essi associati, la classe principale di transazioni potrebbe essere ulteriormente classificata:
- le transazioni di routine sono legate ad attività finanziarie ricorrenti (ad es. vendite, incassi);
- le transazioni non di routine che si verificano solo periodicamente (ad es. rilevazione inventario fisico);
- le transazioni che comportano stime sono attività che comportano giudizio e/o supposizioni (ad es. valutazione del fondo svalutazione crediti).

6. Identificazione delle sedi e/o delle business unit
Nei casi in cui l'azienda è strutturata in più sedi o da una sola sede che gestisce più linee di business, la direzione dovrà tenerne conto nella progettazione del sistema di controllo e monitoraggio.

7. Documentazione della progettazione dei controlli
Non esiste un *format* specifico per la predisposizione della documentazione, la documentazione deve includere quanto segue:
- progettazione dei controlli su tutte le asserzioni pertinenti i conti significativi;
- informazioni su come le transazioni significative vengano avviate, autorizzate, registrate, elaborate e segnalate;
- informazioni sufficienti sul flusso delle transazioni per identificare i punti in cui potrebbero verificarsi errori materiali dovuti a errori o frodi;
- controlli disegnati per prevenire o rilevare frodi, identificazione di chi esegue i controlli e separazione dei compiti;
- controlli nel processo di formazione del bilancio alla fine del periodo;
- controlli sulla salvaguardia dei beni;
- risultati dei test e delle valutazioni della direzione.

Una documentazione inadeguata è una carenza nel sistema di controllo interno dell'azienda.

8. Valutazione dei controlli da parte della direzione

Il processo della direzione per valutare l'efficacia del sistema di controllo interno sull'informativa finanziaria dovrebbe includere i seguenti elementi:

- determinazione dei controlli da documentare e testare, inclusi i controlli su tutte le asserzioni relative a tutte le voci significative. Tali controlli includono:
  - controlli sull'avvio del processo, l'autorizzazione, la registrazione, l'elaborazione e la segnalazione di conti significativi;
  - controlli sulle procedure per la registrazione delle transazioni in contabilità generale;
  - controlli sulla selezione e l'applicazione delle politiche contabili;
  - la progettazione e l'implementazione di programmi e controlli antifrode;
  - controlli sul processo di formazione dei dati trimestrali e di fine anno;
  - controlli automatici dell'Information Technology;
  - controlli su transazioni significative non di routine e non sistematiche;
  - controlli sulla salvaguardia dei beni;
  - controlli a livello aziendale, tra cui l'ambiente di controllo, la valutazione dei rischi, l'elaborazione e i controlli centralizzati e i controlli durante il processo di reporting finanziario di fine periodo;
- valutazione del rischio che il fallimento di un controllo possa portare a errori materiali;
- valutazione della progettazione e dell'efficacia operativa dei controlli.

9. Test e documentazione dell'efficacia operativa dei controlli

La direzione è tenuta annualmente a monitorare e testare i controlli sui processi significativi, nonché su controlli generali. SEC e PCAOB hanno dichiarato pubblicamente che si aspettano che i test svolti dalla società siano maggiori di quelli svolti dal revisore.

La direzione nel monitoraggio deve considerare quanto segue:

- natura del controllo;
- frequenza dell'operazione;
- importanza del controllo (dipende dalla misura in cui l'azienda si basa sull'efficacia del controllo e dal grado in cui il controllo supporta l'efficacia di altri controlli);
- complessità del controllo.

10. Valutazione delle carenze di controllo interno ed espressione di conclusioni sulla sua efficacia complessiva

Esistono carenze quando la progettazione o il funzionamento di un controllo non consente alla direzione o ai dipendenti, nel normale corso dell'esecuzione

delle funzioni assegnate, di prevenire o rilevare errori tempestivi. Queste carenze possono variare da *Inconsequential* a *Significant deficencies* o *Material weaknesses*. Il PCAOB le ha così definite:

- *Inconsequential:* le eccezioni identificate sono considerate trascurabili o insignificanti, singolarmente. Tuttavia, due o più carenze irrilevanti possono costituire una carenza significativa.
- *Significant deficencies:* qualora siano ravvisabili una una combinazione di carenze nei controlli tali da rendere "più probabile che remota" la possibilità che esistono conseguenti e verosibilmente non trascurabili errori nel bilancio e nell'informativa di bilancio non prevenuti o scoperti.
- *Material weaknesses:* qualora siano ravvisabili una o una combinazione di più carenze significative tali da rendere "più probabile che remota" la possibilità che esistono errori sostanziali "Material Missatements" nel bilancio e nell'informativa di bilancio non prevenuti o scoperti.

11. Comunicazione dei risultati al comitato di audit e al revisore
La direzione dovrebbe comunicare gli aspetti importanti riguardanti il sistema di controllo interno al comitato di *audit* e al revisore, così come l'identificazione di eventuali carenze significative o debolezze materiali.

12. Documentare il processo di valutazione dei controlli interni
La direzione deve lasciare evidenza delle attività poste in essere per la valutazione dei controlli interni e avviare tutte quelle attività necessarie a eliminare le eventuali carenze riscontrate.

8.2.2 Gli elementi del Controllo interno: CoSO Framework (*rinvio*)

Il *PCAOB*, per accelerare il processo, ha assunto come primo riferimento nella redazione dello standard n. 2, l'"*Internal Control – Integrated Framework*" elaborato dal *CoSo*, riconosciuto come il modello di controllo più noto già utilizzato negli Stati Uniti. Il modello *CoSo* include criteri di valutazione di adeguatezza del sistema di controllo interno basato su componenti. Nel 2004 il *Committee of Sponsoring Organization of the Treadway Commission* ha pubblicato un modello di riferimento l'*Enterprise Risk Management (ERM) Framework* che di fatto rappresenta un'evoluzione, del *CoSO Report*. Una successiva evoluzione del Modello *ERM* del 2004 è rappresentata dal framework "*Enterprise Risk Management – Aligning Risk with Strategy and Performance*": i concetti in esso contenuti, pur non essendo completamente nuovi, spostano il *focus* sui requisiti necessari a far funzionare l'*ERM* nell'organizzazione. Lo *standard 2* (successivamente sostituito dal n. 5) del *PCAOB* ammette che si possano utilizzare altri modelli, a condizione che siano generalmente riconosciuti e siano stati

sviluppati da esperti mediante un procedimento pubblico e che posseggano alcune caratteristiche, già previste dagli "*International Standard on Auditing*". Per l'analisi delle componenti del *Co.So "framework"* si rinvia *supra* al Capitolo 6.

8.3 La responsabilità del revisore esterno

8.3.1 Premessa

Il revisore deve esprimere un parere sulla valutazione fatta dal *management* sull'efficacia del controllo interno della società per la redazione dell'informativa finanziaria. Per costituire una base per esprimere tale parere, il revisore deve pianificare ed eseguire l'*audit* per ottenere una ragionevole certezza circa il mantenimento, in tutti gli aspetti significativi, dell'efficacia del sistema di controllo interno nella redazione dell'informativa finanziaria ad una specifica data. Mantenere un controllo interno efficace significa che non esistono carenze significative (*material weeaknesses*). Per ottenere una ragionevole garanzia che non esistano carenze significative, il revisore deve ottenere e valutare le evidenze relative alla progettazione e al funzionamento efficace dell'*ICFR* (*Internal Control over Financial Reporting*).

8.3.2 Le attività di revisione del sistema di controllo interno

Le attività del revisore esterno possono essere così sintetizzate:
1. pianificare l'impegno;
2. valutare l'efficacia del processo *ICFR* (*Internal Control over Financial Reporting*), della direzione;
3. ottenere e capire i processi *ICFR*;
4. valutare l'efficacia del disegno;
5. testare e valutare l'efficacia del disegno del controllo interno sulla rendicontazione finanziaria;
6. testare e valutatare l'efficacia operativa del controllo interno sui processi *ICFR*;
7. redigere l'*opinion* sull'efficacia del sistema di controllo interno.

1. Pianificazione dell'impegno
Quando si pianifica l'impegno, il revisore deve valutare in che modo le seguenti questioni influiranno sulle procedure:
- conoscenza dell'ICFR dell'azienda;
- analisi del settore in cui opera l'azienda, struttura del capitale ecc.;
- cambiamenti nell'azienda, nelle sue operazioni o nei suoi ICFR;

- processo della Direzione per valutare l'efficacia dell'ICFR;
- giudizio preliminare su materialità, rischio e altri fattori relativi alla determinazione delle carenze significative;
- carenze di controllo precedentemente comunicate all' audit commitee o alla direzione;
- questioni legate alla normativa di settore;
- tipo ed entità delle evidenze disponibili relative all'efficacia dell'ICFR;
- giudizio preliminare sull'efficacia dell'ICFR;
- numero di sedi o unità aziendali significative.

2. Valutare il processo ICFR della direzione

Il revisore deve comprendere e valutare l'efficacia del processo dell'ICFR posto in essere dall'azienda. Egli deve considerare se il processo comprende i seguenti elementi:

- determinare quali controlli devono essere testati, sulle asserzioni delle voci più significative del bilancio; inclusi i seguenti:
  - controlli sull'autorizzazione, la registrazione, l'elaborazione dei fatti amministrativi;
  - controlli sulla selezione e l'applicazione delle regole contabili;
  - programmi e controlli antifrode;
  - controlli generali dell'information technology sui quali dipendono altri controlli;
  - controlli su transazioni significative non di routine e non sistematiche;
  - controlli a livello di direzione aziendale.
- valutazione della probabilità che il fallimento del controllo possa provocare un errore;
- analizzare le sedi o le business unit da includere nella valutazione;
- valutazione dell'efficacia del disegno;
- valutazione dell'efficacia operativa dei controlli. Esempi di tali procedure sono:
  - verifica dei controlli mediante audit interno;
  - test da parte di altri sotto il coordinamento della direzione;
  - ispezione delle prove dell'applicazione dei controlli;
  - test mediante un processo di autovalutazione.

3. Procedure per comprendere l'ICFR

- colloqui con la direzione, la vigilanza e il personale;
- ispezione dei documenti aziendali;
- osservare l'applicazione di controlli specifici;
- traccia delle transazioni attraverso il sistema informativo.

Inoltre, il revisore deve comprendere la progettazione dei controlli relativi a ciascun componente dell'ICFR:
- ambiente di controllo;
- valutazione del rischio;
- attività di controllo;
- informazione e comunicazione;
- monitoraggio.

Come considerazione pratica, il revisore dovrebbe prima testare e valutare i controlli a livello aziendale (company-level) che hanno spesso un impatto pervasivo sui controlli a livello di processo, transazione o applicazione.

4. Valutare l'efficacia del disegno

Il controllo interno sull'informativa finanziaria è efficacemente progettato quando si presume che i controlli rispettati prevengano o rilevino errori o frodi che potrebbero comportare errori significativi nel bilancio.

Il revisore deve:
- identificare gli obiettivi di controllo dell'azienda in ogni area;
- identificare i controlli che soddisfano ogni criterio e determinare se i controlli possano effettivamente prevenire o rilevare errori o frodi che potrebbero causare errori materiali.

Per consentire una valutazione dell'efficacia del disegno, il revisore deve eseguire le stesse procedure della direzione:
- identificare i conti e le informazioni significative;
- identificare i processi significativi e le principali classi di transazioni;
- identificare le asserzioni delle voci di bilancio pertinenti.

Il revisore deve eseguire almeno una procedura dettagliata (walkthrough test) per ogni classe principale di transazione. In una procedura dettagliata il revisore traccia una transazione dall'origine attraverso i sistemi informativi dell'azienda fino a quando non si riflette nei documenti finanziari dell'azienda. Queste procedure permettono al revisore di:
- confermare la comprensione del flusso di processo delle transazioni da parte del revisore;
- confermare la comprensione del revisore della progettazione dei controlli identificati per tutti i componenti dell'ICFR;
- confermare la completezza della comprensione del processo da parte del revisore e tutti i punti in cui gli errori potrebbero verificarsi;
- valutare l'efficacia della progettazione dei controlli;
- verificare se i controlli sono stati eseguiti da parte della società.

5. Test e valutazione dell'efficacia del progetto (design)
Per identificare i controlli da testare, il revisore deve valutare quanto segue:
a. punti in cui potrebbero verificarsi errori o frodi;
b. natura dei controlli attuati;
c. importanza di ciascun controllo nel raggiungimento degli obiettivi;
d. rischio che i controlli potrebbero non funzionare in modo efficace. i fattori che influiscono sul fatto che il controllo potrebbe non funzionare in modo efficace sono i seguenti:
e. variazioni del volume o della natura delle transazioni;
f. cambiamenti nella progettazione dei controlli;
g. cambiamenti nel personale chiave che esegue il controllo o monitorarne le prestazioni;
h. che si tratti di un controllo automatico o manuale;
i. complessità di un controllo.

Inoltre, il revisore deve valutare se testare: controlli preventivi, investigativi o la combinazione di entrambi.

Il revisore dovrebbe applicare test di controllo a quei controlli che sono importanti per raggiungere ciascun obiettivo di controllo. Non è necessario testare tutti i controlli né i controlli ridondanti, a meno che la ridondanza non sia essa stessa un obiettivo di controllo (ad esempio nel caso di determinati controlli informatici).

6. Tempistica dei test dei controlli
Il revisore deve eseguire i controlli per un periodo di tempo adeguato a determinare se, alla data indicata nella relazione finanziaria, i controlli necessari per raggiungere gli obiettivi funzionino efficacemente. Il periodo di tempo dipende dalla natura dei controlli e dalla frequenza con cui i controlli operano.

7. La stesura dell'opinion sull'efficacia del sistema di controllo interno
Nel formulare un parere sull'ICFR, il revisore deve valutare tutte le prove ottenute da tutte le fonti, tra cui:
(i) l'adeguatezza della valutazione effettuata dalla direzione e la valutazione del revisore del progetto e dei test di efficacia operativa dei controlli;
(ii) i risultati negativi delle procedure sostanziali eseguite durante l'audit del bilancio (un errore materiale durante l'audit del bilancio è la prova di una carenza significativa nell'ICFR);
(iii) eventuali carenze di controllo identificate.

Come parte della sua valutazione, il revisore dovrebbe rivedere tutte le relazioni dell'audit interno relative ai controlli relativi all'ICFR e può emettere

un parere non qualificato solo quando non sono state identificate "*material weknesses*" e non ci sono state restrizioni sulle procedure da svolgere.

Bibliografia

Amarelli G., *I criteri oggettivi di ascrizione del reato all'ente collettivo ed i reati in materia di sicurezza sul lavoro*, in Diritto penale contemporaneo, 2013

Amato G., *Finalità, applicazione e prospettive della responsabilità amministrativa degli enti*, in Cassazione Penale, 2007

Arena M., Cassano G., *La responsabilità da reato degli enti collettivi*, Milano, Giuffrè, 2007

D'Avirro A., Di Amato A., *La responsabilità da reato degli enti*, Padova, Cedam, 2009

De Vero G., *La responsabilità penale delle persone giuridiche*, Milano, Giuffrè, 2008

Mereu A., *La responsabilità "da reato" degli enti collettivi e i criteri di attribuzione della responsabilità tra teoria e prassi*, in Indice penale, 2006

Veneziani P., Garuti G., Cadoppi A., *Enti e responsabilità da reato*, Torino, Utet Giuridica, 2010