UNIVERSITÀ
DI PAVIA

Dipartimento di Scienze Economiche e Aziendali

Corso di Laurea magistrale in Economia e

Gestione delle Imprese

SOX compliance, impatti e cambiamenti sulla governance aziendale

Relatore:

Prof. Matteo Navaroni

Tesi di Laurea
di Veronica Rossi

Matr. n.523665

Anno Accademico 2023-2024

Indice

Introduzione

Il presente elaborato di tesi mira a illustrare i principali impatti e cambiamenti intercorsi sulla governance delle aziende a seguito dell'introduzione, nel 2002, del *Sarbanes-Oxley Act (SOX)*, una legge americana nata in risposta alla scarsa trasparenza nelle informazioni di bilancio di alcune delle più importanti società dell'epoca, con particolare focus sull'evoluzione dei controlli interni aziendali.

Il motivo che mi ha ispirata a scegliere questo tema come base su cui sviluppare il mio progetto di tesi nasce in seguito ad un periodo di stage curriculare svolto nella posizione di *Business Analyst* presso *DedaGroup Stealth*, azienda operante nel settore del *Fashion* internazionale che offre soluzioni tecnologiche e innovative di *Cloud Sourcing* progettate per l'intera *Supply Chain* del comparto moda. Dopo essere stata inserita all'interno del gruppo *finance* internazionale, ho iniziato ad interfacciarmi con clienti del settore ricadenti sotto i canoni della normativa *SOX*. Da qui scaturisce l'interesse e la curiosità di approfondire la tematica, capire come vengono operativamente gestiti i nuovi requisiti normativi e comprendere come questi abbiano influenzato il rinnovamento della governance aziendale.

L'approccio utilizzato per la stesura della prima parte dell'elaborato, nella quale vengono narrate le dinamiche che hanno determinato la nascita della legge, è prettamente descrittivo. Contrariamente, per la redazione degli ultimi due capitoli l'approccio è stato più empirico, caratterizzato dall'utilizzo di testi meno accademici ma più operativi.

Il lavoro è introdotto da una breve lettura storica, essenziale per poter comprendere come si presentava il sistema capitalistico verso la fine del '900. Per meglio intuire le motivazioni che hanno giustificato la nascita della nuova legge federale, nel primo capitolo viene esposto uno degli scandali finanziari più importanti degli ultimi decenni che vede protagonisti la *Enron Corporation* e la società di revisione *Arthur Andersen*, per poi proseguire con una prima analisi della nuova legge *SOX* evidenziando e commentando le sezioni che hanno avuto

maggior impatto sul tema dei controlli interni.

Il secondo capitolo continua proponendo un'analisi dei *framework COSO ICIF*, *ERM* e *COBIT*. Partendo dallo studio del primo modello del 1992, l'obiettivo è quello di mettere in evidenza le principali evoluzioni dei controlli interni e come il cambiamento delle realtà societarie abbia portato tale concetto ad inserirsi gradualmente all'interno dell'attività di gestione dei rischi.

Terminata la ricostruzione del progresso normativo in ambito di controlli interni, viene posta l'attenzione sul ruolo dei sistemi informativi che, considerata la crescente complessità dei processi aziendali, risultano ad oggi essere il polmone informatico delle aziende e un indispensabile supporto per una corretta rendicontazione finanziaria. Nasce da questa assunzione l'analisi proposta nel secondo capitolo circa l'importanza di monitorare i rischi correlati alla componente tecnologica presente nelle aziende e la necessità di disporre di nuove figure professionali, con competenze sempre più trasversali, che sappiano fornire una valutazione circa l'adeguatezza e sicurezza dei sistemi IT e indicarne spunti di miglioramento per supportare quanto richiesto dalla normativa a livello pratico ed operativo. Il capitolo si conclude con una descrizione delle procedure comunemente adottate dagli auditor IT per revisionare i controlli interni delle società con lo scopo di prevenire eventuali frodi, garantire l'integrità delle informazioni finanziarie e incentivare la responsabilità.

L'elaborato termina con il terzo capitolo, nel quale viene illustrato un caso pratico rappresentato da un progetto *SOX Compliance* a cui ho preso parte durante il periodo di stage. L'obiettivo di questo capitolo è enfatizzare l'importanza di istituire controlli volti a garantire la sicurezza dei sistemi informativi ma soprattutto dimostrare come l'adeguamento al *Sarbanes Oxley Act* rappresenti uno sforzo esteso a tutta l'organizzazione e come, malgrado le linee guida proposte dai *framework* possano costituire una solida base di partenza, senza l'impiego di risorse con una forte preparazione sulla specificità della normativa e sui processi aziendali difficilmente si riuscirà ad ottenere un risultato vincente.

Capitolo 1 – La nascita della normativa SOX

1.1 Eventi scatenanti la necessità di una riforma: il caso Enron Andersen

Alla fine degli anni ’90 si assistette alla nascita di nuovo ciclo economico denominato *New Economy*, nato dalla quotazione di *Netscape*, la prima società a sviluppare *browser* disponibili al pubblico.

Una nuova era digitale, figlia della diffusione globale di *internet* e delle nuove tecnologie dell’informazione.

Negli Stati Uniti, l’immediata reazione a questo fenomeno fu l’emergere e la quotazione di innumerevoli *start-up* con conseguente allocazione di ingenti capitali verso queste società, il cui business era rigorosamente legato al settore tecnologico e dunque apparivano come promettenti durante l’era della *New Economy*.[1] Questi eventi portarono, nella seconda metà degli anni Novanta, all’inizio di un fenomeno contraddittorio tale per cui la maggior parte delle società tecnologiche videro le proprie quotazioni schizzare alle stelle, nonostante operassero in perdita. Questo perché gli investitori, attratti da prospettive di alti rendimenti a fronte di investimenti relativamente esigui, iniziarono ad attuare comportamenti imitativi tra di loro investendo nelle imprese emergenti, senza tener sempre conto dei risultati espressi dai loro indicatori di redditività.

Con l’avvento del *world wide web,* le informazioni economiche iniziarono ad essere a disposizione di tutti, così come le attività borsistiche che si estesero anche a chi non era un professionista del settore.

A partire da questo assetto, nacque nel 1994 la bolla delle *dot.com*, denominata in questo modo in ragione delle estensioni *“.com*” nei domini *web* di queste *start-up*. Quest’ultima rappresenterà una delle bolle speculative più imponenti della storia dei mercati finanziari, caratterizzata da uno stadio iniziale di crescita ingiustificata del prezzo delle azioni susseguito da un repentino e significativo crollo delle stesse. La bolla si intensificò a partire dal 1997, anno durante il quale le aziende del *Nasdaq*, prima borsa al mondo esclusivamente elettronica,

[1] G. Campanelli, *Vent'anni dalla bolla delle dot-com: da Netscape a Tiscali, le società implose (e non)* in “Corriere Della Sera”, 4/03/2020.

iniziarono a registrare delle quotazioni record, anche grazie al taglio dei tassi di interesse voluto dalla *Federal Reserve*.

In questa situazione, la maggior parte delle aziende tecnologiche capitalizzava più dei colossi dell'industria di allora.

Osservando l'andamento del *Nasdaq* durante la bolla, è facile intuire come il titolo raggiunse il suo valore più alto nel 2000, anno in cui registrava circa 5000 punti, quadruplicando il suo valore nel corso di soli cinque anni.

Inaspettatamente, da qui in poi si assisterà ad un'inversione di marcia poiché i bilanci pubblicati da molte aziende iniziarono a mostrare risultati d'esercizio disastrosi, mettendo in guardia gli investitori sulla possibilità di un fallimento dei propri investimenti. Dal grafico si può infatti notare un inizio di calo delle quotazioni causato dalle vendite dei titoli da parte degli investitori più attenti che temevano un'ulteriore svalutazione degli stessi. Il *Nasdaq* in tre giorni perse circa il 9%.

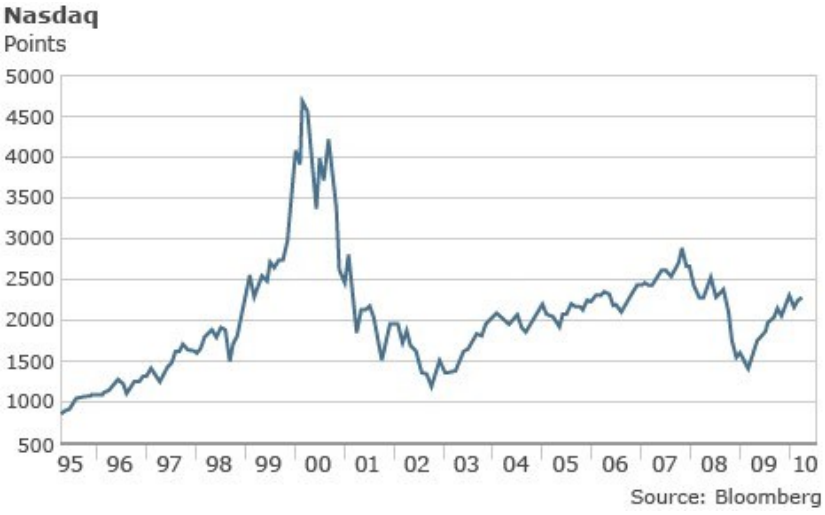


Grafico 1: Performance del Nasdaq dal 1995 al 2010. Fonte: Bloomberg

L'America, che fino a pochi anni prima era pronta ad abbracciare il nuovo paradigma della *New Economy*, si ritrovò in balia della principale crisi della storia della finanza internazionale.

Per meglio comprendere le motivazioni sottostanti la nascita del *Sarbanes Oxley Act,* è fondamentale soffermarsi su un caso protagonista di questi anni che sconvolse *Wall Street*: *il crac della Enron Corporation*.

La *Enron* nacque nel 1985 a *Huston* con *Kenneth Lay* e il suo braccio destro *Jeff Schilling*, dalla fusione tra la *Houston Natural Gas* e la *Internet*; due compagnie energetiche di modeste dimensioni. Questo settore al tempo aveva grandi potenzialità di crescita negli Stati Uniti poiché, durante il governo *Reagan*, si era assistito a notevoli liberalizzazioni che riguardavano in modo particolare l'energia.

Durante i primi anni la *Enron* agiva essenzialmente come distributore di gas naturale, ma già nel 1990 la società si espanse in Argentina, Inghilterra, Brasile e India, iniziando ad offrire servizi per la compravendita di *futures* e derivati energetici, attività che prima delle liberalizzazioni erano sotto lo stretto controllo dello Stato. Inizialmente, gli strumenti finanziari indotti dalla *Enron* erano legati solo al settore del gas e tramite la cessione di quest'ultimi, la società riusciva ad ottenere dai propri acquirenti incassi immediati. In seguito, *Schilling*, iniziò a correlare in modo sistematico gli strumenti finanziari ad ogni attività o investimento della *Enron*, dando vita ad un modello di *business* completamente inedito, tale per cui, la principale fonte di ricavo della società non erano le attività del proprio *core business* ma il *trading* legato ad esse.[2] Questo meccanismo permetteva di sfruttare l'effetto composto degli investimenti, che forniva alla multinazionale più capitale da investire nel breve termine dal quale poi avrebbe ottenuto rendimenti maggiori e più repentini.

A fronte di questa strategia, quasi nessuno si stupì della crescita esponenziale della *Enron*, che iniziò a competere con colossi mondiali come la *General Electric*, con un fatturato che passò da 40 a 101 miliardi di dollari tra il 1999 e il 2000.[3]

Durante questi anni, il prezzo delle sue azioni raggiunge il massimo storico di 90,75 dollari.

[2] E. Di Lella, *Il caso Enron: una truffa da 130 miliardi di dollari* in "Starting Finance", 30/10/2016.

[3] M. Novarini*, La truffa che sconvolse Wall Street: i 20 anni del crac della Enron* in "Forbes Italia", 12/02/2021.

Grafico 1.1: Il calo del prezzo delle azioni di Enron. Fonte: BBC News

La *Enron* era ammirata dal pubblico e dalla stampa, sia per i suoi risultati ineccepibili che per la sua cultura aziendale, di cui i suoi capi di facevano fautori. Come si può osservare nel grafico, il valore delle azioni aumentò senza sosta perfino negli anni 2000, in piena bolla *dot.com*, salendo dell'87% contro il -10% dell'indice *Standard & Poor's 500.*[4]

Proprio in questo periodo, che rese tutti più vigili sui bilanci delle aziende, una giornalista di *Fortune*, *Behan Mclean,* intraprese un'inchiesta sulla *Enron*, dopo essersi accorta che nei bilanci della società mancavano delle informazioni.

I risultati dell'analisi furono pubblicati in un articolo intitolato *"La Enron è sopravvalutata?",* quesito che fino all'ora non si era posto nessuno.

Dopo la sua divulgazione, *Schilling* decise di dimettersi improvvisamente e la società, forzata dalle pressioni esterne, fu costretta a pubblicare per la prima volta un bilancio trimestrale in perdita.

Gli investitori, ormai più che sospettosi che la *Corporate* stesse nascondendo delle potenziali perdite, iniziarono a vendere le proprie azioni facendone precipitare il prezzo a 36 centesimi contro i 90 dollari dell'anno precedente.

Nel 2001, la *Securities and Exchange Commission* (corrispondente della Consob italiana) iniziò a tenere sotto stretto controllo la società e, poco dopo, aprì un'inchiesta per indagare su alcune sue "stranezze contabili".

[4] Ibidem.

Lay, ormai alle strette, dichiarò pubblicamente che i bilanci della società era stati gonfiati di quasi 600 milioni di dollari ogni anno a partire dal 1997, sostenendo, però, di non averne mai saputo niente.

In realtà, il buco di bilancio della *Enron* era molto più importante rispetto a quello dichiarato dal *CEO*.

La reale situazione della società fu chiara a tutti solo dopo il fallimento della fusione in programma con la *Dynegy*, senza la quale la multinazionale incriminata non sarebbe stata in grado di sanare i 690 milioni di dollari di debiti ormai in scadenza.

Il due dicembre 2001, il più grande colosso del mercato energetico fu costretto a dichiarare fallimento, dopo essere stata sentenziato colpevole di frode e cospirazione; la sua bancarotta fu, al tempo, la più grande della storia americana ma, purtroppo, la prima di una lunga serie.

Le liquidazioni degli ex dipendenti, prima depositate in azioni della *Enron* e poi spostate su un altro fondo, persero integralmente il loro valore.

L'azienda più innovativa del pianeta non era altro che "un castello di carte", come sostenuto dalla giornalista *Mimi Smart* sul *Texas Monthly*.[5]

Come è facile intuire, tutto il sistema fasullo non sarebbe potuto sopravvivere senza il supporto di molteplici figure, tra cui i consulenti della *Arthur Andersen*, una delle *big fine* delle società di consulenza di allora che si sarebbe dovuta occupare di certificare la "veridicità" e "correttezza" dei bilanci della multinazionale texana.

La *Andersen* divenne così la prima vittima nei processi del caso; accusata di ostruzione alla giustizia, ad un milione di dollari di multa e al divieto di esercizio di attività di consulenza verso tutte le società quotate degli Stati Uniti.

[5] M. Novarini*, La truffa che sconvolse Wall Street: i 20 anni del crac della Enron* in "Forbes Italia", 12/02/2021.

1.2 Analisi della crisi nascosta nei bilanci societari

Dietro ai numeri esorbitanti dei fatturati della *Enron*, si celavano in realtà delle cifre fasulle determinate attraverso l'utilizzo di alcuni stratagemmi contabili favoriti dai revisori contabili.

A partire dal 1987, la multinazionale iniziò la costruzione di un intricato sistema alla cui base vi era una fitta rete di aziende fittizie chiamate società progetto, situate nei paradisi fiscali delle Isole Cayman, come noto territori che non sono sottoposti a controlli sui capitali. Le aziende allocate in queste isole servivano a nascondere i debiti della *Enron* e a far apparire come "puliti" i suoi bilanci. La *Corporate* non aveva condizioni finanziarie sane e adatte tali da poter ottenere prestiti dalle banche a condizioni agevoli, quindi, a fronte di questa impossibilità, iniziò a cedere alle società di progetto la proprietà di investimenti fallimentari e i debiti annessi, senza però coinvolgere investitori esterni, come invece era previsto per legge.

Le società erano, infatti, capitanate da dirigenti della *Enron* stessa che riusciva in questo modo a raccogliere capitali per finanziare i propri progetti dato che i fondi venivano stanziati alle società di progetto e in seguito girati alla *Enron*. All'epoca, il funzionamento delle società di progetto era legalmente accettato e le relative operazioni non dovevano obbligatoriamente essere registrate in bilancio; le varianti introdotte dalla *Enron*, contrariamente, erano "una strategia che non era solo discutibile dal punto di vista legale, ma anche straordinariamente rischiosa", come sostenuto da *Ledwell* sul *New Yorker.*[6]

Un altro stratagemma utilizzato dalla *Corporate* prevedeva la valutazione degli investimenti tramite un sistema chiamato *Mark to market* che permetteva di considerare ai fini della determinazione in bilancio, il valore di mercato corrente degli *asset* posseduti dalla società. Tale sistema di contabile era adottato principalmente dalle società di *trading* finanziario, approvato dalla *SEC* poiché la *Enron* legava ad ogni sua attività strumenti finanziari derivati. La società, così facendo, poteva inserire le valutazioni dei derivati assimilandole a componenti positivi di reddito, dunque, i ricavi attesi da un contratto venivano inseriti in

[6] Ibidem.

bilancio al momento della sottoscrizione dello stesso, senza però considerare la possibilità che la controparte non fosse in grado di ripagare il debito.[7]

Gli espedienti contabili, tuttavia, non erano sempre sufficienti per raggiungere i risultati fissati dai vertici della multinazionale.

La società texana entrò nel mercato elettrico della California verso la fine degli anni Novanta; durante questo periodo il paese registrò diversi *blackout* ingiustificati. Solo dopo il fallimento della *Enron* emerse che quest'ultima aveva utilizzato diverse strategie per causare delle interruzioni di servizio nelle varie centrali californiane. Il blocco degli impianti causava una diminuzione dell'offerta facendo salire alle stelle il prezzo dell'energia.

I vertici della multinazionale avevano inoltre una vasta rete di intrecci con il mondo della politica americana; in particolar modo *Kenneth Lay* aveva ampiamente sostenuto, a livello monetario, il Partito Democratico sia ai tempi di *George W. Bush* sia ai tempi del suo predecessore *Clinton*, ottenendo come "ricompensa" una politica energetica favorevole all'ascesa della propria società. Anche quando le sorti della *Corporate* erano ormai scritte, la *Enron* tentò di confabulare con il Tesoro americano per ottenere dei finanziamenti. Tuttavia, la politica nel 2001 ignorò le richieste d'aiuto di *Lay*, lasciandolo fallire.[8]

Lo scandalo della *Enron* sarà il primo di una lunga serie di default di colossi finanziari come *WorldCom, Washington Mutuale* e soprattutto *Lehman Brothers,* tutti accomunati da gravi irregolarità contabili.

Questa successione di tracolli indusse molti esperti a riflettere sulla gravità di quanto accaduto e cercare di comprendere quali fossero state le carenze del sistema capitalistico americano. I principali punti deboli emersi dall'analisi riguardarono:

- La revisione contabile, priva di professionalità ed etica;
- Carenze normative in tema di controlli interni e responsabilità del *management*;

[7] Esemplificando, la società investì miliardi di dollari in India registrando immediatamente le entrate che sosteneva di poter realizzare negli anni successivi, senza però calcolare che gli indiani non avrebbero potuto permettersi di comprare quell'energia. L'investimento fece perdere alla Enron 900 milioni di dollari.

[8] L. Balzarotti, B. Micco lupi, *La truffa di Enron, 15 anni fa. Le tappe del default nelle pagine d'Archivio* in "Corriere Della Sera", 3/12/2016.

- La rappresentazione forviante delle realtà aziendali da parte delle aziende.

In merito, osserva il professor *Paul Krugman*: «Tra dieci anni, non le stragi dell'11 settembre, ma lo scandalo *Enron* sarà visto come la grande svolta degli Stati Uniti», nella speranza che questo evento potesse fare da movente per alzare la guardia sui meccanismi del mondo finanziario.[9]

1.3 L'istituzione del Sarbanes-Oxley Act e del PCAOB

Come già evidenziato in precedenza, numerosi sono stati i default finanziari intercorsi durante l'ultimo ventennio e se la *Enron* non rappresenta il caso più grave, è stata sicuramente il simbolo della spregiudicatezza finanziaria, diventando un punto di svolta per l'economia americana.

Questo periodo di trasgressioni economico-finanziarie danneggiò enormemente la fiducia degli investitori e la capitalizzazione di mercato di molte società, dando vita ad un contesto di confusione e incertezza che portò le autorità americane ad intervenire tempestivamente affinché non si ripetessero casi equivalenti.

Il mondo della finanza dal 2001 fu caratterizzato da diverse evoluzioni, in particolar modo nell'ambito dei controlli interni.

Nel marzo del 2001, quando la *Enron* rappresentava l'unico caso rivelato, venne presentato dal Presidente *G. W. Bush* il *te-point-plan;* un intervento per risollevare la fiducia degli attori nei mercati finanziari. L'ideologia alla base di questo piano, tuttavia, non prevedeva una modifica del sistema normativo fino allora adottato, ma solo un inasprimento di quest'ultimo.[10]

Il *Committee on Banking, Housing, and Urban Affairs* del Senato, presieduto dal Senatore *Paul S. Sarbanes,* andò oltre la proposta del Presidente avanzando un nuovo progetto di legge chiamato *Public Company Accounting Riforma and Investor Protection Act of 2002,* il quale rappresentò il punto di riferimento per i lavori che condurranno alla nascita del *Sarbanes-Oxley Act.*

[9] Ibidem.

[10] S. Cammarata, *Interventi del Sarbanes-Oxley Act of 2002 sulla corporate responsibility nelle società quotate statunitensi* in "Archivio Ceradi", (2002), pp. 1.

Il 16 luglio 2002 il *Sarbanes-Oxley Act* fu approvato con l'unanimità del Senato e in data 30 luglio 2002, il Presidente *Bush* firmò il nuovo atto.

Il nuovo disegno di legge entrò in vigore con una prontezza legislativa senza precedenti, ciò non destò stupore dal momento che il Presidente *Bush* dichiarò pubblicamente che avrebbe approvato qualsiasi testo del Congresso, sebbene non fosse stato in linea con la sua proposta iniziale (*te-point-plan)*. Questa decisione, secondo la stampa, fu probabilmente influenzata dall'avvicinarsi delle elezioni e dalla perdita di popolarità del Presidente in seguito agli ultimi scandali.[11] Tali motivazioni costrinsero *Bush* a sostenere che "l'autoregolazione è importante ma non abbastanza".[12]

La nuova legge federale, oggi comunemente chiamata SOX o *Sbarbo*, nacque dalla fusione di due proposte di legge unificate, presentate da *Paul Sarbanes*, come già accennato, e da *Mike Oxley.* L'obiettivo principale della norma fu quello di sanare alcune "falle" all'interno della legislazione americana al fine di tutelare gli investitori da errori di contabilità, prassi fraudolente, rendere più trasparente le divulgazioni aziendali e migliorare la *Corporate Governance*[13]*,* agendo anche dal punto di vista penale.[14]

La norma in esame è estesa a tutte le società quotate al *New York Stock Exchange* operanti negli Stati Uniti e prevede che tutte le società per azioni presentino una valutazione annuale sull'efficacia dei propri controlli interni di *audit* finanziario alla *Security Exchange Commissioni.* La *SEC* svolge un ruolo estremamente critico nel garantire l'integrità dei mercati finanziari e proteggere gli investitori ma è la sua funzione è altrettanto essenziale quando si parla di governo societario, a questo scopo l'autorità collabora con organismi internazionali per promuovere rapporti finanziari di qualità e nuovi standard normativi.

---

[11] Ibidem.

[12] D.E. Sanger*, Corporate conduct: The overview* in "The New York Times",17/07/2002.

[13] La Corporate Governance rappresenta l'insieme di norme, prassi, consuetudini operative utilizzate dalle imprese per assumere decisione che consentano oro di allocare il capitale conferitogli dagli azionisti, raggiungere gli equilibri della gestione, creare valore e perdurare nel tempo. Comprende inoltre l'insieme di relazioni tra i dirigenti di una società, il Consiglio di Amministrazione, gli azionisti e tutte le altre parti interessate.

[14] S. Cammarata, *Interventi del Sarbanes-Oxley Act of 2002 sulla corporate responsibility nelle società quotate statunitensi* in "Archivio Ceradi", (2002), pp. 2.

Principio cardine della *Sbarbo* è la trasparenza, l'ideologia sottostante prevede che le società debbano sempre rendere noto quali siano le responsabilità e gli obblighi dei propri collaboratori, così come la divulgazione di materiale utile per fornire informazioni chiare a chiunque abbia investito nella società.
I punti focali introdotti della legge federale sono:

- Riconoscimento di maggior responsabilità al *management* per quanto riguarda l'accuratezza delle informazioni contenute nei bilanci aziendali e nelle relazioni finanziarie;
- Creazione di una autorità di controllo e supervisione dei revisori esterni;
- Inasprimento delle pene per crimini contabili e illeciti fiscali.

Simultaneamente al *Sarbanes-Oxley Act* venne istituito il *Public Accounting Overnight Board* (*PCAOB*), un'organizzazione senza scopo di lucro finanziata da società quotate con sede a *Washington DC*, che rappresenta il consiglio di vigilanza sui bilanci delle società quotate. Il *Board* nasce con il fine principale di controllare l'attività dei controllori esterni ed ha il compito di regolamentare due attività fondamentali:

- *Auditing* e i relativi standard di attestazione e controllo qualità delle procedure utilizzate per l'emissione dei report;
- Condotta da assumere per intervenire in modo appropriato al fine di proteggere gli interessi degli investitori.

Il *Sarbanes-Oxley Act* definisce le principali funzioni principali del *PCAOB*:

- Registro delle Società di Revisione che preparano le relazioni di *auditing* per gli emittenti, gli intermediari e i commercianti registrati presso la *SEC*;
- Assicurare che gli *audit* adottino linee guida rigorose, accurate ed indipendenti nella preparazione delle relazioni di revisione;
- Agire al fine di supervisionare i revisori delle aziende per tutelare gli investitori e gli altri *stakeholder,* imponendo sanzioni per le infrazioni.

Lo scopo principale del *Board* è dunque quello di ridurre il rischio di *audit* che si manifesta sostanzialmente quando il giudizio di revisione certifica i rendiconti finanziari nonostante il bilancio non sia veritiero e corretto. Un altro obiettivo è migliorare la qualità della revisione attraverso un controllo continuo sull'operato

delle società di *auditing* attraverso l'emissione di *Audit Standard,* i quali non sono da considerare dei principi di revisione ma delle linee guida per effettuare il controllo sull'attività di revisione.[15]

Il Consiglio di amministrazione del *PCAOB* è formato da cinque membri compreso il Presidente, due dei quali devono essere contabili pubblici certificati. I componenti sono nominati ogni cinque anni dalla *SEC,* con preliminare consultazione con il Presidente del Consiglio dei governatori del *Federal Reserve System* e il segretario del Tesoro.

Il *PCAOB* è sottoposto inoltre al controllo della *Securities and Exchange Commission* dal 2010, la quale ha il potere di approvare le regolamentazioni del Consiglio, gli standard di revisione e i budget annuali.

Se la nascita della SOX può essere letta come un riscontro al caso *Enron*, il *PCAOB*, allo stesso tempo, lo è nei confronti di società come la *Andersen*.

1.4 Le principali sezioni della normativa SOX

Il Sarbanes-Oxley Act impone un quadro contabile di ampia portata per tutte le società per azioni che operano negli Stati Uniti. Sono interessate alla normativa anche le consociate interamente controllate e tutte le società non statunitensi quotate in borsa che operano negli Stati Uniti. Inoltre, anche le società private che si stanno preparando per la loro offerta pubblica iniziale (IPO) devono rispettare alcune disposizioni del *Sarbanes-Oxley Act.*

Il contenuto del disegno di legge della *Sbarbo* è suddiviso in undici sezioni.[16]

I punti cardine che guidano il testo di legge riguardano l'aumento delle sanzioni penali per frodi, con clausole aggravanti in caso di appurata responsabilità

[15] P. Riva, *Ruoli di Corporate Governance*, EGEA spa, Milano, 2023.

[16] Titolo I – Public Company Accounting Oversight Board
Titolo II – Auditor Independent
Titolo III – Corporate Responsability
Titolo IV – Enhanced Financial Disclorusw
Titolo V – Analyst Conflict of Interest
Titolo VI – Commission Resources and Authority
Titolo VII – Studies and Reports
Titolo VIII – Corporate and Criminal Fraud Accountability
Titolo IX – White-Collar Crime Penalty Enhancement
Titolo X – Corporate Tax Returns
Titolo XI – Corporate Fraud and Accountability

individuale o collettiva. L'esercizio di pressioni verso i revisori al fine di ottenere dichiarazioni non veritiere sullo stato dei conti societari si caratterizza ora come reato penale. Viene inoltre stabilito il divieto di accorpare l'esercizio di revisione contabile e quello di consulenza a capo della stessa società, con obbligo di rotazione dei soggetti addetti alla revisione. Viene assegnato alla *SEC* il potere si sospendere, senza necessità di preventiva autorizzazione giudiziaria, gli amministratori considerati colpevoli di abuso dei propri poteri. Un ruolo cardine è svolto dall'autorità di vigilanza *PCAOB* a cui viene riconosciuto il potere di infliggere sanzioni, fino all'impedimento dell'esercizio della professione.[17]
Le sezioni di maggior impatto in termini di conformità sono riconducibili alla:

- *Sezione 302: Responsabilità delle imprese per le relazioni finanziarie*

La sezione 302 rappresenta la sezione più rilevante dell'atto legislativo e conferisce maggior responsabilità ai firmatari aziendali, Amministratore Delegato e *CFO*, per l'accuratezza, la documentazione, la presentazione di tutti i rapporti finanziari e per la struttura ed efficacia del controllo interno. Le due figure assumono così l'obbligo di certificare in prima persona che i controlli e le procedure di divulgazione vengano implementate.
Per ogni dichiarazione trimestrale, *CEO* e *CFO* hanno l'obbligo di:

- Essere responsabili dei controlli contabili interni;
- Valutare l'efficacia dei controlli;
- Esaminare tutti i rapporti finanziari, assicurando che siano presentati correttamente e che non contengano dichiarazioni false;
- Segnalare qualsiasi carenza nei controlli contabili interni o qualsiasi frode che coinvolga la direzione del comitato di *audit*;
- Presentare le conclusioni in merito all'efficacia dei controlli;
- Indicare eventuali modifiche sostanziali nei controlli contabili interni.

Il *PCAOB* ha delineato tre tipi di carenze di controllo interno:

- Irrilevanti: sono carenze quasi insignificanti se considerate singolarmente ma non vanno comunque sottovalutate;

[17]S. Nisticò, *Dall'euforia alla crisi: etica e fiducia nei mercati* finanziari in"University Library of Munich", Germany, (2005).

- Carenze significative: questa combinazione di carenze rende probabile la possibilità di avere errori nel bilancio non trascurabili;
- Debolezze materiali: questo insieme di carenze rende probabile la possibilità che ci siano inesattezze rilevanti nel bilancio.[18]

Questa disposizione impone alle aziende una significativa alterazione dei ruoli: Il CEO deve ora riconoscere direttamente la propria responsabilità per il controllo interno, in precedenza ampliamente delegata al CFO.[19]

Alcuni mandati previsti dalla sezione in esame possono risultare a tratti scoraggianti per le organizzazioni, si faccia riferimento ad esempio all'obbligo di rivalutare trimestralmente i controlli e le procedure in materia di pubblicità declinato all'interno di una organizzazione dinamica che sta lanciando sul mercato nuovi prodotti, mettendo in atto fusioni e acquisizioni, stringendo *partnership* e riorganizzando il proprio assetto societario.

- *Sezione 401: Informativa nelle relazioni periodiche*

"La sezione 401 specifica che le informazioni finanziarie fornite al pubblico nelle relazioni fornite alla *SEC* non conterranno dichiarazioni false o omissioni di fatti rilevanti e saranno conformi ai principi contabili generalmente accettati (*GAAP*). Le relazioni comprenderanno tutte le operazioni fuori bilancio rilevanti".

- *Sezione 404: Valutazione della gestione dei controlli interni*

La sezione 404 si compone di due parti, l'aspetto innovativo introdotto dalla prima parte prevede la richiesta che la relazione annuale stilata dalle società contenga al suo interno un "rapporto di controllo interno del *management*" che assolva le seguenti finalità:

- Indichi la responsabilità di *CEO e CFO* per la creazione e il mantenimento di un'adeguata struttura di controllo interno e di procedure per l'informativa finanziaria;

[18] P. Riva, *Ruoli di Corporate Governance*, EGEA spa, Milano, 2023.
[19] *Moving Forward–A Guide to Improving Corporate Governance Through Effective Internal Control in* "Deloitte&Touche", (2003), pp 10.

- Contenga una valutazione, alla fine dell'anno fiscale più recente, sull'efficacia della struttura di controllo interno e sulle procedure di informativa finanziaria, supportata da idonea evidenza;
- Dichiari che le società di *audit* esterne abbiano attestato l'accuratezza in merito alla valutazione dei controlli interni e delle procedure di informativa finanziaria messi in atto dal *management*, questo processo viene effettuato attraverso una relazione separata da parte della società di revisione.

I punti salienti della responsabilità del *management* sono:

- Valutazione del rischio di errori materiali;
- Identificazione dei controlli a livello aziendale;
- Identificazione di conti significativi e informazioni;
- Identificazione delle asserzioni delle voci di bilancio pertinenti;
- Identificazione di processi significativi;
- Identificazione delle sedi e/o delle *business uniti*;
- Documentazione della progettazione dei controlli;
- Valutazione dell'efficacia progettuale dei controlli;
- Test e documentazione dell'efficacia operativa dei controlli;
- Valutazione delle carenze di controllo interno ed espressione di conclusioni sulla sua efficacia complessiva;
- Comunicazione dei risultati;
- Documentazione del processo di valutazione dei controlli interni.[20]

Al *management* viene dunque richiesto di istituire un processo per valutare periodicamente i propri controlli interni sull'informativa finanziaria, il cosiddetto *Management Assesment Processi.* Questo procedimento ha lo scopo di identificare i controlli da sottoporre a valutazione e fornire un'analisi del rilievo dei controlli identificati rispetto alla probabilità che il loro mancato funzionamento possa causare errori. Il *management* deve fornire una valutazione dell'efficacia del disegno e dell'operatività dei controlli, per poi identificarne le carenze che in base alla loro significatività si classificano, come già esposto, in

[20] P. Riva, *Ruoli di Corporate Governance*, EGEA spa, Milano, 2023.

carenze significative o debolezze materiali. I risultati della valutazione devono poi essere comunicati al revisore esterno e/o al Comitato di audit.[21]

La seconda parte della sezione stabilisce l'obbligo della società di revisione di emettere una relazione separata contenete, oltre a quanto esposto nell'elenco precedente, dettagli sul modello di controllo utilizzato per la valutazione dei controlli interni, che deve essere idoneo e riconosciuto. Deve includere inoltre una descrizione esaustiva degli obiettivi di controllo imposti dal *management* e dei sistemi informativi a supporto di quest'ultimi.

Il fine ultimo di tale relazione è esprimere un "opinione" circa le affermazioni fatte dal *management.*

Nell'ambito dell'informativa finanziaria, esempi di obiettivi di controllo potrebbero riguardare:

- Autorizzazioni, approvazioni e verifiche;
- Separazione dei compiti;
- Controlli dei sistemi informativi;
- Sicurezza delle attività;
- Revisione degli indicatori di performance.[22]

Senza l'adozione di un quadro di controllo interno adeguato, la piena conformità con la sezione 404 del *Sarbanes-Oxley* risulterebbe poco plausibile poiché, in questo modo, all'interno dell'azienda non ci sarebbero criteri per permettere ai revisori indipendenti di misurare l'efficacia del modello di controllo.

La sezione 404 obbliga le società per azioni con una capitalizzazione di mercato superiore a 75 milioni di dollari a rendere operativi i loro quadri di rendicontazione finanziaria per il loro primo rapporto di fine anno fiscale dopo il 15 novembre 2006. Per le aziende di dimensioni minori, la conformità è invece richiesta a partire dal primo rapporto finanziario di fine anno fiscale.

Disponendo del quadro completo delle sezioni 302 e 404, è possibile per le società gestire i mandati delle due parti della Legge utilizzando un'unica

[21] M.Bozzola, *Sarbanes-Oxley Act Sezione 404 (Internal Control over Financial Reporting)* in "Ernst&Young", (2010).

[22] *Moving Forward–A Guide to Improving Corporate Governance Through Effective Internal Control in* "Deloitte&Touche", (2003), pp. 24.

metodologia, attraverso l'impiego di un programma di controllo interno che consenta di soddisfare i requisiti trimestrali della sezione 302 e quelli annuali della 404, e che prenda inoltre in considerazione le esigenze degli *auditor* indipendenti per eseguire le loro procedure di attestazione. Questa soluzione risulterebbe molto efficace ma non sempre semplice, soprattutto per le imprese più piccole che spesso non dispongono di un'infrastruttura sufficientemente robusta per gestire questo procedimento.[23]

- *Sezione 409: Informativa sull'emittente in tempo reale*

"Gli emittenti sono tenuti a rivelare al pubblico, su base urgente, informazioni su cambiamenti rilevanti nelle loro condizioni finanziarie o operazioni. Queste informazioni devono essere presentate in termini di facile comprensione e supportati da trend, informazioni qualitative e presentazioni grafiche, a seconda dei casi."

Esempi di informazioni che le aziende sono tenute a divulgare sono la violazione di dati, eventuali attacchi informatici e qualsiasi carenza nel funzionamento del controllo interno.

- *Sezione 802: Sanzioni penali per la modifica dei documenti*

"La sezione in esame del *Sarbanes Oxley Act,* impone pene fino a 20 anni di reclusione per l'alterazione, la distruzione, la mutilazione, l'occultamento, la falsificazione di registri, documenti o oggetti tangibili con l'intento di ostacolare, impedire o influenzare un'indagine legale. Un contabile o revisore contabile che viola consapevolmente e intenzionalmente l'obbligo di conservare i registri contabili per cinque anni può essere soggetto a un massimo di dieci anni di carcare."

La sezione 103 eleva a sette anni l'obbligatorietà di tenuta per tutti i documenti coinvolti nella revisione contabile.

Tuttavia, la legge non stabilisce puntualmente quali informazioni devono essere indispensabilmente archiviate dalle aziende.

[23] *Moving Forward–A Guide to Improving Corporate Governance Through Effective Internal Control in* "Deloitte&Touche", (2003), pp. 9.

- *Sezione 806: Tutela dei dipendenti di società quotate che forniscono prove di frode*

Questa sezione, meglio conosciuta come "Protezione degli informatori", nasce in risposta agli avvenimenti del caso *Worldcom,* analogo a quello della *Enron Corporation,* che venne reso noto grazie ad un dipendente che scoprì e segnalò la frode in atto. Attraverso questa sezione la legge mira a proteggere gli informatori da possibili ritorsioni da parte della società e delega il Dipartimento di Giustizia a sporgere denuncia penale contro i responsabili.

Al dipendente viene riconosciuta protezione quando segnala la presenza di:

- Frode federale di posta, bonifico, banca o titoli;
- Violazione della legge federale in materia di frode contro gli azionisti;
- Violazione di qualsiasi regolamento della SEC.

- *Sezione 906: Responsabilità sociale per le relazioni finanziarie*

Quest'ultima sezione più breve prevede sanzioni per i dirigenti che certifichino un rapporto falso o fuorviante. Il *CEO* e il *CFO* hanno l'obbligo di firmare la relazione periodica contenente i rendiconti finanziari, certificando così che quest'ultima risulti conforme ai requisiti di *reporting* previsti dalla *SEC* e che rappresenti verosimilmente la condizione finanziaria dell'azienda. Il mancato rispetto della disposizione in esame comporta multe fino a cinque milioni di dollari e la reclusione fino a vent'anni; le suddette misure vengono applicate sia nel caso di non conformità consapevole che intenzionale.

Tutte le sezioni del *Sarbanes-Oxley Act* sono ad oggi in vigore, ad eccezione della 409.

Il *Sarbanes-Oxley Act* ha profondamente influenzato il ruolo delle società di revisione e le responsabilità dei *manager;* due dei punti cardine ritenuti responsabili dell'andamento assunto dalla finanza americana durante gli anni precedenti alla sua entrata in vigore.

Tra i vantaggi apportati dalla nuova legge vi è sicuramente il miglioramento della *Corporate Governance* e l'aumento della trasparenza, dal momento che rende le società maggiormente responsabili dei confronti dei propri *stakeholders*

e amplia i requisiti di trasparenza nelle comunicazioni sociali. Un ulteriore beneficio prodotto è il riconoscimento di protezione per gli informatori di frodi aziendali; ciò ha senz'altro incoraggiato più soggetti ad esporsi su queste tematiche senza temere di pregiudicare la propria posizione all'interno dell'azienda. L'aumento delle responsabilità dei funzionari aziendali ha inoltre contributo alla diffusione di comportamenti più scrupolosi, note le conseguenze amministrative e penali in caso di rapporti finanziari fuorvianti. Un altro effetto positivo è riconducibile alla prevenzione della nascita di episodi di conflitto di interesse all'interno delle aree aziendali, attraverso l'imposizione di divieti di cumulo di funzioni.

Il testo di legge è stato anche sottoposto ad alcune critiche perché considerato eccessivamente oneroso e costoso in termini di conformità e per aver contribuito a ridurre la competitività delle aziende statunitensi, in quanto sottoposte all'obbligo di rispettare linee guida più rigide rispetto alle controparti straniere.

L'implementazione dei controlli previsi dalla *SOX* è indubbiamente una sfida rilevante che ha comportato un cambiamento di grande ampiezza per la maggior parte delle aziende, chiamate a progettare diversi protocolli che possono talora essere percepititi come degli "intoppi" allo svolgimento ordinario del lavoro. In questo senso, diventa essenziale per le aziende comprendere cosa potrebbe impattarle negativamente e delineare come il cambiamento in atto possa limitare i propri punti deboli.

I progetti inerenti al *Sarbanes-Oxley Act* sono per natura lunghi e corposi, una comunicazione aziendale coerente ed efficace, così come la raccolta e l'analisi di *feedback*, sono elementi indispensabile per poter superare gli ostacoli al cambiamento e per permettere alle risorse aziendali di comprenderne i motivi e i benefici.

I requisiti espressi dalla Legge americana sono alquanto complessi e richiedono una formazione specifica, per poter dar vita a un progetto di successo è quindi necessario dare alle persone le competenze adeguate. All'interno delle organizzazioni molto spesso può accadere che un cambiamento non abbia successo perché il personale non viene opportunamente incentivato. Considerare la definizione degli obiettivi di conformità alla *SOX* all'interno del processo di

valutazione dei dipendenti potrebbe essere una soluzione per favorire le probabilità di successo del progetto rendendone il risultato una doppia vittoria sia per l'azienda e per il personale.[24]

In seguito agli sviluppi del *Sarbanes Oxley Act* il concetto di *governance* aziendale si è evoluto notevolmente, dalla sua introduzione ad oggi si sono infatti susseguite numerose riforme e iniziative, tra le quali:

- Un maggior riconoscimento del ruolo della tecnologia nel miglioramento dei processi di *governance* nei settori della *privacy* e della sicurezza informatica. Un esempio è l'introduzione del regolamento generale sulla protezione dei dati (GDPR);
- L'integrazione della sostenibilità e della responsabilità sociale all'interno del governo societario. Sempre più aziende stanno accorpando i fattori ESG[25] nei loro processi decisionali così come è in aumento il numero di rapporti non finanziari legati alla sostenibilità (i.e. bilancio di sostenibilità);
- Maggior enfasi sulla diversità dei consigli di amministrazione attraverso il riconoscimento dei benefici apportati dalla diversità di genere e di etnia all'interno degli organi aziendali;
- Iniziative di risalto sui diritti degli azionisti, come l'introduzione dell'attivismo nelle pratiche di governo societario.

Il tema del governo societario è in costante evoluzione e richiede alle aziende di mantenere un approccio proattivo e vigile per affrontare i rischi e le sfide emergenti. Ai giorni d'oggi le ripercussioni più consistenti si registrano nel settore dell'*Information Technology* con l'introduzione del termine *IT governance,* che fa riferimento a quella parte del governo d'impresa finalizzata alla gestione dei sistemi informativi.[26]

---

[24] C. Fox, P. Zonneveld, *Il ruolo dell'IT nel progetto e nell'implementazione dei controlli interni per la predisposizione del reporting finanziario*, traduzione italiana a cura dell'Associazione Italiana Information Systems Auditors (AIEA), Milano, (2007).

[25]L'acronimo ESG (Environmental, Social, Governance) viene utilizzato in ambito economico/finanziario per definire tutte quelle attività legate agli investimenti responsabili (IR) che perseguono gli obiettivi tipici della gestione finanziaria tenendo in considerazione aspetti di natura ambientale, sociale e di governance.

[26] R. Garelli, *Controlli interni e requisiti del Sarbanes-Oxley Act* in "Impresa Progetto", 2 (2009), pp.1.

Il dibattito sulle iniziative da mettere in atto per prevenire casi di frode e cattiva gestione societaria ha interessato anche l'Italia già ai tempi di alcuni scandali finanziari, tra cui Cirio e Parmalat, i quali hanno rimarcato l'esigenza di adottare soluzioni adeguate.

A questo proposito, il legislatore italiano ha provveduto ad emanare una nuova legge nazionale: la legge sul risparmio n.262 del 28 dicembre 2005, dal titolo "Disposizioni per la tutela del risparmio e la disciplina dei mercati finanziari."

Oltre all'esigenza di conformarsi alla disciplina *SOX*, detta legge è stata pensata anche con l'intento di armonizzare e migliorare l'informativa finanziaria delle società quotate.

La legge italiana presa in esame risulta molto corposa e tratta di svariati temi, le principali disposizioni riguardano:

- La *Governance* aziendale, attraverso l'introduzione di nuovi obblighi per gli organi amministrativi e di controllo;
- La trasparenza finanziaria, attraverso l'imposizione dell'adozione di standard contabili internazionali per la redazione dei bilanci delle società italiane quotate in borsa;
- La tutela dei risparmiatori, inasprendo le sanzioni in caso di violazioni delle norme di mercato e introducendo nuovi diritti per gli azionisti di minoranza.

Il miglioramento di questi tre temi rappresenta l'obiettivo cardine della Legge.

Ai fini dell'analisi in corso è interessante affrontare le novità introdotte nell'ambito della *Corporate Governance,* dove sono presenti molte analogie rispetto a quanto sancito dalle sezioni più rilevanti del *Sarbanes-Oxley Act.*

L'articolo 154-bis comma 2, presente nella sezione V-bis del D.lgs. n. 58/59 TUF, analizza la redazione dei documenti contabili societari e sancisce la nomina di un Dirigente Preposto (DP) incaricato di redigere i documenti societari. Tale figura deve certificare che gli atti della società inerenti all'informativa contabile siano corrispondenti alle risultanze documentali, deve inoltre sottoscrivere ogni documento diffuso a terzi al fine di attestare la corrispondenza al vero dei dati economici, patrimoniali e finanziari contenuti. È

evidente come il contenuto di questo articolo richiami la sezione 302 della SOX, secondo il quale *CEO* e *CFO* hanno l'obbligo di attestare l'informativa finanziaria presente nel bilancio.

Il comma 3 dell'articolo, stabilisce che al Dirigente devono essere conferiti i poteri e i mezzi adeguati a poter predisporre procedure amministrative e contabili idonee alla redazione delle comunicazioni di carattere finanziario, Il DP deve poi attestare, attraverso un'apposita relazione, l'adeguatezza e l'effettiva applicazione di tali procedure da parte degli organi amministrativi. Questo capoverso si rifà alla sezione 404 della SOX, secondo la quale è necessario definire un *Interna Control Report* per disporre di una struttura adeguata ai fini del controllo interno delle società.

Al comma 5, l'articolo prevede l'attestazione da parte degli organi amministrativi e del Dirigente, attraverso una relazione, dell'applicazione adeguata delle procedure contabili e della corrispondenza del bilancio alle risultanze delle scritture, secondo un modello stabilito dalla Consob, da allegare al bilancio d'esercizio e, se previsto, a quello consolidato.

Infine, il comma 6, introduce la responsabilità, anche penale, degli amministratori e dei Dirigenti preposti alla redazione dei documenti contabili societari. L'assonanza di questo comma con il *Sarbanes-Oxley Act* si ritrova nella sezione 906, che prevede sanzioni per i dirigenti che certifichino un rapporto falso o fuorviante.

La legge esaminata è stata emanata per perfezionare il decreto legislativo n.231 del 2001, il quale ha introdotto la responsabilità amministrativa delle società per reati commessi da soggetti appartenenti ad essa. I soggetti cui si riferisce si identificano in coloro che svolgono funzioni di direzione, amministrazione e controllo. Il D.lgs. stabilisce che la società sia esonerata da responsabilità qualora i soggetti sopracitati adottino un modello di gestione tale da prevenire i reati e una verifica periodica di quest'ultimo, per assicurare che sia sempre in linea con i mutamenti dell'organizzazione.[27]

[27] *Decreto legislativo n. 23 8 giugno 2000,* Gazzetta Ufficiale n.140 del 19/06/2001.

Per giungere all'attuale assetto della Legge sul risparmio si sono susseguite diverse modifiche nel corso degli anni, ciò a dimostrazione della continua evoluzione della materia in funzione delle esigenze del settore.

Nonostante l'obiettivo comune delle due disposizioni di legge sia il medesimo, sono comunque presenti alcune differenze tra le due giurisdizioni. Una di queste è da ricercare nell'approccio regolatorio della norma; la *Sbarbo* si caratterizza per avere un approccio dispositivo alquanto dettagliato contenente specifici requisiti di *compliance* e precise sanzioni in caso di non conformità. La Legge 262/2005 è al contrario più flessibile e basata su principi e linee guida.

A differenza di quanto sancito dalla sezione 404 della *SOX*, la normativa italiana non prevede che avvenga una verifica e un'attestazione da parte del revisore esterno sui processi e sulle procedure stabilite dal *management* come supporto alle proprie dichiarazioni, ne richiede indicazioni di dettaglio sui requisiti minimi del sistema, dei processi e delle procedure oggetto di attestazione da parte del *management*, come invece previsto dall'*Auditing Standard n°2.*

Inoltre, la Legge n.262 prevede delle disposizioni limitatamente alle società controllate con sede in paesi che non garantiscono la trasparenza societaria, secondo le quali, gli atti e i bilanci della società estera, allegati al bilancio della società italiana, debbano essere sottoscritti dagli organi di amministrazione, dal Direttore Generale e dal Dirigente Preposto alla redazione dei documenti contabili societari di quest'ultima, al fine di attestare la veridicità e la correttezza della rappresentazione della situazione patrimoniale, finanziaria e del risultato economico di esercizio. Il bilancio della controllante italiana deve inoltre includere una relazione degli amministratori inerente ai rapporti intercorrenti tra la società italiana e la estera controllata.

Diversamente, nel *Sarbanes-Oxley Act* non esistono direttive specifiche per le società controllate.

1.5 Il ruolo fondamentale del controllo interno

L'attività del controllo interno trova la sua ufficializzazione in Florida nel 1940, anno in cui fu fondato l'*Institute of Interna Auditors*, che lo disegnò come un mero strumento di difesa nei confronti dell'attività svolta dai revisori esterni.[28] Da questo periodo in poi si susseguiranno diverse dichiarazioni il cui scopo era definirne gli obiettivi e il raggio d'azione.

Fino agli anni Cinquanta del Novecento, la concezione dell'*auditing* era coscritta alla sola rendicontazione finanziaria; solamente alla fine del 1970, attraverso il *Foreign Corruppe Practices Act,* il controllo interno diventò un "un requisito per le società quotate ai sensi del *Securities Exchange Act* del 1934".[29]

Come già trattato, nonostante le diverse evoluzioni in materia, gli anni successivi vedranno susseguirsi molti default societari, tali da far sì che nel 1985, l'*American Institute of Certified Public Accomunante* incaricò una commissione, la *Tramway Commission*, di condurre un'inchiesta per comprendere le principali cause alla base della crisi di molteplici società americane. La commissione presentò le proprie conclusioni attraverso un rapporto, denominato *Tramway Report,* dal quale risultò che la prima causa di fallimento societario fosse la mancanza di misure di controllo interno adeguate e la concezione di base, condivisa dalla maggior parte degli attori, che quest'ultimo rappresentasse un insieme di attività ispettive.

Nasce da qui l'esigenza di definire un modello di riferimento per la gestione dell'attività di controllo interno, tema che verrà analizzato nei prossimi capitoli. Ripercorrendo l'analisi dettagliata effettuata sulle varie sezioni della *Sarbanes Oxley Act* è facile comprendere il ruolo cardinale svolto dal controllo interno. Il testo di legge non definisce i controlli interni in quanto tali, tuttavia, il *PCAOB Auditing Standard* n. 2, ne offre un'interpretazione nel contesto dell'*auditing*, definendo i controlli interni come: "Un processo progettato da o sotto la supervisione del principale dirigente della società e dei principali funzionari

[28] G. Trequattrini, *Origini e sviluppo dell'internal auditing: nuovi rischi e prospettive* in "Banca d'Italia-Pubblicazioni" Roma, (2022), pp.2.

[29] G. Gasparri, *I controlli interni nelle società quotate in "*CONSOB - Quaderni Giuridici", Milano, (2013), pp.15.

finanziari, o persone che svolgono funzioni simili , ed effettuato dal consiglio di amministrazione della società, dalla direzione e da altro personale, per fornire una ragionevole garanzia in merito all'affidabilità dell'informativa finanziaria e alla redazione del bilancio per scopi esterni in conformità con i principi contabili generalmente accettati […]."

I principali obiettivi delle attività di controllo interno sono:

- Prevenire frodi; aiutando le aziende a migliorare i propri processi garantendo, ad esempio, che nessuna risorsa aziendale abbia il pieno controllo su determinate operazioni;
- Garantire la conformità a requisiti legali e normativi;
- Proteggere i beni aziendali; siano essi beni fini fisici o immateriali (i.e. proprietà intellettuale);
- Migliorare il *reporting* finanziario; i controlli interni aiutano a garantire la conformità e l'affidabilità dei rendiconti finanziari.

Nell'anno di entrata in vigore della *SOX*, la maggior parte delle società non disponeva di una struttura solida e di uno staff abbastanza ampio tali da poter assolvere a determinate richieste, dunque, le imprese dovettero adattarsi riorganizzandosi strutturalmente, acquisendo nuove competenze e conoscenze. I costi di conformità furono considerevoli, includevano ed includono in parte tutt'ora, costi diretti per la formazione dei dipendenti e dei consulenti sul controllo interno, spese per l'acquisizione di nuove tecnologie a supporto del controllo interno, parcelle degli *auditor* indipendenti per l'esecuzione di test che certificassero l'efficacia del controllo interno. I costi indiretti erano invece sostenuti principalmente per la riallocazione delle risorse all'interno dell'organizzazione.

Naturalmente, alcune aziende hanno dovuto apportare cambiamenti più radicali di altre, ciò in relazione della portata delle modifiche necessarie per conformarsi. In linea generale si potrebbe pensare che implementare misure di controllo interno in una società piccola possa risultare più semplice poiché composta da meno persone, divisioni, e processi. Eppure, molto spesso le imprese di minori

dimensioni dispongono di un'infrastruttura così informale che potrebbero rendersi necessarie misure correttive alquanto significative. [30]

La sfida principale con cui le aziende si sono dovute interfacciare e si interfacciano anche oggi riguarda la definizione di obiettivi e politiche di controllo interno chiari e condivisi. L'inabilità di comunicare in modo adeguato le procedure di controllo e di fornire una idonea formazione al personale aziendale può impedire l'istituzione di un sistema di controllo interno efficace. Un ulteriore aspetto critico da prendere in considerazione, che caratterizza ancora oggigiorno molte realtà aziendali, riguarda l'utilizzo di processi manuali e la mancanza di automatizzazione. Queste pratiche rischiano di assoggettare il sistema controllo interno ad errori, inefficiente e ritardi. Inoltre, sottoporre i controlli interni a regolare monitoraggio e revisione è fondamentale per le organizzazioni al fine di poter captare proattivamente eventuali problematiche prima che diventino incontrollabili e implementare miglioramenti. Un'ultima componente estremamente importante per le aziende, finalizzata a garantire la sostenibilità del controllo interno, è attuare una solida segregazione dei compiti (*segregati on of duties/SOD*); principio fondamentale del controllo interno orientato ad assicurare che solo gli attori ritenuti idonei possano eseguire determinate funzionalità aziendali, permettendo di mitigare i rischi di frode.[31]

È dunque facile intuire come i controlli interni costituiscano il pilastro per disporre di una buona struttura di governo societario.

Ad oggi, tutto ciò si deve integrare con l'immensa mole di dati ed informazioni presenti, ormai protagonisti dei contesti aziendali. La componente IT risulta essere sempre più annidata all'interno dei processi delle imprese ed assicurare una corretta *data governance*, quindi protezione e trasparenza da possibili manipolazioni dei dati, è ormai un elemento imprescindibile per potere adempiere correttamente alla nuova normativa.

All'interno della guida di *Deloitte&Touche* per migliorare la *Corporate Governance* attraverso un efficace controllo interno viene proposta la seguente

[30] *Moving Forward–A Guide to Improving Corporate Governance Through Effective Internal Control in* "Deloitte&Touche", (2003), pp 12.

[31] Ad esempio, la risorsa aziendale responsabile dell'approvazione degli acquisti non dovrebbe essere la stessa che gestisce i pagamenti o riconcilia gli estratti conto bancari.

procedura per lo sviluppo di un programma di controllo interno mirato ad affrontare le disposizioni del *Sarbanes-Oxley Act*:

- Affrontare le disposizioni delle sezioni 302 e 404 attraverso l'utilizzo di un'unica metodologia;
- Comprendere quanto sforzo è necessario all'azienda per potersi conformare alla *SOX,* attraverso un'analisi delle proprie caratteristiche di business;
- Utilizzare un quadro di controllo interno adeguato e riconosciuto;
- Creare un comitato di divulgazione per assicurare che le procedure aziendali di divulgazione siano accurate, tempestive e complete, come richiesto dalla sezione 302;
- Stabilire un programma di controllo interno.[32]

Stabilire un programma di controllo interno può rappresentare un grande sforzo, soprattutto per quelle entità che non dispongono già di una funzione di audit interno attendibile.

Attraverso uno strumento chiamato *Interna Control Reliability Model* le aziende possono valutare il grado di affidabilità del proprio controllo interno, in ottica *sa is* e *to be*.

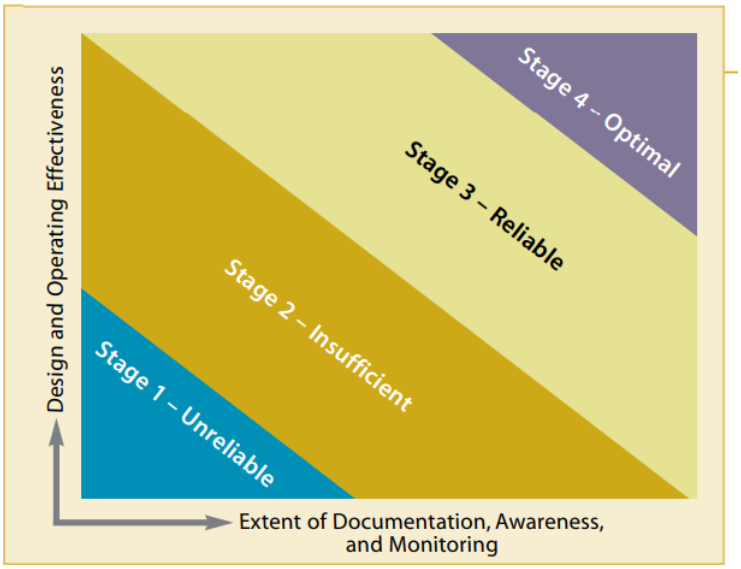


Figura 1: Interna Control Reliability Model. Fonte: Deloitte&Touche.

[32] *Moving Forward–A Guide to Improving Corporate Governance Through Effective Internal Control in* "Deloitte&Touche", (2003), pp 4.

Questo modello categorizza graficamente l'affidabilità del controllo interno in quattro fasi, brevemente discusse di seguito.

Un controllo interno inaffidabile e insufficiente è caratterizzato dall'assenza di politiche e procedure e da scarsa conoscenza da parte dei dipendenti della loro responsabilità in termini di controllo interno. Ciò implica che la struttura di controllo interno non è sufficientemente solida per adempiere ai requisiti della nuova Legge; è dunque richiesto all'entità un livello di sforzo significativo per documentarsi, testare e implementare rimedi correttivi.

In caso di controllo interno affidabile si è in presenza di politiche e procedure adeguatamente documentate e da consapevolezza da parte dei soggetti interni della propria responsabilità per le attività di controllo interno. Un'azienda che si posiziona in questo stadio valuta periodicamente l'efficacia operativa delle proprie attività di controllo ed è in grado di indentificare e sanare in modo tempestivo eventuali carenze.

In conclusione, un ottimale sistema di controllo interno è caratterizzato dallo sfruttamento del fattore tecnologico al fine di documentare i processi, gli obiettivi, le attività di controllo e per individuarne possibili lacune. Inoltre, le aziende in questo stadio utilizzano processi di autovalutazione per esaminare la progettazione e l'efficacia dei propri controlli e monitorarli in tempo reale. Tutto ciò permette un uso efficiente delle risorse interne e un miglioramento del proprio processo decisionale, disponendo di informazioni tempestive e di alta qualità.

L'onere della conformità con le disposizioni relative al controllo interno del *Sarbanes-Oxley* può essere dunque agevolato attraverso l'utilizzo di strumenti di conformità strategici.[33]

Attraverso l'istituzione della *SOX* si è inoltre assisto ad un'evoluzione della revisione esterna, nata a seguito dell'obbligo imposto alle società di dover sottoporre a verifica, da parte di un ente indipendente, la veridicità dei dati esposti nei propri bilanci.

[33] *Moving Forward–A Guide to Improving Corporate Governance Through Effective Internal Control in* "Deloitte&Touche", (2003), pp 20.

Un sistema di controllo effettuato unicamente a livello interno non era più sufficiente a garantire un'opinione corretta sui rendiconti finanziari, poiché, come dimostratosi, avrebbe potuto portare il *management* a manipolare determinate informazioni contabili o addirittura a falsificare direttamente i dati esposti in bilancio. Quando neanche la presenza di società di revisione indipendenti riuscì a risolvere il problema degli illeciti di bilancio, fu istituito il *PCAOB* che, come già esposto, assumerà il ruolo di controllare le attività del controllore esterno.

Il ruolo dei revisori indipendenti è sempre più fondamentale per migliorare il *reporting* finanziario delle aziende. Quest'ultimi sono chiamati a rispettare degli standard di audit emanati dall' *American Institute of Certified Public Accomunante (AICPA)* e dal *Public Company Accounting Overnight Board (PCAOB),* finalizzati a garantire che il processo di revisione venga condotto rispettando criteri di integrità e indipendenza.

Lo scopo principale della revisione esterna è verificare l'accuratezza dei rendiconti finanziari garantendo che siano redatti in conformità con i principi contabili generalmente accettati (GAAP). Con l'introduzione della nuova Legge federale i revisori indipendenti sono anche chiamati a valutare l'efficacia dei controlli interni e dell'informativa finanziaria messi in atto dalle organizzazioni per prevenire eventuali frodi, senza però entrare nel merito della bontà della struttura di controllo interno, motivo per cui le procedure di verifica da loro effettuate non sono finalizzate alla soddisfazione dei requisiti di attestazione.

Prima di accettare un incarico, le società di revisione devono dimostrare di essere in possesso dei requisiti di indipendenza e obiettività e di disporre di personale professionale competente, nonché del tempo necessario per svolgere il proprio ruolo in modo adeguato. Tale requisito di indipendenza deve perdurare per l'esercizio a cui si riferiscono i bilanci sottoposti a revisione e durante il periodo in cui viene effettivamente eseguita la revisione. Devono inoltre valutare la possibile presenza di rischi che potrebbero pregiudicare la propria indipendenza e se siano state adottate misure opportune per mitigarli.

Le leggi statunitensi vietano alla società di revisione di svolgere determinate funzioni, tra le quali:

- Servizi di tenuta dei libri contabili;
- Progettazione e attuazione di sistemi di informativa finanziaria;
- Servizi di outsourcing di audit interno;
- Servizi legali;
- Broker/dealer, consulenza d'investimento o servizi di investment banking;
- Funzioni svolte dal *management*, dalle risorse umane e servizi fiscali.

Per quanto riguarda le società statunitensi quotate è stabilito per Legge che l'*Audit Committee*[34] approvi preliminarmente tutti i servizi professionali che la società di revisione andrà a svolgere.[35]

Secondo quanto contenuto nel titolo II del *Sarbanes – Oxley Act* i revisori esterni devono riferire se concordano o meno con la valutazione fatta della Direzione del controllo interno della società sulla rendicontazione finanziaria. Per poter esprimere un giudizio circa il sistema di controllo interno è necessario che il revisore esterno esegua le seguenti attività:

- Valuti il *Management Assesment Processi;*
- Effettui a valle dei test sull'efficacia dei controlli a livello aziendale;
- Valuti i controlli progettati dal *management* destinati a mitigare i rischi di frode;
- Identifichi conti e asserzioni significative;
- Effettui test sui controlli interni;
- Valuti eventuali carenze nei controlli interni.[36]

Per permettere alle società di revisione di assolvere il proprio incarico e consentire alle aziende di conformarsi alla sezione 404, si rende necessaria l'adozione di un quadro di controllo interno che sia concorde con una procedura standard e si basi su criteri oggettivi e valutabili.

[34] L'*Audit Commitee* è un Comitato del consiglio di amministrazione responsabile della supervisione del processo di rendicontazione finanziaria, della selezione del revisore indipendente e della ricezione dei risultati della revisione, sia interna che esterna.
[35] P. Riva, *Ruoli di Corporate Governance*, EGEA spa, Milano, (2023).
[36] M.Bozzola, *Sarbanes-Oxley Act Sezione 404 (Internal Control over Financial Reporting)* in "Ernst&Young", (2010).

A tal punto, e al fine di sostenere le organizzazioni a gestire, valutare e migliorare il proprio del controllo interno, sono stati istituiti diversi *framework* che saranno oggetto di discussione nel prossimo capitolo.

Capitolo 2 – L'importanza del controllo interno e di una solida governance IT

2.1 Il framework COSO Internal Control Integrated Framework (ICIF)

Prima della nascita del *Sarbanes-Oxley Act,* le azioni intraprese da parte delle aziende sul sistema di controllo interno erano prettamente di natura spontanea e basate su molteplici modelli di riferimento. La *SEC* ha poi predisposto l'obbligo di utilizzare un modello di controllo interno riconosciuto e in grado di soddisfare criteri di obiettività, misurabilità, completezza e rilevanza, questo sia nell'ipotesi in cui l'azienda non disponesse di nessuna struttura preesistente sia nel caso in cui dovesse rafforzare il proprio quadro di controllo vigente.[37]

Per comprendere le origini e le motivazioni alla base della nascita del *framework* oggetto di discussione è necessario richiamare alcuni passaggi affrontati nel capitolo precedente.

Verso la fine della seconda metà del 1900, venne costituita la *Treadway Commission*, conosciuta anche come *National Commission on Fraudolent Financial Reporting,* nata grazie al supporto di alcune associazioni statunitensi, tra cui *American Institute of Certified Public Accountant, American Accounting Association* e *Financial Executive Institute*. La Commissione era incaricata di effettuare uno studio sulle principali cause responsabili dei casi di falsi di bilancio, che al tempo proliferavano nel mercato americano.

Come già sopraindicato, i lavori della delegazione si conclusero con la pubblicazione del *Report on Fraudulent Financial Reporting,* o *Treadway Report.* Attraverso questo scritto, la Commissione raccomandava alle aziende l'adozione di un'appropriata politica di *risk management* tale da poter segnalare anticipatamente i comparti aziendali con maggior esposizione al rischio e, contemporaneamente, tutelare e potenziare le aree più fragili. Il report

[37] *Moving Forward–A Guide to Improving Corporate Governance Through Effective Internal Control in* "Deloitte&Touche", (2003), pp 15.

evidenziava anche l'esigenza di sviluppare un modello standard di controllo interno.

A fronte di questa necessità, le associazioni che avevano supportato la *Treadway Commission* costituirono un nuovo gruppo di lavoro chiamato *Committee of Sponsoring Organizations of the Treadway Commission (COSO)* preposto alla definizione di un modello di riferimento di controllo interno che aiutasse il *management* ad esprimere una valutazione misurabile in merito. Lo studio venne svolto in compartecipazione con l'attuale società di revisione *PricewaterhouseCoopers* e ne scaturì un rapporto finale di quattro volumi denominato *Internal Control: Integrated Framework*, più noto come *COSO* Report.[38]

Di conseguenza, molte aziende hanno costruito la propria struttura di controllo interno intorno alle raccomandazioni del Comitato delle organizzazioni promotrici della *Treadway Commissione*.

Il *COSO Report* costituisce un vero e proprio manuale operativo il cui scopo è aiutare le aziende a gestire e migliorare il proprio controllo interno; ad oggi è il modello più conosciuto e utilizzato come *best practice* a livello mondiale per valutare l'adeguatezza di tale sistema, con particolare focus sull'informativa economico-finanziaria. Tale documento rappresenta uno strumento utile anche per soggetti esterni all'organizzazione, come investitori, stakeholders e revisori. Con riferimento ai controlli interni, il *COSO* ha emanato nel corso degli anni i seguenti documenti ed i relativi aggiornamenti:

- *Internal Control -Integrated Framework*, pubblicato nel 1992;
- *Internal Control Issues in Derivatives Usage*, pubblicato nel 1996;
- *Internal Control over Financial Reporting — Guidance for Smaller Public Companies*, pubblicato nel 2006;
- *Guidance on Monitoring Internal Control Systems*, pubblicato nel 2009;
- *Internal Control - Integrated Framework*, pubblicato nel 2013 (revisione del documento del 1992).[39]

[38] G. Gasparri, *I controlli interni nelle società quotate,* Quaderni Giuridici – CONSOB, Milano, 2013

[39] S. Pastorino, *Il sistema di controllo interno, l'applicazione dei principi del CoSo 2013-*

Focalizzando l'analisi sull'*ICIF*, le modifiche di maggior rilievo rispetto alla versione del 1992 riguardano:

- Una maggior evidenza circa la capacità del Sistema di Controllo interno di prevenire frodi;
- La centralità della tematica di *Corporate Governance*;
- Il riconoscimento del ruolo significativo assunto dalla tecnologia nell'implementazione del Sistema di Controllo Interno.

Il *framework* del 2013 evidenzia l'importanza del *management* nel processo di valutazione del sistema di controllo, per tale ragione prevede tre linee di controllo/difesa, a differenza della versione del 1992 che ne concepiva solo due. La prima linea di controllo spetta al *management* a cui è dato il compito di effettuare i controlli necessari per gestire il rischio inerente alle attività operative. La seconda linea riguarda le funzioni aziendali che svolgono attività di monitoraggio in ausilio al *management*, possono identificarsi ad esempio in funzioni di *risk management*, controllo di gestione e sicurezza sul lavoro, caratterizzate da autonomia di giudizio e limitata indipendenza.
Infine, la terza linea di controllo spetta alle funzioni di Revisore, Collegio Sindacale e *Internal Audit*¸ quest'ultimi svolgono uno *screening* indipendente sull'adeguatezza del sistema di controllo interno e gestione dei rischi e riferiscono direttamente al vertice dell'organizzazione.
Con l'istituzione del *Sarbanes-Oxley Act* il *framework* venne citato dal *PCAOB* come quadro di riferimento da adottare per valutare i controlli interni.
Tale rapporto fu utile a dare una definizione unanime del controllo interno, definito come "un processo, svolto dal Consiglio di Amministrazione, dai Dirigenti e da altri operatori della struttura aziendale, che si prefigge lo scopo di fornire una ragionevole sicurezza sulla realizzazione dei seguenti obiettivi:

- efficacia ed efficienza delle attività operative;
- attendibilità delle informazioni di bilancio;

Introduzione al CoSO Report, Webinar del Mercoledì INRL 2022 – INRL – Istituto Nazionale Revisori Legali, 09/03/2022.

- conformità alle leggi e ai regolamenti in vigore."[40]

Da questa definizione è possibile trarre cinque aspetti fondamentali del controllo interno. In primo luogo, **il controllo interno è un processo dinamico**, non un evento, costituito da attività continue, non fini a sé stesse, ed effettuato da persone e dalle azioni da esse intraprese a tutti i livelli di un'organizzazione. È possibile affermare inoltre, **che un efficace sistema di controllo interno sia in grado di fornire una garanzia ragionevole, ma non assoluta, all'alta Dirigenza e al Consiglio di Amministrazione delle società**. Viene utilizzato il termine garanzia, e non certezza, poiché il *framework* riconosce l'esistenza di limitazioni in tutti i sistemi di controllo interno, causate da incertezze che nessuno può prevedere, come ad esempio l'errore umano. Una ragionevole garanzia non implica che un'entità raggiungerà sempre i suoi obiettivi ma che un controllo interno efficace aumenti la probabilità di raggiungerli.

Il controllo interno si presta per essere adattabile alla struttura dell'organizzazione, flessibile nell'applicazione per l'intera entità, per una particolare controllata, divisione, unità operativa o processo aziendale. Concludendo, il processo di controllo interno è finalizzato alla realizzazione di obiettivi di una o più categorie distinte ma sovrapposte.

La definizione di obbiettivi allineati con la *mission*, *vision* e con le strategie dell'entità è un prerequisito per l'attività di controllo interno e una parte fondamentale del processo di gestione relativo alla pianificazione strategica. L'organizzazione, in questo senso, fissa gli obiettivi che vuole raggiungere, i quali possono riferirsi all'entità nel suo complesso o mirati ad attività specifiche. Esiste una stretta relazione tra gli obiettivi che un'entità stabilisce di conseguire, le componenti necessarie per raggiungere tali obiettivi e la struttura dell'entità stessa, che rappresenta l'organizzazione nel suo complesso, composta dalle unità operative, le divisioni, le funzioni e altre strutture.[41]

[40] G. Gasparri, *I controlli interni nelle società quotate in "*CONSOB - Quaderni Giuridici", Milano, (2013), pp 16.

[41] Committee of Sponsoring Organizations of the Treadway Commission (COSO), COSO Internal Control Certificate - Participant Manual, (2015).

Questa relazione è rappresentata nel *framework* sotto forma di un cubo.

Figura 2: Il cubo CoSo. Fonte: Accounting Internal Control

Gli **obiettivi** sono indentificati nelle tre colonne, le **componenti** sono rappresentate dalle cinque righe mentre la **struttura dell'entità** si trova nella terza dimensione del cubo.

Gli obiettivi assumono un ruolo fondamentale poiché risulterebbe poco pratico implementare un sistema di controllo interno senza aver prima concordato degli obiettivi specifici, misurabili, osservabili, raggiungibili, pertinenti e con una determinata scadenza.

Il *framework* definisce gli obiettivi raggruppandoli in tre categorie:

- Economicità (*Operations*): riguardano l'efficacia e l'efficienza delle operazioni dell'entità, compresi gli obiettivi di performance operativa e finanziaria e la salvaguardia degli *assets* contro le perdite.
- Attendibilità (*Reporting*): riguardano l'attendibilità della reportistica aziendale per scopi interni ed esterni per assolvere a finalità di informativa finanziaria e non finanziaria. Questo obiettivo è stato ampliato dal *framework* del 2013 attraverso l'introduzione dell'informativa interna ed enfatizzando il ruolo delle informazioni non finanziarie;
- Conformità (*Compliance*): riguardano il rispetto di leggi e normative cui l'entità è soggetta, siano esse di natura legislativa o volontaria.[42]

[42] L. Graham, *Internal control audit and compliance: documentation and testing under the new COSO framework*, John Wiley & Sons, (2015).

Il sistema di controllo interno (SCI) mira a facilitare il perseguimento dei suddetti obiettivi minimizzando le perdite economiche dell'organizzazione.
Avendo partecipato ad un progetto di *SOX Compliace*, per il cui sviluppo sono state prese come riferimento le linee guida del suddetto *framework*, ho potuto constatare che per permettere al SCI di contenere eventuali danni economici collegati a performance carenti a livello di economicità, attendibilità e conformità è necessario che le organizzazioni valutino anticipatamente la vulnerabilità dei propri sottosistemi aziendali, il grado di affidabilità dei sistemi di controllo interno e correlino i punti precedenti con valutazioni quantitative tramite tecniche di analisi di costi-benefici.[43]
Ciò a dimostrazione di quanto il sistema di controllo interno sia flessibile e per tale ragione deve essere progettato tenendo conto delle necessità specifiche dell'azienda che lo implementerà.
Gli attori che partecipano al controllo interno sono molteplici; il Consiglio di Amministrazione è chiamato a definire le linee guida del SCI e a supervisionare sulla loro effettiva attuazione. *CFO* e *CEO* sono responsabili di progettare e implementare un efficace sistema di controllo interno mentre al management operativo spetta il compito di implementare ed eseguire i controlli sui processi necessari a gestire i rischi nelle attività quotidiane. Le altre funzioni aziendali sono fondamentali per dare una guida e una valutazione del SCI relativamente alle loro aree di competenza, i revisori Interni forniscono garanzia e consulenza alla direzione del controllo interno promuovendone un miglioramento continuo, mentre i Revisori Indipendenti sono incaricati di verificare ed esaminare l'efficacia del controllo interno sull'informativa finanziaria esterna. È importante specificare che nonostante la natura della professione, questi non rappresentano a un sostituto ad un adeguato sistema di controllo interno.

Disponendo ora di un quadro dettagliato degli obiettivi previsti dal *framework* è possibile analizzare le componenti, che si identificano nelle cinque righe del cubo della figura 2.1

[43] S. Pastorino, *Il sistema di controllo interno, l'applicazione dei principi del CoSo 2013-Introduzione al CoSO Report,* Webinar del Mercoledì INRL 2022 – INRL – Istituto Nazionale Revisori Legali, 09/03/2022.

2.2 I cinque elementi del controllo interno e i relativi principi

Il *framework* del 2013 divide il controllo interno in cinque componenti, al fine di semplificare il compito del *management* di amministrare e supervisionare le attività che fanno parte di una struttura di controllo interno di successo. Tali componenti rappresentano gli elementi necessari per raggiungere i tre obiettivi analizzati precedentemente (economicità, attendibilità, conformità); ad ogni componente sono correlati dei principi, in totale diciassette, che ne costituisco i concetti fondamentali.

I diciassette principi servono a specificare quali sono i requisiti obbligatori di ogni componente del sistema di controllo interno ed ogni principio è modulabile a diverse realtà aziendale. Nonostante ciò, vale una presunzione di rilevanza di ognuno di essi, quindi, i casi aziendali nei quali un principio non viene applicato sono alquanto rari.

I componenti e i principi del *framework* devono quindi essere presenti e funzionare in modo integrato.

I cinque componenti del cubo *COSO* sono:

1. Ambiente di controllo;
2. Valutazione del rischio;
3. Attività di controllo;
4. Informazione e comunicazione;
5. Attività di monitoraggio.

L'ambiente di controllo comprende ogni aspetto del quadro di controllo interno ed è il componente fondamentale. Raggruppa l'insieme di standard, processi e strutture che forniscono la base per l'esecuzione del controllo interno e guidano gli attori nello svolgimento delle loro responsabilità in materia.

L'ambiente è influenzato da diversi fattori interni ed esterni, tra cui la storia dell'azienda, i valori, il mercato di riferimento e il panorama competitivo e normativo. La partecipazione al progetto prima menzionato mi ha permesso di comprendere operativamente quale sia il ruolo cardinale assunto da questa prima

componente del modello e come un'organizzazione che dispone di un solido ambiente di controllo si presenti più resiliente a fronte di pressioni negative interne ed esterne. L'ambiente di controllo è determinato da variabili di tipo individuale, rappresentate dalle caratteristiche delle risorse umane dell'organizzazione, da variabili di tipo sociale, derivanti dalle relazioni tra i soggetti aziendali, da variabili di tipo tecnico, inerenti al tipo di tecnologia utilizza e da variabili di tipo istituzionale, rappresentate dalla *governance* aziendale.[44]

A questo primo componente sono associati cinque principi.

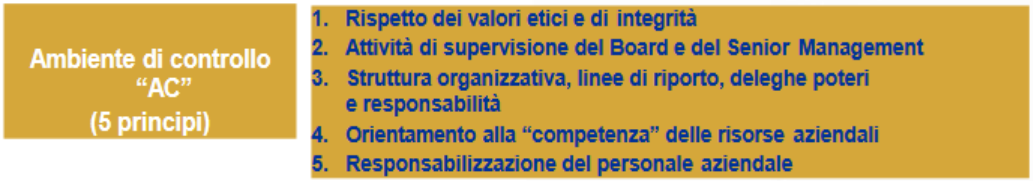


Figura 2.1: I 17 principi secondo il CoSo 2013. Fonte: revisori.it

Secondo il primo principio l'organizzazione deve dimostrare impegno per l'integrità e i valori etici.

Il Consiglio di Amministrazione e la Direzione devono dimostrare, attraverso i propri comportamenti, l'importanza dell'integrità e dei valori etici per sostenere il corretto funzionamento del sistema di controllo interno, attraverso la definizione di standard di condotta diffusi a tutti i livelli dell'organizzazione. Gli standard di condotta guidano l'azienda nel comportamento, nelle attività e nel perseguimento degli obiettivi stabilendo ciò che è giusto e sbagliato, fungendo da base per valutare l'aderenza dell'organizzazione all'integrità e all'etica. La direzione deve quindi valutare l'adeguatezza delle norme di condotta e risolvere in modo tempestivo qualsiasi deviazione da quest'ultime.

Il modo in cui le aspettative dell'alta dirigenza sono comunicate e applicate a tutta l'organizzazione è influenzato dallo stile operativo e della condotta personale del *management*, nonché dal loro atteggiamento verso il rischio, stile direzionale e grado di formalità.[45]

[44] F. Venturelli, *I processi di controllo interno sulla rendicontazione e la loro revisione: l'esperienza statunitense*. Cacucci Editore, (2007).

[45] L.Provaroni, *Il sistema di controllo interno nelle piccole e medie imprese,* Ordine dei Dottori

Delle linee guida coerenti e condivise unite ad una forte cultura organizzativa abbracciata da tutta l'entità, rappresentano due elementi imprescindibili per il funzionamento del sistema di controllo interno.

Il secondo principio identifica le responsabilità del Consiglio di Amministrazione, che deve operare in modo indipendente dalla Direzione e assicurare la supervisione del sistema di controllo interno del quale ne risulta responsabile per quanto riguarda la progettazione, l'attuazione e la condotta. Il Consiglio definisce inoltre le competenze necessarie tra i suoi membri tali da poter porre domande di verifica ai Dirigenti e intraprendere azioni commisurate.

Il terzo principio relativo all'ambiente di controllo prevede che la direzione stabilisca, con la supervisione del Consiglio, la struttura organizzativa e le linee di rendicontazione necessarie a programmare, gestire e valutare periodicamente le attività dell'organizzazione e ad espletare le varie responsabilità.
La Direzione autorizza le risorse ad agire come richiesto per un determinato ruolo, ma è anche necessario definire delle limitazioni per poter raggiungere gli obiettivi dell'entità. La tecnologia, in questo senso, viene sfruttata per facilitate la definizione e la limitazione dei ruoli e delle responsabilità all'interno dei processi aziendali.
Il Gruppo di Ricerca Governance di Assirevi valorizza la necessità di effettuare una valutazione del SCI prendendo in considerazione tutti gli elementi che caratterizzano l'attività di un'organizzazione, quindi i prodotti, le linee di business, le società e i mercati. Effettivamente, se da un lato la valutazione del sistema di controllo effettuata prendendo in considerazione un solo elemento, potrebbe in certi casi non rilevare particolari carenze, dall'altro una visione completa dei vari elementi potrebbe invece segnalare la concentrazione di rischi attorno a determinati fattori, così da consentire l'individuazione del rischio e l'avviamento delle linee guida per la loro mitigazione, che, diversamente, non sarebbero state individuate.[46]

Commercialisti e degli Esperti Contabili, Roma, (2023).
[46] Gruppo di Ricerca Governance, *Monografia n.1 - COSO Framework: guida alla lettura*, ASSIREVI, Milano, (2019).

Esemplificando, se un'organizzazione considerasse all'interno del proprio quadro di controllo solamente delle linee di prodotto, senza però valutare l'andamento del mercato e del business di riferimento, difficilmente potrà disporre di una visione estesa del contesto in cui si colloca, andando a compromettere la validità del proprio sistema di controllo interno e valutazione del rischio.

Secondo il quarto principio l'organizzazione deve dimostrare impegno ad attrarre, sviluppare e mantenere al proprio interno risorse competenti. La definizione di politiche e pratiche rappresenta la base per specificare le competenze necessarie a supportate il controllo interno all'interno dell'organizzazione, un esempio potrebbe essere la conoscenza del funzionamento delle piattaforme IT alla base dei processi aziendali. Politiche e pratiche sono funzionali a valutare eventuali carenze e a definire azioni correttive, costituiscono inoltre un mezzo per reagire dinamicamente al cambiamento.

Infine, il quinto ed ultimo principio relativo all'ambiente di controllo, stabilisce che l'organizzazione ritiene il personale aziendale responsabile per l'esecuzione delle responsabilità di controllo interno nel perseguimento degli obiettivi.
Le prestazioni sono fortemente influenzate dalla misura in cui gli individui sono ritenuti responsabili e da come sono ricompensati. In questo senso, le Direzione e il Consiglio di Amministrazione devono stabilire misure di performance e incentivi adeguati alle responsabilità previste a tutti i livelli dell'organizzazione, considerando il raggiungimento di obiettivi a breve e a lungo termine. I meccanismi di ricompensa supportano l'efficacia del controllo interno nel momento in cui si adattano dinamicamente agli obiettivi dell'entità.[47]

La valutazione del rischio rappresenta la seconda componente del cubo, la sua rilevanza deriva dal fatto che ogni entità è sempre più frequentemente chiamata

[47] Committee of Sponsoring Organizations of the Treadway Commission (COSO), COSO Internal Control Certificate - Participant Manual, (2015).

ad affrontare una varietà di rischi provenienti da fonti interne ed esterne. Il rischio rappresenta la probabilità che un evento si verifichi e influenzi negativamente il raggiungimento degli obiettivi. La valutazione del rischio comporta un processo dinamico e iterativo finalizzato ad individuare ed analizzare i fattori che possono pregiudicare il raggiungimento degli obiettivi dell'organizzazione e come questi richiedono di essere gestiti. Logicamente, per poter identificare il rischio è prima necessario individuare le tre tipologie di obiettivi collegati ai diversi livelli dell'entità, analizzate in precedenza.
Difatti, il rischio spesso aumenta quando gli obiettivi differiscono dalle prestazioni, questo accade quando un'entità non esplicita i propri obiettivi perché ritiene che i suoi risultati siano già accettabili.
Il processo di *risk management* si articola nelle seguenti fasi:

- Identificazione degli eventi negativi;
- Valutazione di probabilità e impatto economico;
- Individuazione dei rimedi applicabili.[48]

I rischi possono derivare da fattori esterni, come il cambiamento tecnologico, e da fattori interni che invece fanno riferimento a variabili come la competenza del personale e l'obsolescenza dei sistemi informatici aziendali.
Un altro elemento fondamentale di questa componente è la tolleranza del rischio, ovvero il livello accettabile di variazione delle prestazioni rispetto agli obiettivi. Come per la definizione degli obiettivi, la fissazione dei livelli di tolleranza è una condizione preliminare alla valutazione del rischio. In linea generale, la Direzione si avvale di discrezionalità nella definizione della tolleranza, tuttavia, quando sono presenti dei requisiti esterni come quelli sulla rendicontazione, la tolleranza al rischio è determinata considerando leggi, norme, regolamenti e standard.
Senza un'applicazione pratica delle disposizioni del modello non avrei potuto comprendere la differenza notevole che esiste tra la valutazione dei rischi, che è

[48] L.Provaroni, *Il sistema di controllo interno nelle piccole e medie imprese,* Ordine dei Dottori Commercialisti e degli Esperti Contabili, Roma, (2023).

parte integrante del sistema di controllo interno, e la gestione del rischio, che contrariamente è parte del processo manageriale.
Alla componente "valutazione del rischio" sono correlati quattro principi:

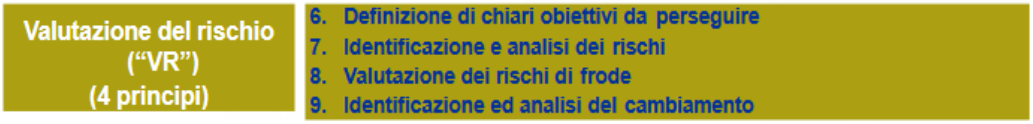


Figura 2.2: I 17 principi secondo il CoSo 2013. Fonte: revisori.it

Il primo principio richiama la necessità che l'entità specifichi anticipatamente gli obiettivi operativi, di informativa e di conformità con sufficiente chiarezza per consentire l'individuazione e la valutazione dei rischi correlati ad essi.
Il secondo principio rappresenta il principio cardine dei sistemi di controllo interno e di gestione del rischio, richiedendo all'organizzazione di identificare e analizzare i rischi a livello di entità, divisioni e unità operative. Per l'identificazione è necessario che l'organizzazione consideri sia fattori interni che esterni e il relativo impatto sulla gestione, per la valutazione è invece richiesto il coinvolgimento dei vari livelli dell'organizzazione per definire come il rischio dovrebbe essere gestito. Una volta identificati, i rischi verranno analizzati per determinarne la potenziale significatività. La metodologia di analisi può variare, soprattutto perché molti rischi sono di difficile quantificazione; a prescindere dal metodo utilizzato, il processo include la valutazione della probabilità che il rischio si verifichi e la stima del suo impatto. I rischi presi in considerazione dalla gestione sono i rischi intrinsechi e i rischi residui, i primi rappresentano il rischio per il raggiungimento degli obiettivi di un'entità in assenza di azioni per alterarne la probabilità o l'impatto, il secondo è invece il rischio che rimane dopo che tutte le precauzioni e misure di sicurezza sono state attuate. Una volta valutata l'importanza potenziale dei rischi, la Direzione considera come gestirli attraverso un bilanciamento tra rischio e tolleranza. Le possibili risposte ai rischi sono: accettarli, evitarli, ridurli o condividerli.

Le responsabilità per l'identificazione e l'analisi dei rischi sono a capo della Direzione e delle sottounità aziendali.[49]
Il Gruppo di Ricerca Governance sostiene che tale attività non possa prescindere dal coinvolgimento del management, il quale, controllando quotidianamente le operazioni aziendali, risulta essere l'attore più idoneo ad individuare i rischi correlati ai vari processi aziendali.

Il terzo principio prevede che l'organizzazione consideri il potenziale rischio di frode nella valutazione dei rischi. I tipi di frode più comuni sono la segnalazione fraudolenta, che si verifica quando i report di un'entità sono i intenzionalmente redatti con omissioni, la salvaguardia dei beni, che fa riferimento alla protezione contro l'uso inappropriato di beni e di altre risorse di un'entità e la corruzione, particolarmente rilevante per la categoria di obiettivi di conformità.
Nell'ambito della valutazione del rischio di frode, l'organizzazione deve anche considerare possibili incentivi, pressioni e opportunità che potrebbero indurre gli individui a commettere tale reato.

Il quarto e ultimo principio sollecita le organizzazioni a identificare e valutare cambiamenti significativi che potrebbero avere un impatto sul sistema di controllo interno. Tali cambiamenti possono avvenire nell'ambiente esterno, quindi normativo, economico e fisico in cui opera l'azienda, a livello di *business model,* ad esempio tramite l'implementazione di una nuova tecnologia, e a livello di *leadership* che può far riferimento a cambiamenti rilevanti all'interno delle risorse aziendali.

Le attività di controllo costituiscono il terzo componente del *framework* e rappresentano l'insieme di politiche e procedure che contribuiscono a garantire l'attuazione delle direttive di gestione, finalizzate ad attenuare i rischi. Tali attività possono essere di natura preventiva o investigativa e comprendono attività manuali e automatizzate.

[49] Committee of Sponsoring Organizations of the Treadway Commission (COSO), COSO Internal Control Certificate - Participant Manual, (2015).

È possibile individuare tre categorie di attività di controllo:

- Controlli inerenti agli aspetti operativi;
- Controlli sulle informazioni di bilancio;
- Controlli sul rispetto di vincoli normativi e regolamentari.[50]

I principi relativi a questa componente del cubo sono i seguenti:

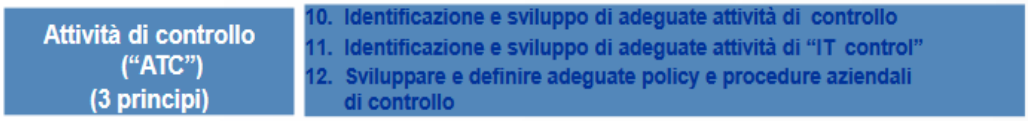


Figura 2.3: I 17 principi secondo il CoSo 2013. Fonte: revisori.it

Secondo il primo principio l'organizzazione deve selezionare e sviluppare attività di controllo che contribuiscano alla mitigazione dei rischi per il raggiungimento degli obiettivi. Per farlo, è necessario integrare questa attività con quella di valutazione del rischio, in questo modo la Direzione individua le azioni necessarie per attuare risposte specifiche al rischio.

Nel determinare quali azioni mettere in atto è importante prendere in considerazione i fattori specifici e i processi aziendali rilevanti dell'entità in esame. Assirevi pone l'accento sull'importanza di correlare il processo di identificazione delle attività di controllo con l'attività di individuazione dei rischi aziendali. Questa considerazione è di estrema importanza proprio perché la finalità primaria dell'implementazione delle attività di controllo è quella di assicurare che i modi con cui l'organizzazione risponde ai rischi siano adeguati e abbiano effettiva attuazione. È pertanto fondamentale effettuare una rilevazione e rappresentazione dei rischi al fine di consentire un efficace disegno delle attività di controllo. Un altro punto portato alla luce dal Gruppo riguarda l'importanza di definire attività di controllo tanto più stringenti quanto più è limitato il livello di tolleranza del rischio, che deve essere quindi conosciuto e diffuso a tutta l'organizzazione.

Un fattore su cui il *framework* non si sofferma, ma che a livello operativo risulta cardinale, è assicurare che le misure di controllo siano estese anche ad eventuali

[50] F. Venturelli, *I processi di controllo interno sulla rendicontazione e la loro revisione: l'esperienza statunitense*. Cacucci Editore, (2007).

processi o parti di processo gestiti al di fuori del perimetro dell'azienda, attraverso controlli sulla contrattualistica ma anche sulle misure adottate dai fornitori di servizi esterni.[51]

Il secondo principio esplicita l'importanza di identificare e sviluppare attività di controllo che includano la tecnologia.

Da un lato la tecnologia rappresenta un rischio da mitigare, considerato il crescente volume di dati gestiti per via informatica, dall'altro uno strumento per svolgere i controlli.

L'affidabilità dei controlli automatizzati dipende dallo sviluppo e implementazione di adeguate attività di *IT control* o controlli generali sulla tecnologia, che permettono di garantirne il funzionamento corretto e continuo.

I numerosi utilizzi della tecnologia sottolineano l'importanza della gestione della sicurezza, le cui minacce possono provenire da fonti esterne ed interne. Le minacce esterne sono particolarmente rilevanti negli ambienti aziendali altamente interconnessi di oggi, attraverso le attività di controllo della sicurezza vengono impediti, ad esempio, utilizzi ed accessi non autorizzati del sistema informativo, garantendo così l'integrità del programma, dei dati e limitando gli intenti dolosi.[52] Il modello tratta il tema dei controlli sulla sicurezza informatica ad alto livello, senza dettagliare come far fronte alla complessità delle infrastrutture tecnologiche odierne. Il Gruppo di Ricerca di Assirevi, attraverso una monografia sul *framework,* aggiunge alcuni spunti essenziali per sviluppare controlli generali sui sistemi informativi che comprendano attività sugli accessi non autorizzati a supporto della *segregation of duties*, specificando l'importanza di configurare i sistemi in modo da riconoscere solo le utenze autorizzate dalla Direzione e prevedere apposite modalità per l'autenticazione degli user. Tale lettura operativa del modello è risultata molto utile per comprendere come applicare a livello pratico le disposizioni relative al secondo elemento del cubo.

[51] Gruppo di Ricerca Governance, *Monografia n.1 - COSO Framework: guida alla lettura*, ASSIREVI, Milano, (2019).

[52] Committee of Sponsoring Organizations of the Treadway Commission (COSO), COSO Internal Control Certificate - Participant Manual, (2015).

L'ultimo principio previsto dal *framework* richiede all'organizzazione di definire *policy* e procedure che riflettano ciò che deve essere messo in atto per effettuare il controllo. Viene evidenziata l'importanza di includere all'interno delle procedure i tempi di esecuzione delle attività di controllo ed eventuali azioni correttive. Un altro aspetto da considerare operativamente è la riesamina e l'aggiornamento periodici del sistema di attività di controllo ogniqualvolta si verifichi un cambiamento significativo all'interno dell'entità.

La quarta componente riguarda il flusso informativo e prevede che le informazioni e le comunicazioni relative al controllo interno vengano trasmesse dall'entità internamente ed esternamente, in modo da consentire agli attori di svolgere i propri compiti. Questa componente supporta il funzionamento di tutte le altre ed è rafforzata dai sistemi informativi aziendali. Le comunicazioni possono avvenire verso il basso, quindi verso i dipendenti, verso l'alto, dirette alla Direzione oppure trasversalmente a tutta l'organizzazione e verso i vari *stakeholders*.
Il quadro distingue questa componente con la categoria di obiettivi di rendicontazione interna ed esterna, specificando che per il raggiungimento di quest'ultimi è necessaria la coesistenza di tutti e cinque i componenti del *framework.*
Di seguito i principi relativi alla componente in esame:

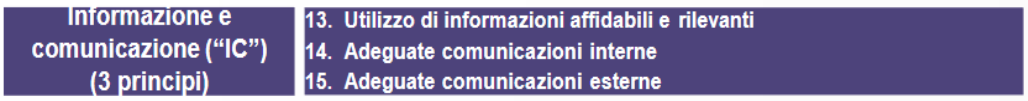


Figura 2.4: I 17 principi secondo il CoSo 2013. Fonte: revisori.it

Il *management* deve divulgare informazioni provenienti da fonti pertinenti interne ed esterne e selezionare quelle più rilevanti e utili per la propria struttura organizzativa e modello di *business*. Il Gruppo di Ricerca aggiunge un punto di attenzione sostenendo che tanto più nelle organizzazioni ci si sposta verso il basso tanto più è fondamentale una verifica preventiva dell'effettiva disponibilità delle informazioni, specificando l'importanza di muoversi con

largo anticipo per ottenere dati da una fonte. Ho potuto constatare la veridicità di questa assunzione attraverso la partecipazione al progetto *SOX Compliance,* durante il quale ho compreso che il processo di acquisizione delle informazioni è tanto più critico quanto più delicate sono tali informazioni per il raggiungimento degli obiettivi di controllo.[53]

In questo senso, i sistemi informativi vengono implementati a supporto dei processi aziendali per poter acquisire ed elaborare grandi volumi di dati per poi trasformali in informazioni significative e utili a soddisfare i requisiti informativi. Se da un lato un maggior accesso alle informazioni rappresenta un *driver* di miglioramento per il controllo interno, dall'altro l'aumento del volume di dati può anche creare rischi di conformità, *privacy* e sicurezza.

Un elemento fondamentale per un efficace sistema di controllo interno è la qualità delle informazioni; dati incompleti o inesatti potrebbero portare a decisioni di gestione potenzialmente errate. La qualità delle informazioni diffuse è valutata in base al contenuto, alla tempestività, all'aggiornamento, all'accuratezza e all'accessibilità delle stesse.[54]

Comunicare internamente le informazioni è necessario per poter consentire a tutto il personale di comprendere ed eseguire le proprie responsabilità in termini di controllo interno.

Assirevi analizza il ruolo svolto dalla comunicazione interna enfatizzando la necessità di effettuare una separazione tra linee informative per garantire un corretto funzionamento del sistema di controllo interno e della gestione del rischio. Ad esempio, la creazione un canale di *whistleblowing* potrebbe essere un modo efficiente per attivare comunicazioni confidenziali e anonime.

L'organizzazione deve anche stabilire dei canali di comunicazione con l'esterno per fornire ai propri *stakeholders* evidenze sugli obiettivi dell'entità ma anche per ricevere informazioni di ritorno come tendenze, normative, eventi, reclami e richieste. I risultati dell'analisi del processo di *risk assesment* generalmente non

[53] Gruppo di Ricerca Governance, *Monografia n.1 - COSO Framework: guida alla lettura*, ASSIREVI, Milano, (2019).

[54] L.Provaroni, *Il sistema di controllo interno nelle piccole e medie imprese,* Ordine dei Dottori Commercialisti e degli Esperti Contabili, Roma, (2023).

vengono divulgati all'esterno poiché potrebbero essere percepiti come carenze da parte dei clienti, stakeholder o concorrenti.
Nonostante ciò, un contatto aperto con l'esterno è indubbiamente un ulteriore supporto per mantenere un ambiente di controllo sano.

Quinta ed ultima componente del cubo *COSO* è il monitoraggio; i sistemi di controllo interno necessitano di essere monitorati per valutarne le performance e accertare la presenza e il funzionamento di tutte le cinque attività analizzate. Le valutazioni possono essere continue e/o specifiche.
Le valutazioni continue sono operazioni di routine e forniscono informazioni tempestive, mentre le valutazioni specifiche possono variare in funzione della valutazione dei rischi e vengono svolte da soggetti altamente specializzati e indipendenti, un esempio sono le attività di *internal auditing* [55]

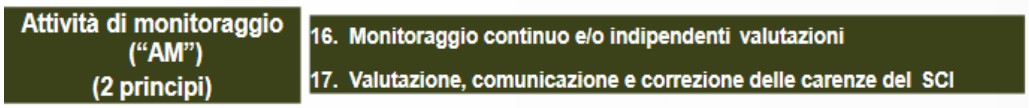


Figura 2.5: I 17 principi secondo il CoSo 2013. Fonte: revisori.it

Al quinto componente sono associati gli ultimi due dei diciassette principi previsti dal *framework* da cui si evince la finalità delle attività di monitoraggio, ossia accertare, attraverso valutazioni continue e periodiche, che le componenti del SCI siano presenti e funzionanti o, in caso contrario, se necessario attuare dei cambiamenti. Le attività di monitoraggio forniscono un prezioso input per controllare se il sistema di controllo continui ad essere performante e sia in grado di affrontare nuovi rischi. Un ulteriore fattore che ho compreso partecipando al progetto riguarda la distinzione tra le attività di monitoraggio e le attività di controllo; a livello operativo le prima servono a valutare se i controlli interni relativi a ciascuno dei cinque componenti funzionino come dovrebbero, mentre le attività di controllo rispondono specificatamente ad un determinato rischio.

[55] Committee of Sponsoring Organizations of the Treadway Commission (COSO), COSO Internal Control Certificate - Participant Manual, (2015).

Nel caso in cui vengano riscontrate carenze di controllo interno, come lacune reali o potenziali in qualche componente, l'organizzazione deve provvedere a comunicarle tempestivamente ai soggetti responsabili al fine di adottare misure correttive.

Il *COSO framework* mira ad andare oltre alla concezione del controllo interno inteso come una mera attività ispettiva, aiutando il *managemen*t a controllare al meglio l'organizzazione e fornendo al *Board* una capacità aggiuntiva di supervisionare il controllo interno.

Il concetto principale che ho potuto constatare attraverso l'applicazione pratica del modello in un contesto aziendale è che il controllo interno diventa efficace solo se percepito come parte integrante dell'attività di impresa, e non come un adempimento sostanzialmente improduttivo.

2.3 L'evoluzione dei controlli interni: l'*ERM* a supporto della gestione dei rischi

In un mondo in constante evoluzione, stare al passo con il cambiamento è determinante per le aziende per poter raggiungere i propri obiettivi di business.

Un esempio lampante è stata la crisi generata dal COVID-19, che ha rimarcato la necessità di implementare processi di *risk management* appropriati e integrati nei processi decisionali.

I *framework* proposti dal *COSO* sono inevitabilmente chiamati a seguire costantemente le evoluzioni con adeguamenti progressivi; i nuovi modelli proposti di seguito sono i più rilevanti ai fini dell'analisi.

Approcci più recenti tendono infatti a sottolineare la centralità del rischio nel sistema di controllo interno, a tale scopo è stato pubblicato da parte del Consiglio del *COSO* l'*Enterprise Risk Management-Integrated Framework* del 2004.

"L'*ERM* è un processo, posto in essere dal Consiglio di Amministrazione, dal *management* e da altri operatori della struttura aziendale, utilizzato per la formulazione delle strategie in tutta l'organizzazione e progettato per individuare eventi potenziali che possano influire sull'attività aziendale, gestire il rischio

entro limiti accettabili e fornire una ragionevole sicurezza sul perseguimento degli obiettivi aziendali.»[56]

L'*Entreprise Risk Management* è utile al *management* per mettere in atto un'efficace ed efficiente gestione delle condizioni di incertezza e dei correlati rischi e opportunità, con il fine ultimo di salvaguardare e creare valore.

Negli ultimi dieci anni, tale pubblicazione ha ottenuto un'ampia accettazione da parte delle organizzazioni nei loro sforzi per la gestione il rischio. Tuttavia, ad oggi, la complessità del rischio è notevolmente cambiata; se da un lato sono emersi nuovi rischi d'altro canto sia i Consigli di amministrazione che i Dirigenti hanno migliorato la loro consapevolezza e supervisione della gestione del rischio aziendale, chiedendo al contempo la nascita di nuovi *framework* più aggiornati.

A tal proposito il documento del 2004 è stato revisionato ed è stato pubblicato nel 2017 un aggiornamento intitolato *Enterprise Risk Management–Integrating with Strategy and Performance*. Tale versione mira ad affrontare l'evoluzione della gestione del rischio aziendale e a sostenere le necessità delle organizzazioni di migliorare il loro approccio per soddisfare le esigenze di un ambiente di business sempre in evoluzione.

Di seguito verranno brevemente discusse le principali evoluzioni del COSO *framework.*

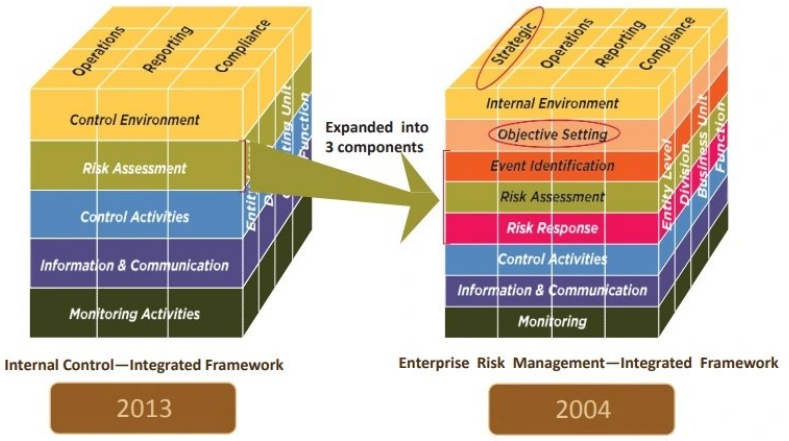


Figura 2.6: From COSO ICIF to COSO ERM. Fonte: "Strategic Finance"

[56]Committee of Sponsoring Organizations of the Treadway Commission (COSO), Enterprise Risk Management – Integrated Framework Executive Summary, (2004).

Osservando la figura 2.7 è possibile notare le principali differenze rispetto al *framework ICIF* del 2013, precedentemente analizzato.

In primo luogo, l'*ERM* prevede una nuova categoria di obiettivi (obiettivi strategici) ad un livello superiore rispetto agli altri tre già presenti.

Le componenti del cubo da cinque sono passate ad otto attraverso l'introduzione dell'elemento "fissazione degli obiettivi" e la scomposizione del fattore "valutazione del rischio" nelle tre componenti che articolano il tipico processo di gestione del rischio: identificazione degli eventi negativi (*event identification*), valutazione della probabilità e impatto economico (*risk assesment*) ed individuazione delle contromisure da applicare (*risk response*).

Se la dimensione d'analisi prevista dal cubo del 2013 è declinata ad attività, processi e unità organizzative, attraverso l'*ERM* viene estesa all'intera azienda.

L'*ERM framework* integra la versione *ICIF* rendendo il controllo una parte integrante della gestione del rischio imprenditoriale.[57]

Come già precedentemente annunciato, la dinamicità dei contesti aziendali ha reso necessario un cambiamento nel modo di pensare ed approcciare al rischio. A fronte di queste necessità è stata emanata una nuova versione del *COSO ERM* nel 2017.

Le principali innovazioni introdotte dal nuovo *framework* riguardano l'introduzione di una nuova struttura, le otto componenti presenti nella versione del 2004 sono state ridotte a cinque alle quale sono stati correlati venti principi idonei ad essere applicati ad ogni tipo di azienda. Un ulteriore aspetto positivo sono i benefici apportati dell'*ERM* poiché il nuovo *framework* integra maggiormente la gestione del rischio con la definizione di obiettivi strategici e il controllo delle performance. La concentrazione sull'integrazione della gestione del rischio permette inoltre di migliorare la gestione del rischio collegandolo alla strategia, alle attività quotidiane e alla cultura aziendale. La prospettiva del *framework*, scritto dal punto di vista del business, rende le conversazioni sul rischio rilevanti e universali e attraverso la fissazione di definizioni e principi fondamentali pensati per tutti i livelli di gestione coinvolti nella progettazione,

[57] J. Stephen McNally, *Leveraging Effective Risk Management, and Internal Control* in "Strategic Finance", pp. 29-36, (2014).

implementazione e conduzione di pratiche *ERM*. Infine, il focus sul ruolo evolutivo dell'*Information Technology* mette in risalto come le tendenze aziendali, la proliferazione di dati, l'intelligenza artificiale e l'automazione influenzino la strategia di un'organizzazione, il contesto aziendale e la gestione del rischio.

Le cinque nuove componenti prima citate sono le seguenti:

- *Governance* e cultura aziendale: rappresentano gli elementi fondamentali per un efficace *Enterprise Risk Management,* una cultura del rischio diffusa a tutta l'organizzazione è la base per sostenere valori etici, di integrità, trasparenza e *accountability*;
- Definizione della strategia e degli obiettivi di business: questa componente si focalizza sulla pianificazione strategica e sul modo in cui l'organizzazione comprende l'effetto di fattori interni ed esterni sul rischio;
- Performance: questa fase comprende l'individuazione dei rischi che potrebbero influire negativamente sui risultati e sulle prestazioni, la loro valutazione e la selezione delle strategie di risposta per condurre il profilo del rischio all'interno di soglie ritenute accettabili;
- Controllo e revisione: riesaminare i potenziali rischi e i cambiamenti in atto al fine di rimodulare le strategie intraprese e migliorare il processo è una componente fondamentale del *framework*;
- Informazione, comunicazione e *reporting*: quest'ultima componente, come già analizzato nel *framework* del 2013, puntualizza l'importanza di condividere, comunicare e riportare le informazioni rilevanti a tutti i livelli dell'organizzazione, sfruttando al meglio le tecnologie a disposizione.[58]

[58] Committee of Sponsoring Organizations of the Treadway Commission (COSO), Enterprise Risk Management Integrating with Strategy and Performance Executive Summary, (2017).

I venti principi correlati alle componenti sono in parte similari a quelli del *COSO ICIF* del 2013 e rappresentano le iniziative che le aziende sono chiamate a mettere in pratica per realizzare processi integrati di gestione del rischio.

Figura 2.7: I principi dell'ERM integrato con strategia e prestazioni Fonte: www.coso.org

Il Gruppo di Ricerca Governance di Assirevi, all'interno della Monografia n.3 - *COSO ERM,* propone un'analisi più operativa dei venti principi sopra riportati. Particolarmente interessanti sono le considerazioni esposte riguardanti la definizione della propensione al rischio, dove viene enfatizzato il fatto che non può esistere una strategia di definizione standardizzata e applicabile indistintamente a qualsiasi organizzazione. Il Gruppo propone inoltre una serie di parametri che, se integrati alla lettura del *framework*, possono aiutare le aziende a definire la propria propensione al rischio in modo più dettagliato, mettendo in evidenza l'importanza di valutare possibili scenari alternativi così da poter scegliere la strategia più adatta per creare valore e proponendo gli approcci più diffusi per effettuare tale valutazione, tra cui l'analisi dei *competitors* e la *scenario analysis*.

Gli autori della monografia in oggetto puntualizzano un ulteriore elemento poco discusso all'interno del modello, ossia la necessità di effettuare un'analisi prospettica del rischio e non fermarsi alla considerazione dei soli dati storici. Questo è un dettaglio che, se preso in considerazione, oggi può fare una grande differenza, considerato che le organizzazioni non possono più far affidamento su scenari stabili e tassi di crescita in linea con il normale ciclo economico, fatto e considerazione che ho potuto rilevare, con la mia esperienza diretta in questo progetto, essere ancora più applicabile al mondo della moda.

Un altro spunto stimolante analizzato nello studio, in riferimento ai principi relativi alla comunicazione e al reporting, sono le opportunità apportate dall'intelligenza artificiale e dal *data mining,* che consentono alle aziende di gestire importanti volumi di dati non strutturati a supporto del processo di elaborazione delle informazioni e della gestione del sovraccarico di dati.[59]
Proseguendo con l'analisi del modello, osservando la figura 2.9 si può notare come la struttura sia completamente diversa dalla versione precedente. Il passaggio grafico da un cubo tridimensionale a un diagramma rappresenta il sostanziale mutamento del *framework.*

Figura 2.8: La nuova struttura dell'ERM. Fonte: risk&compliance.it

Questo nuovo approccio, non meramente grafico, vuole enfatizzare come le cinque componenti avvolgano tutti gli step principali dello sviluppo e dell'esecuzione di una strategia aziendale, posizionando il processo di gestione del rischio al centro della catena del valore. Il nastro a tre bande rappresenta i processi comuni che scorrono all'interno di un'entità mentre il nastro a due bande raffigura il meccanismo di supporto fornito dell'*ERM.*
Anche le direttive contenute nel *framework* in discussione sono state utilizzate per l'esecuzione del progetto di *SOX Compliace.* Difatti, l'applicazione operativa di quest'ultime mi ha permesso di comprendere che soltanto attraverso una totale integrazione tra le componenti e i classici elementi della gestione

[59] Gruppo di Ricerca Governance, *Monografia n.3 - COSO ERM: guida alla lettura*, ASSIREVI, Milano, (2020).

aziendale come *Mission*, *Vision*, valori, strategia e obiettivi le aziende possono arrivare a creare, conservare e realizzare valore.[60]

L'obiettivo principale è quindi creare le condizioni necessarie affinché le organizzazioni possano assumere decisioni consapevoli volte al raggiungimento dei propri obiettivi strategici.

L'adattabilità al contesto e alle esigenze di qualsiasi azienda rappresenta il principale punto di forza del modello.

Altri vantaggi apportati sono:

- Una connessione più chiara tra la gestione del rischio aziendale e le aspettative degli *stakeholders*;
- Consentire alle organizzazioni di anticipare il rischio con la consapevolezza che il cambiamento possa portare a nuove opportunità e non sempre ad una potenziale crisi;
- Posizionare il rischio all'interno del contesto delle performance di un'organizzazione, piuttosto che considerarlo come un evento isolato.

La gestione del rischio aziendale è e continuerà ad essere un elemento importante per affrontare un futuro colmo di volatilità, complessità ed in continuo cambiamento. Diverse tendenze hanno particolare impatto sulla gestione del rischio, basti pensare alla proliferazione dei dati, allo sfruttamento dell'intelligenza artificiale e dell'automazione, al tema della sostenibilità e all'introduzione dell'omnicanalità; tutte evoluzioni che hanno apportato numerose opportunità di business ma che al contempo hanno aumentato i rischi di introdurre anomalie, di non rispettare leggi locali o ancora di incorrere in casi di *greenwashing*.[61] In tal senso, il Gruppo di Ricerca Governance di Assirevi propone un'interessante utilizzo del COSO ERM *framework* per la gestione dei rischi ESG attraverso l'integrazione al suo interno dei temi di sostenibilità, accrescendo così ulteriormente il calibro assunto dal modello nella sua declinazione verso il dare consistenza ai nuovi modi di accrescere il valore aggiunto all'analisi dei rischi estesa.

[60] N.Zanghi, *Il Framework ERM e i fattori chiave per l'implementazione* in "Assirevi", Milano, (2020).

[61] Committee of Sponsoring Organizations of the Treadway Commission (COSO), Enterprise Risk Management Integrating with Strategy and Performance Executive Summary, (2017).

2.4 Il ruolo dei sistemi informativi

Nella quasi totalità delle realtà aziendali odierne i processi di *reporting* finanziario sono realizzati attraverso l'utilizzo di sistemi IT, nella maggior parte dei casi rappresentati da *Entreprise Resource Planning*. Tali sistemi fino a pochi anni fa rappresentavano dei semplici raccoglitori ed elaboratori di dati contabili. Oggi, sono il polmone informativo delle organizzazioni e sono profondamente correlati alle transazioni finanziarie e all'intero processo di reporting finanziario, poiché agevolano la gestione e l'elaborazione di moli di dati contabili che risulterebbe impossibile trattare attraverso procedure manuali.

Tuttavia, i benefici apportati derivanti dall'automazione dei processi aziendali sono saldamente correlati alla correttezza ed esattezza utilizzata durante il procedimento di inserimento dei dati nel sistema informativo e alle procedure di elaborazione degli stessi.

Ai fini delle conformità *SOX*, nasce da qui l'esigenza di valutare e gestire i rischi della componente tecnologica presente all'interno delle aziende. [62]

Ciò implica che vengano applicati dei protocolli di supervisione degli elementi IT al fine di migliorare le prestazioni aziendali e aiutare le organizzazioni a fronteggiare in modo strategico i requisiti di *governance*, conformità e gestione del rischio.[63]

Fondamentale è dunque il ruolo del *management,* chiamato a impegnarsi a controllare potenziali rischi tecnologici che potrebbero portare l'azienda a dover fronteggiare considerevoli perdite economiche e reputazionali.

I principali rischi IT riguardano:

- Rischio di selezione: si verifica quando la scelta di una soluzione IT non è allineata agli obiettivi strategici di business;
- Rischio di sviluppo/acquisizione e implementazione: si concretizza quando queste tre fasi causano ritardi ed eccessivi costi portando in alcuni casi l'azienda ad abbandonare il progetto;

[62] U. Bertini, *Il sistema d'azienda*, Giappichelli, Torino, (1990).

- Rischio di disponibilità: ovvero quando il sistema risulta indisponibile in un momento critico, causando interruzioni della attività, perdita di ricavi e ritardi nel processo decisionale;
- Rischio di accesso: si verifica in caso di accessi non autorizzati al sistema, con conseguente furto o cancellazione di dati;
- Rischio di affidabilità del sistema: carenze sistematiche possono portare a incongruenze nel processo di elaborazione dei dati e quindi alla produzione di informazioni inesatte o incomplete;
- Rischio di frode: derivante da un errata separazione dei compiti delle risorse aziendali.

In linea generale, l'associazione *ISACA (Information Systems Audit and Control Association)* definisce il rischio IT come "un rischio aziendale, in particolare il rischio aziendale associato all'uso, alla proprietà, all'utilizzo, al coinvolgimento, all'influenza e all'adozione dell'IT all'interno di un'azienda. Consiste in eventi e condizioni legati all'IT che potrebbero potenzialmente avere un impatto sull'azienda. Può verificarsi con frequenza e incidenza incerte e crea problemi nel raggiungimento di obiettivi e traguardi strategici."[64]

Sono stati sviluppati diversi modelli che sottolineano l'importanza di una corretta gestione dei controlli interni per allinearsi ai requisiti del *Sarbanes-Oxley Act,* al contrario, esistono meno linee guida che enfatizzino il ruolo fondamentale svolto dall'IT e affianchino le aziende nell'implementazione dei controlli a livello tecnologico.

Per poter proseguire in quest'analisi è necessario analizzare brevemente un ultimo *framework* denominato *Control Objectives for Information and related Technology (COBIT). COBIT* è un quadro aziendale redatto per la prima volta nel 1996 dall'associazione professionale internazionale *ISACA* come modello di audit e controllo dell'IT perfettamente in linea con lo spirito del *Sarbanes-Oxley Act*. Alla prima versione sono susseguite nel corso degli anni nuove edizioni sempre più complete e aggiornate, ciò per permettere alle aziende di rimanere

[64] ISACA, *The risk IT Framework*, USA, (2009).

competitive e al passo con le sempre più evidenti potenzialità delle attività IT all'interno dell'*auditing*.[65]

Il *framework* COBIT è caratterizzato da una struttura a tre livelli composta dai requisiti di business, come ad esempio integrità, conformità ed efficienza, dalle risorse IT, tra cui applicativi, informazioni ed infrastrutture, e dai processi IT divisi in domini.

Tutti i processi sono contenuti in quattro domini:

- PO: pianificazione e organizzazione;
- AI: acquisizione e implementazione;
- DS: fornitura e supporto;
- ME: monitoraggio e valutazione.

Come visibile nella figura 3.0, le associazioni tra le risorse e i processi sono rappresentate, come già visto per il *COSO ICIF*, tramite un cubo.

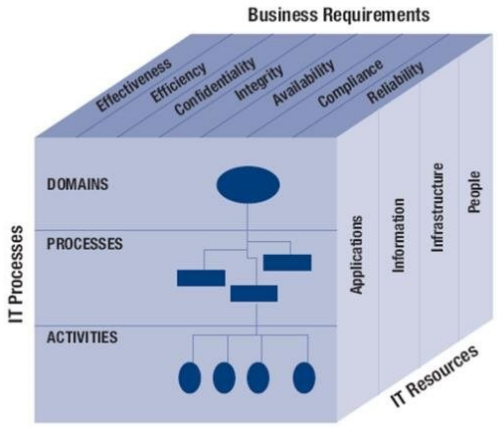


Figura 2.9: Il cubo COBIT. Fonte: bmc.com

L'obiettivo primario del *framework* è collegare gli obiettivi aziendali con quelli dell'IT, al fine di colmare le distanze esistenti tra i modelli di controllo aziendale (e.g. *COSO*) e i modelli di controllo più mirati per l'IT, attraverso la definizione dei requisiti di audit e conformità.

[65] C. Fox, P. Zonneveld, *Il ruolo dell'IT nel progetto e nell'implementazione dei controlli interni per la predisposizione del reporting finanziario*, traduzione italiana a cura dell'Associazione Italiana Information Systems Auditors (AIEA), Milano, (2007).

Il concetto alla base del modello si fonda sul presupposto che il controllo IT si raggiunga concentrandosi sui requisiti necessari per supportare gli obiettivi aziendali.

Garantire l'utilizzo dell'IT in modo efficace ed innovativo per allinearsi agli obiettivi strategici del business, mantenere dati e informazioni di alta qualità per sostenere le decisioni aziendali e gestire il rischio correlato all'IT sono alcuni dei principali vantaggi apportati.[66]

È bene precisare l'esistenza di diversi standard di sicurezza che potrebbero sostituire il *framework* in oggetto, nonostante non siano considerati ugualmente efficaci.

In aggiunta a quanto già esposto, uno dei principali punti di forza percepibili mediante la lettura del COBIT riguarda la semplicità di linguaggio, caratteristica che permette di avvicinare i temi informatici a risorse aziendali "meno addette" e consentire ai vertici aziendali di avere visibilità sull'andamento dei controlli sull'IT.

Ciò malgrado, anche il modello in oggetto presenta alcuni limiti. Attraverso una pubblicazione delle associazioni itSMF italia, AIEA e SDA Bocconi si evince come il modello richiami costantemente l'utilizzo di standard, best practice e di procedure formalizzate senza però raccomandare alle aziende di investire sull'innovazione e sulla flessibilità. Nella divulgazione le tre associazioni sostengono inoltre come il COBIT eviti di spingersi nell'effettiva operatività delle attività di controllo.

Effettivamente, avendo interrogato il modello durante il progetto a cui ho partecipato, ho constato che quest'ultimo non contenga linee guida finalizzate ad aiutare le aziende ad utilizzare la tecnologia e sfruttarla nel miglior modo, al contrario, propone un approccio che non richiede alle organizzazioni un grande sforzo di ridefinizione dei propri processi e delle proprie conoscenze, specialmente se queste provengono dall'utilizzo di altri standard di riferimento (i.e. ISO27001).[67]

---

[66] C. Kidd, *what is COBIT? COBIT Explained* in "BCM blogs", (2019).

[67] AIEA, itSMF italia, SDA Bocconi, *COBIT® e ITIL® due framework complementari* in "AIEA", (2007).

Attraverso i contenuti emanati da *PCAOB*, *COSO*, *SEC* e *COBIT* è possibile estrapolare alcune disposizioni sul tema dei controlli IT.

Come precedentemente analizzato, con la nascita del *Sarbanes- Oxley Act* gli *executive manager* delle aziende sono direttamente responsabili dell'implementazione, valutazione e monitoraggio dell'efficacia dei controlli interni inerenti al *reporting* finanziario. Ad oggi, il ruolo *dell'Information Technology* è indispensabile e cruciale per poter adempiere a questa disposizione, è infatti possibile affermare che l'IT si posizioni alla base di un efficacie sistema di controllo interno.

Nonostante ciò, il modello di controllo interno *COSO* tratta il tema dei controlli IT ma non specifica le caratteristiche di tali attività di controllo.

Inoltre, il *PCAOB Auditing Standard* No. *2* dichiara:

"I controlli dovrebbero essere testati, compresi quelli sulle asserzioni riferite a tutti i conti significativi e le comunicazioni nel bilancio. Generalmente, tali controlli includono [tra gli altri]:

- Controlli, compresi i controlli generali IT, da cui dipendono altri controlli [...]"

Lo *Standard* prosegue richiamando il tema dell'IT nella predisposizione del *reporting* finanziario di fine esercizio:

"Come parte dell'apprendimento e della valutazione del processo di predisposizione del *reporting* finanziario di fine periodo, l'auditor dovrebbe valutare [tra gli altri]:

- La portata del coinvolgimento dell'IT in ogni elemento del processo di *reporting* finanziario di fine periodo[...].

Per controlli IT si intende l'insieme di controlli presenti nei processi automatizzati, che permettono di disporre un ambiente operativo affidabile e che supportano il funzionamento dei controlli applicativi. Un esempio possono essere i controlli sugli accessi ai programmi e ai dati.

D'altro canto, i controlli applicativi supportano gli obiettivi di controllo finanziari assicurando completezza, accuratezza, autorizzazione e validità delle transazioni elaborate, si possono trovare all'interno di molti applicativi

gestionali. Alcuni esempi sono il *three-way-match*[68] per le fatture passive o l'emissione automatica della fattura di vendita una volta completata la consegna delle merci.

L'*Auditing Standard* No.*2* esplicita dunque l'importanza dei controlli IT senza però puntualizzare quali includere, lasciandone la scelta a discrezione di ogni organizzazione.

L'implementazione dei controlli orientati a adempiere alle richieste della *SOX* è quindi una sfida importante sia per le strutture finanziarie, meno impattate perché oggetto di audit finanziari da molti anni, sia per le strutture IT, alle quali è richiesto un cambiamento delle attività correnti per potersi conformare alle nuove disposizioni in materia.

Declinando questo concetto alla lettura combinata dei *framework COSO* e *COBIT* risulta necessario che all'interno delle aziende siano presenti competenze per il controllo IT per tutti e i cinque elementi definiti dal modello come essenziali per un controllo interno efficace (ambiente di controllo, valutazione dei rischi, attività di controllo, informazione e la comunicazione, monitoraggio). Contrariamente, in molte realtà aziendali l'IT viene erroneamente considerato come un'entità separata dal business con un proprio ambiente di controllo indipendente.

A titolo esemplificativo, per quanto riguarda la componente monitoraggio ci si può aspettare un controllo IT che riduca il pericolo di accessi non autorizzati al fine di ridurre la probabilità e il rischio di effettuare transazioni abusive. Come già citato in precedenza, l'adeguata separazione dei compiti è infatti un elemento alquanto importante per conseguire gli obiettivi di controllo interno. Il significato alla base di questo concetto è che nessun dipendente possa avere la possibilità di commettere e/o nascondere errori e frodi derivanti dal normale svolgimento dei propri compiti. I tre compiti primari incompatibili e che quindi necessitano di essere separati sono l'autorizzazione/approvazione di transazioni inerenti a beni aziendali, la custodia di beni aziendali e il *reporting* delle relative transazioni.

[68] Procedimento che permette di effettuare un riferimento incrociato della fattura passiva con il relativo ordine d'acquisto e movimento di magazzino al fine di assicurarsi che i dettagli pertinenti corrispondano.

Per i sistemi informativi più obsoleti identificare e separare le mansioni incompatibili risulta facilitato poiché caratterizzati da una struttura di controllo prevalentemente manuale; la motivazione principale è dovuta al fatto che la gestione degli acquisti, dell'inventario e della contabilità avviene nella maggior parte dei casi in applicativi tra loro separati. Lo stesso non si può affermare per i nuovi *ERP*, totalmente automatizzati ed integrati, tali per cui la tradizionale separazione dei compiti ne richiede una forte ridefinizione.
Nel prossimo capitolo verranno presentati alcuni strumenti operativi utili a identificare i conflitti relativi alla *Segregation of Duties*.

2.5 L'attività di *IT Internal Auditor* nel processo di implementazione *SOX*

Come già anticipato, per poter soddisfare i requisiti della nuova disposizione *SOX* si richiede alle aziende di incorporare all'interno del proprio controllo interno aziendale dei processi dedicati alla supervisione della componente tecnologica, un fattore ormai imprescindibile per consentire a *CEO* e *CFO* di valutare a tutto campo l'efficacia del sistema di controllo della propria azienda, nonché di attestare l'informativa finanziaria presente in bilancio.
Naturalmente, così come i controlli interni in generale devono essere sottoposti ad attestazione di accuratezza, anche i controlli IT si richiede che siano assoggettati ad un processo di verifica.
L'*IT internal auditor* è la figura professionale preposta all'analisi e alla valutazione delle infrastrutture IT che supportano dei processi fiscali e contabili presenti all'interno di un'organizzazione. La necessità di tale funzione nasce nel momento in cui i revisori presero consapevolezza del fatto che la componente tecnologica avrebbe sempre più influenzando la loro capacità di svolgere la funzione di attestazione. Inizialmente, l'attività di revisore IT era infatti considerata come una semplice estensione dell'auditing tradizionale.
Ad oggi, il ruolo preponderante assunto dalla tecnologia all'interno dei processi aziendali ha contribuito a rendere l'*audit IT* parte integrante della classica attività

di *internal auditing*.[69] Fornendo un servizio incentrato sull'*Information Technology,* questa figura agisce in supporto ai revisori interni nell'esprimere un giudizio circa la qualità delle informazioni trattate dai sistemi informatici e assicura che i processi IT funzionino secondo criteri di efficienza, sicurezza e conformità. Appurato che il trattamento di dati, informazioni e processi amministrativi/contabili avvenga nella quasi totalità dei casi attraverso l'uso di sistemi informatici automatizzati, sorge la necessità da parte delle aziende di avere certezza circa la correttezza dell'informativa finanziaria esposta in bilancio. Per tali motivazioni, nel processo di valutazione dei controlli è necessario che l'*audit IT* non consideri semplicemente variabili meramente informatiche ma includa aspetti finanziari relativi *all'Information Technology*.
Gli *IT auditor* interagiscono con il *management*, con gli utenti e con i tecnici provenienti da tutte le aree aziendali, ciò richiede loro di avere un bagaglio di conoscenze molto ampio per comprendere la varietà di tecnologie utilizzate nell'attività di elaborazione delle informazioni finanziarie, e spiccate abilità interpersonali per poter relazionarsi con più livelli del personale.

Gli obiettivi primari di un *internal audit IT* riguardano:

- La valutazione del rischio: al fine di definire precisamente il grado di vulnerabilità di un'organizzazione e definire le soluzioni più adatte a migliorare il piano di *disaster recovery*[70] dell'azienda;
- La verifica della conformità: spesso accade che le organizzazioni non riescano ad intercettare in tempo eventuali cambiamenti normativi incorrendo in ingenti sanzioni, una continua verifica di conformità aiuta il *management* ad evitare di essere colto alla sprovvista e ad essere in linea con gli standard e i molteplici aggiornamenti dispositivi.
- La valutazione delle prestazioni: un *internal audit IT* ha il compito di analizzare l'infrastruttura tecnologica delle organizzazioni e determinare

[69] Otero, Angel R, *Information technology control and audit,* Auerbach Publications, (2018).
[70] Un piano di *disaster recovery* ha come obiettivo principale quello di sviluppare, testare e documentare un iter ben strutturato che permetta di recuperare il più rapidamente ed efficacemente possibile da un disastro imprevisto o da un'emergenza che interrompe i sistemi informativi, le piattaforme tecnologiche critiche, l'infrastruttura di telecomunicazioni e le operazioni aziendali.

come questa possa essere migliorata in termini di prestazioni, tempi inattività, vulnerabilità dei dati e capacità di agevolare il raggiungimento degli obiettivi aziendali.[71]

- Supporto all'attività dei revisori esterni: una collaborazione efficiente tra la figura professionale del revisore interno e quella del revisore esterno può apportare benefici all'azienda e migliorare la qualità del processo di audit. Il revisore esterno potrebbe infatti utilizzare i risultati dell'analisi dell*'internal audit* per esprimere un giudizio sulla valutazione della Direzione circa l'efficacia del controllo interno della società.

Nell'attuale panorama digitale la rilevanza dell'audit *IT* non può più essere sottovalutata; data la complessità del rischio tecnologico questa funzione è molto spesso svolta da terze parti tramite contratti di *outsourcing* mentre nelle aziende più strutturate accade che venga svolta da personale interno all'azienda.
Seguire un percorso per la conformità IT è fondamentale per garantire l'efficacia del sistema di controllo interno e far sì gli obiettivi e le responsabilità della funzione IT siano adeguatamente pianificati.
La mappa illustrata di seguito fornisce delle linee guida per la funzione adibita ai controlli IT su come affrontare correttamente le sfide del *Sarbanes – Oxley Act*, ho potuto osservare l'operatività di questo approccio durante l'attuazione del progetto esposto nel terzo capitolo.

[71] L. Ballejos, *Che cos'è un audit IT? Una guida pratica* in "NinjaOne Blogs", 18/03/2024.

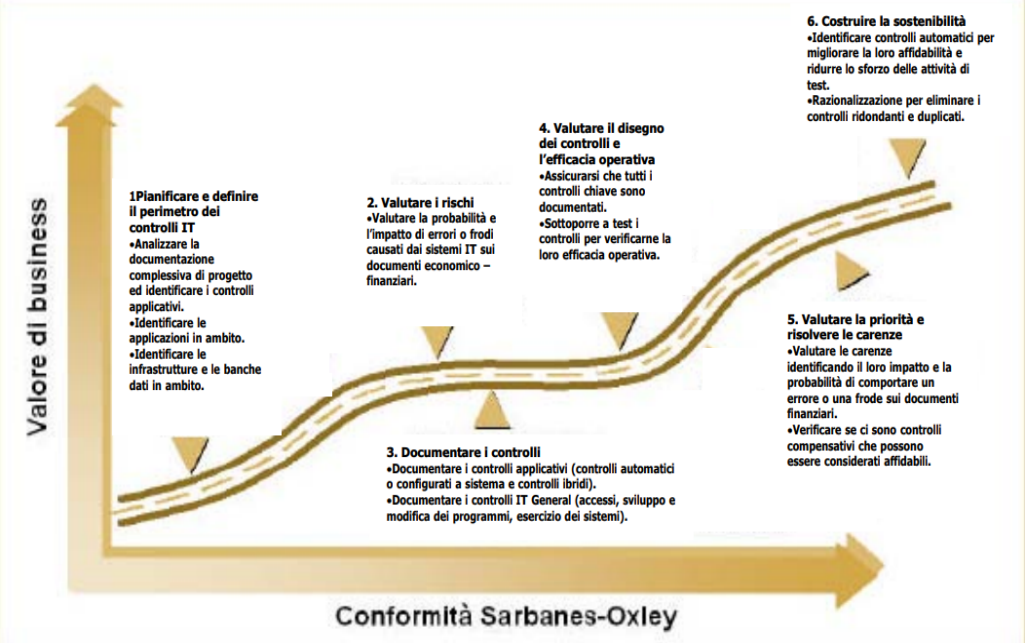


Figura 3: Mappa per la conformità IT Fonte: IT Control Objectives for Sarbanes-Oxley II

Un passo preliminare e fondamentale nel percorso di conformità IT è la creazione all'interno dell'organizzazione di un Comitato di Controllo IT, il cui compito è supervisionare il processo di conformità al *Sarbanes – Oxley* e facilitare il lavoro degli auditor esterni nel momento in cui esprimeranno un giudizio sulla valutazione del controllo interno dell'azienda. Nelle realtà più piccole il Comitato è spesso composto da risorse già presenti all'interno dell'azienda, mentre per le aziende più complesse può essere necessario assumere nuove figure specializzate da dedicare al progetto.

Questa prima fase prevede l'identificazione delle applicazioni IT da includere o escludere nel progetto di conformità. Le aziende sono per natura composte da numerosi processi di business e controlli, tuttavia, la conformità alla *SOX* è circoscritta ai processi e controlli che supportano la predisposizione dei rendiconti finanziari. Per questa ragione, la scelta di inclusione o esclusione degli applicativi viene fatta congiuntamente con il team di business e controllo finanziario, questo appunto perché devono essere compresi nell'analisi solo i programmi che supportano i controlli critici e gli obiettivi di reporting finanziario, ad esempio quelli responsabili dell'integrità di poste di bilancio

significative. Una volta censite le applicazioni dovrà essere predisposta una prima pianificazione delle attività e delle risorse da allocare, in modo da poter disporre di un quadro complessivo delle dimensioni del progetto. Considerate il rilievo e l'impatto che il progetto avrà su molte risorse aziendali è necessario ottenere un'approvazione formale della pianificazione preliminare prima di poter proseguire con gli step successivi.[72]

La seconda fase dell'attività di pianificazione prevede di valutare i rischi che potrebbero incidere sugli applicativi critici precedentemente censiti e l'impatto che questi avrebbero sul business. Non tutti i sistemi e i processi IT devono essere inclusi in quest'analisi poiché non tutti contribuiscono ad esporre il bilancio ad un eventuale rischio di frode. L'output della valutazione è l'identificazione della tipologia di controlli e test necessari a gestire determinati rischi emersi e a ridurli a un livello ragionevole. Il processo di valutazione e le relative conclusioni devono poi essere opportunamente documentati, soprattutto per tracciare se alcuni sistemi sono stati esclusi dall'analisi.[73] A supporto del processo di *risk assesment* sono stati istituiti diversi *framework* contenenti delle linee guida per permettere agli auditor interni di effettuare la valutazione. Un esempio è il modello ISO27001, uno standard internazionale per la gestione della sicurezza delle informazioni che fornisce un approccio alla gestione del rischio coerente con tutte le altre linee guida. Questo *framework* esplicita l'importanza di effettuare una valutazione del rischio prima di selezionare e/o implementare qualsiasi tipo di controllo e puntualizza inoltre che la selezione di ogni controllo deve essere giustificata da una previa valutazione del rischio.[74] Certificazioni ulteriormente evolute e ancora più stringenti sono i modelli *SOC1* e *SOC2*, (*Service Organization Controls*) , due standard per i controlli interni volti a proteggere la riservatezza delle informazioni elaborate e archiviate da *provider* di servizi *cloud*. Il *SOC1*, in particolare, è indirizzato a valutare l'efficacia dei controlli interni di fornitori di servizi *cloud* quando i dati forniti da tale servizio

[72] C. Fox, P. Zonneveld, *Il ruolo dell'IT nel progetto e nell'implementazione dei controlli interni per la predisposizione del reporting finanziario*, traduzione italiana a cura dell'Associazione Italiana Information Systems Auditors (AIEA), Milano, (2007).
[73] Ibidem.
[74] A. Calder, S. Watkins, *IT Governance: An International Guide to Data Security and ISO27001/ISO27002,* Kogan Page Ltd, (2012).

risultano rilevanti ai fini del reporting finanziario delle società clienti che ne fanno uso. La partecipazione al progetto *SOX* mi ha permesso di comprendere come, in determinati casi, l'utilizzo di questi modelli può non essere sufficiente a garantire il successo della fase di valutazione poiché potrebbe rendersi necessario introdurre nuovi rischi non contemplati, o dover adattare i controlli a particolari processi della società in questione.

Ai fini della conformità al *Sarbanes-Oxley Act* le aziende sono tenute a documentare i controlli sul reporting finanziario e a verificare la loro efficacia operativa. La nuova legge federale non indica un'unica metodologia di documentazione; dunque, quest'ultima può variare in base alle dimensioni e alla struttura delle aziende. Nonostante ciò, la documentazione dei controlli IT include per la maggioranza delle aziende:

- Documentazione dei controlli aziendali IT: i controlli aziendali sono una delle componenti fondamentali del modello *COSO* e devono includere anche le attività IT a supporto della rendicontazione finanziaria.
- Documentazione dei controlli applicativi a supporto del reporting finanziario: la crescente attenzione al tempo necessario ad individuare un errore di frode ha reso tali controlli sempre più importanti. Se diversi anni fa era ammissibile aspettare diverse settimane per rilevare una frode, ai giorni d'oggi tali ritardi non sono più concessi. Molto spesso questi i controlli applicativi sono già inclusi nella documentazione dei processi di business. In linea generale le aziende documentano due tipologie di controlli applicativi: i controlli automatici, eseguiti da sistemi applicativi e che non richiedono interventi manuali, e i controlli manuali dipendenti dall'IT, anche detti ibridi, sono essenzialmente controlli manuali che dipendono da sistemi automatici.
- Documentazione dei controlli generali IT: questi controlli sono necessari a garantire l'attendibilità dei controlli applicativi. Di rado i controlli generali supportano direttamente l'informativa finanziaria ma essi sono permeabili su tutti i controlli interni. Dunque, se un controllo generale IT considerato rilevante risulta inefficace, impatterà su tutti i sistemi

sostenuti da quel controllo.[75] I controlli generali impattano su tre aree, l'area di *Manage Change,* che riguarda controlli su modifiche, manutenzioni e aggiornamenti effettuati sugli applicativi IT, l'area di *Manage Access,* che verifica che gli accessi agli ambienti IT vengano effettuati da soli utenti abilitati e che le azioni messe in atto da quest'ultimi siano compatibili con le autorizzazioni a loro attribuite, e l'area di *Manage IT Operations*, volta a verificare che le informazioni siano elaborate correttamente, assicurando che gli applicativi finalizzati ad effettuare i *backup* funzionino in modo adeguato e che i *database* non siano bersaglio di attacchi informatici.[76]

Alle aziende non viene imposto di documentare tutti i controlli relativi a qualsiasi rischio, lo sforzo richiesto è infatti quello di limitare il processo di documentazione ai soli controlli rilevanti. Pur non esistendo una definizione univoca di "controllo rilevante" essi fanno riferimento a quei controlli su cui le organizzazioni fanno maggior affidamento per poter raggiungere gli obiettivi di controllo finanziari. L'importanza di documentare i controlli deriva dal fatto che una documentazione inadeguata della struttura dei controlli su asserzioni rilevanti relative a conti e informazioni significative costituisce una carenza nel controllo interno della società sull'informativa finanziaria, una casistica di questo genere potrebbe anche indurre i revisori esterni a considerare che una documentazione inadeguata rappresenti una limitazione al proprio incarico.

L'*auditing Standard* No. 2 descrive diverse forme di controllo che possono essere utilizzate dagli auditor esterni durante la verifica dell'efficacia operativa dei controlli. Uno strumento largamente utilizzato sono le interviste al personale responsabile all'interno dell'azienda supportate da altre attività quali l'esame della documentazione utilizzata durante l'esecuzione dei controlli. Nell'ipotesi in cui non fosse prevista alcuna evidenza documentale, le interviste verrebbero affiancate da un'ulteriori forme di controllo, come l'osservazione delle attività aziendali. Gli auditor possono anche decidere di rieseguire nuovamente i

[75] C. Fox, P. Zonneveld, *Il ruolo dell'IT nel progetto e nell'implementazione dei controlli interni per la predisposizione del reporting finanziario*, traduzione italiana a cura dell'Associazione Italiana Information Systems Auditors (AIEA), Milano, (2007).
[76] K. Kinzer, *What Are IT General Controls (ITGC)* in "Jumpcloud blogs", 23/08/2023.

controlli per rilevare indipendentemente potenziali carenze, questo accade soprattutto quando la qualità del disegno dei controlli non risulti sufficientemente probante.

Le varie forme di controllo messe in atto dai revisori hanno lo scopo di comprendere varie informazioni, tra le quali, come sono eseguiti i controlli all'interno dell'azienda, quali dati vengono utilizzati durante lo svolgimento dei controlli, in che modo vengono gestite le eccezioni e se verranno apportate modiche sul controllo durante il periodo di audit.[77]

La funzione principali svolta dagli *internal audit* è valutare il disegno e l'effettività dei controlli. Difatti, durante la fase di *Walk-Thorugh Test,* la funzione IT effettua un'analisi denominata *design of control,* la quale permette di valutare se i controlli sono stati disegnati efficacemente e quindi accertare l'effettiva capacità del programma di controllo di ridurre il rischio IT ad un livello considerato accettabile per l'organizzazione. Nel caso in cui venissero captate delle carenze significative nella struttura, verrebbero rilevate delle debolezze materiali nel disegno dei controlli.

Una volta appurata l'efficacia del *design of control*, si procede con l'esecuzione di test preliminari e di routine per valutare l'efficacia operativa del sistema di controlli, fase chiamata *Test of Effectiveness*. Per poter svolgere questa attività l'azienda deve selezionare un campione di item la cui ampiezza è direttamente proporzionale alla frequenza dell'operazione di controllo. Così facendo viene verificato che il sistema funzioni come prescritto del disegno prestabilito, l'obiettivo di questa operazione è consentire al *management* di poter documentare le verifiche effettuate sull'efficacia operativa dei controlli, così come stabilito dalla Legge, in modo da poter esprimere le proprie conclusioni e permettere agli auditor di rieseguire le operazioni di verifica in fase di revisione. Nel caso in cui durante la fase di test venissero individuate delle eccezioni rispetto a quanto definito nella fase di *design*, l'auditor dovrà indagare insieme

[77]C. Fox, P. Zonneveld, *Il ruolo dell'IT nel progetto e nell'implementazione dei controlli interni per la predisposizione del reporting finanziario*, traduzione italiana a cura dell'Associazione Italiana Information Systems Auditors (AIEA), Milano, (2007).

alla società per risalire alle cause di tali variazioni.

A conclusione dei tutti i test agli *internal auditor IT* spetta il compito di redigere un documento finale al fine di dettagliare e comunicare il periodo temporale coperto dal test, la descrizione del controllo, la numerosità della popolazione del campione, la frequenza del controllo, eventuali eccezioni identificate durante il test e come queste non invalidino il controllo e una conclusione sull'efficacia operativa del periodo revisionato.

La fase di valutazione dell'efficacia operativa dei controlli viene eseguita in un determinato periodo dell'anno fiscale che dipende dalla natura e dalla frequenza del controllo. Controlli come l'approvazione delle richieste d'accesso degli utenti sono sempre attivi, mentre altri vengono effettuati solo periodicamente.[78]

Al fine di ottenere una visibilità completa viene eseguita una terza di verifiche *roll-forward* che serve ad accertare, attraverso dei test aggiuntivi, che non siano intercorsi cambiamenti tra il periodo in cui sono stati eseguiti i test e la fine dell'anno fiscale. Qualsiasi difetto riscontrato a questo stadio può compromettere il corretto funzionamento dei controlli interni dell'azienda e, soprattutto, rappresentare un impedimento per il *management* nel riportare di informazioni finanziarie corrette. [79]

Tutte le debolezze identificate nei controlli IT non dovrebbero essere valutate separatamente ma andrebbero analizzate con il team di compliance finanziario, soprattutto se inerenti a controlli applicativi che supportano controlli sul reporting. L'*Auditing Standard* No. 5 identifica due tipologie di carenze:

- Debolezze strutturali: sorgono nella fase di *design of control*, si tratta di *deficiency* strutturali poiché il controllo non è stato progettato adeguatamente per il suo funzionamento. Sono dovute a controlli inadeguati, assenti e/o mancanza di documentazione di supporto;
- Debolezze operative: vengono identificate in fase di test, in questa casistica il controllo è stato progettato in modo adeguato ma non funziona

[78] Ibidem.
[79] *The Future of IT Internal Controls –Automation: A Game Changer* in "Deloitte&Touche", (2018).

come previsto.

Molto spesso accade che debolezze individuali dei controlli vengano considerate insignificanti ma l'effetto combinato con altre può diventare un problema significativo per l'azienda. La fase di assestamento delle carenze rappresenta per molte entità la fase del progetto durante la quale sono richiesti maggiori sforzi economici. Se vengono rilevate eccezioni nel controllo è necessario stabilire se questo possa considerarsi efficiente o meno, l'auditor dovrà quindi verificare la natura e le cause della deviazione analizzandone gli effetti sui controlli identificati, così da classificarla come sistematica o casuale. Se la carenza non influisce sulla copertura dei rischi di controlli, il SCI può essere considerato comunque efficiente.[80]

L'obiettivo dell'ultima fase di consolidamento è trasformare il progetto di controllo IT in un vero e proprio processo. Per raggiungere questo obiettivo le aziende dovrebbero mettere in atto alcune operazioni, come ad esempio effettuare una verifica dopo l'implementazione del progetto *Sarbanes-Oxley* identificando gli elementi del piano che hanno avuto riscontro positivo ed eventuali nuove variabili da considerare. Un'altra iniziativa che andrebbe effettuata è la razionalizzazione dei controlli; è naturale che nel lungo termine alcuni controlli che sono stati documentati non risultino più utili, motivo per cui le aziende dovrebbero rivalutarli periodicamente per identificare quali rimuovere e quali automatizzare.[81] La presenza di fattori esterni come il Regolamento Generale sulla Protezione dei Dati (GDPR) possono influenzare e allo stesso tempo dare un contributo al processo di conformità IT delle aziende stabilendo regole e principi sull'utilizzo di utenze nominali e sulla gestione generale della privacy.

L'aspetto fondamentale, appreso dall'applicazione pratica di questa *road map* di conformità, che consente alle aziende di soddisfare i requisiti della *Sarbox*, e quindi dimostrare che le proprie applicazioni finanziarie, sistemi e servizi siano

[80] C. Fox, P. Zonneveld, *Il ruolo dell'IT nel progetto e nell'implementazione dei controlli interni per la predisposizione del reporting finanziario*, traduzione italiana a cura dell'Associazione Italiana Information Systems Auditors (AIEA), Milano, (2007).
[81] Ibidem.

adeguatamente protetti, risiede nel riuscire a sostenere l'esecuzione di tutte queste procedure IT attraverso un processo alla base adeguatamente strutturato ed organizzato e che coinvolga diverse figure professionali con competenze distinte.

Nel prossimo capitolo verrà presentato un esempio pratico finalizzato a documentare le prime fasi del progetto *SOX compliance* così da sottolineare l'importanza della pianificazione e della collaborazione a più livelli organizzativi.

Capitolo 3 – Case study. L'applicazione *SOX* su *Stealth Platform*

3.1 Implementazione *SOX* su *Stealth Platform*

Il caso di studio riportato in quest'ultimo capitolo descrive un progetto a cui ho partecipato durante il periodo di tirocinio curriculare che ho svolto presso la società *DedaGroup Stealth*, nella posizione di consulente all'interno dell'area *Finance*.

DedaGroup Stealth opera nel settore del *Fashion* internazionale offrendo soluzioni tecnologiche e innovative di *Cloud Sourcing* progettate per l'intera *Supply Chain* del comparto moda.

Per i primi tre mesi di stage ho partecipato ad una *Digital Academy*: una scuola d'impresa full time progettata per entrare gradualmente nel mondo del lavoro dell'*Information Technology,* per poi essere inserita ufficialmente nel team *Finance* in affiancamento ad una risorsa *Senior.*

L'ispirazione al tema *Sarbanes Oxley Act* come base su cui sviluppare il mio progetto di tesi nasce dopo il mio inserimento all'interno del gruppo *Finance* internazionale, nel quale i consulenti si interfacciano quotidianamente con clienti del comparto moda dislocati in diversi Paesi, tra cui l'America. Essendo il prodotto *Stealth* un *Entreprise Resource Planning*, sulla base di quanto esposto nei capitoli precedenti, è necessario che rispetti determinati requisiti e che venga sottoposto a procedure di controllo nel momento in cui viene implementato e utilizzato da aziende quotate operanti in territorio americano, ricadenti quindi sotto i canoni decretati dalla normativa *SOX*.

In questo capitolo verranno descritte le attività di implementazione di recente introduzione e gli allestimenti già nativi sulla piattaforma *Stealth* tali da consentire la gestione dei requisiti *SOX* per un cliente appartenente al comparto *Moda&Luxury,* con particolare attenzione ai temi di controlli interni e segregazione dei compiti. La stessa verrà di seguito riportata come "Società X". Il cliente in oggetto utilizza l'*ERP Stealth* da alcuni anni, da poco è stato acquisito da una grande gruppo americano; questo cambiamento aziendale ha

inevitabilmente richiesto degli interventi aggiuntivi sul sistema al fine per garantirne la conformità agli attributi previsti dalla *SOX*.

È bene ricordare che le sezioni 302 e 404 della Legge richiedono che i *CEO* e i *CFO* certifichino l'accuratezza dell'informativa finanziaria e valutino annualmente l'efficacia dei propri controlli interni su tale informativa.

Ciò implica che i sistemi IT utilizzati dalle organizzazioni per generare le informazioni finanziarie debbano essere considerati come affidabili; per giungere a tale certezza è necessario che questi vengano inclusi nella valutazione annuale dei controlli da parte delle società di revisione.

Come linee guida per lo sviluppo di questo progetto sono state utilizzate le disposizioni contenute nelle principali evoluzioni del *COSO framework,* in particolare l'*Internal Control Integrated Framework e* l'*Enterprise Risk Management Frameworks,* al fine di adottare un'appropriata politica di *risk management* e sviluppare un modello standard di controllo interno.

Gli attori coinvolti nel progetto della Società "X" sono rappresentati, in linea generale, nel seguente schema:

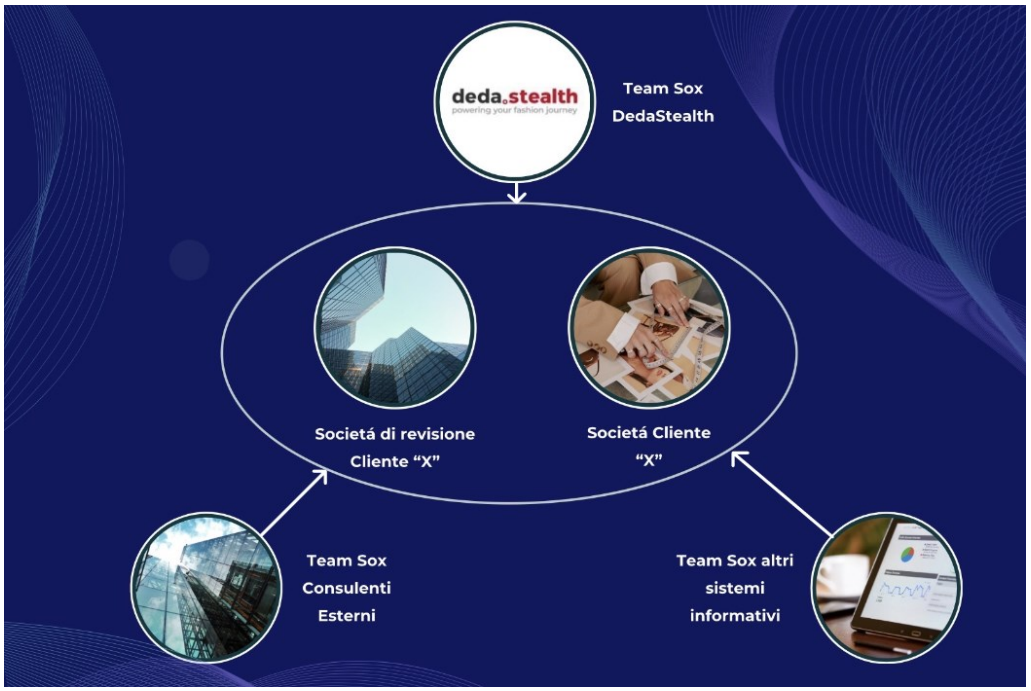


Figura 3.1: Attori coinvolti nel progetto "X"

Il team *SOX* di *Deda Stealth* presenta al suo interno diverse figure professionali, tra cui il responsabile della conformità, i consulenti delle varie aree organizzative gestite dal software in veste di analisti dei processi, responsabili di analizzare i processi aziendali e identificare potenziali vulnerabilità che potrebbero pregiudicare la conformità alla normativa, e risorse più operative appartenenti al reparto IT.

Il presupposto cardine per la realizzazione del progetto è stato poter prestabilire il singolo elemento di sistema a cui l'utente della Società X, che utilizza *Stealth,* ha accesso. Per poter mettere in pratica questo principio di base si è reso necessario prendere in considerazione alcuni elementi rilevanti:

- Gli ID utente: il processo di creazione degli ID utente è un'attività estremamente importante che deve essere descritta e documentata da una procedura aziendale;
- I ruoli aziendali e le regole a loro applicate: la veste con cui gli utenti accedono a sistema è fondamentale ai fini della conformità.

I controlli su questi fattori rientrano nei controlli generali IT esposti nel capitolo precedente, in particolar modo nei controlli di accesso, i quali devono garantire che solo le risorse aziendali autorizzate possano accedere a determinati dati critici.

L'implementazione di un ambiente *SOX Compliant* richiede che tutte queste fasi siano accompagnate da idonea documentazione e da modelli di controllo che guideranno il reparto IT nelle attività di costruzione dei ruoli aziendali, nelle procedure di definizione delle autorizzazioni e assegnazioni dei profili agli utenti e nella progettazione dei controlli e della valutazione.

3.2 Elementi operativi di controllo interno

Come enunciato nel capitolo precedente, la valutazione del rischio rappresenta un elemento imprescindibile per poter disporre di efficace sistema di controllo interno. Seguendo le fasi di *risk management*, la prima attività che ho svolto insieme al team di progetto è stata un'analisi dei processi aziendali del cliente

che hanno impatto diretto sul bilancio, al fine di individuare i rischi a cui l'azienda era maggiormente esposta. Ad ogni rischio è stato poi assegnato un punteggio direttamente proporzionale alla probabilità di verifica.

Una valutazione iniziale sullo stato attuale dei controlli della "Società X" è stata fondamentale per poterne identificare le aree di miglioramento, quest'attività è spesso svolta singolarmente dalle società di consulenza a cui si appoggia il cliente. In questo specifico progetto, tale attività è stata svolta a quattro mani con una società di consulenza, avendo già collaborato in fase di disegno inziale dei processi della Società X.

Per l'individuazione dei potenziali rischi è stata utilizzata la matrice *SOD.*[82]

Il modello da noi adottato per la definizione di tale matrice prende in considerazione due elementi:

- Le *function*, che rappresentano famiglie di transazioni che costituiscono una parte di un processo;
- I rischi, cioè le *function*, quindi le parti del processo, in conflitto tra loro.

La metodologia adottata mira a identificare i rischi, valutare l'impatto degli stessi e definire le azioni necessarie per minimizzarli o eliminarli. Lo scopo ultimo del processo di valutazione dei rischi è la definizione della priorità delle azioni da realizzare. Al riguardo, si è convenuto ricorrere alla valutazione del rischio attraverso una metrica qualitativa che permette una maggiore rapidità di esecuzione della valutazione stessa e consente di impostare con tempestività le eventuali azioni necessarie al contenimento del rischio.

La valutazione considera i singoli eventi determinando per ciascuno di essi la probabilità di accadimento (frequenza) e l'effetto delle conseguenze (gravità) sulle attività dell'azienda cliente.

Nel merito, l'effetto delle conseguenze (gravità) di un evento è stato classificato come segue:

[82] All'interno della matrice SOD vengono rappresentati i potenziali rischi e conflitti annessi ad ogni processo critico.

BASSO	L'evento pur non mettendo a rischio le attività svolte ed erogate, evidenzia possibili lacune nelle modalità operative messe in campo per evitare il rischio effettivo o potenziale
MEDIO BASSO	L'evento potrebbe comportare notevoli disagi che potranno essere superati con alcune difficoltà (costi aggiuntivi, diniego di accesso ai servizi ecc.)
MEDIO ALTO	L'evento risulta aziendalmente negativo con il rischio di non rendere affidabili i servizi erogati edi non garantire la continuità interna/verso i clienti
ALTO	L'evento può comportare una diminuzione del grado di fiducia parte del mercato fino a provocare la sospensione delle attività, l'insoddisfazione dei clienti, la minaccia del mancato rispetto della normativa di legge con tutti i conseguenti impatti negativi

Figura 3.2: Classificazione dell'impatto di un evento

Mentre la frequenza di accadimento di un evento (probabilità) è stata determinata adottando la seguente metrica:

MOLTO PROBABILE	Alta probabilità che l'evento possa verificarsi - evento che si è verificato in un periodo passato e in presenza di misure di mitigazione in essere, evento che potrebbe verificarsi a causa di uno scenario profondamente modificato
PROBABILE	Media probabilità che l'evento possa verificarsi - evento che si è verificato in un periodo passato e in mancanza di misure di mitigazione oggi in essere
IMPROBABILE	Quando la probabilità che si verifichi l'evento è praticamente nulla - evento che non si è mai verificato neanche ad altri operatori del settore

Figura 3.3: Classificazione della probabilità di un evento

La combinazione tra le due grandezze considerate per ciascun evento ha determinato l'impatto dei rischi e la relativa valutazione.

	IMPATTO			
PROBABILITA'	Basso	Medio basso	Medio alto	Alto
Molto probabile	3	6	9	12
Probabile	2	4	6	8
Improbabile	1	2	3	4

Figura 3.4: Combinazione tra impatto e probabilità di un evento

I valori del rischio risultanti dall'intersezione della tabella sopra esposta sono i seguenti:

Tollerabile	1-3	Rischio accettabile
Indesiderabile	4-6	Rischio da mitigare con tutte le azioni possibili
Intollerabile	8-12	Rischio non accettabile da eliminare con priorità massima

Figura 3.5: Classificazione del rischio di un evento

Di seguito sono riportate alcune delle attività mappate e i relativi rischi identificati, correlati ai diversi processi aziendali. Sono stati utilizzati dei colori differenti per evidenziare se il rischio è applicabile a *Stealth* o anche ad altre applicazioni con cui il software si interfaccia:

- Blu: attività gestite completamente in *Stealth*;
- Verde: attività parzialmente gestite in *Stealth* e parzialmente in un altro *ERP*;
- Nero: attività esterne alla gestione di *Stealth.*

Sales Department			
Risk ID	**Risk Description**	**Function 1**	**Function 2**
S001	Un utente potrebbe creare un'anagrafica cliente fittizia e avviare ordini di vendita fraudolenti per quel cliente.	Gestione anagrafica clienti	Processare ordine di vendita
S002	Un utente potrebbe creare un ordine di vendita fittizio per coprire una spedizione non autorizzata.	Processare ordine di vendita	Processare spedizioni
S003	Un utente potrebbe creare o modificare in modo inappropriato i documenti di vendita e generare il documento di fatturazione.	Processare ordine di vendita	Gestione fatturazione
S004	L'utente potrebbe creare un'anagrafica cliente fittizia ed elaborare la fatturazione per quel cliente.	Fatturazione	Gestione anagrafica clienti
S005	Le condizioni di prezzo potrebbero essere manipolate dall'utente per fornire sconti o incentivi inappropriati ai clienti attraverso l'emissione di una fattura errata.	Processare fattura cliente	Manutenere le condizioni di vendita
S006	L'utente potrebbe creare una nota di credito fittizia ed eseguire la fatturazione per richiedere un pagamento al cliente. Il cliente potrebbe fornire una tangente all'utente interno.	Processare note di credito	Fatturazione
S007	L'utente potrebbe inserire un ordine di vendita e abbassare i prezzi tramite le condizioni di vendita.	Processare ordini di vendita	Manutenere le condizioni di vendita

S008	L'utente potrebbe potenzialmente azzerare il saldo di un cliente prima di apportare la stessa modifica al documento di fatturazione per lo stesso cliente, liberandolo dall'obbligo.	Modificare estratto conto clienti	Gestione fatturazione
S009	L'utente potrebbe modificare i record della contabilità clienti per coprire le differenze con gli estratti conto dei clienti.	Gestione cash Applications	Gestione documenti di vendita
S010	L'utente potrebbe avviare un pagamento non autorizzato al cliente inserendo note di credito fittizie.	Gestione note credito clienti	Pagamenti Accounts Recivable (AR)
S011	Le commissioni o gli incentivi potrebbero essere pagati in base al numero di ordini di vendita. Si potrebbero inserire ordini fraudolenti per ottenere maggiori commissioni.	Processare ordini di vendita	Processare Payroll

Tabella 1: Rischi associati ai processi - Sales Department

Purchase Department			
Risk ID	**Risk Description**	**Function 1**	**Function 2**
P001	L'utente potrebbe gestire un fornitore fittizio e inserire una fattura fornitore con pagamento automatico.	Gestione dati fornitori	Processare fatture fornitori
P002	L'utente potrebbe immettere ordini di acquisto fittizi per uso personale e accettare la merce tramite entrata merci.	Gestione ordini d'acquisto	Gestione entrata merci su ordine
P003	L'utente potrebbe immettere fatture fornitore fittizie e accettare la merce tramite entrata merci.	Gestione fatture fornitore	Gestione entrata merci su ordine
P004	L'utente potrebbe acquistare un oggetto in modo inappropriato e manipolare l'inventario fisico per nasconderlo.	Gestione ordini d'acquisto	Gestione movimenti di import
P005	L'utente potrebbe immettere contratti d'acquisto fittizi e inserire fornitori fittizi o modifica fornitori esistenti.	Gestione dati fornitori	Gestione accordi d'acquisto
P006	L'utente potrebbe mantenere un fornitore fittizio e creare pagamenti per quel fornitore.	Pagamenti Accounts Payable	Gestione dati fornitore

		(AP)	
P007	L'utente potrebbe immettere fatture fornitore fittizie ed effettuare il pagamento al fornitore.	Gestione fatture fornitori	Pagamenti Accounts Payable (AP)
P008	L'utente potrebbe immettere accordi di acquisto fittizi ed eseguire il pagamento.	Pagamenti Accounts Payable (AP)	Gestione accordi d'acquisto
P009	L'utente potrebbe nascondere le differenze tra i pagamenti bancari e i record di Accounts Payable registrati.	Gestione riconciliazioni bancarie	Registrazione fatture fornitori

Tabella 1.1: Rischi associati ai processi - Purchase Department

Inventory				
Risk ID	**Risk Description**	**Function 1**	**Function 2**	**Function 3**
M001	L'utente potrebbe accettare merci tramite entrata merci ed eseguire successivamente una rettifica del movimento di magazzino.	Accettazione beni	Registrazione movimenti di magazzino	Cancellazione rettifiche di magazzino

Tabella 1.2: Rischi associati ai processi – Inventory

Lavorando quotidianamente a stretto contatto con i clienti, la figura del consulente *finance* è fondamentale al fine di individuare i processi tipici della società in oggetto impattati dai requisiti *SOX,* così da fornire le linee guida alle risorse operative del progetto (i.e. *IT Specialist*) su come impostare la definizione dei ruoli aziendali e delle relative autorizzazioni.

È necessario precisare che i processi inseriti in fase di progetto nella matrice di rischio presentata siano più numerosi di quelli qui esposti. Lavorando in affiancamento ad una risorsa Senior, ho deciso di riportare i soli processi rientranti nella responsabilità del dominio *finance* che ho direttamente potuto contribuito a identificare. Tale ragionamento è esteso a tutti gli altri esempi che verranno riportati di seguito.

Come esposto nella tabella precedente, le funzioni 1 e 2, e talvolta 3, se gestite dallo stesso utente possono rappresentare un rischio per la qualità dei dati della "Società X". Il fatto che siano a capo dello stesso ruolo aziendale, o a ruoli diversi ma assegnati allo stesso utente, può causare la realizzazione del rischio descritto.

Una volta definita la matrice, è stata effettuata un'analisi del rischio attraverso un censimento degli utenti del cliente attivi nel sistema *Stealth* durante l'anno 2023, al fine di evidenziare quali rischi essi generavano. In seguito, partendo dalla matrice *SOD* generica di cui sopra sono stati presi in considerazione i vari flussi limitatamente alle attività gestite in *Stealth* ripresentando il menu del software in una matrice di attribuzione dei ruoli. Le attività sono elencate sia verticalmente che orizzontalmente, il segno "X" identifica le casistiche in cui le due funzioni non dovrebbero essere autorizzate allo stesso utente.

Il risultato di questo studio ha permesso di avere evidenza delle autorizzazioni non coerenti con i ruoli assegnati ai singoli utenti e quali di essi disponevano di un set di autorizzazioni potenzialmente in contrasto con le regole imposte dalla *SOX*.

			Sod Activity/Role Attribute																			
Menù ST3K	Activity	Sod Activity/ Role Attribute	POM	POL	API	SOM	SOL	ARI	WHM	INM	SAM	SHM	DBM	WOM	WOP	MRP	MMM	BMM	CMM	VMM	AMM	COM
	Description		Purchase Order Mgnt	Purchase PriceLists	AP Invoice Mgnt	Sales Order Mngt (Orders + Sales Offers)	Sales Pricelists	AR Invoice Mgnt (Invoices+ Intrastat+Prjetcions)	Warehouse Mgnt (WH, Lists, Serial Nr,Package Border aux, ASN)	Inventory management (Stock Inventary)	Assignments	Prebolle	Diba Mgnt (Distinta Base + Varians+Prod.Cycles)	Work Orders + Pick.Lists +Prod.Progress	Pricelists	Prod. Needs	Material Mgnt (Model + Part, etc.)	Bank data Mgnt	Customer MD Mgnt	Vendor MD Mgnt	Agent MD Mngt	CME, Standard Costs, Periodical Costs, Versions,
Acquisti	Purchase Order Mgnt	POM		X	X				X	X			X	X	X	X	X	X		X		X
Acquisti	Purchase PriceLists	POL	X		X				X	X			X	X	X					X		
Acquisti	AP Invoice Mgnt	API	X	X					X											X		
Vendite/Ordini/Proposte Ordini	Sales Order Mngt (Orders + Sales Offers)	SOM					X	X	X	X									X		X	
Vendite/Listini	Sales Pricelists	SOL				X		X	X	X												
Vendite/Fatture/Intrastat/Proiezioni	AR Invoice Mgnt (Invoices+ Intrastat+Prietcions)	ARI				X	X		X	X									X		X	
Produzione	Work Orders + Pick.Lists +Prod.Progress	WOM											X		X							X
Produzione	Pricelists	WOP	X	X									X	X		X						X
Produzione	Prod. Needs	MRP	X	X											X							X
Oggetti	Material Mgnt (Model + Part, etc.)	MMM	X	X																X		
Soggetti	Bank data Mgnt	BMM	X	X	X	X	X	X														
Soggetti	Customer MD Mgnt	CMM				X	X	X														
Soggetti	Vendor MD Mgnt	VMM	X	X	X																	
Soggetti	Agent MD Mngt	AMM				X	X	X														

Figura 3.6: La matrice SOD riferita al sistema Stealth

Una volta ottenuto il risultato della fase di analisi de rischio, sono state definite le modifiche da apportare ai ruoli. In questa fase è stato necessario attuare una forte collaborazione tra le risorse assegnate al progetto e gli utenti del business del cliente, con i quali si è cercato di determinare come risolvere i rischi.

Per soddisfare le necessità *SOX* per i suddetti rischi sono state identificate diverse soluzioni:

- Distribuire le attività tra diversi utenti, non sempre attuabile poiché non è sempre possibile segmentare sufficientemente il processo per tutti gli utenti;
- Implementare controlli di sistema che ostacolino la possibilità di manipolare a proprio vantaggio i dati coinvolti;
- Implementare controlli che dissuadano gli utenti dal commettere abusi sul sistema e consentano ai supervisori di tenere sotto controllo i risultati dei processi.

Nell'affrontare questa situazione, in accordo con il cliente, si è deciso di adottare un approccio *brownfield*, che prevede di partire dall'assetto attuale presente sul sistema cercando di modificarlo per giungere al risultato desiderato. Un'altra soluzione sarebbe stata utilizzare un approccio *greenfiled,* il quale al contrario prevede di ricostruire i ruoli aziendali del cliente da zero. La motivazione della scelta della prima opzione risiede nel fatto che la versione standard di *Stealth Platform,* utilizzata finora dal cliente, disponeva di per sé di un buon controllo sugli accessi, tale da non giustificare la completa ridefinizione degli stessi.

Come per il progetto oggetto di discussione, spesso accade che le dimensioni ridotte delle organizzazioni non permettano di rispettare completamente le regole richieste dalla *SOX*, non risulta infatti sempre possibile per tutti gli utenti attuare una completa separazione dei compiti contrastanti, una delle cause può essere la carenza di personale addetto per una determinata parte del processo aziendale. Se questa è la situazione non significa che non si possa fare niente per introdurre un controllo che garantisca lo stesso livello di conformità ai principi *SOX*. Difatti, circostanze di questo genere richiedono che le attività in contrasto vengano giustificate da numeri, organigrammi e richieste di autorizzazione da

parte della Direzione, tutto ciò deve sempre essere documentato e registrato. Si è quindi reso necessario introdurre alcuni controlli compensativi preventivi o di consumo. I controlli di consumo prevedono che gli strumenti di monitoraggio implementati (normalmente report o tracciatura di quello che viene fatto da un utente) vengano controllati a posteriori. Ad esempio, si andrà a identificare cosa l'utente ha fatto al fuori dalle proprie competenze dopo che lo ha commesso, agendo in tempi stretti affinché non si ripeta.

La *best practice* richiede di preferire i controlli preventivi, ove possibile.

Tali controlli devono essere una predisposizione di attività automatiche in luogo di attività manuali al fine di evitare atti non intenzionali. Devono quindi essere completi, coerenti, conformi, documentati nella forma, nelle procedure e nelle loro esecuzioni, ricorrentemente eseguiti e aggiornati periodicamente in base a tutte le modifiche che interessano la creazione di ruoli, per definire se sono necessari nuovi controlli o se rimuovere quelli obsoleti.

Di seguito sono riportati due esempi pratici di controlli compensativi implementati ad hoc per la "Società X".

Sales Department			
Risk ID	**Risk Description**	**Function 1**	**Function 2**
S003	Un utente potrebbe creare o modificare in modo inappropriato i documenti di vendita e generare il documento di fatturazione.	Processare ordine di vendita	Fatturazione

Tabella 1.3: Controlli compensativi – Sales Department

Essendo le due funzioni inevitabilmente assegnate allo stesso utente, i controlli compensativi sono stati implementati attraverso una combinazione di più interventi.

In primo luogo, mediante la creazione di un report, eseguito mensilmente o settimanalmente ed inviato direttamente al supervisore, che elenchi gli ordini creati e fatturati dall'utente con data e ora di creazione. Ciò darà la percezione all'utente che il suo lavoro sia supervisionato e che eventuali frodi possano

essere rilevate sul nascere.

Un ulteriore soluzione individuata prevede il tracciamento dei dati sensibili, come ad esempio quale utente è responsabile delle modifiche apportate al documento. Se i dati relativi all'attività di ordine di vendita venissero rintracciati e gli utenti ne fossero informati, si ridurrebbe il rischio che questi possano essere manipolati in modo inappropriato.

Creando un processo di approvazione incorporato nel sistema. Attraverso tale procedimento l'ordine di vendita viene creato in uno stato di "bozza" e può essere confermato e modificato in uno stato "definitivo" solo dal supervisore nel ruolo di "*Sales Order Approver*"; esclusivamente quando l'ordine verrà approvato potrà essere spedito e fatturato. Per evitare di richiedere l'autorizzazione su piccoli ordini, è possibile impostare una soglia minima oltre la quale è necessario ricevere l'approvazione.

Infine, aggiungendo un automatismo in ausilio al processo di approvazione, che trasformerà automaticamente i documenti confermati in fatture e attribuendo diverse autorizzazioni all'utente con riferimento all'ordine di vendita che può creare/mantenere e alle fatture che può emettere.

Purchase Department			
Risk ID	**Risk Description**	**Function 1**	**Function 2**
P001	L'utente potrebbe gestire un fornitore fittizio e inserire una fattura fornitore con pagamento automatico.	Gestione dati fornitori	Processare fatture fornitori

Tabella 1.4: Controlli compensativi – Purchase Department

All'interno della Società X la funzione di gestione dei dati anagrafici non è del tutto centralizzata; dunque, gli utenti dedicati alla creazione e al mantenimento dei dati dei fornitori svolgo anche funzioni di acquisto e fatturazione. Si è quindi reso necessario creare un report che elenchi i nuovi dati anagrafici creati e i relativi ordini d'acquisto. L'esecuzione del report dovrebbe essere programmata o automatica, così da inviare i risultati al supervisore e verificare quanti dati

vengono creati e/o modificati. Come per l'esempio precedente, mediante il tracciamento dei dati sensibili sarà possibile individuare l'utente responsabile delle modifiche nei dati anagrafici del venditore e nelle fatture. Per impedire e rendere più difficoltosa la creazione di un fornitore fittizio, si è intervenuti per impostare come obbligatori alcuni dati durante la creazione di un nuovo fornitore (i.e. codice IVA). Un ulteriore intervento è stato provvedere ad una distribuzione difforme delle attività, così facendo, ad esempio, un utente autorizzato a creare dati anagrafici per fornitori domestici potrà effettuare ordini solo per fornitori non domestici, ciò è stato effettuato tramite l'attività di *Role Building* che prevede una segregazione dei dati sui quali l'utente può operare.

Purchase Department			
Risk ID	**Risk Description**	**Function 1**	**Function 2**
P006	L'utente potrebbe mantenere un fornitore fittizio e creare pagamenti per quel fornitore	Gestione dati fornitori	Pagamenti Accounts Payable (AP)

Tabella 1.5: Controlli compensativi – Purchase Department

Dal colore verde con cui è segnalato il rischio si può evincere che le due funzioni siano svolte in due *ERP* differenti, in quanto *Stealth* non è un sistema contabile. Questo potrebbe di base essere un buon motivo per pensare che non siano gestite dal medesimo utente, ma per implementare un forte sistema di controllo interno deve sussistere la certezza che due diversi utenti siano responsabili delle due attività. Questa ragionevole certezza può essere raggiunta attraverso un controllo incrociato sui due sistemi che elenchi tutti gli utenti che in *Stealth* possono gestire le anagrafiche dei fornitori e lo confronti con l'elenco degli utenti che nel sistema di contabilizzazione (in questo caso *SAP*) sono addetti alla gestione dei pagamenti *Accounts Payable.* Nel caso in cui ci fossero situazioni positive (utente corrispondente nei due sistemi) dovrà essere presa la decisione di aggiornare i loro ruoli in uno dei due sistemi. Se da un punto di vista organizzativo non dovesse risultare possibile modificare i ruoli in nessun applicativo, dovranno essere attuati dei controlli compensativi sul sistema

contabile.

3.3 Design del modello SOX

L'insieme di tutti gli interventi che è stato necessario implementare sul sistema del cliente "X" prende il nome di *Stealth SOX Model Design*, costituito dagli elementi e dalle regole che portano all'obiettivo principale della conformità *SOX.*

Tale modello nasce come una composizione di quattro aree di intervento:

- **User Id, Password e Autorizzazioni**: le caratteristiche di questi tre elementi devono essere coerenti con le *best practice*, deve sussistere un sistema di gestione delle autorizzazioni pervasivo sulle attività consentite a livello di utente o organizzazione;
- **Segregazione dei compiti;** assicura che solo risorse aziendali considerate idonee possano eseguire transazioni "*sensitive*", risulta quindi necessario segmentare i processi per evitare che un'utente presenti un rischio di frode;
- **Tracciabilità;** consente di verificare se è stato commesso un reato e da chi. La forza di questa funzione risiede non solo nel fatto che i dipendenti colpevoli possono essere accusati, ma anche nel deterrente che rappresenta per chi è interessato a tentare di commettere una frode;
- **Reportistica su profili e ruoli utenti**: può aiutare a rilevare eventuali attività che normalmente sono considerate a rischio se associate allo stesso utente. La segnalazione, se prodotta in modo ricorrente e attentamente analizzata, è un buon strumento nelle mani dei supervisori per rintracciare dati insoliti o sospetti.

Il rischio collegato alla prima area di intervento **User Id, Password e Autorizzazioni** si identifica nel possibile abuso di privilegi da parte degli utenti, è per questo molto importante che vengano rispettate alcune regole fondamentali per la creazione e la gestione degli User ID utilizzati per accedere al sistema. Per

ovviare tale rischio è necessario definire per ogni sistema un processo di registrazione e cancellazione per gli utenti autorizzati ad avere un account, che contempli:

- L'utilizzo di Personal User ID in modo che gli utenti siano responsabili delle proprie attività svolte sul sistema, l'utilizzo di User ID collettivo è consentito solo per specifiche necessità aziendali previa pre-autorizzazione e conservazione della documentazione.
- La verifica che l'accesso richiesto sia allineato al principio "*least privilege*" secondo il quale si concederà l'accesso all'utente soltanto nel caso in cui i dati richiesti siano necessari per poter svolgere il proprio lavoro;
- La rimozione immediata degli User ID degli utenti che hanno lasciato l'azienda;
- Il controllo periodico sull'eventuale presenza di User ID incoerenti o che dovrebbero essere rimossi perché cessati o obsoleti.

Il rischio legato alle autorizzazioni utente è il medesimo, quindi un possibile abuso dei privilegi da parte dell'utente. La soluzione è stata definire un processo per l'assegnazione e la revoca delle autorizzazioni di accesso agli utenti identificati da un User ID personale. Così facendo, l'accesso al sistema dovrà essere soggetto ad autenticazione tramite User ID o username e credenziali personali (password, PIN, token), l'autorizzazione all'accesso avverrà entro i limiti definiti dal principio "*least privilege*" e tutte le autorizzazioni di accesso verranno registrate in un sistema di anagrafica centralizzata costantemente aggiornato. Eventuali eccezioni alle autorizzazioni di accesso dovranno essere limitate, registrate e approvate dall'amministratore del sistema e dai suoi supervisori.

Nel caso venissero attribuite autorizzazione di accessi privilegiate (i.e *Super User*[83]), è necessario che queste vengano supervisionate attraverso un processo che permetta di registrate tutti i privilegi assegnati, la loro scadenza, e che

[83] Utente che dispone del massimo controllo sul sistema; esso è il solo in grado di compiere operazioni non consentite agli utenti standard.

effettui un esame periodico delle competenze dell'utente a cui è stata assegnata l'autorizzazione.

Riesaminare frequentemente le autorizzazioni è importante per evitare il rischio che l'utente abbia accessi non autorizzati alle informazioni e ai dati. Tale verifica deve essere effettuata dopo ogni modifica del profilo degli utenti, ad esempio, dopo un licenziamento la revoca delle autorizzazioni deve avvenire prima della risoluzione del contratto. In questo caso, il tempismo entro il quale viene effettuata la riesamina è fondamentale per limitare il rischio di corruzione deliberata di informazioni da parte del dipendente licenziato, o la conservazione di informazioni strategiche e riservate per usi futuri.

Eventuali lacune nella sicurezza dei dati d'accesso potrebbero causare rischi di divulgazione di informazioni riservate, accessi non autorizzati ai sistemi e furto di informazioni personali. Possibili soluzioni individuate dal gruppo di progetto risiedono nell'utilizzo di ACL (liste di controllo degli accessi) e nell'utilizzo di algoritmi di crittografia standard per memorizzare dati sensibili.

Tali disposizioni sono state attuate dal reparto IT il per definire un processo di creazione degli utenti in *Stealth* conforme con le richieste *SOX* di seguito riportato.

In seguito alla creazione dello User Id, il reparto IT assegnerà una password all'utente, la quale dovrà essere da esso modificata dopo il primo utilizzo. La password verrà impostata con una data di scadenza per limitare il furto di dati sensibili e di accessi non autorizzati causati da comportamenti scorretti dei dipendenti. Allo scadere di tale data, un messaggio avvertirà l'utente della necessità di cambiare la password. L'utente potrà essere autorizzato a svolgere sia singole attività sia gruppi di attività e un report dettaglierà quali utenti sono assegnati a quali attività, in tal modo potrà essere facilmente controllato se l'utente è stato impostato correttamente in base alle richieste d'accesso ricevuto e pervenute dal Dipartimento IT, se un dipendente ha diritto a più di un User ID, se l'ID dell'utente che ha lasciato l'azienda è stato cancellato o se l'ID del dipendente le cui mansioni sono state modificate è stato aggiornato.

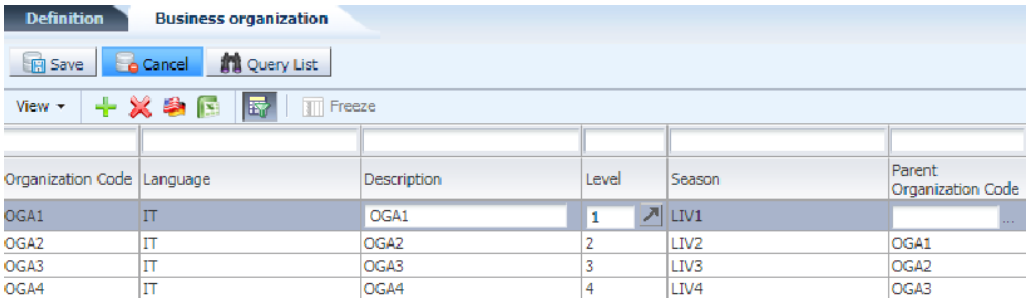
Attraverso uno nuovo report verranno inoltri identificati gli utenti che sono stati

autorizzati a svolgere attività in conflitto in termini di conformità *SOD* e *SOX*, facilitando così i controlli e il mantenimento di una corretta frequenza di esecuzione.

Sulla base di quanto previsto dall'attuale codice in materia di protezione dei dati personali, D.lgs. 196/03, e dal nuovo regolamento europeo GDPR UE 2016/679 in vigore dal 24/05/2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, il processo di creazione degli utenti in *Stealth* deve prevede misure di protezione idonee al trattamento e la tutela dei dati personali degli utenti. Un esempio è l'applicazione della password policy, secondo la quale la creazione e gestione e delle password deve rispettare determinati requisiti tecnici (i.e. la password deve essere obbligatoriamente cambiata al primo utilizzo e successivamente almeno ogni sei mesi).

Attraverso lo *Stealth SOX Model Design* sono state implementate alcune nuove funzionalità al fine di garantire una corretta **segregazione dei compiti**.

Innanzitutto, è stata creata l'Organizzazione aziendale**,** un'entità che permette di assegnare compiti specifici agli utenti che ne fanno parte e che rappresenta una gerarchia basata su più livelli.



Organization Code	Language	Description	Level	Season	Parent Organization Code
OGA1	IT	OGA1	1	LIV1	
OGA2	IT	OGA2	2	LIV2	OGA1
OGA3	IT	OGA3	3	LIV3	OGA2
OGA4	IT	OGA4	4	LIV4	OGA3

Figura 3.7: L'Organizzazione aziendale nel sistema Stealth

I livelli sono stati inseriti all'interno di un'apposita lista di valori[84], mostrata di seguito, che permette di definire la posizione dell'utente all'interno delle strutture e dei reparti aziendali. Gli incarichi potranno essere assegnati al dipendente in base alla sua appartenenza ad uno specifico livello dell'Organizzazione Aziendale, se non diversamente specificato nel proprio

[84] Lista esclusiva dei valori che possono popolare un campo di un record in un Database.

profilo.

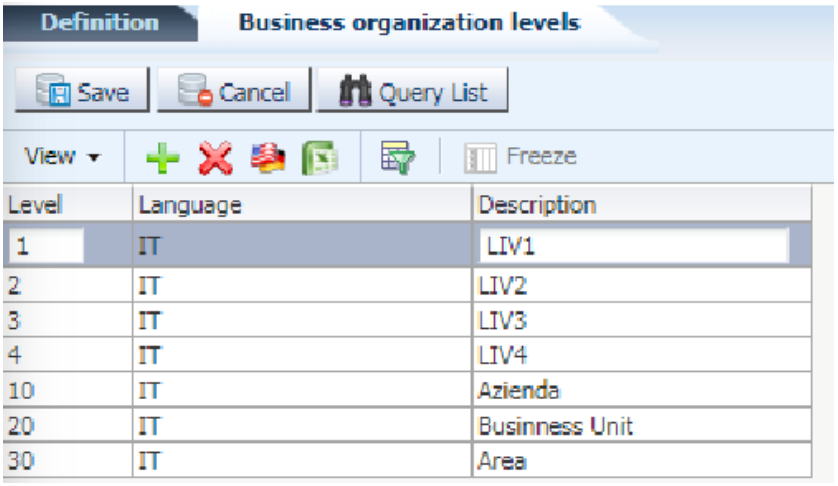


Figura 3.8: I livelli dell'organizzazione aziendale nel sistema Stealth

Nella versione standard di *Stealth* (utilizzata da clienti non soggetti alle disposizioni *SOX*), è già possibile impostare dei filtri su alcuni dati specifici, ad esempio i dati di ordini di vendita. Seguendo lo stesso principio è stata predisposta dal Dipartimento IT un'ulteriore funzionalità che permette di filtrare i dati su qualsiasi elemento primario (i.e. Causale di fatturazione) permettendo così di determinare su quali valori dell'elemento primario sono autorizzati ad operare gli utenti attraverso l'utilizzo del flag "*Enable*".

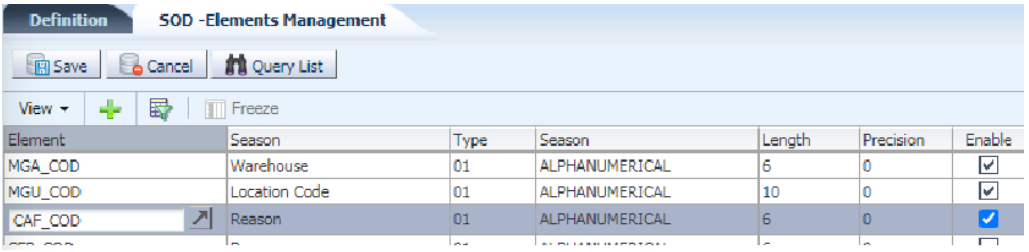


Figura 3.9: SOD – Elements Management

Un esempio pratico: un utente abilitato ad inserire un movimento di entrata merci solo se il codice magazzino è pari a '103' troverà solo tale valore da poter utilizzare nelle liste valori per la selezione del magazzino. Questo perché tutte le liste valori esistenti sul sistema, correlate agli elementi rilevati per la segregazione dei compiti, seguiranno le regole a cui tali elementi sono soggetti.

Per tener traccia di chi è responsabile dei dati memorizzati sul sistema è stata

implementata una funzionalità di **tracciabilità** che consente di archiviare grandi volumi di dati per lunghi periodi di conservazione (fino a sette anni di conservazione per scopi *SOX*). La nuova applicazione permette di definire un'area di tracciabilità, di associarne i campi da tracciare e visualizzare tutti i dati registrati all'interno del sistema.

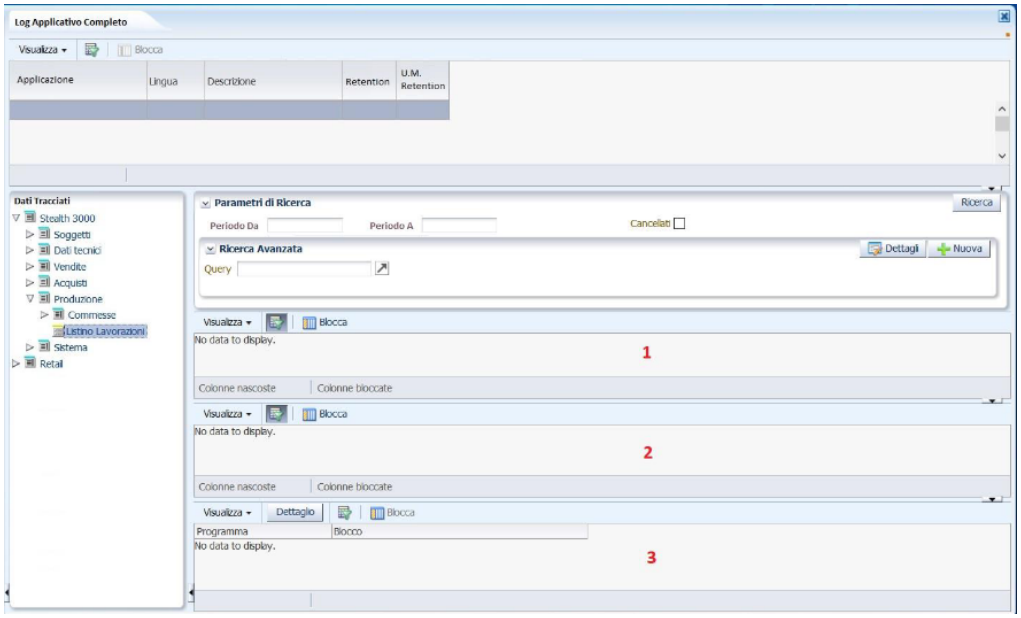


Figura 4: La funzionalità "tracciabilità" nel sistema Stealth

Attraverso il parametro di selezione "Periodo da – a" è possibile scegliere l'intervallo temporale dei dati da estrarre. Nella sezione "1" sono mostrati tutti i dati inseriti, aggiornati e cancellati relativi al periodo selezionato. Nella sezione "2" sono riportati l'ID della persona o dell'applicazione che ha creato, modificato o eliminato il record in analisi. La sezione "3", infine, permette di visionare il dettaglio di ogni singolo record estratto. Ogni giorno, i dati tracciati vengono poi trasmetti automaticamente ad un *repository* tramite un programma automatico.

Per facilitare e documentare i controlli sulle autorizzazioni degli utenti, sulle attività in conflitto e sulla consultazione dei dati sensibili memorizzati sono stati sviluppati alcuni nuovi **report**. I report, sviluppati appositamente per scopi di conformità *SOX,* si basano sul concetto di gruppo di attività; tali gruppi vengono inseriti a sistema tramite una tabella finalizzata ad evitare conflitti sui singoli ruoli utente. Inoltre, i gruppi permettono al cliente gestire eventuali eccezioni,

abilitando il singolo utente o l'intera organizzazione a svolgere determinate funzionalità.

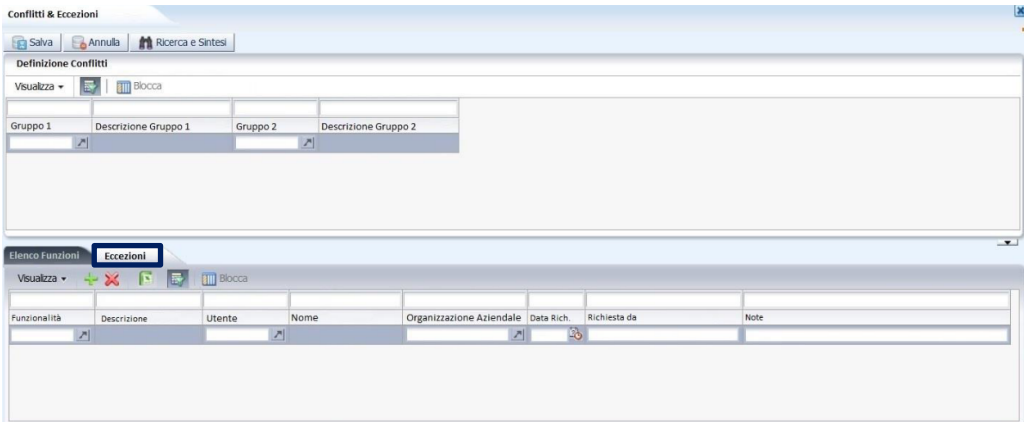


Figura 4.1: La gestione dei conflitti e delle eccezioni nel sistema Stealth

L'esempio riportato di seguito è il report "Utenti con attività in conflitto", il quale permette di confrontare le funzioni autorizzate al singolo utente con le funzioni appartenenti a un gruppo con il quale potrebbe entrare in conflitto.

Nella prima sezione del layout sono elencati i conflitti rilevati sul profilo dell'utente mentre nella seconda sezione sono mostrate l'elenco delle autorizzazioni come bypass al conflitto, comprese le eccezioni.

Figura 4.2: Report "Utenti con attività in conflitto"

Trattandosi di report automatici potrebbero essere rilevate alcune situazioni critiche sugli utenti che in seguito si rivelano false. La giustificazione risiede nel fatto che i report possono approfondire transazioni e parametri solo fino a un certo livello di dettaglio. Una volta prodotto il report, si richiede dunque che venga effettuata un'attività analitica per constatare se le attività sono da considerarsi realmente in contrasto.

L'analisi dei risultati forniti da tale report potrà quindi indurre il cliente a:

- Cancellare delle autorizzazioni per il singolo utente;
- Modificare i ruoli;
- Giustificare un “falso positivo”;
- Impostare controlli compensativi.

Un ulteriore esempio è il report “Gruppi attività e conflitti”:

Figura 4.3: Report “Gruppi attività e conflitti”

Nella prima sezione del layout sono presenti i dati anagrafici dei gruppi in conflitto:

- Codice del gruppo;
- Descrizione del gruppo;
- Funzionalità disponibili nel gruppo;
- Descrizioni delle funzionalità;
- Percorso del menu per raggiungere la funzione.

Nella seconda sezione del layout sono riportati gli utenti / organizzazioni con gruppi di attività in conflitto:

- ID utente;
- Descrizione dell'utente;
- Funzioni in conflitto;

- Elenco di autorizzazioni come bypass al conflitto.

Le opzioni di selezione di questo rapporto sono l'elenco dei gruppi e dei conflitti da analizzare.

È molto comune che gli ambienti aziendali odierni implichino l'utilizzo di un numero elevato di applicazioni che condividono e trasmettono dati tra loro ma che svolgono sostanzialmente attività diverse. Potrebbe accadere, in questa distribuzione applicativa di attività e ruoli, che l'utente sia autorizzato ad operare i due sistemi diversi. Rispetto al passato, ci sono sempre più software in gioco, ciascuno specializzato per la propria area di processo (*Best of Breed*[85]); quindi, tutte le funzioni non risiedono più su un sistema solo ma quasi regolarmente su più di un applicativo. In presenza di tale situazione, un controllo delle attività e della loro segregazione sull'utente è difficilmente possibile unicamente tramite l'utilizzo di report automatici. Quando vengono distribuiti i ruoli e quando li si verifica ai fini della conformità al *Sarbanes-Oxley Act,* è dunque fondamentale mettere in pratica dei controlli incrociati sulle autorizzazioni degli utenti nelle varie applicazioni

3.4 Considerazioni a conclusione del progetto

Essendo il go live di questo progetto previsto per gennaio 2025, non è ancora possibile valutare l'effettiva bontà delle nuove implementazioni per la Società X.

Tuttavia, realizzazioni simili a quelle sopra descritte sono state rilasciate per altri clienti, nello specifico per un cliente del comparto moda ("Società Y"), da me vissuto a posteriori, solo durante le sue fasi finali, poco prima dell'inizio di questo progetto.

Un dato confortante della bontà di tali soluzioni risiede nell'esito positivo a conclusione del ciclo di audit della Società Y.

Dopo essersi conclusi i test relativi ai controlli IT, da parte degli auditor IT della

[85] Un software viene definito "best of breed" quando rappresenta il miglior sistema nella sua categoria di riferimento.

società di revisione del cliente, non sono state rilevate particolari anomalie nel funzionamento dell'applicativo in fase di revisione, per cui, nessun controllo testato è stato considerato come inefficace.

Attraverso un rapporto fornito alla Funzione IT della Società Y, il sistema informativo è stato definito come "di supporto" per effettuare una corretta revisione del bilancio.

Il progetto della Società X sarà sottoposto al medesimo ciclo di auditing, la cui time line sarà scandita dalle normative di chiusura del bilancio contabile. Durante tale periodo vi sarà una fase di supporto lato *Stealth* al fine di intercettare tutte le mancanze e correggerle per avvicinarsi ad un ambiente pienamente sicuro. Come descritto nel capitolo precedente, una volta eseguita la valutazione dei sistemi del cliente, i risultati dei test verranno riportati dalla società di revisione alla Funzione IT della Società X, attraverso un rapporto contenente tutti gli aspetti analizzati ed eventuali spunti di miglioramento al fine di mitigare accuratamente i rischi IT.

Mediante la partecipazione a questo progetto, ho appreso operativamente come la conformità *SOX* rappresenti uno sforzo continuo che richiede una completa integrazione nei processi aziendali, nelle politiche e nei sistemi informativi. Il sistema di controllo che un'organizzazione imposta durante un progetto di implementazione SOX è un oggetto vivo. Poiché le aziende vivono e cambiano in qualsiasi momento, è importante che le procedure di controllo siano sottoposte a continui miglioramenti e valutazioni rispetto ai cambiamenti organizzativi. I dipendenti vengono licenziati o lasciano l'azienda, le descrizioni delle mansioni cambiano e potrebbero essere seguite da cambiamenti nei ruoli e nelle strutture aziendali. Possono verificarsi fusioni, acquisizioni e licenziamenti, tutti questi eventi esprimono la necessità di predisporre procedure formalmente approvate e scritte che consentano all'organizzazione di evolvere in modo proattivo il proprio sistema di controllo. Ho inoltre compreso che per ottenere un risultato efficiente e applicare correttamente le implicazioni della nuova legge federali si renda necessaria una grande collaborazione tra diverse funzioni aziendali. Il fulcro del *Sarbanes Oxley-Act* è la qualità dei dati, la legge istituisce meccanismi che

mirano a garantire determinati livelli di qualità dei dati finanziari per ridurre al minimo il rischio che le informazioni finanziarie riportate siano involontariamente o intenzionalmente fuorvianti. Pertanto, il dipartimento IT svolge indubbiamente un ruolo cruciale per la conformità, diventando un attore attivo quando si rendono necessarie nuove implementazioni a sistema. Nonostante ciò, senza una meticolosa fase iniziale di valutazione e analisi sui processi del cliente non sarebbe possibile disporre di un importante punto di partenza sul quale permettere al reparto IT di poter lavorare. Per ottenere dei risultati puntuali è necessario articolare il sistema di controllo su tre livelli di responsabilità; il primo, livello composto dalle funzioni di business che rappresentano gli *owner* dei singoli processi aziendali e ne gestiscono direttamente i rischi. Il secondo livello, composto da funzioni di *compliance* e *risk management*, addette al monitoraggio dei rischi e dell'efficacia delle procedure aziendali. Il terzo livello, rappresentato dalla figura dell'*internal audit* che, come già specificato, deve verificare l'efficacia del sistema di controllo interno e validare il funzionamento del processo di *risk management*, andando a identificare eventuali opportunità evolutive.

Conclusione

Con questo lavoro di tesi ho voluto approfondire le disposizioni della normativa *SOX* nella sua parte relativa alle richieste di compliance fiscali e, attraverso il mio periodo di stage, la sua applicazione pratica in un contesto aziendale.

Se da un lato le linee guida contenute nei *framework* precedentemente descritti sono state senza dubbio fondamentali nelle fasi iniziali di progetto al fine di impostare un processo organizzato coerente e comprendere quali controlli interni implementare, dall'altro, ho potuto constatare come, a livello operativo, per ottenere l'esito desiderato, la mera applicazione di quanto esposto in questi modelli necessita di una fondamentale sensibilità nella sua componente di applicazione pratica. Diventa quindi sempre più importante e vincente, per ruoli come quello a cui mi sono affiancata, avere a disposizione un bagaglio di esperienze e di casistiche molto più ampio e trovare, tra queste, quella che si avvicina maggiormente ad essere applicata alla realtà ed organizzazione del cliente, senza snaturarla, ma allo stesso tempo permettendo alla stessa di rispettare quanto previsto dalla normativa. Tutto ciò anche a beneficio e supporto dei processi di controllo interno e gestione rischi dei clienti derivanti da una loro gestione non appropriata, quindi non necessariamente dipendenti da una mancata applicazione della normativa, sapendo identificare quella che tra le *best practice* è la migliore *good practice* per lo specifico progetto.

La collaborazione con i consulenti *Stealth* mi ha inoltre permesso di apprendere che ogni cliente e progetto sono unici nei loro modi di lavorare e di organizzarsi, ho quindi potuto constatare come questo tipo di consulenza richieda, oltre ad una preparazione sulla specificità della normativa, forti componenti di conoscenza sui processi e sulle organizzazioni aziendali, apprendimento continuo delle loro evoluzioni e situazioni, guidate da un business sempre più esigente e concorrenziale sul mercato, capacità di mettere a fattor comune le diverse esigenze degli stakeholder, interessati in un mix di relazioni e di competenze che diventa vincente quando si ha la capacità di arrivare a trovare il giusto equilibrio e compromesso che permetta di raggiungere l'obiettivo finale.

Bibliografia

AIEA, itSMF italia, SDA Bocconi, *COBIT® e ITIL® due framework complementari* in "AIEA", (2007).

A. Calder, S. Watkins, *IT Governance: An International Guide to Data Security and ISO27001/ISO27002,* Kogan Page Ltd, (2012).

C. Fox, P. Zonneveld, *Il ruolo dell'IT nel progetto e nell'implementazione dei controlli interni per la predisposizione del reporting finanziario*, traduzione italiana a cura dell'Associazione Italiana Information Systems Auditors (AIEA), Milano, (2007).

C. Kidd, *what is COBIT? COBIT Explained* in "BCM blogs", (2019).

Committee of Sponsoring Organizations of the Treadway Commission (COSO), *COSO Internal Control Certificate - Participant Manual*, (2015).

Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Enterprise Risk Management Integrating with Strategy and Performance Executive Summary*, (2017).

Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Enterprise Risk Management – Integrated Framework Executive Summary*, (2004).

D.E. Sanger*, Corporate conduct: The overview* in "The New York Times",17/07/2002.

Decreto legislativo n. 23 8 giugno 2000, Gazzetta Ufficiale n.140 del 19/06/2001.

E. Di Lella, *Il caso Enron: una truffa da 130 miliardi di dollari* in "Starting Finance", 30/10/2016.

F. Venturelli, *I processi di controllo interno sulla rendicontazione e la loro*

revisione: l'esperienza statunitense. Cacucci Editore, (2007).

G. Campanelli, *Vent'anni dalla bolla delle dot-com: da Netscape a Tiscali, le società implose (e non)* in "Corriere Della Sera", 4/03/2020.

G. Gasparri, *I controlli interni nelle società quotate in "*CONSOB - Quaderni Giuridici", Milano, (2013), pp.15.

G. Trequattrini, *Origini e sviluppo dell'internal auditing: nuovi rischi e prospettive* in "Banca d'Italia-Pubblicazioni" Roma, (2022), pp.2.

Gruppo di Ricerca Governance, *Monografia n.1 - COSO Framework: guida alla lettura*, ASSIREVI, Milano, (2019).

Gruppo di Ricerca Governance, *Monografia n.3 - COSO ERM: guida alla lettura*, ASSIREVI, Milano, (2020).

ISACA, *The risk IT Framework*, USA, (2009).

J. Stephen McNally, *Leveraging Effective Risk Management*, and Internal Control in "Strategic Finance", pp. 29-36, (2014).

K. Kinzer, *What Are IT General Controls (ITGC)* in "Jumpcloud blogs", 23/08/2023.

L. Ballejos, *Che cos'è un audit IT? Una guida pratica* in "NinjaOne Blogs", 18/03/2024.

L. Balzarotti, B. Micco lupi, *La truffa di Enron, 15 anni fa. Le tappe del default nelle pagine d'Archivio* in "Corriere Della Sera", 3/12/2016.

L.Provaroni, *Il sistema di controllo interno nelle piccole e medie imprese,* Ordine dei Dottori Commercialisti e degli Esperti Contabili, Roma, (2023).

M. Novarini*, La truffa che sconvolse Wall Street: i 20 anni del crac della Enron* in "Forbes Italia", 12/02/2021.

M.Bozzola, *Sarbanes-Oxley Act Sezione 404 (Internal Control over Financial Reporting)* in "Ernst&Young", (2010).

Moving Forward–A Guide to Improving Corporate Governance Through Effective Internal Control in "Deloitte&Touche", (2003).

N.Zanghi, *Il Framework ERM e i fattori chiave per l'implementazione* in "Assirevi", Milano, (2020).

Otero, Angel. R, *Information technology control and audit*, Auerbach Publications, (2018).

P. Riva, *Ruoli di Corporate Governance*, EGEA spa, Milano, 2023.

R. Garelli, *Controlli interni e requisiti del Sarbanes-Oxley Act* in "Impresa Progetto", 2 (2009), pp.1.

S. Cammarata, *Interventi del Sarbanes-Oxley Act of 2002 sulla corporate responsibility nelle società quotate statunitensi* in "Archivio Ceradi", (2002).

S. Nisticò, *Dall'euforia alla crisi: etica e fiducia nei mercati* finanziari in "University Library of Munich", Germany, (2005).

S. Pastorino, *Il sistema di controllo interno, l'applicazione dei principi del CoSo 2013-Introduzione al CoSO Report*, Webinar del Mercoledì INRL 2022 – INRL – Istituto Nazionale Revisori Legali, 09/03/2022.

The Future of IT Internal Controls –Automation: A Game Changer in "Deloitte&Touche", (2018).

U. Bertini, *Il sistema d'azienda*, Giappichelli, Torino, (1990).

Sitografia

About PCAOB, https://pcaobus.org/about, ultimo accesso:12/03/2024.

Auditing Standard No. 5 - An Audit of Internal Control Over Financial Reporting that is Integrated with an Audit of Financial Statements, https://pcaobus.org/oversight/standards/archivedstandards/details/Auditing_Standard_5_Appendix_A, ultimo accesso: 30/04/2024.

Come l'internal audit può collaborare con il revisore, https://www.revisore.it/come-l-internal-audit-puo-collaborare-con-il-revisore/, ultimo accesso:02/04/2024.

Controllo interno, oltre la conformità: controllo interno e monitoraggio dei costi, https://fastercapital.com/it/contenuto/Controllo-interno--oltre-la-conformita--controllo-interno-e-monitoraggio-dei-costi.html, ultimo accesso: 12/04/2024.

CoSO Report I e CoSO Framework SCIGR: Applicazione nella revisione legale e nel MOGC ex D Lgs 231/2001, https://www.formazionerevisori.net/articoli/2020.1%20CoSO%20Report%20I%20e%20coSO%20Framework%20SCIGR.pdf, ultimo accesso: 19/03/2024.

D.Chesley, *the top changes to the COSO ERM Framework you need to know now* https://www.linkedin.com/pulse/top-changes-coso-erm-framework-you-need-know-now-dennis-chesley/, ultimo accesso 30/04/2024.

Decreto legislativo n. 58 24 febbraio 1998, https://www.consob.it/documents/1912911/1962639/dlgs58_1998.pdf/72a502a7-c9ed-a632-81b2-0434d82ae0aa

Enron: il più grande fallimento degli Stati Uniti, https://www.wallstreetitalia.com/enron-il-piu-grande-fallimento-degli-stati-uniti/, ultimo accesso: 12/03/2024.

Enterprise Risk Management, https://www.coso.org/enterprise-risk-management, ultimo accesso: 30/04/2024.

Financial Trend Analysis, *NASDAQ: cos'è e come funziona il mercato, https://www.borsaitaliana.it/notizie/sotto-la-lente/nasdaq.htm,* ultimo accesso: 12/03/2024.

Il controllo interno e il documento di riferimento COSO, https://www.giovannellapolidoro.com/it/il-controllo-interno/, ultimo accesso:12/03/2024.

I*l Sarbanes Oxley Act e la Legge italiana 262/2005*, https://www.uniaudit.it/2024/03/11/il-sarbanes-oxley-act-e-la-legge-italiana-262-2005/, ultimo accesso: 10/04/2024.

Il Sarbanes Oxley Act e la Normativa Italiana: l'impatto sulle Imprese, https://addconsulting.it/2010/01/20/il-sarbanes-oxley-act-e-la-normativa-italiana-limpatto-sulle-imprese/, ultimo accesso:12/03/2024

IS Audit & Compliance Support, https://www.bdo.it/it-it/services-it/advisory/digital-consulting/is-audit-compliance-support, ultimo acesso:30/04/2024.

Is Enron Overpriced, https://fortune.com/2015/12/30/is-enron-overpriced-fortune-2001/, ultimo accesso: 12/03/2024.

La bolla delle dot.com: racconto di una delle più grandi crisi finanziarie, https://davideberti.it/blog/la-bolla-delle-dot-com-racconto-di-una-delle-piu-grandi-crisi-finanziarie-della storia?highlight=WyJkb3QiLCJjb20iLCJjb20nXHUwMGU4IiwiZG90IGNvbSJd, ultimo accesso: 12/03/2024.

Lo scoppio della bolla delle dot.com, https://www.consob.it/web/investor-education/la-bolla-delle-c.d.-dotcom, ultimo accesso: 12/03/2024.

Navigazione nel governo societario una prospettiva Sarbanes Oxley Act, https://fastercapital.com/it/contenuto/Navigazione-nel-governo-societario--una-prospettiva-Sarbanes-Oxley-Act.html, ultimo accesso: 16/04/2024.

PCAOB Auditing Standard N. 2, https://pcaobus.org/oversight/standards/archived-standards/details/Auditing_Standard_2, ultimo accesso:05/04/2024.

Section 302: Corporate Responsibility for Financial Reports, https://www.soxlaw.com/sox-section-302/,ultimo accesso:12/03/2024.

Section 401: Disclosures in Periodic Reports, https://www.soxlaw.com/sox-section-401/, ultimo accesso:12/03/2024.

Section 404: Management Assessment of Internal Controls, https://www.soxlaw.com/sox-section-404/, ultimo accesso:12/03/2024.

Section 409: Real Time Issuer Disclosures, https://www.soxlaw.com/sox-section-409/,ultimo accesso:12/03/2024.

Section 802: Criminal Penalties for Altering Documents, https://www.soxlaw.com/sox-section-802, ultimo accesso:12/03/2024.

Section 806: Protection of Employees of PTC, https://www.soxlaw.com/sox-section-806/, ultimo accesso:12/03/2024.

Section 906: Corporate Responsibility for Financial Reports, https://www.soxlaw.com/sox-section-906/, ultimo accesso:12/03/2024.

SOX Compliance Requirements & Overview, https://www.auditboard.com/blog/sox-compliance/, ultimo accesso:12/03/2024.

Technology risk, https://www.pwc.com.au/risk-controls/technology-risk.html, ultimo accesso: 30/04/2024.

The Board, https://pcaobus.org/about/the-board, ultimo accesso:12/03/2024.

The Sarbanes Oxley Act, https://sarbanes-oxley-act.com/, ultimo accesso:12/03/2024.

Una panoramica sui Report SOC: i controlli per la cybersecurity, https://aksiliagroup.com/blog/2021/03/31/report-soc/, ultimo accesso: 02/04/2024.