



LA TRASPARENZA DELLE INFORMAZIONI FINANZIARIE

LEGGE 262 E SARBANES OXLEY ACT: UNA COMPARAZIONE FRA LE DUE LEGGI PER INDIVIDUARE APPROCCI METODOLOGICI COMUNI, TENUTO CONTO ANCHE DELL'ESPERIENZA MATURATA DA VODAFONE OMNITEL NELL'IMPLEMENTAZIONE DEGLI OBBLIGHI IMPOSTI DALLA SOX

■ Introduzione ■ Il COSO Internal Control framework ■ Le analogie e le differenze fra la SOX e la Legge 262 ■ L'esperienza SOX di Vodafone in Italia.

1. Introduzione

Il presente articolo ha lo scopo di confrontare sinteticamente la normativa statunitense relativa al controllo interno sul financial reporting, ovvero la "section 404" del Sarbanes Oxley Act, e l'analoga regolamentazione introdotta in Italia dalla Legge 262 del 2005.

In particolare, l'analisi si concentrerà sui "framework" di riferimento per il sistema di controllo interno descrivendo come il COSO, individuato dalla regolamentazione statunitense come

framework di riferimento cui ancorare il giudizio di adeguatezza del sistema, possa esserlo anche per la regolamentazione Italiana.

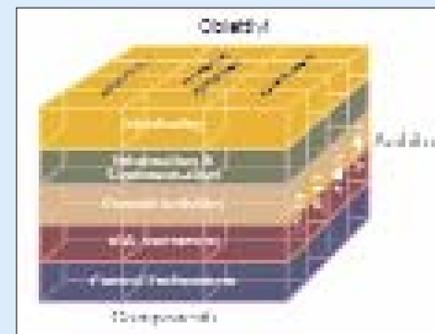
Considerato, infine, il "successo" in termini di ottimizzazione dei costi di compliance dell'applicazione SOX in Vodafone, il presente documento contiene la descrizione dell'approccio adottato da Vodafone Italia e le considerazioni relative alla valorizzazione di quanto già implementato per garantire il soddisfacimento delle disposizioni normative contenute nella Legge 262.

2. Il COSO Internal Control framework

Nei primi anni Novanta, su incarico del Committee of Sponsoring Organizations of the Treadway Commission ("COSO", che include le più prestigiose associazioni professionali d'America), la Coopers & Lybrand (oggi PricewaterhouseCoopers) ha elaborato un modello innovativo di sistema di controllo interno delle imprese, il CoSO Report - Internal Control Integrated Framework ("COSO IC"), fondendo a tutte le parti interessate un comune concetto di controllo.

Il modello presentato nel CoSO Report è diventato il modello di riferimento utilizzato sia dai codici di autodisciplina da parte di associazioni di categoria, sia dalla normativa nazionale ed internazionale in materia di Corporate Governance. In particolare, il PCAOB (Public Accounting Oversight Board), l'agenzia di supervisione e di regolamentazione delle attività di revisione contabile istituita dalla SOX sotto la guida della Securities and Exchange Commission (SEC), ha assunto, quale standard di riferimento per la valutazione di adeguatezza del sistema di controllo interno in ambito amministrativo-contabile (Internal Control Over Financial Reporting - ICOFR) il framework COSO IC.

Il Codice di Autodisciplina per le società quotate in Borsa (il c.d. "codice Preda" emanato nel 1999 ed aggiornato nel 2006), inoltre, riprende la definizione di sistema di controllo e le caratteristiche del controllo interno evidenziate nel CoSO Report. Secondo il CoSO Report, il sistema di controllo interno è definito come un processo, ossia una serie di azioni, svolto dal Consiglio di Amministrazione, dai dirigenti e da tutto il personale aziendale, finalizzato a fornire una ragionevole certezza sul raggiungimento degli obiettivi aziendali (classificati di seguito). Esiste, inoltre, un rapporto diretto tra gli obiettivi, ossia ciò che l'azienda persegue, e i componenti, ossia ciò che occorre per realizzarli. Questo rapporto è schematizzato nella matrice tridimensionale (cubo) di seguito riportata:



Le tre categorie di obiettivi sono rappresentate nelle colonne verticali del cubo, i cinque componenti nelle righe orizzontali; nella terza dimensione della matrice, invece, sono rappresentate le unità operative o le singole attività dell'azienda.

Obiettivi operativi

Gli obiettivi operativi sono legati all'efficienza ed all'efficienza delle attività e dei processi aziendali. Assumono, pertanto, rilevanza sia il modello organizzativo sia le procedure, definiti e diffusi al fine di garantire un impiego efficace ed efficiente delle risorse aziendali.



di CLAUDIO LESCA

Direttore Amministrazione e Tesoreria Vodafone Omnitel N.V. Dottore Commercialista e Revisore Contabile Consigliere e Responsabile Controllo Interno del Fondo TELEMACO Presidente CDAF e Membro del Consiglio Direttivo ANDAF

cia ed all'efficienza delle attività e dei processi aziendali. Assumono, pertanto, rilevanza sia il modello organizzativo sia le procedure, definiti e diffusi al fine di garantire un impiego efficace ed efficiente delle risorse aziendali.

Obiettivi di financial reporting

Tali obiettivi attengono all'attendibilità ed alla tempestività del financial reporting. In tale ambito, la finalità dei processi di controllo interno è quella di fornire ragionevole certezza circa l'attendibilità dei dati, delle informazioni e del processo utilizzati per la predisposizione del reporting finanziario e circa il rispetto della tempistica prevista. Gli obiettivi relativi alle informazioni di bilancio si riferiscono alla redazione dei bilanci pubblicati, inclusi i bilanci intermedi e sintetici ed i dati significativi destinati ad essere comunicati al pubblico. Il termine "attendibile" implica che i bilanci siano predisposti in modo "corretto e veritiero" ed in conformità ai principi contabili di generale accettazione o a pertinenti ed appropriati principi contabili e disposizioni obbligatorie ai fini esterni. Questi obiettivi sono supportati da un insieme di presupposti di base, quali l'esistenza delle operazioni registrate in un certo periodo, la completezza della registrazione di tutte le operazioni e gli eventi che si sono verificati, la corretta valutazione o allocazione dell'ammontare registrato in conformità con i principi contabili e la correttezza della descrizione e classificazione delle informazioni che figurano a bilancio. In tale contesto, gli aspetti legati ai sistemi informativi da cui l'azienda estrae ed elabora i dati per la predi-

sposizione dell'informativa finanziaria assumono, pertanto, rilevanza.

Obiettivi di compliance

Gli obiettivi di compliance attengono alla conformità delle attività dell'azienda alle leggi e ai regolamenti in vigore.

Componenti del sistema di controllo interno

I cinque componenti del sistema di controllo interno, interconnessi tra loro, sono i seguenti:

- **Control Environment:** L'ambiente di controllo è influenzato dalla storia e dalla cultura dell'azienda e incide, a sua volta, sulla sensibilità del personale alle esigenze di controllo. A tal fine, vengono elaborate linee guida e procedure appropriate, spesso accompagnate da un codice di condotta, che favoriscono l'adesione ai valori dell'organizzazione e la collaborazione nel raggiungimento degli obiettivi.
- **Risk Assessment:** Tale attività è considerata una pre-condizione rispetto alla selezione dei controlli: è necessario, infatti, individuare e valutare il rischio prima di definire le specifiche attività di controllo.
- **Control Activities:** sono composte dalle procedure e dalle direttive che il management ha introdotto per assicurarsi che le proprie linee guida siano rispettate; si tratta di un'attività di controllo da attuarsi in tutta la struttura ed in tutti i suoi livelli, da realizzarsi attraverso approvazioni, autorizzazioni, verifiche, con adeguata separazione dei compiti e delle responsabilità.
- **Information & Communication:** si compone dei sistemi e delle procedure informative che producono e distribuiscono le informazioni all'interno ed all'esterno dell'azienda.
- **Monitoring:** le metodologie ed i sistemi di controllo devono essere periodicamente soggetti a processi di revisione volti a verificarne l'adeguatezza e l'efficacia; obiettivo del monitoraggio è quello di mantenere, aggiornare e migliorare la qualità del sistema di controllo interno. L'ultima dimensione descritta dall'Internal Control Integrated Framework è relativa all'ambito di applicazione, che può essere "modulare" per quanto riguarda l'estensione ed il livello di profondità. A tale proposito, una delle più frequenti applicazioni pratiche di tale modello è stata proprio quella che ha come ambito i processi aziendali con rilevanza ▶



LA TRASPARENZA DELLE INFORMAZIONI FINANZIARIE

amministrativo-contabile, al fine di raggiungere l'obiettivo di adeguatezza del financial reporting.

3. Le analogie e le differenze fra la SOX e Legge 262

Esistono numerose analogie fra la Legge 262 e la SOX: innanzitutto, entrambe attribuiscono precise responsabilità nella predisposizione dei documenti contabili.

L'art. 154-bis del T.U.F., infatti, così come modificato dalla Legge 262, al comma 2 stabilisce che "gli atti e le comunicazioni della società previste dalla legge o diffuse al mercato, contenenti informazioni e dati sulla situazione economica, patrimoniale o finanziaria della stessa società, sono accompagnati da una dichiarazione scritta del direttore generale e del dirigente preposto alla redazione dei documenti contabili societari, che ne attestano la corrispondenza al vero".

E', pertanto, attribuita al direttore generale ed al dirigente preposto alla redazione dei documenti contabili societari una responsabilità analoga a quella che la sezione n. 302 della SOX ha stabilito per il CEO ed il CFO, tenuti a certificare la veridicità dei report annuali e trimestrali, dell'informativa di bilancio e degli altri documenti contabili.

Una seconda analogia è relativa al sistema di controllo interno di cui l'azienda deve dotarsi per garantire il raggiungimento degli obiettivi di cui sopra, vale a dire la corrispondenza al vero dell'informativa di bilancio.

Il comma 3 dell'art. 154-bis del T.U.F., così come modificato dalla Legge 262, stabilisce che "il dirigente preposto alla redazione dei documenti contabili societari predispone adeguate procedure amministrative e contabili per la predisposizione del bilancio di eser-

cizio e, ove previsto, del bilancio consolidato nonché di ogni altra comunicazione di carattere finanziario".

Al successivo comma 5, è inoltre stabilito che "gli organi amministrativi delegati e il dirigente preposto alla redazione dei documenti contabili societari attestano con apposita relazione, allegata al bilancio di esercizio e, ove previsto, al bilancio consolidato, l'adeguatezza e l'effettiva applicazione delle procedure di cui al comma 3 nel corso dell'esercizio cui si riferisce il bilancio, nonché la corrispondenza del bilancio alle risultanze dei libri e delle scritture contabili. L'attestazione è resa secondo il modello stabilito con regolamento dalla CONSOB".

Risulta evidente l'analogia con quanto richiesto dalla sezione n. 404 della SOX e, cioè, che il bilancio annuale delle società quotate sul mercato statunitense includa un "internal control report" che attesti la responsabilità del management nell'implementare e mantenere un'adeguata struttura di controllo interno relativa al reporting economico-finanziario, e nel quale l'efficacia di tale struttura di controllo sia valutata alla data di riferimento.

Una differenza è relativa al fatto che la normativa americana prevede, al contrario di quella italiana, la verifica e l'attestazione da parte del Revisore Esterno del sistema di controllo interno definito dal management a supporto delle proprie dichiarazioni.

In Italia, invece, il T.U.F. prevede all'art. 149, l'esistenza di un soggetto istituzionale preposto, il Collegio sindacale, il cui compito è quello di vigilare sull'adeguatezza della struttura organizzativa della società per gli aspetti di competenza, del sistema di controllo interno e del sistema amministrativo-contabile nonché sull'affidabilità di quest'ultimo nel rappresentare correttamente i fatti di gestione.

Le indicazioni di dettaglio sui requisiti "minimi" del sistema di controllo interno oggetto di attestazione da parte del management sono state definite negli Stati Uniti dall'Auditing Standard n. 2 emanato dal PCAOB che ha assunto come standard di riferimento il Framework COSO IC, mentre in Italia si attende l'emanazione di un regolamento CONSOB che, probabilmente, indicherà anche il modello di riferimento.

A differenza della realtà americana, il principio di revisione italiano sul sistema di controllo interno non rimanda ad un modello di riferimento (documento n. 400 della Commissione paritetica per la statuizione dei principi di revisione relativo alla "Valutazione del rischio e il sistema di controllo interno").

Ulteriori differenze sono poi relative alle disposizioni sulle società controllate (vedi art. 165, comma 2 e 3). Sulla base di quanto sopra, pertanto, può essere ragionevole ritenere che un'azienda "SOX compliant" possa utilizzare i processi definiti a fronte dell'applicazione di quella normativa come base per valutare la conformità con le disposizioni della Legge 262.

4. L'esperienza SOX di Vodafone in Italia

Il gruppo Vodafone, ed al suo interno Vodafone Omnitel NV, la Operating Company (Opco) Italiana, in quanto soggetto con l'obbligo di essere compliant con la SOX, si è focalizzata su due problemi principali, uno di carattere organizzativo ed uno di carattere metodologico.

Il primo problema è stato relativo alla individuazione degli enti all'interno del gruppo e delle singole società che dovessero essere coinvolti nel processo di valutazione e certificazione del sistema di controllo interno, il secondo invece era indirizzato a definire una metodologia comune che garantisse il raggiungimento degli obiettivi ma anche la non proliferazione dei controlli.

L'approccio che il gruppo Vodafone ha impresso al progetto è stato caratterizzato sin dall'inizio da un coordinamento delle attività delle singole Operating Companies, sia da un punto di vista di gestione di progetto attraverso l'emanazione di policies e procedure, sia attraverso l'indicazione di processi, rischi e controlli comuni a tutte le società del gruppo.

Tale approccio ha consentito di limitare il numero di controlli chiave ne-

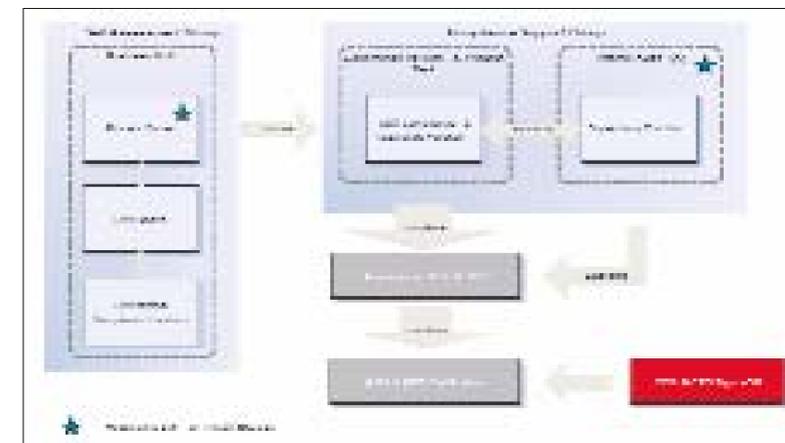
cessari per il monitoraggio del rischio ed ha contribuito a diffondere la cultura del controllo interno nelle singole società, responsabilizzando le unità operative all'interno del business come esecutori dei controlli e garanti del sistema del controllo interno.

L'utilizzo di diversi strumenti ad hoc, tra cui SOX Express, utilizzato come repository di tutta la documentazione prodotta a fini SOX (processi, rischi e controlli) ha inoltre consentito una maggiore efficienza e trasparenza nel processo di documentazione e valutazione del sistema di controllo interno.

Da un punto di vista organizzativo, sono stati istituiti diversi ruoli ed assegnate responsabilità in tutta l'organizzazione, così riassumibili:

- in ogni OpCo è stato nominato un *Local Champion* con la responsabilità di coordinare le attività di *compliance* nella propria OpCo e di farsi garante dell'utilizzo di adeguate risorse, della corretta applicazione di strumenti e metodologie e del costante aggiornamento della documentazione;
- in ogni OpCo e per ognuno dei processi identificati, è stato nominato un *Process Owner*, responsabile della costante valutazione dei rischi e dell'efficacia dei controlli in essere. Il ruolo fondamentale del process owner è rappresentato dal continuo presidio del processo da lui governato attraverso un costante monitoraggio dei rischi legati all'evoluzione del business e dei processi ed un conseguente aggiornamento dei controlli chiave necessari;
- *SOX Liaison*: è il punto di contatto per il processo di riferimento ed il primo riporto del Process Owner. Il SOX Liaison deve apporre la propria firma in SOX Express al fine di certificare l'operating effectiveness di ogni controllo chiave testato nel proprio processo;
- *SOX Internal Compliance Function*: responsabile della manutenzione di tutta la documentazione prodotta ai fini SOX (processi, rischi e controlli) e per lo svolgimento dei test sui controlli chiave identificati;
- *Control Owner*: è colui che è responsabile che un controllo sia svolto in maniera efficace;
- *Control Performer*: è colui che svolge il controllo.

La tabella successiva descrive in maniera grafica gli enti ed i relativi flussi informativi identificati per raggiungere e gestire la compliance.



Vodafone Omnitel NV, considerata la criticità e delicatezza del progetto si è dotata di una struttura cui è stata assegnata la responsabilità della documentazione di tutti i sotto-processi identificati come *in scope*, interfacciandosi, da un lato, con il GPMD per recepire Policy e Guidance, e dall'altro con tutti i dipartimenti della OpCo Italiana, al fine di ottenere le necessarie informazioni per documentare i processi stessi.

La metodologia definita a livello di gruppo e applicata dalle singole OpCo può essere sintetizzata come segue:

- Definizione dell'ambito: basandosi sul Bilancio, definire quali accounts e quindi quali processi sono *in scope*;
- Valutazione dell'ambiente di controllo interno a livello di OpCo: ogni OpCo svolge un Entity Level Control Assessment (ELCA), basandosi su questionari di auto-valutazione preparati dal Gruppo;
- Valutazione del sistema di controllo interno a livello di processo: ogni OpCo identifica e documenta il vigente sistema di controllo interno su ogni singolo processo *in scope*. La documentazione consiste in:

- un *flowchart*, che rappresenta graficamente il processo;
- un *narrative*, da leggersi assieme al *flowchart* poiché ne descrive le attività nel dettaglio;
- una *Risk & Control Matrix*, che contiene la mappatura di tutti i rischi esistenti lungo il processo ed i controlli in essere per mitigare i rischi identificati;
- un *Walkthrough*, che dettaglia l'esito di una verifica svolta sui sotto-processi e sui controlli chiave, al fine di verificare che gli stessi fosse disegnati correttamente (*Design effectiveness*);
- un *Testing*, che dettaglia specifici test svolti sui controlli chiave, al fine di verificare che operassero come descritto (*Operating effectiveness*);

• un *Remediation Plan*, che dettaglia le attività di miglioramento in corso sui sotto-processi o sui controlli chiave identificati come inefficienti (*Ineffective*).

- Test dei controlli chiave: i controlli chiave (Key Controls) sono testati su base annuale.

- *Management Certification*: il management rilascia la certificazione sul sistema di controllo interno;

- *Attestation* del Revisore: il Revisore Esterno effettua un *audit* del sistema di controllo e ne rilascia una valutazione sull'*effectiveness*;

Un ultimo aspetto caratterizzante la gestione del progetto di compliance di Vodafone è stato la valutazione del sistema di controllo interno relativo all'area informatica e la valutazione dei controlli informatici sui processi operativi. A tale proposito, la cooperazione tra gli specialisti dell'area informatica ed i responsabili operativi dei processi ha consentito di ridurre il numero di controlli chiave e di modificare le tipologie di controlli esistenti da "detective" a "preventive" migliorando il sistema di controllo interno nel suo complesso.

Dopo i primi due anni la SOX ha smesso di essere un progetto per entrare in regime di *Business As Usual*: si è provveduto pertanto a trasferire la responsabilità per il mantenimento della documentazione prodotta ai fini SOX da un dipartimento centralizzato ad ogni singolo *process owners*.

Un grazie a tutti coloro che hanno lavorato alla predisposizione di questo documento ed in particolare alla mia collaboratrice Sharon Grant, responsabile del dipartimento Governance, Policies & Process nonché SOX Champion di Vodafone Italia, ed ad Andrea Samaja, Giuseppe Garzillo e Carlo Marsano, partner e managers di PriceWaterhouseCoopers. □