Obiettivi di controllo IT per il Sarbanes-Oxley Act

IL RUOLO DELL'IT NEL PROGETTO E NELL'IMPLEMENTAZIONE DEI CONTROLLI INTERNI PER LA PREDISPOSIZIONE DEL REPORTING FINANZIARIO

2° EDIZIONE

SETTEMBRE 2006

LUGLIO 2007
Traduzione Italiana a cura di
Associazione Italiana Information Systems Auditors AIEA
Capitolo di Milano di ISACA

INGLESE

This Work is translated into Italian from the English language version of IT Control Objectives for Sarbanes-Oxley 2nd edition by the Milan Chapter of the Information Systems Audit and Control Association (ISACA) with the permission of the IT Governance Institute. The Milan Chapter assumes sole responsibility for the accuracy and faithfulness of the translation.

ITGI created IT Control Objectives for Sarbanes-Oxley, 2nd Edition ("Work") primarily as an educational resource for controls professionals. ITGI makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, the controls professional should apply his or her own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

ITALIANO

Autorizzazione

Il presente Prodotto è tradotto in lingua italiana dalla versione inglese di IT Control Objectives for Sarbanes-Oxley II edizione a cura del Capitolo di Milano di Information Systems Audit and Control Association (ISACA) con l'autorizzazione dell'IT Governance Institute.
Il Capitolo di Milano si assume la sola responsabilità della accuratezza della traduzione e della aderenza alla versione originale.

Copyright

Disclaimer

ITGI ha prodotto IT Control Objectives for Sarbanes-Oxley, 2nd Edition (Prodotto) innanzitutto come una risorsa formativa per gli esperti del controllo.
ITGI non assicura alcun risultato dovuto all'utilizzo del Prodotto. Il Prodotto non deve essere considerato come comprensivo di tutte le informazioni, procedure e test relativi ai controlli, o alternativo ad altre informazioni, procedure e test che ragionevolmente possono permettere di ottenere lo stesso risultato. Nel determinare l'applicabilità di ciascuna specifica informazione, procedura o test, l'esperto dei controlli deve valutare sotto la propria responsabilità la particolare circostanza influenzata dallo specifico sistema o dallo specifico ambito tecnologico.

Avvertenze

Pubblicazione edita in Italia con autorizzazione di IT Governance Institute (ITGI).
La traduzione italiana è curata da:
AIEA – Associazione Italiana Information Systems Auditors - Capitolo di Milano di ISACA.
Per usi commerciali si suggerisce di abbinare il testo italiano con quello inglese che si può acquisire da ITGI.

AIEA – Associazione Italiana Information Systems Auditors
20141 Milano - Via Valla, 16
Tel 0039 02 84742.365- Fax 0039 02 84742212
E-mail: aiea@aiea.it; Sito: www.aiea.it
P.IVA 10899720154

L'AIEA – Associazione Italiana Information Systems Auditors (Capitolo di Milano di ISACA) – ringrazia tutte le aziende di appartenenza dei componenti il Gruppo di Lavoro per la disponibilità e per il valore del contributo apportato dai rispettivi rappresentanti. A questi ultimi un particolare ringraziamento per l'impegno, la professionalità dimostrate e per aver contribuito al successo dell'iniziativa.

Coordinamento

Daniela Bolli, CISA	Poste Italiane Consigliere AIEA
Silvano Ongetta, CISA, CISM	Presidente AIEA

Gruppo di Ricerca

Luigi Giambarini, CISA, CISM, CIA	Banche Popolari Unite
Roberto Tarrusio, CISA	Banca Popolare di Vicenza
Francesco Passi, CISA, CISM	Telecom Italia
Fabio Di Sansa, CISA	TWT
Ezio Miozzo,	Ing. Miozzo
Michele Colucci, CISA	Poste Italiane
Silvia Tagliaferri, CISA	Between
Sergio Tagni	Banca Popolare di Sondrio
Simone Tomirotti, CISA	Mediaset
Marco Vernetti, CISA	RAI
Luciano Orifiammi, CISA	Unicredit Servizi Informativi
Guido Leone, CISA	EDS

Comitato di Qualità

Dario Carnelli, CISA, CISM	Felcra BCC
Bruno Ghisu, CISA	Banco di Sardegna
Silvano Ongetta CISA, CISM	Presidente AIEA

IT Governance Institute®

L'IT Governance Institute (ITGI™) (*www.itgi.org*) è stato fondato nel 1998 con l'intento di promuovere i concetti e gli standard internazionali relativi alla gestione e al controllo del sistema informativo delle imprese. Un efficace IT governance assicura che l'IT supporti gli obiettivi del business, ottimizzi gli investimenti delle imprese nell'IT e gestisca in modo appropriato i rischi e le opportunità legate all'IT. L'ITGI offre le risorse elettroniche, ricerche specifiche e casi di studio per supportare i dirigenti d'impresa e i consigli di amministrazione per quanto riguarda le loro responsabilità nel governo dell'IT.

Copyright

IT Governance Institute

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.590.7491
Fax: +1.847.253.1443
E-mail: research@itgi.org
Web site: www.itgi.org

ISBN 1-933284-76-5
IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition
Printed in the United States of America

Disclaimer

L'IT Governance Institute, ISACA® e quanti hanno contribuito alla stesura del documento non garantiscono che l'utilizzo del presente documento assicuri un risultato positivo. Il presente documento non dovrebbe essere considerato come il compendio di controlli IT, procedure e test che potrebbero essere ragionevolmente presenti in un efficace sistema di controllo interno sul reporting finanziario. Nel determinare la correttezza di un qualsiasi specifico controllo, procedura o test, le aziende soggette al controllo da parte della Securities and Exchange Commission (SEC) dovrebbero analizzare in modo adeguato le modalità di controllo previste dagli specifici sistemi o dagli ambienti di information technology.

Per i lettori di questo documento è importante notare che lo stesso non ha ricevuto l'approvazione da parte della SEC, che è responsabile di regolamentare le aziende ad azionariato diffuso, o dal US Public Company Accounting Oversight Board (PCAOB), che è responsabile di regolamentare l'attività delle società di revisione. Gli argomenti trattati in questa pubblicazione sono destinati a evolversi nel tempo. Per questo, le aziende dovrebbero richiedere ausilio ai loro consulenti e/o auditor sui rischi.
Coloro che hanno contribuito a questo documento non danno garanzie e non forniscono assicurazioni che l'uso di questo documento porti a controlli di rilevazione, procedure, controlli interni e procedure per il reporting finanziario che:

- Siano conformi ai requisiti di controllo interno del Sarbanes-Oxley Act.
- Rendano i piani dell'organizzazione sufficienti per indirizzare e correggere tutte le imperfezioni che impedirebbero all'organizzazione stessa di raggiungere la certificazione richiesta o di produrre reporting finanziari a norma del Sarbanes-Oxley Act.

I controlli interni, per quanto siano ben progettati e funzionanti, possono fornire soltanto la ragionevole assicurazione che gli obiettivi di controllo di un'azienda siano realizzati. La probabilità di successo è influenzata dalle limitazioni insite nel controllo interno. Queste includono la reale possibilità che il giudizio umano nell'assunzione di decisioni possa essere erroneo e che i malfunzionamenti nel controllo interno accadano per errori umani di varia natura. Inoltre, i controlli, sia manuali sia automatici, possono essere bypassati dalla collusione di due o più persone o dall'inappropriato comportamento del management che può annullare l'effetto dei controlli interni stessi.

Ringraziamenti

Dall'editore
L'IT Governance Institute desidera ringraziare:

I principali collaboratori per la stesura di questo documento
Christopher Fox, ACA
Paul Zonneveld, CISA, CA

I seguenti collaboratori
Gordon Bloom, CISA, RSM McGladrey Inc., USA
Michael Cangemi, CISA, CPA, Cangemi Company LLC, USA
Nancy Cohen, CPA, AICPA, USA
Roger Debreceny, Ph.D., FCPA, University of Hawaii, USA
Robert Frelinger, CISA, Sun Microsystems Inc., USA
Kenneth S. Gabriel, CPA, KPMG LLP, USA
Michael Garber, CIA, CPA, Motorola Inc., USA
John Gimpert, CPA, Deloitte & Touche LLP, USA
John Hainaut, Jefferson Wells, USA
Hussain Hasan, CISM, CISSP, RSM McGladrey Inc., USA
Edward Hill, CIA, CPA, Protiviti, USA
Tara Janos, BP Amoco, USA
Peter Koltun, Jefferson Wells, USA
Phillip Lageschulte, CPA, KPMG LLP, USA
Elsa K. Lee, CISA, CISM, CSQA, AdvanSoft International Inc., USA
Anthony Noble, CISA, CCP, Viacom Inc., USA
Heriot Prentice, MIIA, FIIA, QiCA, The Institute of Internal Auditors, USA
Debbie Sanneman, Motorola, USA
Sheryl Skolnik, CISA, CISM, CPA, BDO Seidman LLP, USA
Tracy Stewart, CISA, CISSP, CCP, CIA, Allstate Insurance Company, USA
Doug Underwood, CPA, McGladrey & Pullen, USA
Mickey Vaja, CISA, CCNA, CISSP, Grant Thornton LLP, USA
Kenneth Vander Wal, CISA, CPA, CSP, Ernst & Young LLP, USA
Timothy Van Ryzin, CISA, CISM, Harley-Davidson, USA
Jeffrey Ward, CISA, CPA, CITP, Stone Carlie & Company LLC, USA
Margaret Yocher, United Technologies-Carrier, USA
Paul Zonneveld, CISA, CA, Deloitte & Touche LLP, Canada

L' ITGI Advisory Panel
Ronald Saull, CSP, Great-West Life Assurance and IGM Financial, Canada, Chair
Roland Bader, F. Hoffmann-La Roche AG, Switzerland
Linda Betz, IBM Corporation, USA
Jean-Pierre Corniou, Renault, France
Rob Clyde, CISM, Symantec, USA
Richard Granger, NHS Connecting for Health, UK
Howard Schmidt, CISM, R&H Security Consulting LLC, USA
Alex Siow Yuen Khong, StarHub Ltd., Singapore
Amit Yoran, Yoran Associates, USA

Gli affiliati e gli sponsor di ITGI
I Capitoli ISACA, American Institute for Certified Public Accountants,ASIS International , The Center for Internet Security, Commonwealth Association of Corporate Governance Information Security Forum, The Information Systems Security Association, Institut de la Gouvernance des Systèmes d'Information, Institute of Management Accountants, ISACA, ITGI Japan,Solvay Business School ,University of Antwerp Management School,Aldion Consulting Pte. Ltd, CA, Hewlett-Packard, IBM ,LogLogic Inc., Phoenix Business and Systems Process Inc., Symantec Corporation, Wolcott Systems Group, World Pass IT Solutions

Indice

Executive summary

Nell’aprile 2004, l’IT Governance Institute ha pubblicato “Obiettivi di Controllo IT per il Sarbanes-Oxley Act ” per aiutare le aziende a valutare e a migliorare il loro sistema di controllo interno. Da allora, la pubblicazione è stata utilizzata dalle imprese di tutto il mondo come strumento per la valutazione dei controlli IT a supporto della conformità al Sarbanes-Oxley Act.

Conformità e IT Governance

Non esiste un ambiente privo di rischi e la conformità al Sarbanes-Oxley Act non crea un tale ambiente. Tuttavia, è probabile che il processo che la maggior parte delle aziende seguirà per migliorare il proprio sistema di controllo interno e per conformarsi al Sarbanes-Oxley Act, fornisca benefici durevoli. Una corretta governance dell’IT riguardo la pianificazione e il ciclo di vita degli obiettivi di controllo dovrebbe portare a reporting finanziari più accurati e tempestivi.

Il lavoro richiesto per adeguarsi ai requisiti del Sarbanes-Oxley Act non dovrebbe essere considerato come un processo di conformità, ma piuttosto come un'occasione per istituire modelli robusti di governo progettati per portare a definire responsabilità e fornire risposte alle necessità di business. Lo sviluppo di un robusto programma di controllo interno per l’IT può essere di ausilio per:

- Guadagnare vantaggio competitivo attraverso attività operative più efficienti e più efficaci
- Migliorare le competenze di risk management e la definizione delle priorità di intervento in materia
- Migliorare l’IT governance complessiva
- Migliorare la comprensione dell’IT fra gli executive manager dell’azienda
- Ottimizzare le attività operative con un approccio integrato alla sicurezza, disponibilità e integrità delle elaborazioni
- Permettere di effettuare scelte migliori per il business fornendo informazioni di più elevata qualità e più tempestive
- Contribuire alla conformità con altri requisiti normativi, quali la legge sulla privacy
- Allineare le iniziative di progetto con i requisiti di business
- Prevenire la perdita di proprietà intellettuali e le possibilità di violazione del sistema.

Miglioramenti alla pubblicazione con la seconda edizione

Molto si è appreso riguardo al reporting finanziario e ai controlli IT da quando è stato pubblicato il primo documento – in particolare, la necessità di adottare un approccio top-down, risk-based nei programmi di conformità al Sarbanes-Oxley Act per aiutare ad accertarsi che fosse prestata un’adeguata attenzione alle aree a elevato rischio.

Di conseguenza, l’ITGI ha revisionato la precedente pubblicazione per fornire ulteriori linee guida relative all’IT sulle aree di maggiore importanza per il controllo interno del reporting finanziario, nonché per condividere quanto appreso riguardo la conformità dell’IT al Sarbanes-Oxley Act. La seconda edizione è stata resa disponibile al pubblico per un periodo 60 giorni e le osservazioni ricevute sono state utilizzate per effettuare diverse revisioni, fino a giungere a questa pubblicazione finale.

Sebbene molto sia stato appreso dal rilascio iniziale della pubblicazione, le linee guida fondamentali fornite nell’aprile del 2004 rimangono valide. Lo scopo di integrare la pubblicazione iniziale è di condividere le lezioni apprese dalle aziende e fornire ulteriori linee guida su come migliorare l'efficienza e

l'efficacia della conformità usando un approccio risk-based. Qui di seguito un sommario delle aggiunte alla pubblicazione iniziale:

- Aumento del focus sull'ambito delle verifiche e sul risk assessment – Sono state aggiunte delle linee guida per aiutare le aziende nell'applicazione dell'approccio top-down, risk-based. In particolare, sono state aggiunte delle linee guida di ausilio per effettuare un risk assessment dell'IT secondo il Sarbanes-Oxley Act.
- Definizione delle priorità dei controlli – Sono state aggiunte delle linee guida per aiutare le aziende nella definizione "dei controlli più rilevanti". Usando queste linee guida, alcuni controlli dell'appendice C, controlli generali IT, sono stati identificati come i controlli più attinenti.
- Gestione dell'elemento umano del cambiamento – Sono state aggiunte delle considerazioni sulla gestione delle problematiche umane e culturali correlate per evidenziare i fattori specifici che devono essere considerati quando si vuole aderire al Sarbanes-Oxley Act.
- Miglioramento delle linee guida riguardo i controlli applicativi – Sono state aggiunte delle linee guida per aiutare le aziende a identificare e considerare vari tipi di controlli applicativi ed è stato fornito un business case per l'utilizzo di tali controlli.
- Approccio per i fogli elettronici – Sono state aggiunte delle linee guida per aiutare le aziende nella predisposizione dei fogli elettronici, comprese le best practice per i controlli.
- Semplificazione della leggibilità della road map – Sono stati fatti cambiamenti nella leggibilità della road map per semplificare il processo.
- Riferimenti incrociati ai processi di COBIT® 4.0.
- Le lezioni apprese – E' stata aggiunta una lista delle lezioni apprese così da poter condividere le esperienze effettuate, relativamente alla conformità, nelle aziende di tutto il mondo; comprende i punti da considerare per rendersi conto dei benefici o per evitare i trabocchetti più comuni.
- Considerazioni e approccio riguardo all'uso dei SAS *70* examinations reports.
- Miglioramento delle ulteriori linee guida sulla separazione dei compiti per le applicazioni più significative.

Considerazioni per le piccole imprese

Nel luglio 2006, il Commitee of Sponsoring Organizations of the Treadway Commission (COSO) ha pubblicato "Guidance for Smaller Public Companies Reporting on Internal Control Over Financial Reporting". La pubblicazione di COSO ha evidenziato le sfide affrontate dalle piccole aziende nell'aderire a normative come il Sarbanes-Oxley Act e ha proposto dei suggerimenti per affrontare queste sfide.

Le piccole aziende possono anche trovare difficoltà ad affrontare le considerazioni sui controlli IT che sono previsti nel Sarbanes-Oxley. Di conseguenza, è importante evitare una strategia "one-size-fits-all" (comune per le aziende di tutte le dimensioni), e adottare invece un approccio risk-based implementando solo quei controlli IT che sono necessari e pertinenti alle circostanze. Per esempio, le piccole aziende usano spesso per le applicazioni finanziarie dei prodotti di mercato standard (off-the-shelf, OTS) e relativamente semplici, piuttosto che grandi sistemi ERP (Enterprise Resource Planning) personalizzabili. In questi casi, il rischio di errori nel rendiconto finanziario che derivano dall'applicazione è tipicamente inferiore a quello dei sistemi più grandi e complessi. Di conseguenza, la natura e l'ampiezza dei controlli richiesti per la piccola azienda dovrebbero essere minori rispetto a quelli di aziende più grandi. Anche se ci sono sempre eccezioni alla regola, le piccole aziende dovrebbero valutare con attenzione i loro rischi ed effettuare soltanto i controlli che sono necessari. In tal senso, in questa pubblicazione sono state migliorate le linee guida per il risk assessment.

Allineamento con PCAOB e COBIT

In conseguenza del Sarbanes-Oxley Act sono stati definiti complessivamente 12 obiettivi di controllo IT aderenti al PCAOB Auditing Standard n. 2 e a COBIT. La f**igura 1** fornisce una mappa ad alto livello degli obiettivi di controllo IT per il Sarbanes-Oxley Act descritti in questo documento, i controlli generali IT identificati dal PCAOB e i processi di COBIT 4.0.

Figura 1 – Mappa PCAOB-COBIT

	COBIT	Obiettivi di controllo IT generali PCAOB			
Obiettivi di controllo IT per il Sarbanes-Oxley Act	**Mappa dei processi COBIT 4.0**	**Program Development**	**Program Changes**	**Computer Operations**	**Access to Programs and Data**
1. Acquisire e manutenere applicazioni software	AI2	●	●	●	●
2. Acquisire e manutenere infrastrutture tecnologiche	AI3	●	●	●	
3. Abilitare al funzionamento e all'utilizzo	AI4	●	●	●	●
4. Installare e accreditare soluzioni e cambiamenti tecnologici	AI7	●	●	●	●
5. Gestire i cambiamenti	AI6		●		●
6. Definire e gestire livelli di servizio	DS1	●	●	●	●
7. Gestire servizi di terze parti	DS2	●	●	●	●
8. Garantire la sicurezza dei sistemi	DS5			●	●
9. Gestire la configurazione	DS9			●	●
10. Gestire problemi e incidenti	DS8 DS10			●	
11. Gestire i dati	DS11			●	●
12. Gestire l'ambiente fisico e le attività operative	DS12 DS13			●	●

Utilizzo di questa pubblicazione

Le informazioni contenute in questo documento forniscono utili linee guida e strumenti per le aziende che provano a preparare e a sostenere le loro unità organizzative IT in conformità al Sarbanes-Oxley Act. Tuttavia, ogni azienda dovrebbe considerare attentamente gli obiettivi di controllo IT appropriati, necessari per le proprie caratteristiche. **Le aziende possono scegliere di non includere tutti gli obiettivi di controllo discussi in questo documento e, analogamente, possono decidere di includerne altri non considerati in questo documento.** In entrambi i casi, sarà necessario che cambiamenti nella descrizione degli obiettivi di controllo, dei controlli e dei test dimostrativi, forniti in questo documento, riflettano le specificità di ogni azienda.

Fondamenti per un reporting finanziario affidabile

Esigenza di linee guida per i controlli IT

Nelle aziende odierne, i processi di reporting finanziario sono realizzati con sistemi IT. Tali sistemi, siano essi ERP o altri, sono profondamente legati al ciclo di vita - inizio, autorizzazione, registrazione, elaborazione e reporting delle transazioni finanziarie. Perciò sono indissolubilmente legati all'intero processo di reporting finanziario e devono essere valutati, insieme con altri processi importanti, per la conformità al Sarbanes-Oxley Act.

E' stato scritto molto sull'importanza del Sarbanes-Oxley Act e dei controlli interni in generale, ma esiste poco sul ruolo significativo svolto dall'IT in questa area. Per esempio, il Sarbanes-Oxley Act richiede alle aziende di selezionare e implementare un'adeguata struttura di controllo interno. L' Internal Control—Integrated Framework di COSO è diventata la struttura più comunemente usata dalle aziende che aderiscono al Sarbanes-Oxley Act; tuttavia, COSO non fornisce moltissime linee guida alle aziende per aiutarle nel disegno e nell'implementazione dei controlli IT.

Di conseguenza, le aziende necessitano di linee guida per individuare le componenti IT che riguardano l'intero programma relativo alla conformità del processo di reporting finanziario. Questo documento intende fornire assistenza a tale scopo, utilizzando i contenuti pertinenti di SEC, PCAOB, COSO e di COBIT. Si veda l'appendice B per ulteriori approfondimenti su COSO e COBIT.

Dove trovare i controlli IT

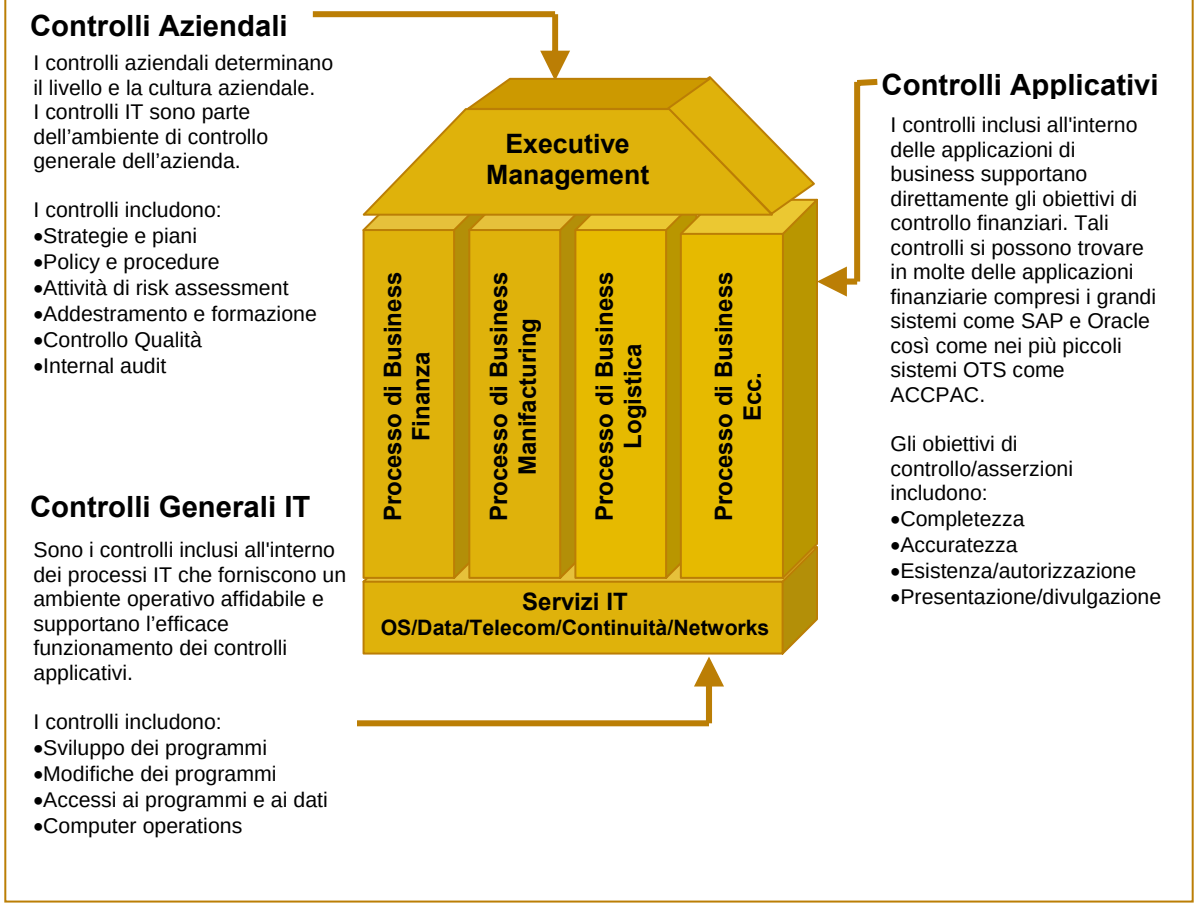
Per capire dove esistono i controlli IT in seno a un'azienda tipo, devono essere presi in considerazione almeno tre elementi: executive management, processi di business e servizi IT.

La figura 2, alla pagina seguente, illustra gli elementi comuni delle aziende.

Executive Management	Processo di Business	Servizi IT
L'Executive Management determina e inserisce le strategie nelle attività di business. A livello di azienda o di singola entità, sono definiti gli obiettivi di business, sono stabilite le policy e sono prese decisioni su come allocare e gestire le risorse dell'azienda. Dal punto di vista dell'IT, vengono definite e comunicate a tutta l'aziendale policy e altre linee guida di natura generale	I processi di business sono il meccanismo attraverso il quale l'azienda crea e distribuisce valore ai suoi stakeholder. Gli input, le elaborazioni e gli output sono funzioni dei processi di business. I processi di business sono stati automatizzati e integrati sempre di più con sistemi IT più efficienti e complessi.	I servizi IT sono il fondamento per le attività operative e sono erogati trasversalmente a tutta l'azienda piuttosto che dedicati al singolo processo di business o alla singola unità di business. I servizi IT comunemente includono la gestione della rete, della base dati, del sistema operativo, dei supporti di memorizzazione dei dati, il facility management e la gestione della sicurezza. Spesso sono gestiti da una funzione IT centralizzata.

I sistemi IT stanno sempre di più automatizzando i processi di business. In tal modo, questi sistemi sostituiscono spesso attività di controllo manuali con attività di controllo automatizzate o IT dipendenti. Di conseguenza, i programmi di conformità devono considerare i controlli basati sui sistemi IT per stare al passo con i cambiamenti nei processi di business e con le nuove funzionalità del sistema.

Figura 2 – Elementi comuni delle aziende



Controlli IT - una sfida unica

Il Sarbanes-Oxley Act rende gli executive manager delle aziende esplicitamente responsabili della implementazione, valutazione e monitoraggio dell'efficacia dei controlli interni relativi al reporting finanziario. Per la maggior parte delle aziende, il ruolo dell'IT è cruciale per realizzare questo obiettivo. Sia attraverso un sistema informativo integrato (ERP) o un insieme non integrato di applicazioni software di amministrazione operativa e finanziaria, l'IT è la base per un efficace sistema di controllo interno sul reporting finanziario.

Tuttavia, questa situazione crea una sfida unica: molti dei professionisti IT, responsabili per la qualità e l'integrità delle informazioni generate dai loro sistemi, non sono abbastanza esperti per la complessa problematica del controllo interno. Ciò non deve far pensare che il rischio non sia stato gestito dall'IT, ma piuttosto che non sia stato formalizzato o strutturato nella maniera richiesta dai manager dell'azienda o dai suoi auditor.

Le aziende hanno bisogno di rappresentanti dell'IT nei loro gruppi di lavoro sul Sarbanes-Oxley Act per determinare se esistono i controlli IT di monitoraggio, generali e applicativi realizzati per il raggiungimento degli obiettivi di conformità. Alcune delle più importanti aree di responsabilità dell'IT includono:

- Capire il sistema di controllo interno dell'azienda e il processo di reporting finanziario
- Mappare l'ambiente IT (servizi e processi) che supporta il controllo interno e il processo relativo al bilancio.
- Identificare i rischi relativi a questi sistemi IT
- Progettare e implementare i controlli atti a mitigare i rischi identificati e monitorarne continuamente la loro efficacia
- Documentare e testare i controlli basati sui sistemi IT
- Accertarsi che i controlli IT vengano aggiornati e modificati in coerenza con i cambiamenti nei controlli interni o nei processi di reporting finanziario
- Monitorare l'efficacia dei controlli IT nel tempo
- Partecipare al comitato di progetto per il Sarbanes-Oxley Act.

I regolamenti SEC che interessano il Sarbanes-Oxley Act sono innegabilmente complessi e la loro implementazione è stata costosa sia in termini di tempo sia di costo. Prima di procedere a definire il programma di controllo per l'IT, ci sono due importanti considerazioni che dovrebbero essere tenute presenti:

- Non c'è la necessità di re-inventare la ruota; virtualmente tutte le aziende ad azionariato diffuso hanno già qualche controllo IT. Anche se possono essere informali e mancanti di un'adeguata documentazione del controllo e dei relativi principi di funzionamento, generalmente i controlli IT esistono in aree quali la sicurezza e il change management.
- Molte aziende possono adattare i processi di controllo IT esistenti per aderire alle disposizioni del Sarbanes-Oxley Act. Frequentemente le carenze sono nella consistenza e nella qualità della documentazione dei controlli e delle specifiche sul loro funzionamento, ma il processo generale viene spesso applicato, e richiede soltanto qualche modifica.

Effettuare una revisione completa dei processi di controllo IT e documentarli senza arrestare l'attività dell'azienda potrebbe essere un'operazione che richiede tempo. La revisione dell'implementazione e dei processi IT dovrebbe essere guidata dai rischi di business e operativi. Senza l'adeguata conoscenza e linee guida, le aziende corrono il rischio di fare troppo o troppo poco. Questo rischio è amplificato quando i responsabili non hanno esperienza nel progetto e nell'assessment dei controlli IT o difettano della necessaria conoscenza o struttura gestionale per identificare e mettere a fuoco le aree di rischio più significative.

Mentre alcune aziende, come quelle di servizi finanziari, hanno familiarità con i rigorosi requisiti di conformità e normativi degli ambienti del libero mercato, la maggior parte delle aziende non lo sono. Per rispondere alle esigenze del Sarbanes-Oxley Act, nella maggior parte delle aziende sono in corso dei cambiamenti culturali. Sono stati richiesti miglioramenti ai sistemi IT e ai processi, in particolare nel disegno dei controlli, nella loro documentazione, nell'archiviazione delle evidenze del loro funzionamento e nella valutazione dell'efficacia nel tempo.

Linee guida PCAOB per i controlli IT

Il PCAOB Auditing Standard No. 2 tratta del rapporto tra l'IT e i controlli interni per il reporting finanziario ed enfatizza l'importanza di identificare i controlli IT e di verificare il loro disegno e l'efficacia operativa.

In particolare, 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.*

Il PCAOB Auditing Standard No. 2 continua descrivendo il processo che gli auditor dovrebbero seguire nella determinazione delle asserzioni o degli obiettivi appropriati per supportare la valutazione del management:

> *Per identificare le asserzioni pertinenti, l'auditor dovrebbe determinare, per ogni conto significativo, la fonte delle probabili potenziali affermazioni errate. Nel determinare se una particolare asserzione è rilevante per un saldo di un conto oppure per una comunicazione, l'auditor dovrebbe valutare [tra gli altri]:*
>
> - *La natura e la complessità dei sistemi, compreso l'uso dell'IT tramite il quale l'azienda elabora e controlla le informazioni che supportano l'asserzione.*

Il PCAOB Auditing Standard No. 2 inoltre richiama specificamente l'IT nella predisposizione del reporting finanziario di fine periodo:

> *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;*

Controlli sui sistemi IT

Il ricorso diffuso ai sistemi IT rende necessari i controlli su tali sistemi, grandi o piccoli che siano. I controlli IT generalmente comprendono controlli sull'ambiente IT, sulle attività operative, sull'accesso a programmi e dati, sui progetti di sviluppo e di modifica delle applicazioni. Questi controlli si applicano ai sistemi che sono stati identificati come finanziariamente significativi.

L'ambiente di controllo IT

L'importanza dell'ambiente di controllo è stata ulteriormente evidenziata nel PCAOB Auditing Standard No. 2. Lo standard afferma che:

> *... A causa dell'effetto dominante dell'ambiente di controllo sull'affidabilità del reporting finanziario, le considerazioni preliminari dell'auditor circa la sua efficacia spesso influenzano la natura, il tempismo e la portata dei test di*

> *efficacia di funzionamento considerate necessarie. Le carenze nell'ambiente di controllo dovrebbero indurre l'auditor a modificare la natura, il tempismo o la portata dei test di efficacia di funzionamento che andrebbero effettuati in assenza delle carenze.*

Inoltre, il PCAOB ha evidenziato che un ambiente di controllo inefficace dovrebbe essere considerato almeno come una mancanza significativa e come indicatore forte che esiste una carenza significativa nel controllo interno relativo al reporting finanziario. Queste osservazioni si applicano all'ambiente di controllo nel suo insieme, che include l'ambiente di controllo IT.

L'ambiente di controllo IT comprende i processi di governo dell'IT, di monitoraggio e di reporting. Il processo di governo dell'IT include il piano strategico dei sistemi IT, il processo di gestione dei rischi IT, la gestione della conformità e delle normative, le policy IT, le procedure e gli standard. Il monitoraggio e il reporting sono necessari per allineare l'IT ai requisiti di business.

La struttura della governance IT dovrebbe essere progettata in modo che l'IT aggiunga valore al business e che i rischi dell'IT siano attenuati. Ciò include anche una struttura organizzativa IT che preveda un'adeguata separazione dei compiti e che promuova il raggiungimento degli obiettivi dell'azienda.

Le attività operative IT *(computer operations)*

Queste includono i controlli relativi alla definizione, l'acquisizione, l'installazione, la configurazione, l'integrazione e la manutenzione dell'infrastruttura IT. I controlli continui sulle attività operative considerano l'attività giornaliera dei servizi informatici e comprendono la gestione dei livelli di servizio, la gestione di servizi di terze parti, la disponibilità del sistema, la gestione del rapporto con il cliente, la gestione della configurazione e dei sistemi, la gestione dei problemi e degli incidenti, la schedulazione delle attività operative e la gestione dell'infrastruttura (facility management).

Le attività operative relative al software di sistema comprendono i controlli sull'efficace acquisizione, esecuzione, configurazione e manutenzione del sistema operativo, dei sistemi di gestione dei database, del software di interoperabilità (middleware), comunicazione, sicurezza e dei programmi di utilità generale (utility) che consentono il corretto funzionamento del sistema e delle applicazioni. Il software di sistema fornisce anche strumenti per la tracciatura degli incidenti, di logging e di monitoraggio. Il software di sistema può tenere traccia sull'uso dei programmi di utilità generale (utilities) consentendo, se qualcuno accede a queste potenti funzioni di modifica dei dati, almeno la registrazione del loro utilizzo e la segnalazione per consentire una verifica.

Accesso ai Programmi e ai Dati

I controlli d'accesso a programmi e dati assumono una maggiore importanza man mano che cresce la capacità di connessione interna ed esterna con le reti aziendali. Gli utenti interni possono essere dall'altra parte del mondo o dietro l'angolo e possono esserci migliaia di utenti esterni che accedono, o cercano di accedere, ai sistemi di un'azienda. Controlli efficaci sulla sicurezza dell'accesso possono fornire un ragionevole grado di sicurezza contro l'accesso improprio e l'uso non autorizzato dei sistemi. Se progettati in modo appropriato, possono bloccare hacker pericolosi, software malevolo e altri tentativi di intrusione.

Attività adeguate di controllo dell'accesso, come password sicure, Internet firewall, crittografia dei dati e chiavi di cifratura possono essere metodi efficaci per la prevenzione degli accessi non autorizzati. I codici di accesso degli utenti (account) e i relativi controlli sui privilegi di accesso limitano le applicazioni o le funzioni applicative ai soli utenti autorizzati che ne hanno bisogno per svolgere il loro lavoro, supportando un'appropriata separazione dei compiti. Dovrebbe esistere una revisione frequente e periodica dei profili che consentono e/o limitano l'accesso. Ex dipendenti o impiegati insoddisfatti possono rappresentare una minaccia per il sistema; quindi le password e i codici di accesso di ex dipendenti dovrebbero essere immediatamente revocati. Prevenendo l'utilizzo e le modifiche non autorizzate al sistema, un'azienda protegge l'integrità dei suoi dati e dei programmi.

Lo sviluppo e la modifica dei programmi

Lo sviluppo e la manutenzione del software applicativo è costituito da due componenti principali: l'acquisizione e l'implementazione di nuove applicazioni e la manutenzione delle applicazioni già esistenti.

Il processo di acquisizione e implementazione di nuove applicazioni tende ad avere un alto livello di insuccesso. Molte implementazioni sono considerate dei completi insuccessi, dato che non soddisfano completamente i requisiti e le aspettative del business o non sono completate nei tempi previsti o non rispettano il budget.

Per ridurre i rischi inerenti l'acquisizione e l'implementazione, alcune aziende utilizzano una metodologia di sviluppo dei sistemi e gestione della qualità. Gli strumenti software standard e le componenti dell'architettura IT spesso supportano questa metodologia. Quest'ultima fornisce inoltre la struttura per l'identificazione delle soluzioni automatizzate, del progetto del sistema e della relativa implementazione, dei requisiti di documentazione, test e approvazione, del project management e dei requisiti di supervisione e valutazione dei rischi di progetto.

La manutenzione delle applicazioni coinvolge l'implementazione di nuove release del software e la gestione delle modifiche (change management). Dovrebbero esistere dei controlli adeguati sulle modifiche del sistema per garantire che vengano realizzate tutte in modo appropriato. Esiste inoltre la necessità di determinare l'ampiezza dei test richiesti per la nuova release di un sistema. Per esempio, l'implementazione della nuova versione di un software può richiedere la valutazione dei miglioramenti al sistema, un test ampio, l'aggiornamento della formazione dell'utente e la revisione delle procedure. I controlli possono comprendere l'obbligo dell'autorizzazione per le richieste di modifica, la verifica sulle modifiche effettuate, le approvazioni, la documentazione, il processo di test, la valutazione di impatto su altre componenti IT e sulle policy di implementazione. Inoltre è necessario che il processo di change management sia integrato con gli altri processi IT, ivi compresa la gestione degli incidenti, la gestione dei problemi, la gestione della disponibilità e il controllo delle modifiche alle infrastrutture.

Gestione dell'elemento umano nel cambiamento

L'implementazione dei controlli finalizzati al Sarbanes-Oxley Act, anche dove ne esistevano già alcuni, è diventata una sfida significativa per la maggior parte delle aziende. In molti casi, le strutture finanziarie all'interno di un'azienda hanno una buona conoscenza dei controlli e della documentazione relativa perché sono state oggetto di audit finanziari da diversi anni. Tuttavia le strutture IT sono meno abituate a queste problematiche e, di conseguenza, l'implementazione di controlli che operano in modo efficace nel tempo si dimostra un'attività difficoltosa.

Per implementare e supportare i controlli con successo, le strutture IT devono innanzitutto comprendere che la necessita di conformità al Sarbanes-Oxley Act richiederà probabilmente dei cambiamenti alle attività correnti. Allo stesso modo, le strutture IT dovrebbero riconoscere che il cambiamento è più che un processo specifico – ha valori significativi a livello culturale e personale che devono essere considerati per ottenere il successo. Ne consegue che le aziende devono avere una strategia per i cambiamenti che rifletta gli atteggiamenti culturali e la capacità del suo personale. Il cambiamento non avviene da solo – deve essere gestito.

Impegno al cambiamento

Il primo passo nella gestione del cambiamento è ottenere l'impegno (commitment). Nella ricerca di questo impegno, un'azienda ha la necessità di definire cosa vuol cambiare e come vorrebbe essere dopo i cambiamenti. La costruzione di una visione della situazione futura agevola la creazione del commitment. Le aziende hanno anche la necessità di comprendere l'impatto che il cambiamento avrà sulla loro organizzazione. Per esempio, il cambiamento è portato a termine meglio con un approccio top-down o bottom-up? Comprendere queste problematiche è importante per ottenere la collaborazione.

Valutazione della situazione attuale

La gestione dei cambiamenti coronata da successo inizia con una valutazione oggettiva della situazione corrente. Tale situazione corrente si riferisce alla preparazione dell'azienda ad aderire al cambiamento. Nella valutazione della situazione in essere devono essere considerati i seguenti fattori:

- Cultura – la probabilità di un cambiamento di successo è quasi certamente condizionata dalla cultura aziendale. Cioè, se l'azienda è abituata a uno stile imprenditoriale flessibile, il cambiamento è già parte della sua cultura e sarà accolto con favore. Se la cultura è *stoica* o rigida, il cambiamento sarà più difficoltoso.
- Ampiezza del cambiamento – più è significativo il cambiamento, meno è probabile che sia coronato da successo. Le aziende hanno bisogno di valutare la portata del cambiamento che tentano di realizzare ed essere realistiche negli obiettivi.
- Impatto sulle persone – per ogni modifica, ci sono persone che la percepiscono positivamente altre negativamente, ed è importante comprendere come le persone saranno coinvolte. Chi vede il cambiamento positivamente è spesso "agente del cambiamento" e chi lo vede negativamente è spesso un "ostacolo", cosicché identificare gli "agenti del cambiamento" da subito e ingaggiarli nel processo sarà un fattore chiave di successo. Analogamente, se c'è un'elevata percentuale di "ostacoli", l'azienda può aver la necessità di ripensare a come il cambiamento può essere introdotto in azienda.

- Punti di forza – l'abilità di un'azienda ad adattarsi ai cambiamenti è spesso proporzionale alle sue competenze ed esperienze. Se il cambiamento richiede aggiornamenti significativi nella formazione o modifiche nella definizione delle competenze, allora, per aver successo, sono necessari investimenti in formazione.

Superamento degli ostacoli

Come parte del processo di valutazione della situazione attuale, un'azienda identifica gli ostacoli rilevanti rispetto al cambiamento al fine di implementare una strategia per superarli. Per esempio, far evolvere un'azienda verso la conformità al Sarbanes-Oxley Act richiede la progettazione e la realizzazione di controlli, che possono essere percepiti come impedimenti a "svolgere il lavoro". D'altronde, se progettati e comunicati correttamente, questi controlli possono essere implementati per migliorare l'efficacia e l'efficienza dei processi di business, conseguendo miglioramenti nelle prestazioni aziendali.

Nel superamento degli ostacoli, ci sono lezioni importanti che devono essere apprese dalle aziende che sono già passate attraverso questo processo, come riportato di seguito:

1. comunicare – una comunicazione efficace è molto più che fornire aggiornamenti regolari. Le aziende hanno una resistenza naturale al cambiamento, e le persone hanno la necessità di comprendere i motivi del cambiamento e i suoi benefici. Alcuni suggerimenti al riguardo sono:
   - Comprendere i "punti di sofferenza" (*pain points*). Comprendere cosa potrebbe impattare negativamente su un individuo o sull'azienda nel suo insieme e assicurarsi che la comunicazione delinei chiaramente come il cambiamento ridurrà la "sofferenza". Ci sono molti punti di inquietudine all'interno del Sarbanes-Oxley Act, il più significativo dei quali è fallire nel soddisfacimento dei requisiti del Sarbanes-Oxley Act stesso. Una volta che le persone comprenderanno come questo può influire su loro stessi, saranno molto più pronte ad aderire ai cambiamenti connessi all'ottemperanza al Sarbanes-Oxley Act.
   - Determinare il mezzo di comunicazione migliore. Newsletter, e-mail, workshop e colazioni di lavoro sono tutti buoni esempi di comunicazione, e in molti casi è necessario più di un mezzo per trasmettere il messaggio. I progetti relativi al Sarbanes-Oxley Act sono lunghi e complessi, quindi una comunicazione continuativa è importante.
   - Ottenere feedback. Raccogliere e analizzare i feedback è importate tanto quanto comunicare. I feedback consentono alle aziende di mostrare flessibilità e adattabilità, dimostrando capacità di ascolto. Una delle principali ragioni per cui il cambiamento non ha successo è perché le aziende spesso non ascoltano. Ci sono molti modi per soddisfare i requisiti del Sarbanes-Oxley Act e le aziende sarebbero sorprese di vedere l'entusiasmo che si genera quando i feedback delle persone sono recepiti e implementati.

2. Formare – se le aziende vogliono evolvere è importante dare alle persone le competenze di cui necessitano. I requisiti formativi dovrebbero essere identificati per ogni figura coinvolta, e dovrebbero essere attuati i piani per erogare questa formazione. I requisiti del Sarbanes-Oxley Act sono complessi e la grande varietà di opinioni relativamente a quale è il giusto carico di lavoro suggerisce che l'addestramento e la formazione sono essenziali per un progetto di successo. Per esempio la formazione è particolarmente importante per comprendere come i *controlli generali automatizzati* sono correlati con i controlli applicativi, così come per molte altre aree prese in considerazione da questa pubblicazione.

3. Motivare – il cambiamento ha più probabilità di successo quando vengono utilizzati opportuni incentivi. Questi forniscono un approccio produttivo e orientato agli obiettivi per far sì che il cambiamento avvenga, e il risultato è spesso una doppia vittoria per l'azienda e il suo personale. Per esempio, considerare la definizione degli obiettivi di conformità al Sarbanes-Oxley Act nel processo di valutazione delle prestazioni di ogni addetto, ed essere il più specifici possibile nella definizione di questi obiettivi in quanto sono rilevanti per il ruolo e le responsabilità di ciascuno.

Stabilire le Regole di Base

Definizione di COSO

Storicamente, gli interventi sul sistema di controllo da parte di un'azienda erano per la maggior parte spontanei e basati su una grande varietà di modelli di controllo interno. Per migliorare la robustezza e la qualità, la SEC ha disposto l'uso obbligatorio di un modello di controllo interno riconosciuto e definito da un organismo o entità che abbia seguito appropriate procedure di stesura, inclusa l'ampia diffusione del modello in modo da recepire numerosi commenti pubblici. Specificatamente, la SEC si è riferita a COSO[1].

COSO è un'organizzazione volontaria di natura privata che si prefigge di migliorare la qualità del reporting finanziario attraverso i principi di etica del business, del controllo interno efficace e della corporate governance. È stato fondato nel 1985 per supportare la National Commission on Fraudulent Financial Reporting, un'organizzazione indipendente privata spesso definita come la Treadway Commission. Tra le organizzazioni che sostengono l'iniziativa ci sono l'American Institute of Certified Public Accountants (AICPA), l'American Accounting Association (AAA), il Financial Executives International (FEI), l'Institute of Internal Auditors (IIA) e l'Institute of Management Accountants (IMA). Le sezioni seguenti forniscono un ulteriore approfondimento relativamente a COSO e alle sue implicazioni con l'IT.

Applicare COSO all'IT

Per anni, l'IT ha rivestito un ruolo importante nell'ambito dei sistemi informativi strategici e gestionali. Oggi, questi sistemi sono strettamente connessi alla capacità aziendale di soddisfare le richieste dei clienti, dei fornitori e degli altri importanti stakeholder. In funzione dell'ampia dipendenza dall'IT dei sistemi gestionali contabili e operativi, i controlli sono stati da tempo riconosciuti necessari, in particolare per i sistemi informativi più significativi. Per enfatizzare questo aspetto, ci si riferisca alla guida fornita nell'Auditing Standard n. 2 del PCAOB:

> *Conosciuto come COSO Report, questo fornisce un modello adeguato e disponibile per la valutazione della gestione. Per questa ragione, le indicazioni relative alle prestazioni e alla documentazione in questo standard sono basate sul modello COSO. Altri modelli utilizzabili sono stati pubblicati in altri paesi e potranno essere sviluppati in futuro.*
> *Questi altri adeguati modelli possono essere utilizzati nella revisione dei controlli interni relativi al reporting finanziario. Anche se modelli differenti possono non contenere esattamente gli stessi elementi di COSO, dovrebbero possedere i principi che corrispondono, in generale, a tutte le tematiche di COSO.*

Ai fini della conformità al Sarbanes-Oxley Act, è importante dimostrare quanto i controlli IT corrispondono al modello COSO. Un'azienda dovrebbe possedere competenze di controllo relativamente all'IT per tutti i cinque elementi COSO individuati come essenziali per un controllo interno efficace.

[1] Committee of Sponsoring Organizations of the Tradeway Commission, *www.coso.org*

Essi sono:

- L'ambiente di controllo
- La valutazione dei rischi
- Le attività di controllo
- L'informazione e la comunicazione
- Il monitoraggio

Ognuno di questi cinque punti è descritto brevemente nei paragrafi a seguire. A questa descrizione seguono considerazioni IT di alto livello relative a ogni specifico componente. Ulteriori obiettivi di controllo IT di dettaglio sono riportati nelle appendici come considerazioni per la conformità al Sarbanes-Oxley Act.

Ambiente di Controllo

L'ambiente di controllo predispone le basi per un controllo interno efficace, stabilisce il "limite alto" e rappresenta il vertice della struttura di corporate governance. Le problematiche emerse relativamente all'ambiente di controllo si applicano a tutta l'azienda. L'ambiente di controllo riguarda in primo luogo le diverse entità aziendali (entity level).

Tuttavia, l'IT spesso possiede caratteristiche che possono richiedere un ulteriore approfondimento sull'allineamento con il business, sui ruoli e responsabilità, sulle policy e procedure e sulle competenze tecniche. Di seguito vengono riportate alcune considerazioni relative all'ambiente di controllo e all'IT:

- L'IT è spesso considerato a torto come un'organizzazione separata dal business e quindi con un ambiente di controllo separato.
- L'IT è complesso, non solo relativamente ai suoi singoli componenti tecnici ma anche per come questi componenti si integrano nel complessivo sistema di controllo interno dell'azienda.
- L'IT può generare rischi addizionali o incrementare alcuni di quelli esistenti, che richiedono nuove o potenziate attività di controllo per ridurli efficacemente.
- L'IT richiede competenze specialistiche particolari che possono scarseggiare.
- L'IT può richiedere dipendenza da terze parti nel caso in cui processi importanti o componenti dell'IT siano stati appaltati a società esterne (*outsourcing*)
- La responsabilità dei controlli IT può non essere chiara, soprattutto per i controlli applicativi.

Valutazione dei Rischi

La valutazione dei rischi comprende l'identificazione e l'analisi, da parte del management, dei principali rischi nel perseguimento degli obiettivi aziendali predefiniti; tali attività costituiscono la base per definire le attività di controllo. E' probabile che i rischi relativi al controllo interno possano essere più pervasivi nell'organizzazione IT che in altri ambiti dell'azienda. La valutazione dei rischi può essere fatta a livello aziendale (entity level - per l'azienda nel suo insieme) o a livello di attività (activity level - per un processo specifico o per una business unit).

A livello aziendale ci si può aspettare quanto segue:

- Un sottocomitato di pianificazione dell'IT nell'ambito del comitato di direzione (Steering Committee) per il Sarbanes-Oxley Act. Tra le sue responsabilità possono essere individuate le seguenti:

- supervisione dello sviluppo del piano strategico del controllo interno IT, la sua implementazione ed esecuzione efficace e tempestiva e la sua integrazione con il piano generale per la conformità al Sarbanes-Oxley Act
- valutazione dei rischi IT: p.es. la gestione dell'IT, la sicurezza dei dati, lo sviluppo dei programmi e la gestione delle modifiche successive

A livello di attività, ci si può aspettare quanto segue:

- Valutazione formale dei rischi inserita nell'ambito della metodologia di sviluppo dei sistemi
- Valutazione dei rischi inserita nella gestione delle infrastrutture e dei relativi processi di modifica
- Valutazione dei rischi inserita nel processo di gestione delle modifiche dei programmi.

Attività di Controllo

Le attività di controllo sono costituite dalle policy, procedure e prassi poste in atto per assicurare il perseguimento degli obiettivi e l'attuazione delle strategie per la riduzione dei rischi. Le attività di controllo sono sviluppate per individuare specificatamente ogni obiettivo di controllo atto a mitigare i rischi individuati.

Senza sistemi informatici affidabili e attività di controllo IT efficaci, le società quotate non sarebbero in grado di produrre reporting finanziari accurati. COSO riconosce questo rapporto e individua due ampi gruppi di attività di controllo del sistema informatico: i controlli generali e i controlli applicativi.

I controlli generali, progettati per assicurare che le informazioni finanziarie generate dai sistemi applicativi di un'azienda siano attendibili, comprendono le seguenti tipologie:

- Controlli delle operazioni del centro elaborazione dati - Controlli quali l'organizzazione dei processi elaborativi automatici (*job*) e la loro schedulazione, le attività degli operatori di sala macchine, le procedure di back-up e di eventuale ripristino dei dati
- Controlli del software di sistema - Controlli sulla reale acquisizione, implementazione e manutenzione dei software di sistema, database management system *(DBMS)*, telecomunicazioni, sicurezza e utility
- Controlli sulla sicurezza degli accessi - Controlli che impediscono l'uso improprio e non autorizzato del sistema a tutti i livelli quali p.es. sistema operativo, database e programmi applicativi
- Controlli sullo sviluppo e la manutenzione del software applicativo - Controlli sulla metodologia di progetto e di sviluppo, incluso il disegno e l'implementazione, che definiscono le singole fasi specifiche dell'attività, i requisiti della documentazione, le procedure di gestione delle modifiche, le approvazioni e i singoli punti di controllo.

I controlli applicativi sono inseriti nei programmi software per impedire o individuare transazioni non autorizzate. Quando sono configurati adeguatamente, o usati in combinazione con altri controlli manuali, i controlli applicativi assicurano completezza, accuratezza, autorizzazione e validità delle transazioni elaborate. Nell'appendice D sono fornite ulteriori linee guida relative ai controlli applicativi.

I controlli generali sono necessari per supportare il funzionamento dei controlli applicativi, ed entrambi sono necessari per assicurare l'elaborazione accurata e l'integrità delle informazioni prodotte e utilizzate

per gestire, amministrare e produrre il reporting relativo all'azienda. Poiché i controlli applicativi sostituiscono in modo crescente i controlli manuali, i controlli generali divengono sempre più importanti.

Informazione e Comunicazione

COSO stabilisce che l'informazione è necessaria a tutti i livelli di un'azienda per condurre l'attività e raggiungere gli obiettivi aziendali di controllo. Tuttavia l'identificazione, la gestione e la comunicazione di informazioni rilevanti rappresenta una sfida sempre maggiore per il reparto IT. La determinazione di quali siano le informazioni richieste per raggiungere gli obiettivi di controllo, e la comunicazione di queste informazioni in una forma e nell'intervallo temporale che consenta al personale di svolgere i propri compiti, supporta gli altri quattro componenti precedentemente elencati della metodologia COSO.

Il reparto IT elabora la maggior parte delle informazioni del reporting finanziario. Tuttavia il suo ambito di intervento è generalmente ben più vasto. Il reparto IT può anche fornire assistenza nell'implementazione meccanismi per identificare e comunicare eventi significativi, come sistemi e-mail o sistemi di supporto alle decisioni manageriali (DSS Decision Support Systems)

COSO inoltre rileva che la qualità delle informazioni comprende l'accertamento che le stesse siano:

- Appropriate – Sono le informazioni giuste?
- Tempestive - Sono disponibili quando richiesto e al momento giusto?
- Aggiornate - Sono quelle disponibili le più recenti?
- Attendibili - I dati sono corretti?
- Accessibili - Le persone autorizzate possono accedervi quando ne hanno la necessità?

A livello aziendale, ci si può aspettare quanto segue:

- Sviluppo e comunicazione delle policy aziendali
- Sviluppo e comunicazione dei requisiti propri della reportistica, compresi i termini di scadenza, i controlli di riconciliazione, il formato e il contenuto dei report gestionali *(management reports)* mensili, trimestrali e annuali
- Consolidamento e comunicazione delle informazioni finanziarie

A livello di attività, ci si può aspettare quanto segue:

- Sviluppo e comunicazione degli standard per raggiungere gli obiettivi propri della policy aziendale (corporate policy)
- Identificazione e comunicazione tempestiva delle informazioni per contribuire al conseguimento degli obiettivi aziendali
- Identificazione e denuncia tempestiva delle violazioni alla sicurezza.

Monitoraggio

Il monitoraggio, che comprende la supervisione del controllo interno da parte del management tramite processi di accertamento continui e tempestivi, sta diventando sempre più importante per il management IT. Esistono due tipi di attività di monitoraggio: monitoraggio continuo e valutazioni separate.

Sempre più la prestazione e l’efficacia IT sono monitorate di continuo usando misure sulle prestazioni che indicano se un controllo sottostante sta operando efficacemente. Consideriamo gli esempi seguenti:

- Identificazione e gestione dell’anomalia - Stabilire metriche e utilizzarle per analizzare i trend dei risultati effettivi; tale confronto può fornire le basi per capire le ragioni degli errori di elaborazione. Correggere queste cause può migliorare l’accuratezza del sistema, la completezza dell’elaborazione e la disponibilità del sistema.
- Monitoraggio della sicurezza - Costruire un’efficace infrastruttura di sicurezza IT riduce il rischio di accessi non autorizzati. Aumentare la sicurezza può ridurre il rischio di elaborare transazioni non autorizzate e di generare report inattendibili ciò dovrebbe comportare una riduzione della indisponibilità dei sistemi chiave nel caso che le applicazioni e i componenti dell’infrastruttura IT siano stati a vario titolo compromessi.

A livello aziendale, ci si può aspettare quanto segue:

- Un continuo monitoraggio centralizzato sulle operazioni informatiche
- Un monitoraggio centralizzato della sicurezza
- Attività di revisione da parte dell’Internal audit IT (mentre l’audit può intervenire a livello di attività, il report delle risultanze di audit, indirizzato all’apposito comitato, è a livello aziendale)

A livello di attività, ci si può aspettare quanto segue:

- Identificazione e gestione delle anomalie
- Monitoraggio locale delle operazioni informatiche o della sicurezza
- Supervisione del personale IT locale.

Percorso (road map) per la conformità IT

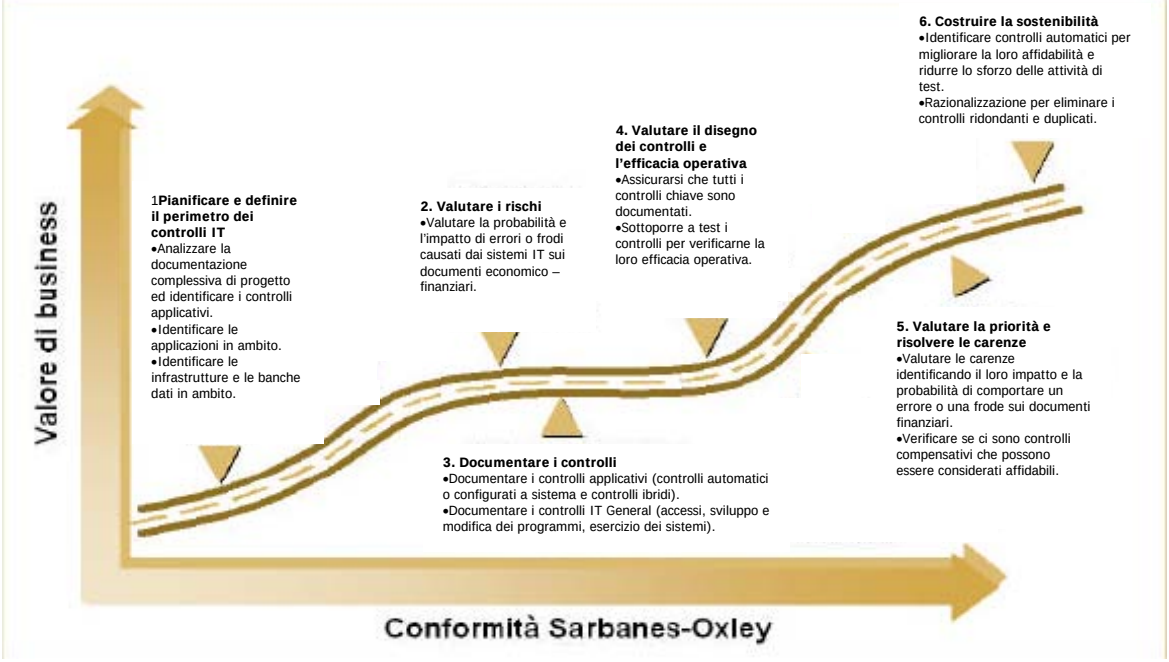
La sezione seguente illustra la mappa di conformità creata per gli obiettivi e le responsabilità specifiche della funzione IT. La mappa è stato semplificata rispetto alla versione presente nella prima pubblicazione, al fine di rendere la sua realizzazione più facilmente gestibile e focalizzare gli sforzi sulle attività principali per la conformità al Sarbanes-Oxley Act.

Comprendere le modalità con cui il Sarbanes-Oxley Act impatta su un'azienda, secondo le caratteristiche specifiche del business, può essere d'ausilio nello sviluppo di un programma di controllo interno. I fattori in gioco sono numerosi, e le aziende di grandi dimensioni dovranno affrontare sfide differenti rispetto a quelle più piccole. Inoltre, il livello di estensione di un robusto sistema controllo interno già adottato avrà un impatto significativo sulle attività da svolgere.

Conformità al Sarbanes-Oxley

La mappa per la conformità, illustrata nella **figura 3,** fornisce al personale IT un'indicazione su come affrontare le sfide del Sarbanes-Oxley Act. I primi due passi della mappa – la pianificazione e definizione degli ambiti e la valutazione dei rischi IT – dovrebbero essere effettuati congiuntamente.

Figura 3 – Mappa per la conformità IT



1. Pianificazione e ambito dei controlli IT

Come in tutti i progetti importanti, deve essere data particolare attenzione alla definizione degli ambiti e alla corretta pianificazione del percorso di conformità IT.

La definizione degli ambiti è il processo di identificazione delle applicazioni IT e dei relativi sottosistemi da includere nel progetto, o viceversa escludere, sulla base delle indicazioni dei team di business/finanziari.

L’inclusione e, viceversa, l’esclusione dei sistemi deve essere effettuata in base alla valutazione dei rischi finanziari complessivi dell’azienda, effettuata dai team di business/finanziari. In altre parole, devono essere incluse nell’analisi solo le applicazioni e i relativi sottosistemi che supportano il business e i controlli critici sul reporting finanziario.

Viceversa, la pianificazione è il processo mediante il quale viene predisposto il diagramma temporale delle attività, che sono assegnate a specifiche risorse e vengono monitorate nel loro svolgimento.

Assegnazione della responsabilità e autorità

Un passo preliminare importante nel percorso di conformità IT è quello di creare un Comitato di Controllo IT. Il Comitato deve operare nell’ambito del più generale Steering Committee per il Sarbanes-Oxley Act e deve rispondere ad esso. Tale comitato deve supervisionare il processo di conformità IT al Sarbanes-Oxley Act, facilitare la comunicazione e l’integrazione con il progetto complessivo Sarbanes-Oxley, nonché agevolare il ruolo degli auditor indipendenti nel processo. Le aziende più piccole possono dedicare le risorse già esistenti con impegno a part-time, mentre le aziende più complesse possono aver bisogno di specifiche risorse dedicate al progetto. Il Comitato IT dovrà nominare un responsabile dei controlli IT e del relativo progetto, al quale sarà data un’adeguata autorità e responsabilità.

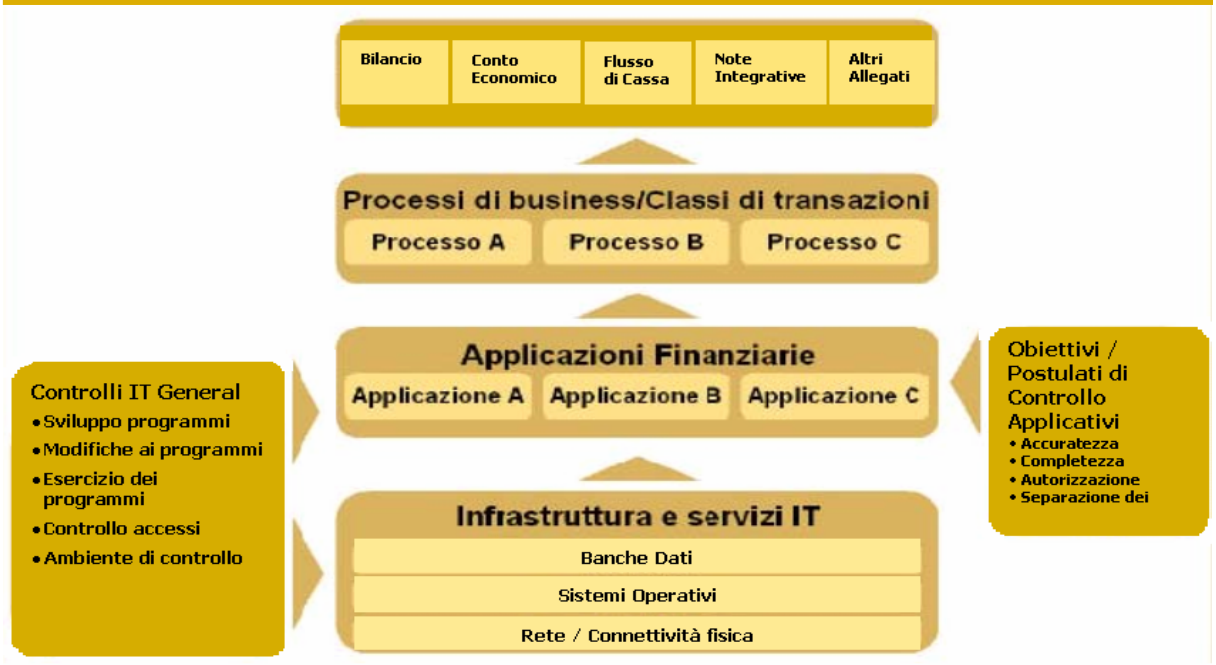
Censimento delle applicazioni IT critiche e dei relativi sottosistemi

Il censimento dei sistemi da includere nel progetto (applicazioni relative al Sarbanes-Oxley Act e relativi sottosistemi) deve essere effettuato, d’intesa con il team dei controlli finanziari e di business, identificando le applicazioni che supportano i controlli applicativi critici, come mostrato in **figura 4.** In generale, dovrebbero essere identificate in questa fase le applicazioni che supportano le autorizzazioni on-line, i calcoli e le valutazioni complesse, o che sono responsabili dell’integrità di significative poste di bilancio (come gli inventari, le immobilizzazioni tecniche o i saldi dei prestiti). L’Appendice D, “Controlli Applicativi”, fornisce una linea guida per la definizione dei controlli applicativi ed esempi su come individuarli all’interno di un’azienda, operando congiuntamente con il team dei controlli finanziari e di business.

Effettuato il censimento delle applicazioni, nonché dei processi IT che gestiscono e guidano tali applicazioni, il team di progetto dei controlli IT potrà identificare tutte le applicazioni di interesse e tutti i sottosistemi che supportano tali applicazioni, come database, server, sistemi operativi e reti (al riguardo si rimanda all’Appendice E, “Campione di applicazioni e censimento dei livelli tecnologici”, per un esempio di foglio elettronico per il censimento delle applicazioni critiche e dei relativi sottosistemi).

Questa fase nel progetto aiuterà l’organizzazione IT anche a comprendere il flusso del processo dei documenti economici – finanziari e a identificare gli elementi tecnologici critici del processo stesso.

Figura 4 – Definizione ambiti progetto per i controlli IT – Metodo Top Down



Il censimento delle applicazioni e dei relativi sottosistemi dovrà essere utilizzato per la pianificazione preventiva del progetto e sarà verificato, tramite analisi dei rischi, nelle fasi successive per identificare la tipologia e l'estensione dei controlli e dei test.

Analisi della documentazione dei processi finanziari e identificazione dei controlli applicativi

Le aziende hanno numerosi processi di business e controlli, tuttavia, la conformità al Sarbanes-Oxley Act è limitata solo a quei processi e controlli che supportano la predisposizione dei reporting finanziari. Perciò, è importante che il team per la conformità IT partecipi all'identificazione dei controlli applicativi. Al riguardo esistono in generale due approcci: le aziende possono avere un team per i controlli IT che supporta il team per i controlli finanziari e/o di business nell'identificazione dei controlli applicativi, oppure, alternativamente, il team per i controlli finanziari e/o di business può identificare preliminarmente tutti i controlli e, quindi, il team per i controlli IT analizzerà tali controlli per identificare quelli supportati da infrastrutture/sistemi IT. L'approccio utilizzato è equivalente, l'importante è che l'azienda identifichi correttamente quali controlli sono supportati da infrastrutture/sistemi IT. Nel far ciò le aziende saranno in grado di pianificare adeguatamente il progetto per i controlli IT, limitando l'analisi ai controlli applicativi che supportano gli obiettivi dei reporting finanziari.

Sviluppo di un piano di progetto preliminare e relativa approvazione

A partire dal censimento di applicazioni e sottosistemi interessati, dovrà essere predisposto un piano di progetto delle attività, utilizzando le sei fasi descritte in **figura 3.** Il piano di progetto sarà modificato e aggiornato successivamente, ma è importante avere una visione complessiva dell'approccio e delle dimensioni del progetto. Nella predisposizione del piano, il tempo richiesto da ciascuna fase può essere valutato utilizzando il sistema di stima dei tempi di progetto riportato in Appendice F.

Predisposto il piano, è importante discutere gli ambiti e l'adeguatezza dello stesso con il team per la conformità dei controlli finanziari e/o di business. Una volta completata questa fase, si dovrà ottenere l'approvazione del piano per poter proseguire con il progetto. Un'approvazione formale è molto importante in considerazione della rilevanza e dell'impatto che il progetto avrà su numerose risorse dell'azienda. Un'approvazione formale consoliderà la posizione degli sponsor del progetto e consentirà di ottenere il supporto da tutti i principali stakeholder e da parte del personale che deve partecipare operativamente.

Individuare la Responsabilità dei Controlli Applicativi

Un'area che generalmente è stata fonte di confusione nel progetto per i controlli IT è: "Chi è il responsabile dei controlli applicativi?". Una mancata chiarezza su tale responsabilità ha comportato significative duplicazioni di attività, test non necessari su controlli rilevanti duplicati e il rischio che un controllo rilevante non sia testato in quanto entrambi i team finanziari e IT ritenevano che fosse in carico all'altro. Si suggerisce che i responsabili (owner) del business siano responsabili degli specifici controlli applicativi. E' responsabilità invece dell'organizzazione IT supportare gli owner dei processi nell'identificare e testare tali controlli, garantendo che i controlli applicativi generali (controllo accessi, controlli sulle modifiche, back-up e ripristino, ecc.) siano funzionanti e affidabili.

Casi di aziende con più sedi

Tra i molti fattori da considerare nella definizione degli ambiti del progetto dei controlli IT vi sono le aziende con sedi distribuite, anche al di fuori dei confini geografici nazionali. Tali aziende devono verificare se le loro attività IT, in ciascuna sede geografica, operano all'interno di un ambiente di controllo singolo o multiplo. Le aziende con un singolo ambiente di controllo generalmente hanno una struttura con un responsabile, mentre le aziende con un ambiente di controllo su più sedi hanno una struttura con diversi responsabili. In generale, nel caso di più sedi, se significative, queste devono essere trattate separatamente e, quindi, ciò comporta un progetto di più grandi dimensioni e maggiore lavoro.

Verificare se le applicazioni possono essere cancellate dall'ambito

Il fatto che un'applicazione sia compresa, indica che essa supporta un controllo applicativo o "ibrido" rilevante ai fini della conformità al Sarbanes-Oxley Act. Nella maggior parte dei casi, l'applicazione e i relativi sottosistemi dovranno essere oggetto di analisi. Tuttavia, se l'applicazione supporta un numero molto limitato di controlli applicativi (ad esempio, un solo controllo), allora si potrebbe considerare di non analizzare il controllo applicativo (e quindi l'applicazione stessa) e identificare un controllo manuale rilevante o, alternativamente, aumentare l'affidabilità dei controlli manuali esistenti al fine di ridurre lo sforzo complessivo. Benché relativa a limitati casi, quella citata è una considerazione utile alle aziende che hanno numerose applicazioni con un limitato numero di controlli. In questi casi si deve prestare attenzione per evitare un involontario eccesso di fiducia (ad esempio, affidarsi a report generati da un solo sistema). Questa è un elemento/decisione da portare all'attenzione dello Steering Committee per il Sarbanes-Oxley Act. Non è una decisione di pertinenza IT.

Identificare il supporto delle società esterne che forniscono servizi (outsourcing)

Alcune aziende utilizzano società esterne affidando loro determinati servizi in outsourcing. Questi servizi fanno comunque parte dell'insieme complessivo delle operazioni dell'azienda e rientrano nelle sue responsabilità generali. Conseguentemente essi devono essere considerati nel complessivo programma di controllo interno IT.

Lo standard di verifica n. 2 PCAOB cita specificamente i report degli auditor delle società di servizi. Esso dichiara che:

> *Il ricorso a società di servizi (outsourcing) non riduce la responsabilità del management a mantenere un efficace controllo interno sui documenti relativi ai risultati di gestione. Al contrario, il management dovrebbe valutare sia i controlli sulle società di servizi, sia i controlli interni all'azienda allorché produce le proprie valutazioni riguardanti il sistema dei controlli interni relativi al reporting finanziario.*

In tali circostanze, le aziende dovrebbero verificare le attività delle società esterne (outsourcer) per conoscere l'affidabilità del loro controllo interno. La documentazione sulle attività di controllo presso gli outsourcer sarà richiesta per le attività di attestazione dell'auditor indipendente. Quindi, sarà richiesta una valutazione dell'organizzazione dell'outsourcer al fine di determinare l'adeguatezza della documentazione ottenuta come evidenza dei controlli.

Tradizionalmente, audit di tipo SAS 70 ("Statements of Audit Standards") sono stati effettuati per le società di servizi. Se questi rapporti di audit non includono i test dei controlli, i risultati dei test e le valutazioni dell'auditor della società di servizi sull'efficacia operativa non possono essere ritenuti sufficienti per la conformità al Sarbanes-Oxley Act. In tali casi, si suggerisce che le aziende consultino i loro auditor indipendenti per identificare specifici requisiti. Particolare attenzione dovrebbe essere prestata al periodo coperto dal SAS 70 e ad assicurarsi che i controlli del SAS 70 coprano l'ambiente, le piattaforme e le applicazioni utilizzate dall'azienda, come pure i risultati dei test e le risultanze complessive. L'Appendice L, "Problematiche nell'utilizzo dei report di analisi SAS 70", fornisce un'analisi più approfondita sull'adeguatezza dei report SAS 70.

2. Valutazione dei rischi IT

In questa fase, le aziende devono valutare i rischi all'interno dei processi IT e dei sistemi che supportano le applicazioni interessate. Uno degli elementi più significativi emersi dai primi anni del progetto di conformità al Sarbanes-Oxley Act è che esso deve essere basato su una valutazione dei rischi. Non tutti i sistemi IT o i processi espongono a un rischio elevato il bilancio e, quindi, non tutti i sistemi IT o i processi devono essere inclusi o valutati con lo stesso livello di analisi. Nell'effettuazione di una valutazione dei rischi, deve essere considerato il rischio inerente piuttosto che il rischio residuo (il rischio che resta dopo aver considerato l'effetto dei controlli). Nell'Appendice F, "Sistemi di stima per il progetto", sono forniti numerosi sistemi di supporto al processo di valutazione dei rischi.

Valutazione del rischio inerente delle applicazioni e dei relativi sottosistemi

Valutare il rischio inerente delle applicazioni e dei relativi sottosistemi, come banche dati, sistemi operativi, reti e ambienti fisici, è necessario per identificare la tipologia e l'estensione dei controlli necessari a gestire tali rischi. Tale valutazione del rischio inerente è anche necessaria per pianificare adeguatamente ed effettuare i test dell'efficacia operativa di tali controlli.

Nella valutazione del rischio inerente, devono essere considerati numerosi fattori di rischio; tuttavia, la valutazione finale è basata sul giudizio umano. Considerare i fattori di rischio più comuni è finalizzato a fornire alle aziende le informazioni critiche, utili a effettuare una solida e ragionevole valutazione dei rischi. Nella valutazione dei rischi, devono essere esaminati sia la probabilità, sia l'impatto dell'evento di rischio. A titolo di esempio, in assenza di un controllo accessi, c'è il rischio che qualcuno acceda alle applicazioni finanziarie critiche e inserisca false transazioni nel sistema. In assenza di controlli, la probabilità di tale evento non è del tutto remota e l'impatto dell'inserimento di false transazioni è significativo. Conseguentemente, questo rischio è considerato significativo e sono necessari controlli per ridurlo. E' importante evidenziare che l'obiettivo è ridurre il rischio a un livello ragionevole, non eliminarlo del tutto.

I seguenti elementi sono generalmente utilizzati nell'effettuazione di un'analisi dei rischi, ma le aziende devono valutare se aggiungerne altri in considerazione delle loro specificità (vedere come ulteriore linea guida l'Appendice G, "Valutazione del rischio inerente e griglia di valutazione delle priorità dei controlli"):

- Tipologia di tecnologia (complessa o semplice)
- Tipologia di risorse (con esperienza o senza)
- Tipologia dei processi (centralizzati o distribuiti)
- Esperienze pregresse
- Importanza del reporting finanziario.

Effettuata una valutazione dei rischi, i risultati possono essere utilizzati nel definire la tipologia e il numero i controlli e test necessari.

L'Appendice C, "Controlli Generali IT", fornisce una linea guida sui controlli IT raccomandati che dovrebbero essere individuati per le applicazioni e i relativi sottosistemi (definiti complessivamente i "livelli tecnologici"). Come si vede nella matrice presente nell'Appendice G, l'analisi dei rischi consentirà di escludere alcuni processi di controlli IT semplicemente perché la probabilità o l'impatto di eventi relativi a quel livello tecnologico non giustifica uno sforzo di analisi. Indipendentemente dai risultati, deve essere conservata la documentazione inerente alle decisioni e al processo razionale di tali decisioni, al fine di analizzarle con il management o gli auditor indipendenti.

Affinare l'ambito e aggiornare il piano di progetto

Effettuata la valutazione dei rischi, il team per i controlli IT potrà affinare e aggiornare l'ambito del progetto escludendo alcune applicazioni e i relativi sottosistemi. Il processo di valutazione dei rischi e le relative conclusioni devono essere adeguatamente documentati, in particolare se alcuni sistemi sono stati esclusi dall'ambito. Allo stesso modo, in caso di modifica di ambito e di risorse previste, dovrà essere coerentemente aggiornato il piano di progetto per riflettere l'approccio risk-based.

3. Documentare i controlli

La documentazione dei controlli fornisce evidenza al management di come sono stati gestiti i rischi relativi alla produzione del reporting finanziario affidabile e consente al management di prendere decisioni consapevoli se accettare il livello residuo di rischio. Ad esempio, se le applicazioni finanziarie si basano fortemente su calcoli complessi, allora sussiste il rischio che modifiche non autorizzate comportino errori significativi nel bilancio. Conseguentemente, è critico identificare e documentare i controlli che prevengano tali accessi non autorizzati o ne evidenzino l'accadimento.

Identificare i controlli a livello aziendale

I controlli aziendali sono relativi a come opera un'azienda. Comprendono le normative, le procedure e le modalità operative di alto livello che definiscono il tono dell'azienda. I controlli aziendali sono una componente fondamentale del modello COSO e dovrebbero essere relativi anche alle attività IT che supportano il reporting finanziario. L'identificazione dei controlli aziendali IT deve essere effettuata in modo integrato con l'analisi complessiva dei controlli a livello azienda. L'esistenza di robusti controlli aziendali IT, così come di normative e procedure definite e diffuse, spesso è indice di ambiente operativo IT affidabile. Analogamente, le aziende con controlli aziendali IT meno robusti, incontrano più facilmente difficoltà nell'effettuazione di adeguate attività di controllo, come la gestione delle modifiche ai programmi e il controllo accessi. Quindi, la robustezza o la debolezza dei controlli aziendali impatterà sulla tipologia, estensione e durata delle attività di test.

Identificare i controlli applicativi

L'identificazione dei controlli applicativi che supportano il reporting finanziario è una fase critica del processo. Una volta individuati tutti i controlli applicativi, si potrà identificare anche come questi supportano i controlli generali IT. Molto spesso, i controlli applicativi sono inclusi nella documentazione dei processi di business. In un processo ideale, gli specialisti IT documentano un processo con gli specialisti dei controlli e insieme identificano i controlli rilevanti per il processo. Tuttavia, in molti casi, la documentazione del processo è già disponibile. Quindi, si dovrà analizzare tale documentazione e identificare i controlli applicativi. L'Appendice D, "Controlli Applicativi", fornisce ulteriori linee guida sull'identificazione dei controlli applicativi.

L'identificazione di controlli automatici può sembrare semplice ma, in molti casi, non lo è. In genere le aziende utilizzano e documentano due tipi di controlli applicativi:

- Controlli automatici – effettuati dai sistemi e di natura binaria, operano come sono stati progettati e non sono soggetti a errori intermittenti. Esempi includono i controlli sui dati inseriti per verifica della quantità di un ordine, o controlli automatici nei sistemi per gli acquisti per consentire ordini entro limiti predefiniti.
- Controlli manuali dipendenti dall'IT ("ibridi") – sono essenzialmente controlli manuali che dipendono dai sistemi IT.

I controlli applicativi IT stanno diventando sempre più importanti con il crescere dell'attenzione al tempo necessario a individuare un errore e all'efficienza dei costi dei controlli. Ad esempio, mentre anni fa era accettabile attendere anche diverse settimane una riconciliazione manuale per rilevare un errore o una frode, oggi un tale ritardo sta diventando sempre meno accettabile. Quindi, non saranno più accettabili

controlli manuali non supportati da un processo automatico. Ulteriori linee guida, inclusi esempi di controlli applicativi, sono fornite nell'Appendice D, "Controlli Applicativi".

I controlli ibridi, in particolare, non sono stati ben documentati da molte aziende, nonostante l'enfasi fornita su di loro dal PCAOB nelle linee guida di novembre 2004:

> *I controlli applicativi possono essere anche controlli manuali che dipendono dall'IT (ad esempio, la verifica da parte di un responsabile dell'inventario di un report di eccezioni generato dall'IT). Benché carenze nei controlli generali IT non comportano direttamente errori nel reporting finanziario, un correlato controllo applicativo inefficace può comportare errori. Quindi, la rilevanza di una carenza di controllo generale IT deve essere valutata in relazione al suo effetto sui controlli applicativi, cioè valutando se i controlli applicativi correlati sono inefficaci.*

Identificare i controlli generali IT

La relazione tra controlli applicativi e controlli generali IT è che questi ultimi sono necessari per garantire l'affidabilità dei controlli applicativi. Ad esempio, assicurare la sicurezza delle basi dati è spesso considerato un requisito per la produzione di affidabili reporting finanziari. Senza sicurezza a livello di base dati, le aziende sarebbero esposte al rischio di modifiche non autorizzate ai dati finanziari.

La sfida con i controlli generali IT è che essi raramente supportano direttamente il bilancio. D'altra parte, il PCAOB afferma che i controlli generali IT hanno un effetto "pervasivo" su tutti i controlli interni. Cioè, se è inefficace un controllo generale IT rilevante (ad esempio, un controllo che verifica gli accessi ai programmi e ai dati), ciò ha un impatto generale su tutti i sistemi che sono supportati da tale controllo, comprese le applicazioni finanziarie. Conseguentemente, se manca la garanzia che solo gli utenti autorizzati hanno accesso alle applicazioni finanziarie, le aziende non possono concludere che solo gli utenti autorizzati hanno predisposto e approvato le transazioni.

Identificare quali controlli sono rilevanti

I rischi finanziari non sono uguali per probabilità e impatto. Analogamente, i controlli finanziari non sono uguali nella loro efficacia nel mitigare i rischi identificati. Inoltre, all'azienda non è richiesto di valutare tutte le attività di controllo relative a un qualsivoglia rischio. Quindi, le aziende devono sforzarsi di limitare il processo di documentazione dei controlli a quelli rilevanti.

La domanda posta dalla maggior parte delle aziende è: "Cos'è un controllo rilevante/significativo?". Sfortunatamente non vi è una definizione univoca di controllo rilevante, nonostante tale termine sia utilizzato continuamente. Anche se può sembrare una risposta elusiva, i controlli significativi sono quelli su cui le aziende confidano per raggiungere un obiettivo di controllo – sono controlli che forniscono la maggiore garanzia, agli owner dei controlli, di soddisfare gli obiettivi di controllo finanziari.

Nella valutazione dei controlli rilevanti, le aziende devono considerare i seguenti elementi:

- I controlli rilevanti in genere includono le normative, le procedure, le prassi e una struttura organizzativa, e sono essenziali affinché il management possa mitigare i rischi significativi e soddisfare i relativi obiettivi di controllo.
- I controlli rilevanti spesso soddisfano più di un obiettivo di controllo. Ad esempio, il controllo accessi supporta l'esistenza di transazioni finanziarie, la valutazione dei conti finanziari, la separazione dei compiti, etc. Nella maggior parte dei casi, una combinazione di controlli rilevanti è un modo efficace per soddisfare un particolare obiettivo o una serie di obiettivi. Affidarsi troppo a un singolo controllo potrebbe creare un singolo punto di criticità per il progetto di conformità.
- I controlli che si riferiscono direttamente a rischi significativi (o che soddisfano direttamente degli obiettivi) sono in genere rilevanti. Ad esempio, il rischio di accessi non autorizzati è un rischio significativo per la maggior parte delle aziende; quindi, sono rilevanti i controlli di sicurezza che prevengono o rilevano gli accessi non autorizzati.
- I controlli di tipo preventivo sono di solito più efficaci dei controlli di rilevazione. Ad esempio, prevenire l'accadimento di una frode è molto meglio di rilevarla dopo che è accaduta. Quindi, controlli preventivi sulle frodi sono spesso considerati rilevanti.
- I controlli automatici sono più affidabili dei controlli manuali. Ad esempio, controlli automatici che forzano gli utenti a cambiare periodicamente la password sono più affidabili di normative generali non applicate. I processi manuali sono anche soggetti a errore umano.

Nell'Appendice C, "Controlli generali IT", è fornita una lista di controlli IT come linea guida per preparare le organizzazioni IT alla conformità al Sarbanes-Oxley Act. All'interno di questa lista, alcuni controlli sono evidenziati come "più rilevanti", a indicare che essi sono quelli più comunemente utilizzati per progettare un ambiente di controllo generale IT protetto e affidabile.

Controlli antifrode basati sull'IT

L'importanza dei controlli antifrode ai fini del Sarbanes-Oxley Act è qualcosa che non può essere mai sottolineata sufficientemente. Le frodi sono la ragione principale per l'introduzione del Sarbanes-Oxley Act, quindi deve essere data a questo tema un'attenzione sufficiente e appropriata.

L'information technology gioca un ruolo significativo nel prevenire e rilevare le frodi, poiché molti controlli antifrode si basano su sistemi IT. Le aziende dovranno considerare i seguenti esempi di controlli antifrode basati sull'IT, per introdurli nei propri progetti di conformità:

- Separazione dei compiti implementata a livello applicativo – La maggior parte dei sistemi consente di definire quali privilegi assegnare agli utenti delle applicazioni. Conseguentemente, il sistema richiede adeguate approvazioni per l'elaborazione delle transazioni ed evita che gli utenti predispongano e anche approvino le transazioni da loro inserite.
- Controllo accessi – La maggior parte dei sistemi ha utenti privilegiati che possono accedere a informazioni critiche, come i dati degli stipendi, consentendo di aggiungere salari fittizi e commettendo quindi una frode. Limitare tali accessi a poche risorse e assicurare che il team dedicato alla produzione del reporting finanziario non abbia questa possibilità di accesso è importante per implementare i controlli interni sul reporting finanziario.

Documentazione dei controlli

Ai fini della conformità al Sarbanes-Oxley Act, le aziende devono documentare i controlli sul reporting finanziario ed effettuare verifiche sul loro progetto e sulla loro efficacia operativa. La documentazione può essere di diverse tipologie, includendo le normative a livello aziendale, normative e procedure IT, documenti descrittivi, diagrammi di flusso, tabelle decisionali, procedure operative o questionari. Il Sarbanes-Oxley Act non indica un'unica tipologia di documentazione, e l'estensione della documentazione può variare, in funzione delle dimensioni e complessità dell'azienda.

Per la maggior parte delle aziende, la documentazione dei controlli IT dovrebbe includere:

- Livello Aziendale:
  - Verifica dei controlli aziendali, incluse le evidenze documentali per supportare l'attestazione e le valutazioni del management.
- Livello di Attività
  - Descrizione dei processi e relativi sottoprocessi (può essere in forma descrittiva, ma può essere più efficace sotto forma di diagrammi di flusso)
  - Descrizione del rischio associato ai processi e ai sottoprocessi, compresa un'analisi dell'impatto e della probabilità di accadimento. Deve essere considerata l'estensione e la complessità dei processi e sottoprocessi e il relativo impatto sui processi di produzione dei documenti finanziari dell'azienda.
  - Dichiarazione dell'obiettivo di controllo individuato per ridurre il rischio del processo o sottoprocesso a un livello accettabile e descrizione della sua aderenza al modello COSO. Descrizione delle attività di controllo disegnate e eseguite per soddisfare l'obiettivo di controllo riferito al processo o sottoprocesso. Ciò dovrebbe includere la tipologia dei controlli (preventivi o di rilevamento) e la frequenza con la quale vengono eseguiti
  - Descrizione dell'approccio seguito testare l'esistenza e l'effettiva operatività delle attività di controllo
  - Conclusioni raggiunte sui controlli attraverso il risultato delle verifiche.

4. La valutazione della struttura dei controlli e dell'efficacia operativa

Valutare il disegno della struttura dei controlli

Il disegno della struttura dei controlli obbliga la funzione IT a fare un passo indietro e a valutare la capacità del proprio programma di controllo della riduzione del rischio IT a un livello accettabile. Più specificatamente, la conclusione del disegno della struttura dei controlli impone al management la valutazione dell'adeguatezza delle caratteristiche dei controlli preventivi, di rilevamento, automatici e manuali.

Per esempio, se viene identificato il rischio che un programma non autorizzato possa essere trasferito nell'ambiente di produzione, un controllo progettato in modo corretto dovrebbe prevenire questo evento. In questo esempio, un controllo di rilevamento che identifica i programmi non autorizzati in produzione dopo che ciò è accaduto può non essere adeguato.

La struttura generica dei controlli nell'ambiente IT non va sopravvalutata. Il PCAOB Auditing Standard No. 2 sottolinea l'importanza dei controlli IT e rafforza l'opinione che determinati controlli sono necessari per supportare l'ambiente di controllo interno nella sua globalità. In particolare, indica che l'efficacia del

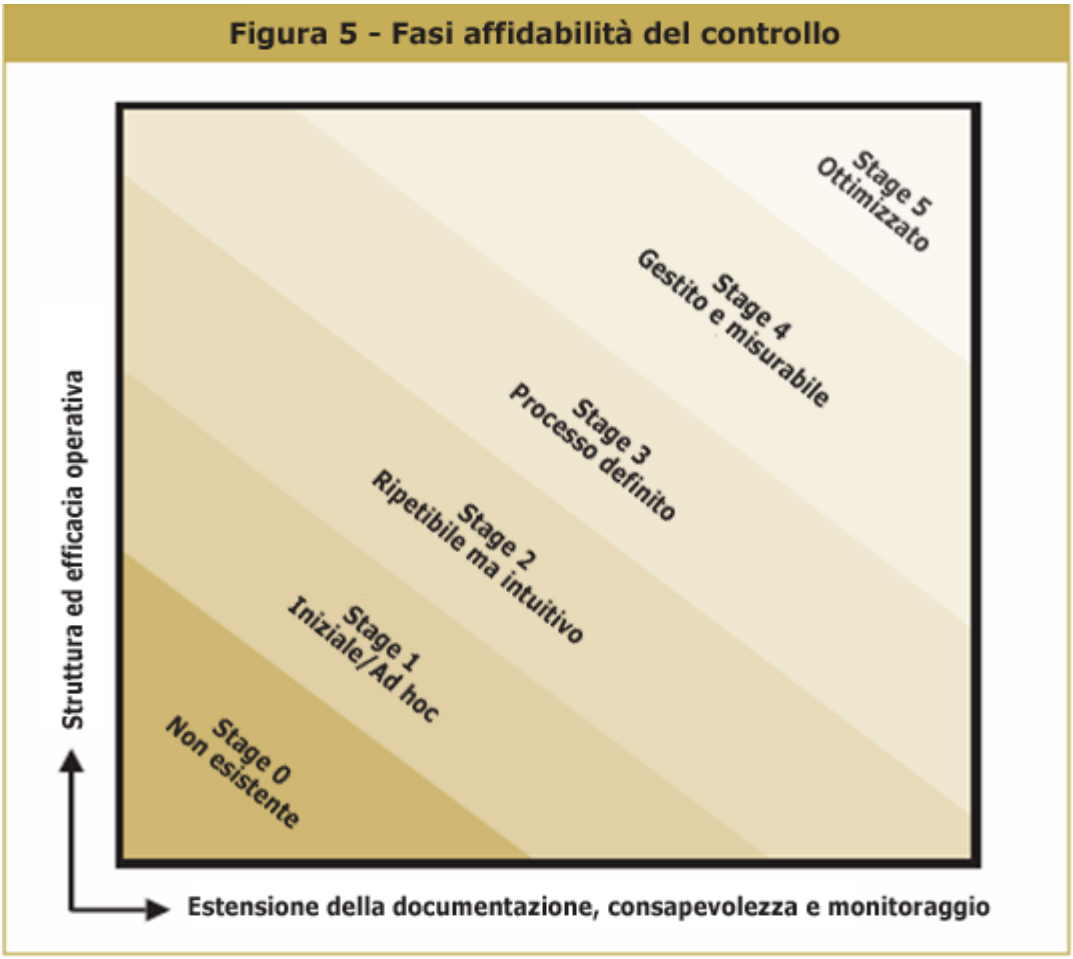
sistema di controllo interno aziendale dipende dall'operatività di altri controlli (per esempio, il controllo ambientale o i controlli generali IT). Di conseguenza, la valutazione della struttura dei controlli è un passo essenziale per la valutazione dell'ambiente di controllo IT.

Per aiutarvi nel processo di valutazione della struttura dei controlli, considerate il disegno dei controlli IT e il modello dell'efficacia in **figura 5**. In relazione a come l'azienda si è strutturata, si può riscontrare la necessità di dedicare uno sforzo al miglioramento della struttura e dell'efficacia del programma di controllo.

La **figura 5** indica le fasi dell'affidabilità del controllo che possono esserci in un'azienda.

Considerando l'obiettivo di stabilire un sistema di controllo interno, è importante sottolineare che le fasi più in alto portano a una maggiore affidabilità del controllo ambientale, mentre le fasi più in basso sono meno affidabili. Anche se il Sarbanes-Oxley Act non richiede alcuna fase, ma solo il requisito per cui i controlli siano documentati e testati, le aziende dovrebbero considerare con attenzione a quale fase (maturità) appartenga l'organizzazione aziendale e come ciò possa rappresentare eventuale rischio di non conformità.

Figura 5 - Fasi affidabilità del controllo



La tabella in **figura 6** mostra le diverse caratteristiche di ogni fase con le implicazioni correlate.

Le organizzazioni IT devono comprendere che ci sono limitate descrizioni o linee guida relative agli attributi o caratteristiche necessarie per conformarsi al Sarbanes-Oxley Act. La SEC ha indicato che nessun modello preciso di documentazione è stato approvato o fissato come requisito, e che il livello di dettaglio della documentazione può variare secondo le dimensioni e della complessità aziendale.

Come detto precedentemente, per fornire una base per supportare le sue asserzioni relativamente all'adeguatezza del disegno del controllo, il management ha bisogno di documentare la valutazione della struttura dei controlli. La documentazione della valutazione del piano di controllo dovrebbe essere sufficientemente dettagliata da permettere agli auditor esterni una valutazione del progetto, ripercorrerne i passi ed eseguire verifiche sull'efficacia del controllo.

L'auditor esterno dovrebbe essere in grado di comprendere la valutazione della struttura di controllo fatta dal management grazie a un livello di dettaglio sufficiente che gli consenta di rieseguire le verifiche del disegno.

In generale, non è sufficiente redigere procedure e manuali senza prevedere la riconciliazione con il processo di valutazione del disegno.

Figura 6 – Qualità del Controllo

	Stage 0 non esistente	Stage 1 Iniziale/ ad hoc.	Stage 2 Ripetibile ma intuitivo	Stage 3 Processo definito	Stage 4 Gestito e misurabile	Stage 5 - Ottimizzato
Caratteristiche	A questo livello, c' è un'assenza totale di un qualsiasi riconoscibile processo di controllo o dell'esistenza di qualunque procedura relativa. L'azienda non è conscia del fatto che c'è un problema che deve essere corretto; pertanto non è stata generata nessuna comunicazione a riguardo	C' è una certa evidenza per cui l'azienda riconosce che i controlli e le relative procedure sono importanti e necessitano di essere considerate. Comunque, i controlli e le relative policy e procedure non sono attuate e documentate. Non è presente un processo di divulgazione in merito agli eventi. Il personale non è consapevole della responsabilità per la sua attività di controllo. L'efficacia di funzionamento delle attività di controllo non è valutata in maniera regolare. Le carenze dei controlli non sono identificate.	I controlli e le relative policy e procedure sono attuate ma non sempre sono adeguatamente documentate. È posto in essere ma non documentato un processo di divulgazione delle notizie. Il personale potrebbe non essere consapevole della sua responsabilità per le attività di controllo. L'efficacia operativa delle attività di controllo non è valutata adeguatamente su base regolare e il processo non è documentato. Le carenze di controllo possono essere identificate ma non sono corrette in maniera tempestiva.	I controlli e le relative policy e procedure sono attuati e sono adeguatamente documentati. Un processo di divulgazione degli eventi è attuato ed è documentato adeguatamente. Il personale è consapevole della sua responsabilità per le attività di controllo. L'efficacia del funzionamento delle attività di controllo è valutata su una base periodica (per esempio trimestralmente); tuttavia, il processo non è completamente documentato. Le carenze di controllo sono identificate e i rimedi sono attuati in modo tempestivo.	I controlli e le relative policy e procedure sono attuati e adeguatamente documentati e il personale è consapevole della sua responsabilità per le attività di controllo. Un processo di divulgazione degli eventi è attuato ed adeguatamente documentato e monitorato, ma non sempre rivalutato in modo da riflettere i principali cambiamenti organizzativi o del processo. L'efficacia operativa delle attività di controllo è valutata su una base periodica (p. es. settimanalmente) e il processo è documentato adeguatamente. E' presente, a fini tattici, un uso limitato della tecnologia per documentare i processi, gli obiettivi di controllo e le attività.	La fase 5 soddisfa tutte le caratteristiche della fase 4. Esiste un programma aziendale di gestione e controllo del rischio tale che controlli e procedure sono ben documentati e continuamente rivisti in modo da riflettere i principali cambiamenti del processo o dell'organizzazione. Un processo di auto valutazione è usato per valutare il disegno e l'efficacia dei controlli. La tecnologia è utilizzata al massimo potenziale per documentare i processi, gli obiettivi di controllo e le attività, identificare le lacune e valutare l'efficacia dei controlli.
Requisiti del Sarbanes-Oxley	L'azienda è totalmente incapace di realizzare un grado di conformità, neppure a un livello minimo.	I controlli, le policy, le procedure e la documentazione disponibili sono insufficienti per supportare le asserzioni del management. Il livello dell'impegno per documentare, esaminare e correggere i controlli è notevole.	Sebbene vi siano i controlli, le policy e le procedure, esiste documentazione insufficiente per supportare la certificazione e le asserzioni del management. Gli sforzi per documentare, esaminare e correggere i controlli è significativo.	Esiste documentazione sufficiente per supportare la certificazione e le asserzioni del management. Lo sforzo necessario per documentare, esaminare e correggere i controlli può essere significativo in base alla situazione contingente dell'azienda.	La documentazione esistente è sufficiente per supportare la certificazione e le asserzioni del management. Il grado di sforzo per documentare, verificare e correggere i controlli può essere meno significativo in base alla situazione contingente dell'azienda.	Sono attuati i requisiti del livello 4. Grazie all'alta qualità e tempestività delle informazioni, è possibile un continuo miglioramento del processo di gestione delle decisioni. Le risorse interne sono usate efficacemente ed efficientemente. Le informazioni sono tempestive e affidabili.

Valutare l'Efficacia Operativa

Una volta che il progetto del sistema dei controlli è stato adeguatamente valutato, devono essere confermate la sua implementazione e la sua efficacia. Durante questa fase dovrebbero essere eseguiti i test preliminari e quelli di routine per verificare l'efficacia operativa delle attività di controllo. I test dovrebbero essere condotti dal personale responsabile dei controlli e dal team di gestione del programma di controllo interno.

Giacché ci sono diversi fattori che influenzano l'ampiezza del campione da selezionare (ad esempio, la presenza di altri controlli da testare, o il tasso di errore atteso), viene rappresentato in **figura 7** una (minima) metodologia comune di selezione del campione utilizzata dalle società di revisione e dagli auditor per verificare l'efficacia operativa dei controlli. L'ampiezza del campione selezionato per la verifica dei controlli generali IT è direttamente proporzionale alla frequenza dell'operazione di controllo.

Figura 7 – Guida per la selezione dell'ampiezza del campione

Tipo Controllo	Frequenza della verifica	Ampiezza minima del campione
Manuale	Diverse volte al giorno	25
Manuale	Giornaliera	25
Manuale	Settimanale	5
Manuale	Mensile	2
Manuale	Trimestrale	2
Manuale	Annuale	1
Automatico	Verificare un'applicazione per ogni attività di controllo programmata (si presume che i controlli generali IT siano efficaci)	
Controlli generali IT	Seguire le sopra esposte linee guida per gli aspetti manuali e automatici dei controlli generali IT	

Il management ha bisogno di documentare le sue verifiche sull'efficacia operativa e le conclusioni raggiunte sul fatto che i controlli da loro valutati significativi operino coerentemente a come sono stati disegnati.

Allo stesso modo della documentazione manageriale sulla valutazione del piano dei controlli, il management ha bisogno di documentarne l'efficacia operativa in modo sufficientemente dettagliato in modo da permettere agli auditor esterni di rieseguire le attività di verifica dell'efficacia operativa eseguita dal management.

In aggiunta alle informazioni documentate nella valutazione del piano di controllo, la documentazione sull'efficacia operativa può includere le seguenti informazioni:

- Tipologia ed estensione quantitativa e temporale delle fasi di verifica eseguite
- Risultato delle verifiche
- Risorsa che ha eseguito la verifica e la data di esecuzione
- Ampiezza del campione e popolazione verificata
- Riferimenti e ubicazione della documentazione di supporto
- Conclusioni sull'efficacia operativa
- Eccezioni identificate e conseguenti piani di sistemazione e/o controlli compensativi

Considerare la natura dell'evidenza richiesta

L'auditing Standard No. 2 descrive diverse forme di evidenza che possono essere ottenute nella verifica della struttura e dell'efficacia operativa dei controlli. In generale ci si attende che gli auditor eseguano un mix tra interviste al personale di riferimento, esame della documentazione significativa, osservazione delle operazioni aziendali, riesecuzione dell'applicazione dei controlli.

Le diverse forme di controllo includono:

a) Intervista – L'intervista è una procedura che consiste nell'ottenimento di informazioni dal personale responsabile all'interno dell'azienda. Nella maggior parte delle organizzazioni aziendali l'intervista viene largamente utilizzata, e spesso è complementare all'esecuzione di altre procedure.

b) Esame della documentazione – Giacché l'intervista da sola non fornisce sufficiente evidenza a supporto della struttura del controllo e della sua efficacia operativa, dovrebbero essere eseguite delle verifiche aggiuntive. Le organizzazioni aziendali, per ottenere sufficiente evidenza della efficacia operativa del controllo, dovrebbero supportare le interviste con altre attività quali verifiche delle relazioni e di altra documentazione utilizzata nell'esecuzione dei controlli.

c) Osservazione – Nei casi in cui l'evidenza documentale dei controlli non esiste perché non è prevista, le aziende dovrebbero supportare le interviste al personale interessato attraverso l'osservazione delle attività aziendali.

d) Riesecuzione – Nei casi in cui la qualità dell'evidenza riguardo al disegno ed efficacia operativa dei controlli non fosse sufficientemente persuasiva, le aziende dovrebbero scegliere di rieseguire i controlli e indipendentemente produrre il report delle eccezioni e investigare di conseguenza. Per esempio, la firma su di un report di eccezioni può non essere sufficiente a dimostrare che queste siano state tutte controllate. In questo caso, le aziende possono scegliere di rieseguire i controlli e indipendentemente produrre il report delle eccezioni e investigare sui casi segnalati.

Considerare la tempistica della verifica del controllo

Conformemente alle date indicate nel report del management, le aziende dovrebbero eseguire le verifiche dei controlli su un arco temporale che fosse adeguato a determinare se i controlli necessari al raggiungimento degli obiettivi della struttura di controllo siano operativamente efficaci.

Il lasso di tempo sul quale le aziende eseguono le verifiche sui controlli varia in funzione della natura del controllo da testare e della frequenza con cui determinati controlli operano e con cui sono applicate determinate procedure.

Alcuni controlli sono sempre attivi (per esempio, l'approvazione della richiesta d'accesso di un utente), mentre altri sono effettuati solo in determinate occasioni (per esempio, verifica periodica del tabulato degli accessi). In linea generale, le aziende dovrebbero svolgere le proprie verifiche nel momento i cui vengono eseguiti i controlli.

Verifiche roll-forward

In diverse aziende le verifiche sui controlli IT sono eseguite a una data intermedia (interim) prima della chiusura dell'anno. Quando le aziende testano i controlli nella fase di interim dovrebbero determinare

quali evidenze aggiuntive saranno necessarie, per ottenere una valutazione sull'operatività del controllo, nel restante periodo di tempo. A tal fine le aziende dovrebbero considerare:

- gli specifici controlli testati prima della data intermedia fissata e il risultato delle verifiche effettuate
- la valutazione ottenuta dalle evidenze rilevate dalla verifica dell'efficacia operativa dei controlli
- la lunghezza del periodo temporale restante
- la possibilità che sia intervenuto qualche cambiamento nel processo di controllo interno sul reporting finanziario successivamente alla data di interim.

5. Classificare ed Eliminare le Carenze

Considerare le linee guida della SEC e del PCAOB

La guida PCAOB pubblicata nel novembre 2004 suggerisce che, le debolezze nei controlli generali IT in assenza di debolezze nei controlli applicativi dovrebbero essere classificati solo come debolezze dei controlli generali IT. Comunque, il PCAOB descrive tre condizioni per cui un inefficiente sistema di controlli generali IT potrebbe comportare più di una debolezza tale da essere considerata una "carenza significativa".

I seguenti casi:

- Debolezze a livello applicativo - L'importanza di una debolezza del sistema di controllo IT dovrebbe essere valutata in relazione a suoi effetti sui controlli applicativi, cioè se i relativi controlli applicativi sono inefficaci. Se la debolezza applicativa è causata da un controllo generale IT, entrambi sono trattati allo stesso modo. Per esempio, se un'applicazione alla base del calcolo della tassazione dà un errore significativo e questi è causato da un controllo inefficace delle variazioni sulla tabella delle tasse, allora il controllo dell'applicazione base (calcolo) e il controllo generale (cambiamento) potrebbero essere classificati come carenze significative.
- Debolezze del controllo ambientale – Dopo che una debolezza dei controlli generali IT è stata valutata in relazione ai suoi effetti sui controlli applicativi, dovrebbe essere valutata anche aggregata alle altre debolezze di controllo. Consideriamo ad esempio che la decisione del management sia quella di non correggere una debolezza dei controlli generali IT e il suo conseguente effetto sul controllo ambientale; se considerata insieme alle altre debolezze che affliggono il controllo ambientale, questo potrebbe portare alla conclusione che si è in presenza di debolezze e carenze significative.
- Fallire nel porre rimedio a una debolezza per un periodo di tempo non ragionevole - In base alle istruzioni del PCAOB Auditing Standard No. 2, l'auditor potrebbe rilevare, per ragionevole prudenza nella conduzione del proprio lavoro, come una debolezza dei controlli generali IT sia una debolezza significativa. In questo caso, una debolezza dei controlli generali IT che è stata comunicata al management e agli opportuni organi preposti, e che ancora non è stata corretta dopo un ragionevole periodo di tempo, è un importante indicatore di carenza significativa.

Identificare e valutare le inefficienze dei controlli generali IT

Tutte le debolezze, incluse quelle IT, dovrebbero essere riviste insieme al team di compliance finanziario e valutate come parte di una più vasta certificazione del controllo interno. Le debolezze IT non dovrebbero essere valutate separatamente. Allo stesso modo anche i controlli applicativi che supportano i controlli sul reporting finanziario necessitano di una rivisitazione e valutazione con il team di compliance.

La guida generale per la valutazione delle debolezze dei controlli generali IT fornita nell'appendice H, "Procedura di controllo e verifica a campione", fornisce un esempio del percorso decisionale e aiuta le aziende nell'analisi preliminare delle debolezze dei controlli.

Comunque, questa è solo un'analisi preliminare che necessita di ulteriori verifiche e conclusioni e necessita di essere eseguita in modo generale con il team di compliance.

In generale ci sono due tipi di debolezze che le aziende devono gestire:

1. Debolezze strutturali - sono dovute all'assenza di controlli, controlli inadeguati, mancanza di supporto documentale o altri errori nella struttura di controllo che non mitigano sufficientemente il rischio a esse correlato.
2. Debolezze dell'efficacia operativa - sono legate alla consistenza con cui i controlli operano, come il fatto che un controllo non sia eseguito come previsto durante l'anno.

Considerare l'effetto aggregato delle inefficienze

In alcuni casi, le debolezze individuali dei controlli possono essere considerate insignificanti, mentre l'effetto combinato con altre debolezze può essere più rilevante. Per esempio, un'azienda che non esegue una verifica periodica del tabulato degli accessi ai suoi applicativi finanziari sarebbe normalmente considerata avere una debolezza della struttura dei controlli. Questa debolezza da sola potrebbe non essere significativa specialmente quando vi sono altri controlli compensativi. Comunque se questa azienda sbaglia anche ad assegnare in modo appropriato i profili autorizzativi di accesso degli utenti, allora l'effetto aggregato delle due debolezze può comportare una debolezza rilevante o una carenza significativa.

In altre parole, l'effetto combinato delle debolezze sui controlli delle richieste d'accesso e sulla verifica degli accessi porterebbe a porsi domande sulla validità degli accessi alle applicazioni finanziarie e, perciò, anche sulla validità delle transazioni registrate nel sistema.

Rimediare alle debolezze dei controlli

La fase di assestamento di molti progetti è quella dove vengono fatti i maggiori sforzi e si spendono più risorse economiche. In certi casi, potrebbero esserci situazioni che consentono rimedi veloci ed economici ma che potrebbero costare molto di più nella fase operativa. Per esempio, il processo manuale per aggiungere, cambiare o modificare i profili utenti è lento e richiede tempo. Comunque, per un'azienda che necessita di una soluzione veloce, spesso l'approvazione e l'inserimento manuale rappresentano la soluzione più veloce.

Comunque, una soluzione a lungo termine potrebbe includere l'acquisto di processo automatico che limiti i profili d'accesso senza appropriate autorizzazioni. Questo approccio costerà sicuramente di più nel breve termine ma tende a essere più stabile ed efficace nel lungo periodo.

6. Crescita sostenibile

A questo punto, i responsabili IT dovrebbero essere in grado di valutare l'efficacia del programma interno dei controlli IT. L'efficacia dei controlli interni, la valutazione dei controlli e le competenze del

management dovrebbero diventare parte e supporto nel tempo dell'organizzazione e della cultura IT. Il controllo non è un evento; è un processo che richiede continuamente supporto e valutazione perché rimanga aggiornato. L'obiettivo finale è quello di convertire il progetto di controllo IT in un processo. Per raggiungere questo obiettivo si dovrebbero considerare le seguenti attività:

- Effettuare una verifica generale dopo l'implementazione del progetto Sarbanes-Oxley identificando cosa va bene e cosa sia da sviluppare
- Rivedere le guide e le interpretazioni recenti della SEC e del PCAOB per determinare gli impatti futuri degli eventuali cambiamenti interpretativi
- Verificare altro materiale indipendente per suggerimenti e opportunità per sviluppare l'approccio da seguire
- Riunioni con pari livello di altre aziende per discutere potenziali sviluppi del processo
- Valutare soluzioni di lungo periodo per gestire le problematiche del Sarbanes-Oxley Act, come l'automazione dei processi e lo sviluppo di software di controllo delle modifiche ai programmi
- Sviluppare un piano preliminare e uno scadenziario per l'anno successivo, rendendolo un processo radicato
- Costituire il processo Sarbanes-Oxley all'interno delle iniziative più globali di controllo IT.

Razionalizzare i controlli

La razionalizzazione (o eliminazione) dei controlli è un'altra iniziativa che dovrebbe essere effettuata nella fase di consolidamento. Ci saranno senza dubbio dei controlli che sono documentati ma che nel tempo sono diventati meno utili. Le aziende dovrebbero rivedere periodicamente i propri controlli per identificare quelli che possono essere eliminati. Nel compiere questa operazione bisognerebbe documentare l'impatto che seguirebbe alla rimozione del controllo, spiegando il motivo per cui il controllo viene rimosso.

Automatizzare i controlli

In molti casi ci sono numerosi controlli manuali che possono essere automatizzati. Nell'appendice D offriamo degli esempi di controlli automatici. Un ottimo punto di partenza per identificare dove trasformare i controlli manuali in controlli automatici sono i controlli applicativi. Le aziende possono verificare gli esempi dell'appendice D e rilevare i controlli manuali da automatizzare.

In molti casi si avrà bisogno di informazioni più dettagliate in funzione degli applicativi utilizzati dall'azienda e della natura dei controlli desiderati. Le aziende che utilizzano ad esempio SAP o Oracle hanno benchmark maggiormente dettagliati dei controlli che le piattaforme citate offrono.

Utilizzare i benchmark applicativi

Il PCAOB, descritto in appendice D, ha introdotto nel novembre 2004 le linee guida del concetto di benchmark dell'applicativo. L'idea è che, una volta che l'applicativo si dimostra stabile attraverso i test, non deve necessariamente essere testato ogni anno. Il risultato è che si possono diminuire gli sforzi rendendo più efficiente ed efficace il processo d'adeguamento.

Appendice A - L'A-B-C del Sarbanes-Oxley Act

Il Sarbanes-Oxley Act esprime la ferma risoluzione del Congresso degli Stati Uniti d'America di accrescere la responsabilità in seno alle aziende. L'Act è stato concepito per recuperare la fiducia degli investitori nei mercati pubblici americani, che era stata danneggiata a seguito di scandali finanziari ed errori nella governance delle aziende. Sebbene l'Act e i regolamenti di supporto abbiano riscritto le regole relative alla responsabilità, alla comunicazione e al reporting, le numerose pagine di termini legali di cui è costituito suffragano una semplice premessa: un'efficace governance d'impresa e corrette prassi di etica nel gestire il business non sono più degli optional.

Informazioni preliminari

Il Sarbanes-Oxley Act fu approvato dal Congresso Statunitense e firmato come legge dal Presidente il 30 luglio 2002. Tra i vari provvedimenti, la sezione 404 dell'Act richiede che le società registrate presso la SEC e i loro auditor annualmente valutino e riferiscano sul progetto e l'efficacia dei controlli interni relativi al reporting finanziario.

Molto è stato scritto sull'importanza dell'Act e dei controlli interni in generale; tuttavia, esiste ben poco per quanto riguarda il ruolo fondamentale dell'information technology in questo ambito. E' opinione diffusa che l'affidabilità del reporting finanziario sia dipendente in massima parte da un ambiente IT adeguatamente controllato. Conseguentemente, vi è un'esigenza di conoscenza da parte delle aziende che devono considerare la tematica dei controlli IT in relazione alla produzione del reporting finanziario. Questo documento è pensato in primo luogo per fornire un supporto adeguato alle società oggetto di controllo da parte della SEC nell'affrontare la tematica dei controlli IT come parte integrante delle loro attività di valutazione; in secondo luogo per essere utilizzato come supporto alle attività di conformità per le aziende registrate in altri stati e che hanno implementato requisiti di certificazione simili per i responsabili del top management (CEO/CFO).

Nella redazione di questa pubblicazione sono stati presi in considerazione diversi controlli IT. Tuttavia è stato fatto uno sforzo notevole per limitare la trattazione a quei controlli maggiormente correlati al controllo interno del reporting finanziario. Conseguentemente, questo documento non tratta deliberatamente i controlli che sovrintendono a risultati operativi e di efficienza. E' tuttavia inevitabile (e auspicabile) che i risultati operativi e di efficienza costituiscano controlli aggiuntivi previsti entro le strutture di controllo e i processi implementati. Per ulteriori indicazioni in queste aree ci si può riferire a ITGI Board Briefing on IT Governance 2nd Edition, e IT Governance Implementation Guide.

Il Sarbanes-Oxley Act - Accrescimento della responsabilità aziendale

Il Sarbanes-Oxley Act ha apportato un profondo mutamento nell'ambito aziendale e normativo. L' Act si prefigge lo scopo di migliorare la governance della azienda attraverso misure atte a rafforzare il controllo e l'equilibrio interni e, in ultima analisi, la responsabilità aziendale. Tuttavia, è importante sottolineare che la sezione 404 non richiede all'alta direzione e ai responsabili dei processi aziendali soltanto di prevedere e mantenere un'adeguata struttura di controllo interno, ma anche di verificare la sua efficacia su base annuale. Questa distinzione è fondamentale.

L'IT gioca un ruolo fondamentale nel controllo interno. Sistemi, dati e le infrastrutture sono componenti critici per i processi di produzione del reporting finanziario.

L'Auditing Standard N. 2 del PCAOB analizza l'importanza dell'IT nel contesto del controllo interno. In particolare stabilisce che:

> *La natura e le caratteristiche dell'utilizzo da parte di un'azienda dell'IT nell'ambito dei propri sistemi informativi influisce sul controllo interno relativo alla predisposizione del reporting finanziario.*

Gli specialisti IT, specialmente coloro che occupano posizioni di responsabilità, hanno bisogno di conoscere bene la teoria e le prassi relative al controllo interno per rispettare i requisiti del Sarbanes-Oxley Act. I CIO e gli altri responsabili per l'adeguatezza dei sistemi devono raccogliere la sfida di:

- Approfondire la loro conoscenza sul controllo interno,
- Conoscere il piano di adeguamento al Sarbanes-Oxley Act della loro azienda,
- Sviluppare un piano di adeguamento rivolto in modo specifico ai controlli IT
- Integrare questo piano con quello per l'adeguamento generale dell'azienda al Sarbanes-Oxley Act.

In relazione a ciò, lo scopo di questa pubblicazione è quello di fornire un valido aiuto ai responsabili dei sistemi IT aziendali, per:

- Rilevare lo stato corrente dell'ambiente di controllo IT
- Definire i controlli necessari per rispettare le direttive del Sarbanes-Oxley Act
- Sviluppare un approccio per testare e mantenere i controlli anche nel futuro
- Identificare le eccezioni e i relativi piani di contromisure e aggiungere controlli che compensino le eccezioni identificate.

L'audit dei Controlli Interni sul Reporting Finanziario

Nel marzo 2004 l'US Public Company Oversight Board (PCAOB) ha approvato il PCAOB Auditing Standard n. 2 intitolato "Un audit sul Controllo Interno relativo sul reporting finanziario eseguito in associazione con un audit sul bilancio". Lo standard divenne operativo da giugno 2004 a seguito dell'approvazione della SEC. Questo standard di audit stabilisce i requisiti per realizzare una verifica sul controllo interno del reporting finanziario e fornisce importanti indicazioni circa il campo d'azione e il tipo di approccio richiesto agli auditor.

Lo standard del PCAOB prevede requisiti specifici per gli auditor ai fini della comprensione dei flussi delle transazioni, compresa anche le modalità con cui le transazioni vengono eseguite, autorizzate, registrate, elaborate e prodotte in output. In molti casi questi flussi di transazioni generalmente prevedono l'uso di sistemi applicativi per l'automazione dei processi nonché un numero significativo di complesse elaborazioni delle stesse transazioni. L'affidabilità di questi sistemi applicativi è, di volta in volta, legata alle varie componenti dell'IT, che comprendono reti, banche dati, sistemi operativi. Queste, considerate assieme, costituiscono i sistemi IT coinvolti nel processo di predisposizione del reporting finanziario dell'azienda e, di conseguenza, devono essere prese in considerazione nella definizione e valutazione del controllo interno.

Lo standard n. 2 del PCAOB sottolinea come l'IT abbia un effetto "pervasivo" sui controlli interni del reporting finanziario. Nella sostanza lo standard di controllo riconosce l'importanza dei controlli IT nell'ambiente di controllo globale e richiede che le aziende comprendano come l'IT viene utilizzato nei processi di produzione di tali documenti e come i controlli siano progettati e applicati per gestire i rischi. Pur se di natura generale, i principi del PCAOB forniscono indicazioni alle aziende soggette al controllo

della SEC sui punti in cui si devono concentrare gli sforzi per verificare se i controlli specifici sulle transazioni siano progettati adeguatamente e se siano effettivamente operanti.

In particolare i quattro principali standard di controlli IT che bisogna prendere in considerazione per il Sarbanes-Oxley Act sono: sviluppo dei programmi, gestione delle modifiche, attività operative, accesso a dati e programmi.

Requisiti per il management specifici del Sarbanes-Oxley Act

La maggior parte del dibattito relativo al Sarbanes-Oxley Act è incentrata sulle sezioni 302 e 404. Un breve riferimento riepilogativo è fornito dalla **figura 8.**

Figura 8 – Requisiti del Sarbanes-Oxley Act - Riferimento

	302	404
Chi	Il management aziendale, con la partecipazione dei principali responsabili operativi e finanziari (gli addetti alla certificazione)	Management, responsabili operativi e finanziari (il termine "management" non è stato definito dal PCAOB)
Che cosa	1. Gli addetti alla certificazione sono responsabili della costruzione e mantenimento del sistema di controllo sulla predisposizione del reporting finanziario. 2. Gli addetti alla certificazione che hanno predisposto tale sistema di controllo sul reporting finanziario, o comunque supervisionato la sua costruzione, devono fornire ragionevole assicurazione riguardo l'affidabilità del reporting finanziario e la preparazione del bilancio in accordo con i principi contabili generalmente accettati.(*) 3. Viene comunicata qualsiasi modifica apportata ai controlli interni dell'azienda che nel corso dell'ultimo trimestre abbiano influito o possano ragionevolmente influire sulla predisposizione del reporting finanziario. 4. Quando il motivo per un cambiamento nei controlli interni afferenti la predisposizione del reporting finanziario è la correzione di un difetto sostanziale, il management ha la responsabilità di determinare se le ragioni del cambiamento e le circostanze che determinano questa modifica sono informazioni essenziali perché il cambiamento venga comunicato, e non costituiscono viceversa informazioni fuorvianti.	1. Dichiarazione di responsabilità del management nella definizione e mantenimento di un adeguato controllo interno ai fini della predisposizione del reporting finanziario dell'azienda 2. Dichiarazione che illustra lo schema utilizzato dal management nel procedere alla prevista valutazione dell'efficacia del controllo interno ai fini della predisposizione del reporting finanziario dell'azienda 3. Una valutazione dell'efficacia del controllo interno della azienda nella predisposizione del reporting finanziario aziendale di fine anno, compresa una dichiarazione esplicita che il controllo interno sulla predisposizione del reporting finanziario dell'azienda è effettivo 4. Una dichiarazione che la società di certificazione responsabile dell'audit del bilancio, incluso quello annuale, abbia emesso un rapporto sulla valutazione del controllo interno sulla predisposizione del reporting finanziario fatta dal management dell'azienda 5. Una dichiarazione conclusiva da parte del management sulla efficacia del controllo interno della azienda in merito alla predisposizione del reporting finanziario inserita sia nella relazione del controllo interno sul reporting finanziario sia nella dichiarazione all'auditor (representation letter). La valutazione conclusiva sull'efficacia del controllo interno della azienda sul reporting finanziario può assumere forme diverse. Tuttavia il management è tenuto a fornire una conclusione diretta sulla reale efficacia del controllo interno della azienda sul reporting finanziario. 6. Il management non può concludere che il controllo interno dell'azienda, in merito alla predisposizione dei reporting finanziari, sia valido se esistono uno o più punti di debolezza sostanziale. Inoltre il management è tenuto a dichiarare qualsiasi punto debole presente alla chiusura dell'anno.
Quando	Già in vigore, dal luglio 2002	Alla fine dell'anno che inizia o dopo il giorno 15 novembre 2004 (**)
Con quale frequenza	Assessment trimestrale e annuale	Verifica annuale da parte del management e dell'auditor esterno

Per la versione più aggiornata dei requisiti della sezione 404, si faccia riferimento al sito web del SEC

(*) Annuale per le aziende private straniere
(**) Le aziende straniere iniziano il 15 luglio 2007 e le imprese minori (bilancio inferiore a 75 milioni di US $) possono ritardare fino al 15 dicembre 2007. Inoltre, sempre le imprese minori hanno tempo fino al 15 Dicembre 2008 per fornire un attestato da parte degli auditor relativo ai controlli interni, come richiesto dalla Sezione 404 (B).

Controlli e procedure di comunicazione.

I controlli e le procedure di comunicazione si riferiscono ai processi in essere atti ad assicurare che tutte le informazioni sostanziali siano divulgate da una società nei documenti che predispone o invia alla SEC. Questi controlli richiedono anche che le comunicazioni siano autorizzate, complete e accurate e che siano registrate, elaborate, riassunte e riportate entro i termini stabiliti dalle norme SEC e con le relative forme. Inadempienze nei controlli, così come modifiche sostanziali nei controlli, devono essere tempestivamente comunicate al comitato di audit e agli auditor dell'azienda. Il direttore esecutivo dell'azienda e il direttore amministrativo devono certificare l'esistenza di questi controlli su base trimestrale.

Sezione 302 Requisiti per il management

Sezione 302:

….richiede alla classe dirigente di un'azienda, in collaborazione con i principali dirigenti esecutivi ed amministrativi (i funzionari che certificano), di effettuare le seguenti attestazioni trimestrali ed annuali relativamente al rispetto del controllo interno dell'azienda sul reporting amministrativo e finanziario:

- *Un'attestazione che i dirigenti certificatori sono responsabili dell'organizzazione e del mantenimento dei controlli interni sul reporting amministrativo e finanziario*
- *Un'attestazione che i dirigenti certificatori sono responsabili del progetto dei controlli interni sul reporting amministrativo e finanziario, o responsabili della supervisione del progetto degli stessi, per fornire ragionevole assicurazione circa l'affidabilità del reporting amministrativo e finanziario e la redazione dei bilanci esterni in sintonia con i principi contabili generalmente accettati*
- *Un'attestazione che il report riporta qualsiasi modifica apportata nel controllo interno dell'azienda sul reporting amministrativo e finanziario nell'ultimo trimestre (il quarto trimestre nel caso di un report annuale) che ha influito materialmente, o che può eventualmente influire materialmente sul comitato di controllo interno dell'azienda in merito al reporting amministrativo e finanziario.*

Quando il motivo di un cambiamento nel controllo interno del report finanziario è la correzione di un errore materiale, la dirigenza ha la responsabilità di stabilire, e l'auditor di valutare, se il motivo del cambiamento e le circostanze che l'hanno determinato siano informazioni rilevanti, e non fuorvianti, per comunicare il cambiamento apportato.

Sezione 404 – Requisiti per il management

Le direttive della sezione 404 del Sarbanes-Oxley Act prevedono che il management predisponga un rapporto annuale sulla sua valutazione del controllo interno in merito al reporting finanziario relativo alla chiusura annuale.

La sezione 404 prevede che:

Il rapporto del management sul controllo interno del reporting finanziario, debba contenere le seguenti informazioni:

- *Una dichiarazione di responsabilità del management nel fissare e mantenere un adeguato controllo interno sul reporting finanziario dell'azienda*
- *Una dichiarazione che fornisca i parametri usati dal management per procedere alla valutazione richiesta sulla validità del controllo interno dell'azienda in merito al reporting finanziario*
- *Una valutazione dell'efficacia del controllo interno dell'azienda sul reporting finanziario alla data di chiusura dell'ultimo esercizio, comprendente un'esplicita dichiarazione dell'efficacia di tale controllo interno sul reporting finanziario*
- *Una dichiarazione che la società di certificazione, che ha effettuato l'auditing dei bilanci annuali, abbia emesso un'attestazione sulla valutazione fatta dal management sul controllo interno in merito al reporting finanziario.*

Il management dovrebbe fornire, sia nel rapporto sul controllo interno del reporting finanziario sia nella representation letter all'auditor, una conclusione scritta della validità del controllo interno della azienda in merito al reporting finanziario. Le conclusioni sulla validità del controllo interno dell'azienda in merito al reporting finanziario può assumere forme diverse; tuttavia al management è richiesto di fornire una conclusione diretta sulla reale efficacia del controllo interno dell'azienda in merito alla predisposizione del reporting finanziario.

Controlli interni sul reporting finanziario.

Il controllo interno sul reporting finanziario è così definito dalla SEC:

Un processo definito, o sotto la supervisione, dei principali manager operativi e finanziari, o di persone che svolgano similare attività, e afferenti al Consiglio d'Amministrazione, (registrant's board of directors) diretto a fornire ragionevole garanzia in merito all'affidabilità del reporting finanziario e alla predisposizione del bilancio per uso pubblico in accordo con i principi contabili comunemente accettati e include quelle policy e procedure che:

- *Sono relative alla conservazione delle registrazioni che, con ragionevole dettaglio, accuratamente e correttamente riflettono le operazioni e le disposizioni dei beni della azienda*
- *Forniscono ragionevole garanzia che le operazioni siano registrate con modalità tali da permettere la predisposizione del reporting finanziario secondo i principi contabili comunemente accettati, che le fatture e le spese siano effettuate solo se autorizzate dal management di competenza*
- *Forniscono ragionevole garanzia relativamente alla prevenzione o alla tempestiva rilevazione di acquisti non autorizzati, l'utilizzo o la disposizione di beni che potrebbe avere un effetto sostanziale sulle poste di bilancio.*

Il PCAOB utilizza la stessa definizione tranne che per la parola "registrant" (n.d.r. per "registrant" si intende la società quotata alla SEC o comunque sottoposta al suo controllo) che è stata modificata in "company".

Al management non è consentito dichiarare l'efficacia del controllo interno della azienda in merito al reporting finanziario se sussistono uno o più carenze sostanziali. Inoltre, al management è richiesto di comunicare qualsiasi carenza sostanziale presente alla chiusura dell'esercizio.

Il management potrebbe essere in grado di sostenere in modo accurato che il controllo interno sul reporting finanziario, a fine esercizio, era efficace anche se erano presenti una o più carenze significative nel corso dell'esercizio. Per poter procedere a questa dichiarazione, il management deve aver prima modificato il controllo interno sul reporting finanziario per eliminare in tempo utile la carenza significativa prima della data di chiusura del bilancio e aver testato in modo adeguato l'efficacia per un periodo temporale adeguato a determinare se, alla chiusura dell'esercizio, il disegno e l'implementazione del controllo interno del reporting finanziario risultavano efficaci.

Focus dell'Auditor in un contesto Sarbanes-Oxley

La sezione 404 richiede che un auditor indipendente fornisca un'attestazione in merito alla valutazione del controllo interno relativo al reporting finanziario svolto dal management.

Le aziende non devono solo assicurare che siano stati attivati controlli appropriati (inclusi i controlli IT), ma anche fornire agli auditor indipendenti la documentazione, le evidenze dell'efficacia dei controlli e la documentazione dei risultati delle procedure di controllo.

Secondo il Sarbanes-Oxley Act, gli standard per l'attestazione dell'auditor sono di competenza del PCAOB. Mentre l'attestazione inerente alla 404 è relativa a una certa data, l'Auditing Standard n. 2 del PCAOB si sofferma specificatamente sui controlli sul reporting finanziario che dovrebbero essere operativi durante un periodo di tempo precedente il termine di attestazione e sui controlli che possono essere effettuati dopo il termine di attestazione. Esso, infatti, stabilisce che:

La verifica dell'auditor in merito all'effettiva operatività di questi controlli dovrebbe avvenire nel momento stesso in cui i controlli sono operanti. Le verifiche a una certa data includono quelle che sono fondamentali per il controllo interno di un'azienda sul reporting finanziario, anche se tali controlli possono non essere operativi dopo questo termine specifico.

Si suggerisce che il management si incontri con gli auditor esterni per fissare il periodo di tempo entro il quale il controllo in oggetto deve essere operativo prima della data di della verifica.

Lo Standard di Auditing n. 2 del PCAOB tratta le responsabilità dell'auditor esterno relativamente alla sezione 302. In particolare stabilisce che:

La responsabilità dell'auditor riguardo le certificazioni trimestrali relative ai controlli interni del reporting finanziario è diversa dalla responsabilità

dell'auditor circa la valutazione annuale degli stessi controlli. L'auditor dovrebbe svolgere trimestralmente delle procedure limitate al fine di determinare se vi sono state delle modifiche sostanziali che, a giudizio dell'auditor, dovrebbero essere riportate nelle dichiarazioni sui cambiamenti nei controlli interni relativi al reporting finanziario affinché le certificazioni siano accurate e corrispondano alle norme stabilite dalla Sezione 302 dell'Act.

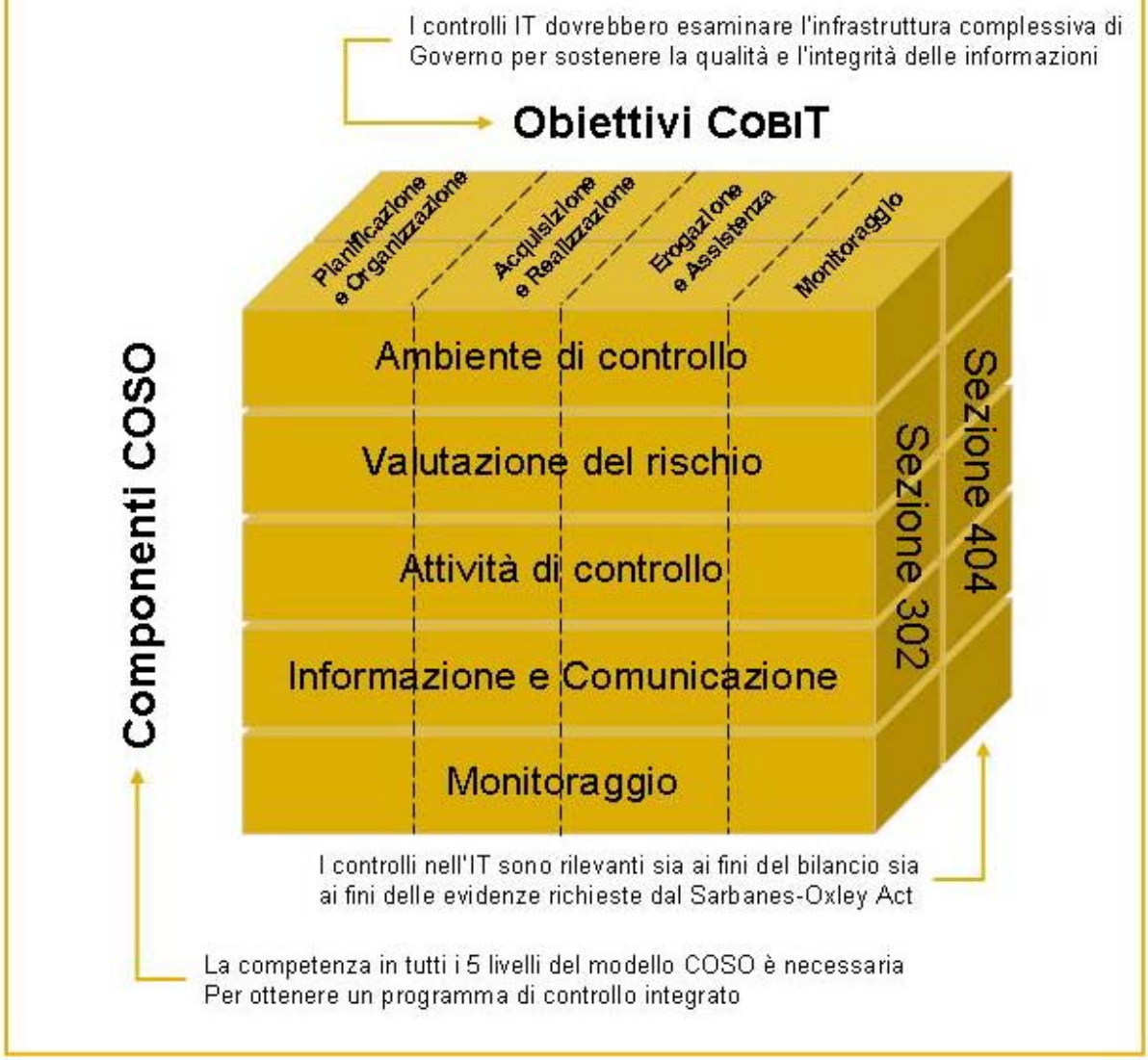
Per assolvere a queste responsabilità, l'auditor dovrebbe eseguire, trimestralmente, le seguenti procedure:

- *Indagine presso il management per eventuali modifiche sostanziali intervenute nel disegno nell'attuazione del controllo interno relativo al reporting finanziario per quanto riguarda la preparazione delle informazioni finanziarie annuali o di interim e successive all'ultimo audit del precedente esercizio o all'ultima revisione svolta;*
- *Valutazione delle implicazioni relative a errori, individuati dall'auditor, nell'ambito della revisione sui fatti successivi alla chiusura del bilancio (vedi AU sez. 722, Interim Financial Information) che siano relative all'efficacia del sistema di controllo sul reporting finanziario;*
- *Valutazione, attraverso una combinazione di osservazioni e indagini, dell'eventualità che un qualsiasi cambiamento nel controllo interno del reporting finanziario abbia influenzato sostanzialmente, o possa ragionevolmente influenzare, il controllo interno dell'azienda sul reporting finanziario.*

Appendice B – COSO e COBIT

Come indicato precedentemente nel documento, COSO divide i controlli interni in cinque componenti. La **figura 9** mostra che questi devono essere posti in essere e integrati per raggiungere gli obiettivi di presentazione e divulgazione del reporting finanziario. COBIT fornisce una guida con un livello di dettaglio analogo per l'IT. I cinque componenti di COSO – a partire dall'identificazione dell'ambiente di controllo fino al monitoraggio dei controlli interni – possono essere visualizzati come le linee orizzontali di un cubo tridimensionale, con i domini COBIT – dalla Pianificazione ed Organizzazione al Monitoraggio – che si applicano a ognuno di loro, sia singolarmente sia congiuntamente.

Figura 9 – Riferimenti incrociati fra le componenti di controllo COSO e COBIT



La **figura 10** illustra i processi IT di COBIT e collega la loro relazione al corrispondente componente COSO. Appare subito evidente che molti processi IT COBIT hanno rapporti con più di un componente COSO. Ciò è prevedibile data la natura dei controlli generali IT, considerato che essi formano la base per

realizzare sistemi informativi affidabili. Questa relazione multipla dimostra ulteriormente perché i controlli IT sono la base per tutti gli altri e sono essenziali per un programma di controllo interno affidabile.

COBIT è una struttura completa per la gestione del rischio e del controllo dell'IT, comprende quattro domini, 34 processi IT e 215 obiettivi di controllo di dettaglio. COBIT include i controlli che fanno riferimento a obiettivi di conformità e operativi, ma sono stati utilizzati per sviluppare questo documento **soltanto** quelli relativi al reporting finanziario. Si tratta di un'infrastruttura liberamente disponibile, che è in linea con lo spirito dei requisiti del Sarbanes-Oxley Act, in modo tale che ogni componente utilizzato sia facile da usare e generalmente condiviso. COBIT fornisce obiettivi sia a "livello aziendale" che a "livello di attività ", unitamente ai controlli associati, ed è largamente usato dalle organizzazioni come integrazione a COSO.

Mentre l'attenzione si è concentrata su ciò che è richiesto per il reporting finanziario, gli obiettivi e le considerazioni di controllo, disposti in questo documento, possono andare oltre ciò che è necessario alle aziende che cercano di conformarsi ai requisiti del Sarbanes-Oxley Act. La struttura di controllo interna suggerita (COSO) che deve essere utilizzata per conformità al Sarbanes-Oxley Act, come suggerito dalla SEC, copre gli argomenti di controlli IT, ma non detta i requisiti di tali obiettivi di controllo e le relative attività di controllo. Analogamente, il PCAOB Auditing Standard n. 2 dichiara l'importanza dei controlli IT, ma non specifica quali in particolare devono essere inclusi. Tali decisioni rimangono a discrezione di ogni azienda. Di conseguenza, le aziende dovrebbero valutare la natura e l'estensione dei controlli IT necessari a sostenere il loro programma di controllo interno caso per caso.

Questa guida non è stata preparata per suggerire "una misura che si adatta a tutto"; mentre, invece, raccomanda che ogni azienda adatti il modello dell'obiettivo di controllo alle proprie circostanze specifiche. Per esempio, se lo sviluppo dei sistemi è considerato a rischio basso, un'azienda può scegliere di modificare o cancellare alcuni o tutti gli obiettivi di controllo suggeriti. Un'azienda dovrebbe anche consultare i suoi auditor esterni per accertarsi che siano coperti tutti gli obiettivi critici di controllo.

Una parte importante di questa pubblicazione è fornire ai professionisti IT una guida sugli specifici obiettivi di controllo che dovrebbero essere considerati congiuntamente a COSO e, in definitiva, essere conformi al Sarbanes-Oxley Act. Perciò, l'appendice C fornisce questa informazione. Le organizzazioni IT dovrebbero considerare la natura e l'estensione delle loro operazioni nel determinare quali obiettivi di controllo, quali controlli esplicativi e quali test di controllo bisogna includere nel proprio programma di controllo interno.

Nello sviluppo di questa guida illustrativa, ogni obiettivo di controllo è stato studiato per assicurare la sua rilevanza e importanza nei requisiti del reporting finanziario secondo il Sarbanes-Oxley Act. Questo processo di valutazione è evidente in alcuni obiettivi di controllo COBIT che vengono esclusi o combinati in un singolo obiettivo per renderli applicabili ai fini del bilancio. Inoltre, ogni obiettivo di controllo IT viene conciliato con COSO per supportare l'allineamento con un programma Sarbanes-Oxley complessivo per l'azienda. Si esamini la **figura 10** per vedere questa riconciliazione.

Figura 10 Aree COBIT / Componenti COSO

Livello Aziendale	Livello Attività	Processi IT COBIT	Componenti COSO: Ambiente di Controllo	Risk Assessment	Attività di Controllo	Informazione e Comunicazione	Monitoring
Pianificazione ed Organizzazione (Ambiente IT)							
●		Definire il piano strategico per l'IT		●		●	●
		Definire l'architettura informatica					
		Definire gli indirizzi tecnologici					
●		Definire i processi, l'organizzazione e le relazioni dell'IT	●			●	●
		Gestire gli investimenti IT					
●		Comunicare gli obiettivi e gli orientamenti del management	●			●	
●		Gestire le risorse umane dell'IT	●			●	
●		Gestire la qualità	●		●	●	●
●		Valutare e gestire i rischi informatici		●			
		Gestire i progetti					
Acquisizione e implementazione (Sviluppo e modifiche dei programmi)							
		Identificare soluzioni automatizzate					
	●	Acquisire e mantenere il software applicativo			●		
	●	Acquisire e mantenere l'infrastruttura tecnologica			●		
	●	Permettere il funzionamento e l'uso			●	●	
	●	Approvvigionamento delle risorse IT					
		Gestire le modifiche		●	●		●
	●	Installare e accreditare soluzioni e modifiche			●		
Erogazione ed assistenza (Funzionamento dei sistemi e accesso ai programmi ed ai dati)							
	●	Definire e gestire i livelli di servizio	●		●	●	●
	●	Gestire i servizi di terze parti	●	●	●		●
		Gestire le prestazioni e la capacità produttiva					
		Assicurare la continuità di servizio					
	●	Garantire la sicurezza dei sistemi			●	●	●
		Identificare e attribuire i costi					
●		Formare e addestrare gli utenti	●			●	
	●	Gestire il Service Desk e gli incidenti			●	●	●
	●	Gestire la configurazione			●	●	
	●	Gestire i problemi			●	●	●
	●	Gestire i dati			●	●	
	●	Gestire l'ambiente fisico			●	●	
	●	Gestione le operazioni			●	●	
Monitoraggio e Valutazione (Ambiente IT)							
●		Monitorare e valutare le prestazioni dell'IT			●	●	●
●		Monitorare e valutare i controlli interni	●				●
●		Assicurare la conformità alla normativa			●	●	●
●		Provvedere alla Governance dell'IT	●				●

Appendice C – Controlli generali IT

Ai fini della conformità al Sarbanes-Oxley Act le aziende devono scegliere e implementare un framework funzionale al controllo interno. COSO's Internal Control-Integrated Framework è divenuto il framework più utilizzato dalle aziende conformi ai requisiti Sarbanes-Oxley. Tale strumento, tuttavia, se da una parte fa riferimento all'importanza dell'IT all'interno del più ampio ambiente di controllo, dall'altra non fornisce precise linee guida per il disegno e l'implementazione degli specifici controlli IT necessari.

Nel presente documento, gli obiettivi di controllo IT, i controlli illustrati e i relativi test sono derivati direttamente da COBIT, vedi appendice B.

Ulteriori arricchimenti sono stati mutuati da ISO 17799, The Code of Practice for Information Security Management, e da ITIL, Information Technology Infrastructure Library per la gestione dei servizi informatici. Ma, mentre tutti questi framework includono anche obiettivi finanziari e operativi, ai fini di questa pubblicazione sono stati scelti e adattati solo quelli significativi rispetto al controllo del reporting finanziario.

Controlli Aziendali IT

Normalmente, i controlli generali IT includono obiettivi di controllo sia a livello di aziendale sia di attività. Questa pubblicazione li comprende entrambi e, in particolare, gli obiettivi a livello di azienda sono presentati come "punti di attenzione". Il loro scopo, infatti, è fondamentalmente quello di consentire la comprensione della cultura e dello stile gestionale delle aziende e poiché è poco frequente che ad essi siano associate specifiche attività, il tentativo di definire controlli e test per ogni area a livello aziendale va oltre lo scopo di questa pubblicazione. In definitiva, il presente documento mette a disposizione una serie di possibili considerazioni che, se messe insieme e aggregate, danno la possibilità di esprimere un giudizio complessivo in merito all'efficacia dei controlli a livello aziendale.

Nell'utilizzare questi punti di attenzione le aziende dovrebbero prestare attenzione a non rispondere semplicemente "si" o "no". Lo scopo del questionario è infatti quello di iniziare un confronto che servirà anche a produrre esempi di come vengono effettuati i controlli e come possono venire documentati attraverso evidenze documentali o attraverso domande convalidanti.

Le figure che vanno dalla **11 fino alla 14** contengono alcune considerazioni per la valutazione a livello aziendale dell'ambiente di controllo di un'organizzazione IT. Poiché molte aziende utilizzano COSO per sviluppare i propri programmi di controllo interno, le figure proposte sono state organizzate secondo lo stesso ordine dato dal COSO e i punti di attenzione sono inseriti in maniera da poter stabilire se un obiettivo a livello aziendale è stato raggiunto.

Ambiente di controllo

L'ambiente di controllo predispone le basi per un controllo interno efficace, stabilisce il "limite alto" e rappresenta il vertice della struttura di corporate governance. Le problematiche emerse nella componente ambiente di controllo si estendono attraverso tutta un'organizzazione IT.

Figura 11 - Considerazioni sull'Ambiente di Controllo		
Punti di attenzione	**Referenze COBIT 4.0**	**Risultati/ Evidenze**
Pianificazione Strategica IT		
1. Il management ha preparato piani strategici per l'IT che allineino le strategie IT con gli obiettivi di business? Il processo di pianificazione include meccanismi per sollecitare input dai più importanti stakeholder, esterni e interni, interessati dal piano strategico IT?	PO1.4	
2. La struttura IT comunica i piani IT ai process owner dei processi di business e ad altri importanti attori all'interno dell'azienda?	PO1.2 PO6.5	
3. Il management IT comunica regolarmente le sue attività, sfide e rischi al CEO e CFO? E condivide tali informazioni anche con il Consiglio d'Amministrazione?	PO1.2 PO6.5	
4. L'organizzazione IT monitorizza il costante allineamento dei propri obiettivi con il piano strategico e reagisce opportunamente nella direzione del raggiungimento degli obiettivi stabiliti?	PO1.3 ME1.2	
Processi IT, Organizzazione e Relazioni		
5. I manager IT hanno sufficiente conoscenza ed esperienza per espletare i compiti loro assegnati?	PO7.2 PO7.4	
6. I sistemi e i dati strategici sono stati catalogati e i loro responsabili identificati?	PO4.9	
7. I ruoli e le responsabilità della struttura IT sono stati definiti, documentati e compresi?	PO4.6	
8. Il personale IT capisce e accetta la propria responsabilità riguardo al controllo interno?	PO4.6 PO6.1 ME2.2	
9. La proprietà e la responsabilità riguardo l'integrità dei dati sono state comunicate ai rispettivi owner che hanno accettato tali responsabilità?	PO4.9 PO6.5	
10 . Il management IT ha implementato una divisione dei compiti e responsabilità che diano una ragionevole garanzia che un singolo individuo non possa compromettere un processo critico?	PO4.11	.
Gestire le risorse umane dell'IT		
11. L'organizzazione IT ha adottato e promosso la cultura aziendale riguardo alla gestione dell'integrità, includendo l'etica, le pratiche operative e la valutazione delle risorse umane?	PO6.1 PO7.7	
Istruire e formare gli utenti		
12. Il management IT fornisce formazione e programmi di addestramento continui che includano la condotta etica, le pratiche di sicurezza per i sistemi, gli standard di riservatezza, e le responsabilità sulla sicurezza di tutto il personale?	PO7.4 DS7.1	.

Informazione e Comunicazione

COSO stabilisce che l'informazione è necessaria a tutti i livelli di un'azienda per favorire il business e raggiungere gli obiettivi di controllo dell'azienda. Comunque, l'identificazione, gestione e comunicazione di informazioni strategiche rappresentano per la funzione IT una sempre crescente sfida e sono richieste per raggiungere gli obiettivi di controllo.

La comunicazione, inoltre, deve avvenire in una forma e inquadramento temporale che consentano alle persone destinatarie di svolgere al meglio i propri compiti e supportino anche gli altri quattro componenti di COSO.

Figura 12 Considerazioni su Informazione e Comunicazione		
Punti di attenzione	**Referenze COBIT 4.0**	**Risultati/ Evidenze**
Gestione della comunicazione Obiettivi e Direzioni		
13. Il management IT rivede periodicamente le proprie policy, procedure e standard in maniera da riflettere i cambiamenti delle condizioni di business?	PO6.3	
14. Il management IT possiede un processo per la valutazione della conformità alle proprie policy, procedure e standard?	ME2	
15. Il management IT comprende il proprio ruolo e le proprie responsabilità riguardo al Sarbanes-Oxley Act?	ME3.1 ME3.2	

Risk Assessment

L'attività di risk assessment richiede l'identificazione e l'analisi da parte del management dei rischi significativi per il raggiungimento degli obiettivi prefissati. Questa attività è la base per la determinazione delle attività di controllo. È verosimile che i rischi riguardanti il controllo interno possano essere di più nell'ambito della funzione IT rispetto a un'altra qualsiasi area dell'azienda. Il risk assessment può essere svolto a livello aziendale (per l'intera azienda) o a livello di attività (per uno specifico processo o business unit).

Figura 13 Considerazioni sul Risk Assessment		
Punti di attenzione	**Referenze COBIT 4.0**	**Risultati/ Evidenze**
Valutare e Gestire i rischi IT		
16. La funzione IT possiede un modello di risk assessment a livello aziendale e attività da usare periodicamente per valutare i rischi per il raggiungimento degli obiettivi del reporting finanziario? È consapevole della probabilità e l'eventualità della minaccia ?	PO9.1	
17. Il modello di risk assessment della funzione IT consente di misurare l'impatto del rischio con criteri sia qualitativi sia quantitativi? Vengono utilizzati input da tutte le aree inclusi, ma non limitati a, visione e riflessioni del management (management brainstorming), pianificazione strategica, audit passati e altri assessment?	PO9.2 PO9.3 PO9.4 ME4.5	
18. Laddove i rischi sono considerati accettabili esiste una formale documentazione dell'accettazione del rischio residuale con relative contromisure incluse un'adeguata copertura assicurativa, responsabilità contrattualmente negoziate, auto assicurazione. E nel caso che i rischi non siano stati accettati, il management è in possesso di un piano d'azione che contenga le relative contromisure?	PO9.5 PO9.6	

Monitoraggio

Il monitoraggio, che rileva eventuali punti di debolezza del controllo interno attraverso continui e puntuali processi di valutazione, sta diventando sempre più importante per il management IT.

Figura 14 Considerazioni sul Monitoraggio		
Punti di attenzione	**Referenze COBIT 4.0**	**Risultati/ Evidenze**
Gestire la qualità		
19. Esiste e viene conservata la documentazione riguardante i processi, i controlli e le attività IT?	PO8.2	
20. Esiste un piano della qualità per le principali attività IT (es. sviluppo e implementazione dei sistemi) che fornisca un approccio coerente che si riferisca alle attività di controllo della qualità sia per i progetti generali sia per quelli specifici?	PO8.1 PO8.6	
Monitorare e Valutare la Performance		
21. Il management IT ha stabilito metriche appropriate per gestire le attività quotidiane della funzione IT?	ME 1.2 ME 1.4	
22. Il management IT monitorizza i servizi erogati per identificare eventuali insufficienze e in quel caso è in possesso di piani d'azione per intervenire?	ME 1.2 ME 1.4	
Monitorare e Valutare i Controlli Interni		
23. Il management IT dispone di revisioni indipendenti delle sue attività, incluse policy, procedure su tutti i sistemi e i processi IT e viene valutata l'aderenza a tali policy e procedure?	ME 1.6 ME 2.1 ME 2.5	
24. L'azienda ha a disposizione una funzione di Internal IT Audit responsabile della revisione delle attività e dei controlli IT inclusi i controlli generali e applicativi? Esiste un processo di follow-up per le azioni residuali? È in essere un meccanismo che consenta di monitorare i controlli interni dei fornitori di servizi esterni ?	ME 2.5 ME 2.6 ME 2.7	

Controlli IT a livello di attività

Fornire le informazione necessarie al management per le attività di reportistica e comunicazione agli organi di controllo istituzionali, agli investitori e agli stakeholder fa parte di un ciclo di vita che comprende attività di raccolta completa e accurata di informazioni e relativa sintesi formale (report) su basi temporali adeguate. Come ci si potrebbe aspettare, questo ciclo di vita è fortemente dipendente dai sistemi informativi: applicazioni, database e altri strumenti utilizzati per accrescere l'efficienza e l'efficacia dell'elaborazione dati.

Questa appendice è pensata per fornire una guida riguardo i controlli IT specificamente disegnati per il supporto al raggiungimento degli obiettivi del reporting finanziario.

Come già sottolineato, non si tratterà di una serie esaustiva di controlli né essi sono completamente rappresentativi di tutto ciò che potrebbe essere preso in considerazione da un auditor esterno. In ogni caso, essi forniscono un punto di partenza su come le aziende determinano quali controlli IT sono necessari per il loro sviluppo. Si faranno anche delle considerazioni sui controlli IT che non potranno essere inclusi nelle tabelle seguenti ma che comunque sono ritenuti significativi per le organizzazioni.

Nelle **figure dalla 15 alla 27**, alcuni controlli dei controlli sono evidenziati con una ★ indicante che il controllo in oggetto è un controllo molto importante. Possono essere definiti i controlli interni più significativi applicabili alle poste di bilancio per includere attività che prevengono o individuano e correggono errori significativi del reporting finanziario o altre comunicazioni richieste, incluse quelle relative alla contabilità generale e al libro giornale (standard, non standard e consolidato). I controlli più significativi possono essere manuali o automatici, di natura preventiva o di rilevamento. Questa definizione è stata applicata ai controlli inseriti nelle **figure dalla 15 alla 27** per identificare quelli che sono comunemente richiesti per essere conformi al Sarbanes-Oxley Act. Si noti che nei titoli delle citate figure, gli obiettivi di controllo COBIT sono elencati in parentesi.

Come detto precedentemente, la guida non intende essere prescrittiva. Il giudizio professionale, come sempre, richiede di essere applicato nell'atto di decidere i controlli necessari da inserire nel programma di conformità, inclusi quelli che in questo documento potrebbero essere non compresi tra i più significativi.

Figura 15 - Acquisire e Mantenere il software applicativo (AI2)		
Linee Guide per i Controlli		
Obiettivo di Controllo - I controlli forniscono una ragionevole garanzia che il software applicativo e di sistema acquisito o sviluppato supporti effettivamente i requisiti del reporting finanziario.		
Fondamenti Logici - Il processo di acquisizione e manutenzione del software include il disegno, acquisizione/costruzione e implementazione di sistemi per il raggiungimento degli obiettivi di business. Questo processo include i principali cambiamenti ai sistemi esistenti. Cioè dove i controlli sono disegnati e implementati per supportare l'inserimento, la registrazione, l'elaborazione e la pubblicazione delle informazioni finanziarie. Eventuali carenze in questa area hanno un significativo impatto sulle fasi di reporting e pubblicazione di dati finanziari. Per esempio, senza sufficiente controllo sui processi di interfacciamento tra le applicazioni, le informazioni finanziarie potrebbero risultate non accurate o incomplete.		
Controlli Illustrati	**Test illustrati dei controlli**	**Referenze COBIT 4.0**
L'azienda ha una metodologia del ciclo di vita di sviluppo dei sistemi (SDLC) che include i requisiti di integrità dei processi e sicurezza dell'azienda. ★	Ottenere la metodologia SDLC dell'azienda. Rivederla per stabilire se include i requisiti di integrità dei processi e sicurezza. Valutare se esiste un numero adeguato di passi atti a determinare se detti requisiti sono tenuti in conto lungo il ciclo di vita di sviluppo o acquisizione; p.es. la sicurezza e l'integrità dei processi vengono considerati durante la fase di individuazione dei requisiti.	PO8.3 AI2.3 AI2.4
Le procedure e policy SDLC dell'azienda considerano lo sviluppo e acquisizione di nuovi sistemi e le principali modifiche ai sistemi esistenti.	Rivedere la metodologia SDLC dell'azienda per determinare se vengono considerati lo sviluppo e le acquisizioni di nuovi sistemi e le principali modifiche ai sistemi esistenti.	PO6.3 AI2 AI6.2
Nella metodologia SDLC è previsto che i sistemi informativi siano disegnati in modo da includere i controlli applicativi che supportino la gestione di transazioni in maniera completa, accurata, autorizzata e valida. ★	Rivedere la metodologia SDLC per determinare se essa prevede controlli applicativi. Valutare se esistono i necessari passi che fan si che i controlli applicativi siano considerati lungo tutto il ciclo di vita di vita, di sviluppo o acquisizione, del software; per esempio, i controlli applicativi dovrebbero essere inclusi nelle fasi di disegno sia concettuale sia di dettaglio.	AI1 AI2.3 AC
L'azienda possiede un processo di acquisizione e pianificazione che risulta essere in linea con la strategia complessiva.	Rivedere la metodologia SDLC per determinare se viene presa in considerazione la strategia complessiva dell'azienda, per esempio, un comitato guida IT dovrebbe rivedere e approvare i progetti in maniera tale da renderli allineati con i requisiti di business strategici e che utilizzino tecnologie approvate.	PO4.3 AI3.1
Per mantenere uno sviluppo affidabile, il management IT coinvolge gli utenti nel disegno delle applicazioni, nella scelta dei software e nelle fasi di test. ★	Rivedere la metodologia SDLC per determinare se gli utenti sono correttamente coinvolti nel disegno delle applicazioni, scelta delle soluzioni applicative e relativi test..	AI1 AI2.1 AI2.2 AI7.2
Attività di revisione post-implementazione sono svolte per verificare che i controlli operino correttamente	Determinare se le verifiche post-implementazione sono effettuate sui nuovi sistemi e sulle modifiche dichiarate significative.	AI7.2
L'azienda acquisisce/sviluppa applicativi secondo il proprio processo di acquisizione, sviluppo e pianificazione. ★	Selezionare un campione di progetti finalizzati all'implementazione di nuovi sistemi finanziari. Rivedere la documentazione e i rilasci di questi progetti per valutare se essi sono stati eseguiti secondo i processi di acquisizione, sviluppo e pianificazione.	AI2

Figura 16 - Acquisire e Mantenere l'Infrastruttura tecnologica (AI3)		
Linee Guide per i Controlli		
Obiettivo di Controllo - I controlli forniscono una ragionevole garanzia che l'infrastruttura tecnologica acquisita fornisce le piattaforme adatte a supportare le applicazioni utilizzate per produrre il reporting finanziario.		
Fondamenti Logici - Il processo di acquisizione e manutenzione dell'infrastruttura tecnologica include il disegno/sviluppo e implementazione dei sistemi che supportano applicazioni e le comunicazioni. I componenti dell'infrastruttura, inclusi server, reti di telecomunicazione e database, sono critici per l'elaborazione sicura e affidabile delle informazioni. Senza un'adeguata infrastruttura aumenta il rischio che le applicazioni utilizzate per produrre il reporting finanziario non consentano l'interazione tra applicazioni, che queste non funzionino e che difetti nelle infrastrutture critiche non siano scoperti tempestivamente.		
Controlli Illustrati	**Test illustrati dei controlli**	**Referenze COBIT 4.0**
Esistono procedure documentate e sono seguite in maniera tale che le infrastrutture, incluse le apparecchiature di rete e il software, siano acquisite sulla base dei requisiti delle applicazioni finanziarie che devono supportare.	Selezionare un campione di sistemi infrastrutturali implementati. Rivedere la documentazione e i risultati prodotti dal progetto per determinare se i requisiti infrastrutturali sono stati considerati tempestivamente durante il processo di acquisizione.	AI3

Figura 17 - Permettere il funzionamento dei sistemi IT (PO6, PO8, AI6, DS13)		
Linee Guide per i Controlli		
Obiettivo di Controllo - I controlli forniscono una ragionevole garanzia che le policy e le procedure che definiscono i processi di acquisizione e manutenzione sono state sviluppate e sono mantenute e che in esse è presente la documentazione necessaria a supportare il corretto utilizzo delle applicazioni e delle soluzioni tecnologiche in essere.		
Fondamenti Logici - Policy e procedure includono la metodologia SDLC e il processo di acquisizione, sviluppo e manutenzione delle applicazioni così come la necessaria documentazione. Per alcune organizzazioni, policy e procedure includono service level agreement, pratiche operative e materiale formativo. Policy e procedure supportano l'impegno di un'azienda nella realizzazione, in maniera coerente e obiettiva, delle attività legate ai processi di business.		
Controlli Illustrati	**Test illustrati dei controlli**	**Referenze COBIT 4.0**
L'azienda possiede policy e procedure riguardo allo sviluppo di programmi, modifica degli stessi, accesso a programmi e dati e ai processi informatizzati; esse vengono periodicamente riviste, aggiornate e approvate dal management. ★	Confermare che l'azienda possiede policy e procedure che vengono periodicamente riviste e aggiornate sulla base dei cambiamenti di business. Quando le policy e le procedure sono cambiate, verificare che il management abbia approvato le modifiche. Selezionare un campione di progetti e determinare che i manuali a disposizione degli utenti, la documentazione sui sistemi e sull'operatività siano disponibili. Considerare se bozze di questi manuali sono presenti nei test di accettazione degli utenti. Determinare se qualsiasi modifica ai controlli previsti risulta dagli aggiornamenti alla documentazione.	PO6.1 PO6.3 PO8.1 PO8.2 PO8.3 AI6.1 DS13.1

Figura 17 - Permettere il funzionamento dei sistemi IT (PO6, PO8, AI6, DS13) (*segue*)		
Linee Guide per i Controlli		
L'azienda sviluppa, mantiene e fa funzionare i propri sistemi e applicazioni in conformità con le policy e procedure supportate e documentate. ★	Ottenere le policy e procedure e determinare se l'azienda gestisce l'ambiente IT in conformità ad esse.	PO6.1 PO6.3 PO8.1 PO8.2 PO8.3 AI6.1 DS13.1

Figura 18 - Installare e certificare le soluzioni e le modifiche (AI7)		
Linee Guide per i Controlli		
Obiettivo di Controllo - I controlli forniscono una ragionevole garanzia che i sistemi sono correttamente testati e validati prima di essere immessi nell'ambiente di produzione e che i controlli associati operano come previsto e supportano i requisiti dell'attività di reporting finanziario.		
Fondamenti Logici - Il processo di installazione, test e validazione si applica alla migrazione dei nuovi sistemi nell'ambiente di produzione. Prima della installazione, appropriate fasi di test e validazione devono essere eseguite per verificare se i sistemi operano come previsto a livello di disegno. Senza test adeguati i sistemi possono non funzionare come previsto, e possono produrre informazioni non valide in particolare nell'ambito del reporting finanziario.		
Controlli Illustrati	**Test illustrati dei controlli**	**Referenze COBIT 4.0**
Viene sviluppata e applicata una strategia di test per tutte le modifiche significative che riguardano applicazioni e infrastrutture tecnologiche (e che comprende test di unità, di sistema, di integrazione e di accettazione) di modo che i sistemi implementati operino come previsto. ★	Selezionare un campione di progetti di sviluppo e aggiornamenti significativi di sistemi (inclusi aggiornamenti tecnologici). Determinare se è preparata e seguita una strategia formale di test. Valutare se la stessa strategia considera i potenziali rischi legati a sviluppi e implementazioni e coinvolge tutte le risorse necessarie per concentrarsi su questi rischi; p.es. se la completezza e l'accuratezza delle interfacce sono essenziali per assicurare la produzione di una completa e accurata reportistica, queste interfacce devono essere incluse nella strategia di test. (Nota: I controlli sul passaggio finale in produzione sono presenti in **figura 19** - Gestire le modifiche.)	AI7.2 AI7.4 AI7.6 AI7.7
I test di carico e stress sono eseguiti secondo un piano e standard di test prestabiliti.	Selezionare un campione di progetti di sviluppo e aggiornamento sistemi significativi per le attività di reporting finanziario. Laddove la capacità e la performance sono considerate potenzialmente importanti, analizzare l'approccio del test di carico e stress. Considerare se è stato utilizzato un approccio strutturato per i test di carico e stress e se tale approccio si basa su modelli adeguati riguardo i volumi previsti, i tipi di transazioni processate, e l'impatto sugli altri servizi che funzionano contemporaneamente.	AI7.2

Figura 18 - Installare e certificare le soluzioni e le modifiche (AI7) (segue)		
Linee Guide per i Controlli		
Le interfacce con gli altri sistemi sono testate per confermare che le trasmissioni di dati sono complete, accurate e valide. ★	Selezionare un campione di progetti di sviluppo e aggiornamento sistemi significativi per le attività di reporting finanziario. Determinare se le interfacce con gli altri sistemi sono state testate per confermare che le trasmissioni di dati sono complete, p.es. se i totali per record sono accurati e validi. Considerate se l'estensione dei test è stata sufficiente e ha incluso il recupero dei casi di interruzione nella trasmissione dei dati.	AI7.5
La conversione dei dati è testata tra l'origine e la destinazione degli stessi per confermare la loro completezza, accuratezza e validità. ★	Selezionare un campione di progetti di sviluppo e aggiornamento sistemi significativi per le attività di reporting finanziario. Determinare se la strategia di conversione è stata documentata. Se include inoltre strategie per la pulizia o per lo scarico dei dati dei vecchi sistemi prima della conversione. Analizzare il piano di test di conversione.	AI7.5

Figura 19 – Gestione delle Modifiche (AI6, AI7)		
Linee Guida per i Controlli		
Obiettivi di Controllo – I controlli forniscono la ragionevole certezza che modifiche significative ai sistemi di reporting finanziario siano autorizzate e adeguatamente testate prima di essere avviate in produzione.		
Fondamenti Logici – La gestione delle modifiche si riferisce al modo in cui un'azienda modifica le funzionalità dei sistemi per supportare il business a raggiungere gli obiettivi del reporting finanziario. Carenze in quest'area potrebbero impattare significativamente sul reporting finanziario. Ad esempio, le modifiche ai programmi di contabilizzazione richiedono adeguate approvazioni e test preliminari all'attuazione delle modifiche, per assicurare la corretta classificazione dei dati e l'integrità del reporting.		
Obiettivo di controllo	**Verifiche**	**Riferimenti COBIT 4.0**
Verificare che le richieste per modifiche ai programmi, variazioni ai sistemi e loro manutenzione (comprese le modifiche al software di sistema) seguano uno standard, siano tracciate, approvate, documentate e soggette a procedure formali per la gestione delle modifiche. ★	Verificare l'esistenza di un documentato processo di gestione, aggiornato ai processi correnti. Verificare che esistano procedure di gestione delle modifiche per tutte le variazioni da apportare all'ambiente di produzione, incluse modifiche ai programmi, manutenzione dei sistemi e modifiche alle infrastrutture. Valutare il processo utilizzato per controllare e monitorare le richieste di modifiche. Verificare che le richieste di modifiche siano correttamente avviate, approvate e tracciate. Verificare che le modifiche ai programmi siano effettuate in un ambiente separato e controllato. Selezionare un campione di modifiche realizzate su applicazioni/sistemi per verificare che siano state adeguatamente testate e approvate prima di essere rilasciate nell'ambiente di produzione. Verificare che il management delle seguenti funzioni sia coinvolto nel processo di approvazione al passaggio in produzione (gestione sistemi / esercizio), sicurezza, gestione dell'infrastruttura IT, responsabile IT. Verificare le procedure disegnate per assicurare che solo modifiche autorizzate/approvate siano passate in produzione. Per un campione di modifiche, tracciare i log delle richieste di modifica e la documentazione a supporto. Verificare che le procedure soddisfino una tempestiva implementazione delle "patch" per i sistemi software. Selezionare un campione per verificare la conformità con le procedure documentate.	AI6.1 AI6.2 AI6.4 AI6.5 AI7.3 AI7.8 AI7.9 AI7.10 AI7.11

Figura 19 – Gestione delle Modifiche (AI6, AI7) (*segue*)		
Linee Guida per i Controlli		
Obiettivo di controllo	**Verifiche**	**Riferimenti COBIT 4.0**
Le richieste di modifica di emergenza sono documentate e soggette a procedure di gestione delle modifiche formali. ★	Verificare l'esistenza di un processo per controllare e supervisionare le modifiche di emergenza. Verificare l'esistenza di "tracce di audit" per tutte le attività di emergenza e che esse siano controllate in modo indipendente. Verificare che le procedure richiedano che le modifiche di emergenza siano supportate da adeguata documentazione. Verificare che per le modifiche di emergenza siano implementate procedure ripristino della situazione precedente (back-out). Verificare che le procedure assicurino che tutte le modifiche di emergenza siano testate e soggette alle procedure standard di approvazione dopo essere state implementate. Su un campione di modifiche classificate come di "emergenza" svolgere le seguenti verifiche: - presenza delle necessarie approvazioni; - blocco degli accessi eventualmente utilizzati per l'emergenza, dopo un determinato periodo di tempo; - adeguatezza della documentazione per l'intero campione di modifiche selezionato.	AI6.3 AI7.10
Sono attivati controlli che consentono solo a personale autorizzato di trasferire i programmi in produzione. ★	Verificare le approvazioni necessarie per trasferire un programma in produzione. Verificare che ci siano le approvazioni degli owner del sistema, del team di sviluppo e dell'esercizio dei sistemi. Verificare che ci sia un'adeguata separazione dei compiti tra lo staff responsabile di trasferire un programma in produzione e lo staff di sviluppo. Richiedere e verificare le evidenze documentali a supporto.	AI7.8
Il management IT implementa i sistemi software in modo che non creino condizioni di rischio per la sicurezza di dati e programmi memorizzati sui sistemi a causa della difformità di approccio introdotta dalle modifiche.	Verificare che sia stata effettuata un'analisi dei rischi degli impatti potenziali delle modifiche sul software di sistema. Verificare le procedure che garantiscono i test delle modifiche ai sistemi in un ambiente di sviluppo prima che siano trasferiti in produzione. Verificare l'esistenza di procedure di back out (ripristino della situazione precedente).	AI6.2 AI7.4 AI7.9

Figura 20 – Definizione e gestione dei Livelli di Servizio (DS1)

Linee Guida per i Controlli

Obiettivi di controllo – I controlli forniscono la ragionevole certezza che i livelli di servizio siano definiti e gestiti in modo sia da soddisfare i requisiti dei sistemi di reporting finanziario, sia da fornire una comune conoscenza aziendale dei livelli di servizio con cui sarà misurata la qualità dei servizi medesimi.

Fondamenti logici – Il processo di definizione e gestione dei livelli di servizio riguarda come un'azienda raggiunga le aspettative funzionali e operative dei suoi utenti e, in ultima analisi, gli obiettivi di business. Sono definiti ruoli e responsabilità ed è utilizzato un modello di misura per assicurare che i servizi siano erogati come richiesto. Carenze in quest'area potrebbero impattare significativamente sul reporting finanziario e sulla diffusione di informazioni che riguardano l'azienda. Ad esempio, se i sistemi sono gestiti non adeguatamente o se le loro funzionalità non sono sviluppate in aderenza ai requisiti, le informazioni finanziarie potrebbero non essere elaborate come previsto.

Obiettivo di controllo	Verifiche	Riferimenti COBIT 4.0
I livelli di servizio sono definiti e gestiti per supportare i requisiti dei sistemi di reporting finanziario.	Estrarre un campione di SLA (service level agreement – accordo sul livello di servizio) e verificare che contengano una chiara definizione del servizio e delle attese degli utenti. Discutere con esponenti dell'azienda responsabili per la gestione dei livelli di servizio e verificare i dati oggettivi per determinare se i livelli di servizio sono gestiti proattivamente. Ottenere e analizzare le evidenze che i livelli di servizio siano adeguatamente gestiti in coerenza con gli SLA. Analizzare con gli utenti se i sistemi per il reporting sui dati finanziari sono stati sviluppati e consegnati in accordo alle loro aspettative ed agli accordi sui livelli di servizio.	DS1.2 DS1.3 DS1.5 DS1.6
È definito un modello per stabilire appropriati indicatori di performance per la gestione dei livelli di servizio, sia interni come esterni	Richiedere i report sulle performance dei livelli di servizio e accertarsi che essi contengano gli indicatori chiave di performance. Rivedere le evidenze sulle performance, identificare le carenze e verificare come i responsabili della gestione dei livelli di servizio stiano operando al fine di colmare tali carenze.	DS1.1 DS1.3

Figura 21 – Gestione del Servizio da terze parti (DS2)		
Linee Guida per i Controlli		
Obiettivi di controllo – I controlli forniscono la ragionevole certezza che i servizi di terze parti siano sicuri, accurati e disponibili, supportando l'integrità dei processi e che siano appropriatamente definiti in contratti che ne indichino le performance		
Fondamenti logici – La gestione dei servizi da terze parti comprende l'utilizzo in outsourcing di service provider a supporto delle applicazioni finanziarie e dei relativi sistemi. Carenze in tale area potrebbero impattare in maniera significativa sul reporting finanziario e successiva comunicazione.(disclosure). Per esempio, controlli insufficienti sull'accuratezza dei processi gestiti da terze parti potrebbero generare dati finanziari non accurati.		
Obiettivo di controllo	**Verifiche**	**Riferimenti COBIT 4.0**
È definito un responsabile per il monitoraggio costante e il reporting sul raggiungimento degli obiettivi di performance dei servizi forniti da terze parti.	Verificare se le responsabilità sulla gestione dei servizi di terze parti siano state assegnate in modo individuale e idoneo.	DS2.2
La selezione dei fornitori di servizi (outsourcer) è svolta in accordo alle policy aziendali sulla scelta dei fornitori.	Richiedere le policy aziendali sulla gestione dei fornitori e chiedere ai responsabili della gestione dei servizi forniti da terze parti se tali standard siano effettivamente seguiti. Richiedere evidenze e verificare che la selezione dei fornitori di servizi sia effettuata in accordo con gli standard aziendali.	PO1.4 PO6.3 DS2
I responsabili IT dovrebbero verificare, prima della selezione, che i potenziali fornitori siano effettivamente classificati attraverso la valutazione delle loro capacità di fornire i servizi richiesti e della loro solidità finanziaria	Richiedere i criteri e le referenze (business case) utilizzati per la selezione degli outsourcer. Verificare che tali criteri includano una valutazione: - della stabilità finanziaria del fornitore - esperienza e conoscenza sui sistemi oggetto di fornitura - controlli sulla riservatezza e integrità dei processi	DS2.3
I contratti per la fornitura di servizi definiscono e comprendono i rischi, i controlli e le procedure di sicurezza per i sistemi informativi e le reti	Selezionare un campione di contratti di fornitura dei servizi e verificare se includano controlli per garantire riservatezza e integrità dei processi in accordo con le policy e le procedure aziendali.	DS2.3

Figura 21 – Gestione del Servizio da terze parti (DS2) (*segue*)		
Linee Guida per i Controlli		
Obiettivi di Controllo	**Verifiche**	**Riferimenti COBIT 4.0**
Dovrebbero essere definite e messe in atto procedure che richiedano che per tutti i servizi forniti da terze parti sia definito e concordato un contratto formale prima dell'inizio della fornitura; tali contratti dovrebbero includere inoltre la definizione dei requisiti di controllo interno e l'accettazione di policy e procedure aziendali.	Analizzare un campione di contratti e verificare se: ▸ I servizi forniti sono ben definiti ▸ Sono state ben definite le responsabilità per i controlli sui sistemi che generano il reporting finanziario. I fornitori hanno accettato di aderire alle policy e procedure aziendali, in particolare a quelle di sicurezza ▸ I contratti sono stati verificati e firmati dalle parti prima dell'inizio della fornitura ▸ I controlli sui sistemi e sottosistemi che generano il report finanziario descritti nei contratti sono allineati a quelli richiesti dalla azienda. Analizzare le eventuali discrepanze e valutare la possibilità di eseguire ulteriori analisi per determinare l'impatto sul reporting finanziario.	DS2.3
Dovrebbero essere effettuate dai fornitori di servizi regolari verifiche sulla riservatezza e integrità dei processi (per es. SAS 70, Canadian 5970 e ISA 402) ★	Verificare se i fornitori eseguano verifiche indipendenti sulla riservatezza, disponibilità e integrità dei processi (p.es. attraverso report di audit). Richiedere un campione delle più recenti verifiche effettuate e individuare eventuali carenze di controllo che potrebbero avere impatto sul reporting finanziario.	ME2.6

Figura 22 – Assicurare la sicurezza dei sistemi (DS5)

Linee Guida per i Controlli

Obiettivi di controllo – I controlli forniscono la ragionevole certezza che i sistemi e sottosistemi che generano il reporting finanziario siano appropriatamente protetti al fine di prevenire uso non autorizzato, divulgazione, modifica, danneggiamento o perdita di dati

Fondamenti logici – La gestione della sicurezza dei sistemi include controlli sia fisici sia logici che prevengano l'accesso non autorizzato. Questi controlli tipicamente supportano l'autorizzazione, l'autenticazione, il non ripudio, la classificazione dei dati e il monitoraggio sulla sicurezza. Carenze in quest'area potrebbero impattare in maniera significativa sul reporting finanziario di un'azienda. Per esempio, controlli insufficienti sulle autorizzazioni alle transazioni finanziarie potrebbero generare report finanziari non accurati.

Obiettivi di controllo	Verifiche	Riferimenti COBIT 4.0
Esiste una policy sulla sicurezza informatica ed è approvata da un appropriato livello di management ★	Richiedere una copia della policy sulla sicurezza informatica e valutarne l'efficacia. In particolare verificare se: ▸ È stata chiaramente definita l'importanza della sicurezza nell'azienda? ▸ Sono stati ben definiti gi obiettivi di sicurezza? ▸ Le responsabilità in materia di sicurezza dei dipendenti e fornitori sono state ben identificate? ▸ La policy è stata approvata da un appropriato livello di management a dimostrazione dell'attenzione del management verso la sicurezza? ▸ Esiste una procedura per la comunicazione e diffusione della policy a tutti i livelli dell'azienda (management e dipendenti)?	PO6.3 PO6.5 DS5.2
Dovrebbe essere sviluppato una struttura di standard di sicurezza per supportare gli obiettivi della policy di sicurezza	Richiedere una copia degli standard di sicurezza. Verificare se gli standard corrispondano effettivamente agli obiettivi della policy di sicurezza. Verificare se i seguenti elementi – in genere definiti negli standard di sicurezza – siano appropriatamente coperti: ▸ Organizzazione della sicurezza ▸ Ruoli e responsabilità ▸ Sicurezza fisica e ambientale ▸ Sicurezza dei sistemi operativi ▸ Sicurezza delle reti ▸ Sicurezza delle applicazioni ▸ Sicurezza delle basi dati Verificare se siano state messe in atto procedure per la comunicazione e manutenzione di tali standard	PO8.2 DS5.2

Figura 22 – Assicurare la sicurezza dei sistemi (DS5) (*segue*)		
Linee Guida per i Controlli		
Obiettivo di Controllo	**Verifiche**	**Riferimenti COBIT 4.0**
Dovrebbe essere definito un piano di sicurezza informatica in accordo con i piani strategici IT.	Ottenere una copia dei piani o delle strategie di sicurezza per i sistemi e sottosistemi di reporting finanziario e valutarne l'adeguatezza in relazione ai piani generali dell'azienda.	DS5.2
Il piano di sicurezza informatica viene aggiornato riflettendo i cambiamenti sia nell'ambiente IT, sia nei requisiti di sicurezza per specifici sistemi.	Verificare che i piani di sicurezza riflettano gli specifici requisiti di sicurezza dei sistemi e sottosistemi di reporting finanziario.	DS5.2
Dovrebbero essere definite e messe in atto procedure per l'autenticazione di tutti gli utenti dei sistemi (sia interni sia esterni) al fine di supportare la validità delle transazioni. ★	Valutare il meccanismo di autenticazione per i sistemi e i sottosistemi di reporting finanziario e il meccanismo che assicura il time out delle sessioni di lavoro dopo un certo periodo di tempo. Verificare che non siano utilizzate user ID condivise (comprese le utenze amministrative).	DS5.3 AC
Dovrebbero essere definite e messe in atto procedure che garantiscano l'efficacia dei meccanismi di autenticazione e accesso (es. periodico cambiamento delle password) ★	Verificare che i controlli di autenticazione (password, user ID, autenticazione a due fattori…) siano messi in pratica in modo appropriato e siano soggetti a requisiti di confidenzialità (ID e password non condivise, password di tipo alfanumerico…).	DS5.3 DS5.4
Dovrebbero essere definite e messe in atto procedure per assicurare azioni tempestive relative a richieste, definizione, creazione, sospensione ed eliminazione di user account (comprese le procedure per l'autenticazione di transazioni generate al di fuori dell'azienda) ★	Verificare che esistano e siano messe in atto procedure per la periodica registrazione, cambiamento e cancellazione degli utenti dai sistemi e sottosistemi che generano il reporting finanziario. Selezionare un campione di nuovi utenti e determinare se l'accesso è stato autorizzato dal management e se il profilo di accesso definito sia conforme ai privilegi di accesso approvati. Selezionare un campione di ex dipendenti e verificare che il loro accesso sia stato inibito e che tale azione sia stata effettuata tempestivamente. Selezionare un campione di utenti attivi, sia privilegiati sia standard, e verificare che le loro credenziali di accesso siano coerenti con le loro funzioni.	DS5.4

Figura 22 – Assicurare la sicurezza dei sistemi (DS5) (*segue*)		
Linee Guida per i Controlli		
Obiettivo di Controllo	**Verifiche**	**Riferimenti COBIT 4.0**
Dovrebbe essere definita e messa in atto una procedura di controllo per la verifica periodica dei diritti di accesso. ★	Verificare che i controlli di accesso per i sistemi e sottosistemi che generano il reporting finanziario siano implementati e rivisti periodicamente dal management. Valutare l'adeguatezza del processo di come le eccezioni sono riesaminate e se i follow-up sono effettuati tempestivamente.	DS5.4
Dove applicabile, dovrebbero essere definiti e implementati controlli per assicurare che nessuna delle parti possa rifiutare le transazioni; deve essere attivato un controllo per il non ripudio sia da parte del mittente sia da parte del destinatario delle transazioni.	Analizzare quali sono i sistemi usati dall'azienda per l'identificazione della responsabilità per l'iniziazione e approvazione delle transazioni. Testare l'uso dei controlli della responsabilità osservando un utente che tenta di introdurre una transazione non autorizzata. Selezionare un campione di transazioni e identificare responsabilità e origine di ciascuna.	DS11.6 AC AC
Sono presenti e sono attivi appropriati controlli, inclusi firewall, sistemi di intrusion detection e vulnerability assessment, al fine di prevenire accessi non autorizzati dalla rete pubblica.	Verificare se i controlli di sicurezza perimetrale (inclusi firewall e sistemi di intrusion detection) siano sufficienti e appropriati. Chiedere se il management ha fatto eseguire revisioni indipendenti sui controlli negli ultimi anni (es. hacking etico, prove di social engineering…). Richiedere una copia dei risultati di tali interventi e analizzare le evidenze, incluse le necessità di follow-up sulle carenze identificate. Verificare che siano utilizzati sistemi antivirus per proteggere integrità e riservatezza dei sistemi e sottosistemi che generano il reporting finanziario. Dove appropriato, verificare se siano utilizzate tecniche di crittografia per supportare la riservatezza delle informazioni finanziarie inviate da un sistema a un altro.	DS5.10

Figura 22 – Assicurare la sicurezza dei sistemi (DS5) (*segue*)		
Linee Guida per i Controlli		
Obiettivo di controllo	**Verifiche**	**Riferimenti COBIT 4.0**
L'amministrazione della sicurezza IT tiene sotto controllo e registra le attività di sicurezza a livello di sistema operativo, base dati e applicativi, e le violazioni di sicurezza rilevate sono riportare alla direzione. ★	Verificare l'esistenza di un ufficio sicurezza che tenga sotto controllo le vulnerabilità di sicurezza a livello applicativo e di base dati e le minacce correlate. Valutare la natura e l'estensione di tali eventi dannosi accaduti nel corso dell'ultimo anno e discutere con il management sul modo in cui ha reagito attraverso i controlli per prevenire accessi non autorizzati o manipolazioni di sistemi o sottosistemi finanziari. Verificare che i tentativi di accesso non autorizzato ai sistemi e sottosistemi che generano il reporting finanziario siano tracciati e i report di log verificati periodicamente.	DS5.5
Esistono e sono attuati i controlli relativi all'appropriata separazione dei compiti nelle fasi di richiesta e di concessione dell'accesso ai sistemi e ai dati. ★	Analizzare il processo di richiesta e di concessione all'accesso ai sistemi e ai dati e accertare che la stessa persona non possa eseguire entrambe le funzioni.	DS5.3 DS5.4
L'accesso all'infrastruttura IT è ristretto al personale autorizzato e prevede un'appropriata procedura di identificazione e autenticazione.	Ottenere le policy e le procedure relative alla sicurezza degli impianti, chiavi e lettori di carte di accesso e determinare se tali procedure operano correttamente nelle fasi di identificazione e autenticazione. Osservare il traffico in entrata e uscita da e per gli impianti IT aziendali al fine di stabilire che l'accesso sia correttamente controllato. Selezionare un campione di utenti e determinare se il loro accesso è coerentemente concesso a fronte delle responsabilità della loro funzione.	DS12.2 DS12.3

Figura 23 – Gestire la configurazione (DS9)		
Linee Guida per i Controlli		
Obiettivi di controllo - I controlli forniscono la ragionevole certezza che le componenti IT, per la parte inerente alla sicurezza e all'elaborazione sono ben protetti; potrebbero prevenire ogni modifica non autorizzata ed essere di supporto nella verifica e nella registrazione della configurazione corrente.		
Fondamenti logici - La gestione della configurazione include procedure che mirano ad assicurare che i controlli sulla sicurezza e integrità delle elaborazioni siano implementati nei sistemi e mantenuti nel tempo con appropriato ciclo di vita. Controlli insufficienti sulle configurazioni possono portare a esposizioni in materia di sicurezza che possono comportare accessi non autorizzati ai sistemi e ai dati e avere di conseguenza impatto sul reporting finanziario. Un ulteriore rischio potenziale è la perdita dell'integrità dei dati derivante da carenze di controllo sulla configurazione durante le modifiche o tramite l'introduzione di componenti di sistema non autorizzate.		
Obiettivo di controllo	**Verifiche**	**Riferimenti COBIT 4.0**
E' permesso l'uso solo di software autorizzato da parte del personale che utilizza strumenti IT aziendali.	Stabilire se sono poste in essere procedure per rilevare e prevenire l'uso di software non autorizzato. Ottenere e riesaminare la policy dell'azienda relativamente all'uso del software per verificare che sia chiara e ben formulata. Prendere in considerazione un campione di applicazioni e di computer per determinare se sono conformi alla policy aziendale.	DS9.2
L'infrastruttura di sistema, compresi i firewall, router, switch, sistemi operativi di rete, server e gli altri relativi dispositivi, è correttamente configurata per prevenire accessi non autorizzati.	Stabilire se la policy aziendale prevede la documentazione della configurazione corrente, come pure i parametri di sicurezza da implementare. Riesaminare un campione di server, firewall, router ecc. per verificare se gli stessi sono stati configurati secondo quanto stabilito dalla policy aziendale.	DS5.3 DS5.4 DS5.10
Il software applicativo e i sistemi di memorizzazione dei dati sono opportunamente configurati ai fini di un accesso individuale basato sulla provata necessità di visionare, aggiungere, modificare o cancellare i dati. ★	Effettuare una valutazione sulla frequenza e la tempestività delle revisioni, da parte del management, delle registrazioni della configurazione. Valutare se il management ha documentato le procedure di gestione della configurazione. Riesaminare un campione delle modifiche, aggiunte o cancellazioni alla configurazione, per determinare se sono state approvate in base a una comprovata necessità.	DS5.4

Figura 23 – Gestire la configurazione (DS9) (*segue*)		
Linee Guida per i Controlli		
Obiettivo di controllo	**Verifiche**	**COBIT 4.0**
Il management IT ha stabilito delle procedure aziendali per proteggere il sistema informativo e l'infrastruttura tecnologica dell'azienda dai virus.	Riesaminare le procedure aziendali previste per la rilevazione dei virus. Verificare che l'azienda abbia installato e stia utilizzando software antivirus nelle proprie reti e nei personal computer.	DS5.9
Viene periodicamente effettuato il test e la valutazione per confermare che il software e l'infrastruttura di rete sono configurati in modo appropriato.	Riesaminare il software e l'infrastruttura di rete per stabilire la loro appropriata configurazione e mantenimento, in accordo con il relativo processo aziendale documentato.	AI3.2 AI3.3

Figura 24 – Gestire i problemi e gli incidenti (DS8, DS10)		
Linee Guida per i Controlli		
Obiettivi di controllo I controlli forniscono la ragionevole certezza che ogni problema e/o incidente genererà una pronta risposta, sarà registrato, risolto o investigato al fine di ottenerne un'adeguata soluzione.		
Fondamenti logici Il processo di gestione dei problemi e degli incidenti indica il modo in cui un'azienda identifica, documenta e reagisce agli eventi che sono al di fuori della normale operatività. Le carenze in quest'area potrebbero impattare in modo significativo sul reporting finanziario dell'azienda.		
Obiettivo di controllo	**Verifiche**	**COBIT 4.0**
Il management IT ha definito e implementato un sistema di gestione degli incidenti e dei problemi per assicurare che gli eventi operativi che non rientrano nell'operatività ordinaria (incidenti, problemi ed errori) siano registrati, analizzati e risolti in modo tempestivo. ★	Stabilire se esiste il sistema di gestione degli incidenti, e il modo in cui è utilizzato. Riesaminare come il management ha documentato le modalità di utilizzo del sistema. Riesaminare un campione di report relativi a incidenti, per verificare se le problematiche sono state affrontate (registrate, analizzate e risolte) in modo tempestivo.	DS8
Il sistema di gestione dei problemi fornisce adeguati strumenti per le tracce di audit che consentono di tracciare l'accaduto dall'incidente alla causa scatenante.	Stabilire se le procedure aziendali includono strumenti per le tracce di audit – localizzazione/tracciatura dei problemi o degli incidenti. Riesaminare un campione di problemi registrati nel sistema di gestione dei problemi per verificare se sono previste e sono utilizzate appropriate tracce di audit.	DS10.2
Esiste un processo di reazione agli incidenti di sicurezza al fine di supportare tempestivamente risposta e indagini su attività non autorizzate.	Verificare che vi siano reazioni tempestive a fronte di tutte le attività non autorizzate e l'esistenza di un processo che preveda adeguate disposizioni.	DS5.6 DS8.3 DS10.1 DS10.3

Figura 25 – Gestire i dati (DS11)		
Linee Guida per i Controlli		
Obiettivi di controllo: I controlli forniscono la ragionevole certezza che i dati registrati, elaborati e resi disponibili rimangono completi, accurati e validi durante il processo di modifica e memorizzazione.		
Fondamenti logici. La gestione dei dati comprende anche i controlli e le procedure usati per mantenere l'integrità delle informazioni, includendo criteri di completezza, accuratezza, autorizzazione. I controlli sono disegnati per supportare la generazione, la registrazione, l'elaborazione e la messa a disposizione di informazioni finanziarie. Carenze in quest'area potrebbero impattare in modo significativo sul reporting finanziario. Per esempio, in mancanza di appropriati controlli di autorizzazione sulla generazione delle transazioni, le informazioni finanziarie risultanti potrebbero non essere attendibili.		
Obiettivo di controllo	**Verifiche**	**COBIT 4.0**
Esistono policy e procedure per la distribuzione e la conservazione dei dati e dei documenti di output.	Riesaminare le policy e le procedure per la distribuzione e la conservazione dei dati e dei documenti di output. Determinare se le policy e le procedure sono adeguate per la protezione dei dati e assicurano la tempestiva distribuzione di tutto il reporting finanziario corretto (inclusi i documenti in formato elettronico) al personale appropriato. Ottenere e verificare le evidenze dell'esistenza di controlli, operanti efficacemente, in materia di protezione dei dati e sulla tempestiva distribuzione del reporting finanziario (anche in forma elettronica) ai destinatari appropriati.	DS11.1 DS11.2 DS11.6
Il management protegge le informazioni sensibili da accessi o modifiche non autorizzati (logicamente e fisicamente, mentre sono memorizzate e durante la trasmissione tra sistemi)	Riesaminare gli esiti dei test di sicurezza. Determinare se sono posti in essere adeguati controlli al fine di proteggere, logicamente e fisicamente, le informazioni sensibili, memorizzate o durante la trasmissione, da accessi o modifiche non autorizzate.	DS11.6
Sono definiti il periodo di conservazione e le modalità di memorizzazione per documenti, dati, programmi, documenti e messaggi (in entrata e in uscita) come pure i dati (chiavi, certificati) usati per la loro cifratura e autenticazione.	Ottenere le procedure inerenti alla distribuzione e alla conservazione dei dati. Verificare che le procedure definiscano il periodo di conservazione e le modalità di memorizzazione dei documenti, dati, programmi, report e messaggi (in entrata e in uscita) come pure dei dati (chiavi, certificati) utilizzati per la loro cifratura e autenticazione. Verificare che i periodi di conservazione siano conformi al Sarbanes-Oxley Act. Confermare che i periodi di conservazione di quanto archiviato precedentemente al Sarbanes-Oxley Act sia in conformità alla norma. Selezionare un campione di materiale archiviato e verificare che tale materiale è stato archiviato in conformità ai requisiti del Sarbanes-Oxley Act.	DS11.2

Figura 25 – Gestire i dati (DS11) (segue)		
Linee Guida per i Controlli		
Obiettivo di controllo	**Verifiche**	**COBIT 4.0**
Il management ha implementato una strategia per il back-up ciclico di dati e programmi. ★	Determinare se l'azienda ha in essere procedure per il back-up dei dati e dei programmi basate sia sulle esigenze dell'IT sia degli utenti. Selezionare un campione di file di dati e di programmi e determinare che siano stati salvati come richiesto.	DS11.5
Il ripristino delle informazioni viene periodicamente provato. ★	Verificare che la conservazione e la memorizzazione dei messaggi, dei documenti, dei programmi ecc. è stata sottoposta a test nel corso dell'anno trascorso. Ottenere e riesaminare i risultati delle attività di verifica. Stabilire che ogni carenza sia stata rilevata e riesaminata. Ottenere la policy di sicurezza dell'azienda in materia di accesso a dati e procedure e discutere con i relativi responsabili se questi ultimi seguono gli standard e le linee guida quando trattano back-up di dati sensibili.	DS11.5
Le modifiche alla struttura dei dati sono autorizzate ed eseguite in accordo con le specifiche tecniche e sono implementate in modo tempestivo.	Ottenere un campione delle modifiche alla struttura dei dati e determinare se sono conformi alle specifiche tecniche e sono state rese operative nel periodo di tempo richiesto.	AI6

Figura 26—Gestione operativa (DS13)

Linee Guida per i Controlli

Obiettivi di Controllo – I controlli forniscono la ragionevole certezza che le elaborazioni autorizzate siano eseguite come pianificato e che le deviazioni rispetto a quanto previsto siano identificate e analizzate, comprendendo controlli sulla schedulazione, sulle elaborazioni e sul monitoraggio degli errori.

Fondamenti logici – La gestione della operatività si riferisce a come l'azienda mantiene sistemi applicativi affidabili, a supporto del business, per generare, registrare, elaborare e fornire informazioni finanziarie.
Carenze in quest'area potrebbero avere un impatto significativo sui dati finanziari dell'azienda.
Ad esempio: interruzioni nella continuità dei sistemi applicativi potrebbero impedire la corretta registrazione di transazioni finanziarie poste in essere dall'azienda con conseguente compromissione della loro integrità.

Obiettivo di controllo	Verifiche	COBIT 4.0
Il management ha stabilito, documentato e segue le procedure standard per le attività operative riguardanti l'IT, compresi la schedulazione, la gestione, il monitoraggio e la risposta a eventi riguardanti la sicurezza, la disponibilità e l'integrità dell'elaborazione ★	Accertarsi che il management abbia documentato le procedure standard per le attività operative riguardanti l'IT e che tali attività siano riviste periodicamente per accertarne la conformità alla documentazione. Rivedere un campione di eventi per confermare che le procedure di risposta stiano funzionando efficacemente. Se utilizzato, rivedere il processo di schedulazione e le procedure presenti per monitorare la completezza dei job.	DS13.1 DS13.2
I dati che descrivono gli eventi di sistema sono mantenuti per un tempo sufficiente in modo da fornire le informazioni cronologiche e i log per permettere la revisione, l'esame e la ricostruzione dei processi di sistema e di elaborazione dei dati.	Accertarsi che si stiano registrando e memorizzando nei log le informazioni cronologiche sufficienti e che, se necessario, siano utilizzabili per il ripristino/ricostruzione. Ottenere un campione di tracce di log per determinare se sono effettivamente sufficienti a permettere la ricostruzione di eventi specifici.	DS13.3
I dati che descrivono gli eventi di sistema sono disegnati per fornire una ragionevole garanzia riguardo alla completezza e alla tempestività dei processi di sistema e di elaborazione dei dati.	Chiedere quali siano i tipi di informazioni che sono usati dal management per verificare la completezza e la tempestività dei processi di sistema e di elaborazione dei dati. Rivedere un campione dei dati che descrivono gli eventi di sistema ed elaborazione dei dati per confermarne la completezza e tempestività.	DS11.1 DS13.3

Figura 27— Elaborazioni degli utenti finali	
Linee Guida per i Controlli	
I seguenti controlli relativi alle elaborazioni degli utenti finali sono stati ricavati dalle linee guida di controllo dalla figura 15 alla 26 e sono presentati per descrivere le caratteristiche di un tipico ambiente di elaborazione distribuito. Per tale ambiente si applicano specifici processi COBIT.	
Obiettivo di controllo	**Verifiche**
Esistono e sono seguite le policy e le procedure relative alle elaborazioni degli utenti finali afferenti alla sicurezza e l'integrità delle elaborazioni stesse ★	Ottenere una copia della policy e delle procedure relative alle elaborazioni degli utenti finali e confermare che richiamino i controlli sulla sicurezza, la disponibilità e l'integrità delle elaborazioni stesse. Selezionare un campione di utenti e domandare se sono informati di queste policy e se le applicano.
Le elaborazioni degli utenti finali, comprese quelle effettuate mediante fogli elettronici (spreadsheet) e altri programmi sviluppati dagli utenti stessi, sono documentate e vengono riviste regolarmente per accertare l'integrità dell'elaborazione, compresa la loro capacità di accuratamente ordinare, totalizzare e produrre report. ★	Verificare se e quanto il management sia a conoscenza dei programmi utilizzati dagli utenti finali. Domandare con che frequenza e in che modo venga rivista l'integrità dell'elaborazione dei programmi degli utenti finali e rivedere un campione di questi per confermarne l'efficacia. Rivedere i sistemi sviluppati dagli utenti finali e verificare la loro capacità di ordinare, totalizzare e produrre report secondo le intenzioni del management.
I sistemi applicativi sviluppati dagli utenti finali e i relativi dati sono regolarmente salvati e conservati in un'ubicazione sicura. ★	Domandare come e dove i sistemi degli utenti finali sono salvati.
I sistemi applicativi sviluppati dagli utenti finali, come i fogli elettronici e altri programmi sviluppati dagli utenti stessi, sono protetti con opportune misure di sicurezza per impedirne l'uso non autorizzato. ★	Rivedere le misure di sicurezza utilizzate a protezione di accessi non autorizzati ai sistemi sviluppati dagli utenti finali. Considerare l'opportunità di osservare un utente che tenta di ottenere l'accesso non autorizzato a tali sistemi. Chiedere come il management sia capace di rilevare il tentativo d'accesso non autorizzato e quali siano le procedure di follow-up per valutare l'impatto di tale accesso. Selezionare un campione di sistemi sviluppati dagli utenti e verificarne chi ha accesso e se tali accessi sono appropriati.

Figura 27— Elaborazioni degli utenti finali *(segue)*	
Linee Guida per i Controlli	
Obiettivo di controllo	**Verifiche**
Gli input, l'elaborazione e gli output delle applicazioni sviluppate dagli utenti finali sono verificati in modo indipendente per assicurarne la completezza e l'accuratezza. ★	Domandare come il management verifica la completezza e l'accuratezza delle informazioni elaborate e prodotte dai sistemi applicativi sviluppati dagli utenti. Determinare chi rivede e approva gli output dei sistemi sviluppati dagli utenti prima del loro impiego per ulteriori elaborazioni o per produrre report definitivi. Valutare se sia il caso di ripercorrere o rivedere la logica usata dai sistemi sviluppati dagli utenti per valutarne completezza e l'accuratezza elaborativa.

Appendice D – Controlli Applicativi

L’importanza dei controlli applicativi

Nell’ambito del complesso ambiente di reporting finanziario dipendente dall’IT, molte aziende, nell’effettuare l’attività di certificazione, non hanno ancora focalizzato la dovuta attenzione sui controlli applicativi. La PCAOB ha sottolineato l’importanza di quest’area e le aziende che non considerano in maniera adeguata tale tipo di controlli possono rischiare di essere non conformi alla normativa Sarbanes-Oxley.

Molto spesso, le aziende ritengono che i loro sistemi di reporting finanziario siano affidabili per il fatto che non hanno mai avuto un problema in tale ambito o ritengono che l’averne testato alcuni punti in passato sia sufficiente. In altri termini, le aziende hanno un approccio a “scatola chiusa” e pongono tutta la loro fiducia sui controlli manuali, non comprendendo la necessità di considerare i rischi esistenti all’interno del sistema. L’incognita in questi casi è rappresentata dalla fiducia non dovuta riposta nel sistema. Le aziende credono nei loro sistemi senza capire come questi ultimi supportano gli obiettivi del reporting finanziario. Tutto ciò può rappresentare una significativa trascuratezza che può portare a una tangibile debolezza nel controllo interno.

In risposta a quanto sopra, molte aziende hanno iniziato a rivedere le applicazioni più importanti per capire come queste ultime supportano il processo del reporting finanziario. Nel fare ciò, queste aziende hanno sviluppato una specifica documentazione relativa all’integrità dell’applicazione mediante un processo chiamato “baselining” o benchmarking.

Definire i controlli applicativi

A livello di processo di business, i controlli sono applicati a specifiche attività di business finalizzate a raggiungere gli obiettivi finanziari. Molti processi di business sono automatizzati e integrati con i sistemi applicativi IT, con il risultato che molti dei controlli sono anch’essi automatizzati. Questi controlli sono noti come controlli applicativi automatizzati.

I controlli applicativi automatizzati si applicano solo ai processi di business che essi supportano. Sono controlli designati all’interno delle applicazioni per prevenire o rilevare transazioni non autorizzate e supportare gli obiettivi di natura finanziaria quali la completezza, l’accuratezza, l’autorizzazione e la validità delle transazioni. Prima di iniziare l’identificazione e la documentazione dei controlli, dovrebbe essere prestata la dovuta considerazione al tipo di controlli che devono essere adottati.

Nel prendere le decisioni in merito a quali controlli devono essere documentati, è importante capire le caratteristiche degli stessi. In generale, ci sono tre tipi di controllo:

- *Controlli manuali*: effettuati senza l'assistenza di applicazioni o altri sistemi tecnologici. Ad esempio i controlli di supervisione, le autorizzazioni scritte, come una firma su un formulario di controllo, le attività manuali, come la riconciliazione degli ordini di acquisto con le note di ricezione dei beni. I controlli manuali sono soggetti al rischio inerente di errori umani e, come risultato, sono spesso considerati meno attendibili.
- *Controlli automatizzati*: effettuati dal computer e di natura binaria funzionano sempre come sono stati definiti e non sono soggetti a errori intermittenti. Ne è un esempio il controllo dei campi di input a validazione delle quantità degli ordini o i controlli configurati nei sistemi di pagamento automatici che consentono l'emissione degli ordini solo entro i limiti predefiniti. Esempi sono costituiti da:

  - attività di controllo di quadratura: sono costituite da controlli che rilevano errori nell'inserimento dei dati attraverso la riconciliazione dell'ammontare acquisito manualmente o automaticamente con un totale di controllo. Ad esempio, un'azienda riscontra automaticamente il numero totale delle transazioni elaborate e passate dal suo sistema di registrazione degli ordini online al numero di transazioni ricevute nel suo sistema di fatturazione;
  - codici di controllo: un algoritmo per validare i dati. I codici degli articoli di un'azienda contengono un carattere di controllo per rilevare e correggere ordini non accurati inoltrati ai suoi fornitori. I codici di prodotto universali includono un codice di controllo per verificare il prodotto e il venditore;
  - liste predefinite di dati: controlli che forniscono all'utente liste predefinite di dati accettabili. Per esempio, un sito intranet di un'azienda potrebbe includere liste predefinite di prodotti acquistabili;
  - test di ragionevolezza dei dati: sono test che comparano i dati acquisiti con un campione di riferimento fisso o parametrizzato per la ragionevolezza dei dati in esame. Per esempio, un ordine a un fornitore fatto da un negozio di accessori per la casa riguardante un numero particolarmente elevato di assi di legname dovrebbe far scattare una verifica;
  - test logici: sono relativi all'uso di limiti di intervallo (*range*) o test sul tipo di dati (numerico/alfanumerico). Per esempio, la carta di credito che ha un formato predefinito;
  - calcoli: algoritmi numerici applicati da una routine automatica implementata all'interno delle applicazioni.

- *Controlli manuali dipendenti dall'IT (ibridi)*: Sono essenzialmente una combinazione di processi manuali e automatizzati. I report generati dal sistema sono normalmente basati su controlli ibridi, poiché forniscono i dati per la revisione del management. Per citare un esempio, la valutazione dei crediti verso i clienti può includere un controllo dove i competenti manager revisionano, per valutarne la ragionevolezza, il report mensile delle scadenze. In questo esempio, un report viene prodotto dalla contabilità clienti (processo automatizzato) e rivisto per la relativa ragionevolezza (processo manuale). Come risultato, sia il processo automatizzato (generazione del report) sia quello manuale (revisione del management) sono necessari per supportare la valutazione dei crediti verso i clienti.

Il "business case" per i controlli applicativi

Ci sono vantaggi e svantaggi nelle attività di controllo manuale e automatico. In alcuni casi, è facile documentare e avere evidenza dell'attività di controllo manuale in piccole aziende con bassa complessità. Tuttavia, la documentazione dei controlli manuali può diventare un'attività molto onerosa in aziende grandi caratterizzate da alta complessità. Per queste ultime, lo sforzo associato con la documentazione e il test dei controlli automatici è molto più conveniente nel lungo termine, poiché i controlli devono essere testati una sola volta, mentre i controlli manuali devono essere provati sulla base della frequenza dell'operatività. E' importante notare che mentre la dimensione del campione per i controlli manuali varia in base alla frequenza di operatività, non è lo stesso per quella dei controlli automatici. Tutto ciò può quindi tramutarsi in un significativo risparmio per l'azienda. Per fare un esempio, consideriamo un'azienda che necessita di identificare 500 controlli per il programma Sarbanes-Oxley e sta prendendo in esame come documentare i controlli manuali o automatici. La **figura 28** è stata predisposta per supportare la relativa analisi.

Figura 28– Comparazione tra gli approcci al controllo manuale e applicativo

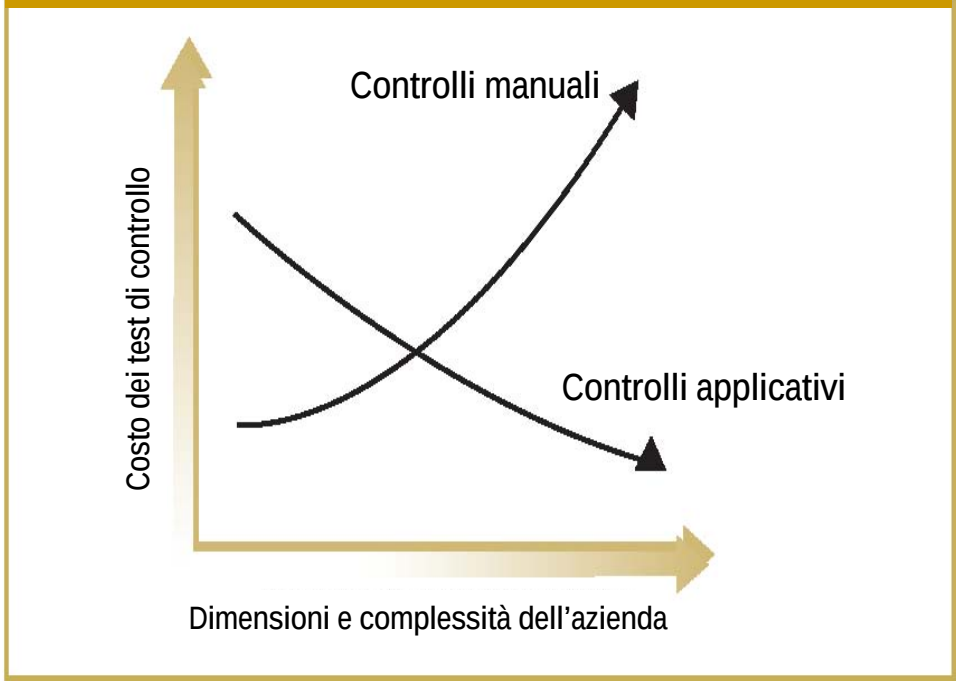
Approccio manuale al controllo		**Approccio automatizzato al controllo**	
Controlli totali	500	Controlli totali	500
Tempo per documentare ogni controllo	1 ora	Tempo per documentare ogni controllo	3 ore
Tempo complessivo per documentare	500 ore	Tempo complessivo per documentare	1.500 ore
Dimensione media del campione per controllo	10	Dimensione media del campione per controllo	1
Totale elementi da testare	5.000	Totale elementi da testare	500
Tempo per i test per ogni campione	30 min.	Tempo per i test per ogni campione	30 min.
Tempo totale per i test	2.500 ore	Tempo totale per i test	250 ore
Tempo complessivo	**3.000 ore**	Tempo **complessivo**	**1.750 ore**

Devono essere fatte alcune precisazioni relativamente a questo esempio. Primo, la tabella mostra che il tempo iniziale per documentare i controlli manuali è minore rispetto a quello necessario per i controlli automatici. Questo deriva dalla complessità dei sistemi IT e dalla necessità di comprendere come funzionano le applicazioni. Successivamente, il tempo richiesto per testare i controlli manuali è maggiore rispetto a quello necessario per i controlli automatici. Ciò dipende dal fatto che i controlli automatici operano nel modo in cui sono stati definiti e necessitano di essere provati una sola volta, dando per assodato che i controlli generali IT sono attendibili (sviluppo di programmi, modifiche ai programmi, accesso ai programmi e ai dati, processi elaborativi).

Tuttavia, se il "mantenimento della conformità" è considerato per un periodo di 5 anni, l'impatto è molto più significativo. In questo esempio, il risparmio nel primo anno è pari a un totale di 1.250 ore, ma nel secondo anno e in quelli successivi, quando l'azienda ha la sola necessità di provare nuovamente i propri controlli, questo risparmio si incrementa fino a 2.250 ore annue. Pertanto, dopo cinque anni di conformità un'azienda può risparmiare 10.250 ore impiegate nel caso in cui venga scelto di documentare e testare i controlli automatici. La **figura 29** illustra come la dimensione e la complessità di un'azienda impatta sullo sforzo prestato e, quindi, sul costo della documentazione e dei test dei controlli manuali rispetto a quelli automatici.

Se si considera inoltre che i controlli automatici sono generalmente più affidabili, i benefici nell'intraprendere questo approccio sono molto evidenti.

Figura 29 – Effetto della dimensione e complessità sullo sforzo necessario per documentare e testare i controlli



Stabilire il benchmark applicativo

Il benchmark applicativo implica la documentazione e il test dei controlli significativi inseriti all'interno delle applicazioni finanziarie che supportano il processo del bilancio al fine di confermare il relativo disegno e l'efficienza operativa. Una volta che questi controlli sono stati identificati e testati, sono qualificati per il benchmarking, che essenzialmente consente una riduzione nella frequenza dei test purché alcune condizioni, descritte nei paragrafi seguenti, siano soddisfatte.

Anche se ci sono costi aggiuntivi necessari per stabilire un benchmark applicativo (come capire in che modo l'applicazione opera e documentare i controlli rilevanti nel suo funzionamento), i benefici possono essere impareggiabili. Come segnalato in **figura 28**, la riduzione dello sforzo necessario per i test costituisce, da sola, un solido business case. Tuttavia, ci sono altri benefici, quali:

- ulteriori riduzioni del tempo dei test dovuto al fatto che i controlli applicativi possono non richiedere dei test annuali, poiché gli stessi non sono soggetti a errori umani e tipicamente operano nel modo in cui sono stati disegnati purché alcune condizioni, descritte nei paragrafi seguenti, siano soddisfatte.

- Il miglioramento dell'attendibilità, nel momento che i controlli applicativi sono tipicamente preventivi e più affidabili dei controlli manuali. Spesso costituiscono un duplice controllo, poiché non supportano solo gli obiettivi di controllo di natura finanziaria, ma possono supportare, nello stesso tempo, attività antifrode.

Il benchmarking applicativo è stato definito dal PCAOB nella sua guida del novembre 2004, stabilendo che l'attività di benchmarking è una pratica accettabile purché talune condizioni siano soddisfatte, esse sono:

- la parte rilevante dell'applicazione che supporta i controlli applicativi sia identificata (a titolo di esempio, il modulo relativo alla contabilità fornitori che supporta lo scadenziario automatico o il modulo relativo all'inventario che a sua volta consente una completa e accurata lista dei saldi)
- I controlli rilevanti dell'applicazione siano appropriatamente progettati
- I controlli rilevanti dell'applicazione non vengano modificati durante l'anno
- I test più recenti dei controlli dell'applicazione confermino la loro efficacia operativa
- I controlli rilevanti a supporto dell'IT, in particolare il controllo degli accessi e delle modifiche alle applicazioni, siano propriamente progettati e operino con efficienza.

Esempi di controlli automatici dell'applicazione

Per assistere l'azienda nell'applicare un approccio al controllo automatizzato, esempi di controlli automatici sono presenti dalla **figura 31 alla 38**. Per la maggior parte, questi controlli possono essere abilitati attraverso l'uso di funzionalità integrate nell'applicazione stessa. Questa caratteristica è comunemente presente negli ambienti integrati (ERP), come SAP, People Soft, Oracle, JD Edwards e altri. Dove questa funzionalità non esiste, questi obiettivi di controllo possono richiedere una combinazione di procedure di controllo manuali e automatiche per soddisfare l'obiettivo di controllo.

Gli obiettivi di controllo presentati dalla **figura 31 alla 38** non dovrebbero essere intesi come una lista esaustiva, ma piuttosto come un esempio dei controlli che sono comunemente fattibili per le applicazioni. Le aziende dovrebbero tenere in considerazione che obiettivi di controllo aggiuntivi possono essere richiesti in particolari settori industriali e ambienti operativi.

Le figure dalla **31 alla 38** fanno riferimento a controlli, riguardanti applicazioni e processi di business, che contribuiscono alla "asserzioni" relative al reporting finanziario e includono controlli di completezza, accuratezza, valutazione e autorizzazione. La definizione e alcuni esempi di queste "asserzioni" sono riassunti nella **figura 30**.

Figura 30— Dichiarazioni finanziarie
Definizioni ed esempi

Asserzioni	Definizioni ed esempi	
	Definizione	**Esempio**
Esistenza	Dichiarazione a proposito dell'esistenza, o dei dati dell'evento correlato, dei beni o delle sopravvenienze di un'azienda a una certa data e se le registrazioni delle transazioni sono avvenute durante un periodo certo.	Il management afferma che il magazzino dei prodotti finiti presenti nel bilancio è disponibile alla vendita. Alla stessa maniera, il management afferma che le vendite, nelle entrate rappresentano lo scambio di beni o servizi con i clienti per contanti o altro.
Completezza	Dichiarazione a proposito della completezza se tutte le transazioni e i conti che dovrebbero essere presentati nel bilancio finanziario sono inclusi.	Il management afferma che tutti gli acquisti di beni e servizi sono registrati e sono inclusi nel reporting finanziario. Alla stessa maniera, il management afferma che le note/fatture passive includono tutti gli impegni di spesa dell'azienda.
Valutazione	Affermazione a proposito della valutazione se tutte le componenti degli asset, sopravvenienze, azioni, tasse e costi sono stati incluse nel bilancio nei giusti valori.	Il management afferma che la proprietà è registrata con costi storici e che tali costi sono sistematicamente attribuiti ai corretti periodi contabili. Alla stessa maniera, il management afferma che i conti vendita sono inclusi nel bilancio e sono dichiarati al valore netto di realizzo.

Figura 31 – Obiettivi di controllo applicativi per il ciclo di chiusura del bilancio	
Obiettivi di controlli illustrati	**Dichiarazioni economiche**
Le registrazioni nell'elaborazione di chiusura sono complete e precise.	Completezza Esistenza
Tempistica di ammortamento automatizzata, periodi e metodi sono appropriatamente e accuratamente inseriti.	Valutazione Esistenza
I report delle differenze sono generati per identificare condizioni di errore o di squadratura	Completezza Esistenza Valutazione
Le entrate standard ricorrenti di fine periodo sottomesse dai partitari sono automatizzate, adeguatamente approvate e inserite accuratamente	Completezza Esistenza Valutazione
I sistemi generano report per tutti gli inserimenti regolari e non regolari registrati	Completezza Esistenza
Tutti gli inserimenti non standard registrati sono tracciati e sono appropriati	Completezza Esistenza
I codici dei conti e gli importi delle transazioni sono accurati e completi e le eccezioni sono riportate	Completezza Esistenza
I saldi di contabilità generale sono riconciliati con i sottoconti	Completezza Esistenza
Gli Importi registrati sono sottoposti a un confronto automatico con importi previsti	Completezza Esistenza
Sono vietate immissioni non quadrate	Completezza Esistenza
Il consolidamento aziendale, compresa l'eliminazione di compensazioni interaziendali standard, è automatizzato ed eseguito attraverso un prodotto software di terza parte	Completezza Esistenza Valutazione
Le funzionalità del sistema supportano la segregazione del caricamento e le funzioni di approvazione	Esistenza
L'accesso ai record di contabilità generale è appropriato e autorizzato	Completezza Esistenza Valutazione
Le transazioni non possono essere registrate al di fuori del cut-off di chiusura finanziario	Completezza Esistenza Valutazione
I ratei ricorrenti approvati annualmente sono accuratamente registrati nei periodi appropriati	Completezza Esistenza Valutazione
Sono in essere controlli di sistema per un'adeguata approvazione della cancellazione di scritture	Esistenza
Le voci di bilancio interconnesse e le voci di entrata sono automaticamente riconciliate	Completezza Esistenza
Le fonti di tutte le entrate sono prontamente identificabili	Esistenza
Le transazioni rifiutate o accettate sono identificate e riportate sul report delle eccezioni nel caso di eccezioni ai dati	Completezza Esistenza
Il piano dei conti è mantenuto aggiornato	Esistenza

Figura 32 – Obiettivi di controllo per la contabilità generale	
Obiettivi di controlli illustrati	**Dichiarazioni economiche**
L'accesso alle voci della contabilità generale è adeguato e autorizzato.	Completezza Esistenza Valutazione
La contabilità generale viene riconciliata con i saldi dei partitari e tali riconciliazioni sono riviste per l'accuratezza e approvate personalmente dal supervisore.	Completezza Esistenza
I report di quadratura interconnessi e i partitari delle entrate subiscono una riconciliazione automatica per confermare l'accuratezza di tali conti.	Completezza Esistenza
I sistemi generano report per le entrate ricorrenti e non del giornale per la revisione di accuratezza da parte del management.	Completezza Esistenza
Le funzionalità del sistema permettono di segregare le funzioni di immissione e approvazione.	Esistenza
Tutti gli inserimenti a giornale non standard sono tracciati ed adeguati	Completezza Esistenza
Le voci dei conti e gli importi delle transazioni sono accurati e completi, le eccezioni sono riportate.	Completezza Esistenza
Le registrazioni degli importi subiscono un confronto automatico con gli importi previsti per confermare l'accuratezza degli inserimenti.	Completezza Esistenza
Gli inserimenti non quadrati sono proibiti.	Completezza Esistenza
Il consolidamento di gruppo, comprese le eliminazioni delle compensazioni interaziendali standard, è automatizzato ed eseguito.	Completezza Esistenza Valutazione
I report sulle modifiche sono generati per identificare gli errori sugli inserimenti e le condizioni di squadratura.	Completezza Esistenza Valutazione
Controlli di sistema sono in essere per l'adeguata approvazione di cancellazioni di registrazioni	Esistenza
Gli inserimenti di importi eccezionali registrati, che sono stati inseriti nella contabilità generale durante il mese, sono segnalati dal sistema e conseguentemente rivisti per garantire l'accuratezza e approvati dal controller o dal CFO dopo la fine del mese.	Completezza Esistenza Valutazione
Un report di tutti gli inserimenti a giornale completati come parte del processo di chiusura è rivisto dal management per confermare la completezza e l'adeguatezza di tutti gli inserimenti registrati.	Completezza Esistenza
Il report delle modifiche al master file della contabilità generale è generato dal sistema ed è rivisto da un addetto che non inserisce tali modifiche	Completezza Esistenza
I report sulla situazione effettiva, quelli relativi a quanto in budget e quelli a consuntivo sono prodotti dal sistema di contabilità generale su base mensile prima della chiusura finale. I report sono distribuiti e rivisti dal controller e dal CFO. Vengono approfonditi gli importi anomali o gli scostamenti e vengono riclassificati dove possibile.	Completezza Esistenza Valutazione
Una mappa standard delle voci è stato approvata dal management ed è utilizzata per tutte le unità del gruppo. Aggiunte o cancellazioni in contabilità generale sono limitate solo a persone autorizzate del reparto amministrativo.	Completezza Esistenza

Figura 32 – Obiettivi di controllo per la contabilità generale (*segue*)	
Obiettivi di controlli illustrati	**Dichiarazioni economiche**
Un report delle voci in sospeso (ad es. riconciliazione degli articoli in sospeso dopo 90 giorni) è generato dal sistema per eseguire il follow-up e la risoluzione tempestiva.	Completezza Esistenza
Gli inserimenti registrati nel processo di chiusura sono completi e accurati.	Completezza Esistenza
L'ammortamento periodico è automatizzato; periodi e metodi sono adeguatamente e accuratamente inseriti.	Valutazione Esistenza
Gli inserimenti ricorrenti di fine periodo, quelli standard provenienti dai sottosistemi di contabilità sono automatizzati, appropriatamente approvati e inseriti accuratamente.	Completezza Esistenza Valutazione
Le transazioni non possono essere registrate oltre il periodo di cut off.	Completezza Esistenza Valutazione
I ratei annuali approvati periodici sono accuratamente registrati nei periodi appropriati.	Completezza Esistenza Valutazione
Le fonti per tutti gli inserimenti sono prontamente identificabili.	Esistenza
Le transazioni rifiutate, o accettate e identificate, sono riportate su report di eccezioni nel caso di eccezioni nei dati.	Completezza Esistenza
La mappa delle voci dei è mantenuta aggiornata.	Esistenza

Figura 33 – Obiettivi di controllo per il ciclo delle vendite	
Obiettivi di controlli illustrati	**Dichiarazioni economiche**
Gli ordini sono elaborati solo per i clienti approvati	Valutazione
Gli ordini sono approvati dal management per prezzi e condizioni di vendita	Esistenza
Gli ordini e le cancellazioni degli ordini sono inseriti accuratamente.	Valutazione
I dati degli ordini inseriti sono trasferiti completamente e accuratamente per la spedizione e la fatturazione.	Valutazione Completezza
Tutti gli ordini ricevuti dai clienti sono inseriti e processati	Completezza
Le fatture sono generate usando le condizioni e i prezzi autorizzati	Esistenza Valutazione
Le fatture sono accuratamente calcolate e registrate.	Valutazione
Le note di credito e gli aggiustamenti della contabilità clienti sono accuratamente calcolati e registrati	Valutazione
Tutti le merci spedite sono fatturate.	Completezza
Le note di credito per tutte le merci rese e gli aggiustamenti della contabilità clienti sono effettuati secondo la policy aziendale	Esistenza
Le fatture sono relative a spedizioni valide	Esistenza
Tutte le note di credito sono relative a merci rese o ad altri aggiustamenti validi.	Completezza
Tutte le fatture emesse sono registrate.	Completezza
Tutte le note di credito emesse sono registrate	Esistenza
Le fatture sono registrate nei periodi di competenza.	Valutazione
Le note di credito sono registrate nei periodi di competenza.	Esistenza Valutazione
Gli incassi in contanti sono registrati nel periodo in cui sono state ricevuti.	Valutazione
Le ricevute di pagamenti in contanti sono inserite per essere elaborate accuratamente	Valutazione
Tutte le ricevute di pagamento con contanti sono inserite per essere elaborate	Esistenza
I dati delle ricevute di pagamenti in contanti sono validi e sono inseriti per essere elaborati una sola volta	Completezza
Gli sconti sono accuratamente calcolati e registrati	Valutazione
La tempistica degli incassi periodici della contabilità clienti è monitorata	Valutazione
Viene gestito un archivio dei clienti	Completezza Esistenza
Solo effettuate solo modifiche valide sull'archivio dei clienti	Completezza Esistenza
Tutte le modifiche valide all'archivio clienti sono inserite ed elaborate	Completezza Esistenza
Le modifiche all'archivio clienti sono accurate	Valutazione
Le modifiche all'archivio clienti sono elaborate periodicamente	Completezza Esistenza
L'archivio dei clienti è mantenuto aggiornato	Completezza Esistenza

Figura 34 – Obiettivi di controllo per il ciclo acquisti	
Obiettivi di controlli illustrati	**Dichiarazioni economiche**
Gli ordini di acquisto sono eseguiti solo con richieste formalizzate e approvate	Esistenza
Gli ordini di acquisto sono accuratamente inseriti	Valutazione
Tutti gli ordini di acquisto sono inseriti ed elaborati	Completezza
Gli importi registrati in contabilità fornitori rappresentano beni o servizi ricevuti	Esistenza
Gli importi nella contabilità fornitori sono accuratamente calcolati e registrati	Valutazione
Tutti gli importi dei beni o servizi ricevuti sono inseriti ed elaborati nella contabilità fornitori	Completezza
Gli importi per i beni o i servizi ricevuti sono registrati nel periodo appropriato	Valutazione
La contabilità fornitori è variata solo per ragioni valide	Completezza Esistenza
Le note di credito e altri relativi aggiustamenti sono accuratamente calcolati e registrati	Valutazione
Tutte le note di credito e relativi aggiustamenti pertinenti alla contabilità fornitori sono inserite ed elaborate.	Completezza Esistenza
Le note di credito ed altri aggiustamenti registrati nel periodo appropriato	Valutazione
I pagamenti sono effettuati solo per beni e servizi ricevuti	Esistenza
I pagamenti sono effettuati ai fornitori pertinenti	Esistenza
I pagamenti sono accuratamente calcolati e registrati	Valutazione
Tutti i pagamenti sono registrati	Completezza
I pagamenti sono registrati nei periodi nei quali sono effettuati	Valutazione
All’archivio fornitori sono apportate solo modifiche valide	Completezza Esistenza
Tutte le modifiche valide all’archivio fornitori sono inserite e processate	Completezza Esistenza
Modifiche all’archivio fornitori sono accurate	Valutazione
Modifiche all’archivio fornitori sono elaborate tempestivamente	Completezza Esistenza
L’archivio fornitori è mantenuto aggiornato	Completezza Esistenza

Figura 35 – Obiettivi di controllo per il ciclo dell'inventario	
Obiettivi di controlli illustrati	**Dichiarazioni economiche**
Le modifiche ai prezzi di inventario o alle quantità sono registrate prontamente e nel periodo di competenza	Esistenza Completezza Valutazione
Le modifiche ai prezzi e alle quantità di inventario sono registrate accuratamente	Valutazione
Le materie prime sono ricevute e accettate solo se hanno un valido ordine di acquisto	Esistenza
Le materie prime ricevute sono accuratamente registrate	Valutazione
Tutte le materie prime ricevute sono registrate	Completezza
Le ricevute delle materie prime sono registrate prontamente e nel periodo appropriato	Valutazione
Le materie prime difettose sono rese prontamente ai fornitori	Esistenza
Tutti i trasferimenti delle materie prime alla produzione sono registrati accuratamente nel periodo appropriato	Valutazione Completezza
Tutte le spese dirette e indirette associate alla produzione sono registrate accuratamente e nel periodo appropriato	Valutazione
Tutti i trasferimenti di unità complete di produzione a prodotti finiti sono registrati completamente e accuratamente nel periodo appropriato	Valutazione Completezza
I prodotti finiti resi dai clienti sono registrati completamente e accuratamente nel periodo appropriato	Valutazione Completezza
I prodotti finiti ricevuti dalla produzione sono registrati completamente e accuratamente nel periodo appropriato	completezza valutazione
Tutte le spedizioni sono registrate	Esistenza
Le spedizioni sono registrate accuratamente	Valutazione
Le spedizioni sono registrate prontamente e nel periodo appropriato	Valutazione
L'inventario viene decrementato solo quando le merci sono spedite con ordini dei clienti approvati	Completezza Esistenza
I costi di spedizione sono trasferiti dall'inventario al costo del venduto	Esistenza Valutazione
I costi di spedizione sono accuratamente registrati	Valutazione
Gli importi imputati al costo del venduto rappresentano quelli associati alla spedizione	Valutazione
Solo le modifiche valide sono riportate nell'archivio dell'inventario	Esistenza Completezza
Tutte le modifiche valide all'archivio dell'inventario sono inserite ed elaborate	Esistenza Completezza
Le modifiche all'archivio dell'inventario sono accurate	Valutazione
Le modifiche all'archivio dell'inventario sono prontamente elaborate	Esistenza Completezza
L'archivio dell'inventario è mantenuto aggiornato	Completezza Esistenza

Figura 36 – Obiettivi di controllo per il ciclo delle immobilizzazioni tecniche	
Obiettivi di controlli illustrati	**Dichiarazioni economiche**
L'acquisizione delle immobilizzazioni tecniche è accuratamente registrata	Valutazione
L'acquisizione delle immobilizzazioni tecniche è registrata nel periodo appropriato	Valutazione
Tutte le immobilizzazioni tecniche acquisite sono registrate	Completezza
Il deprezzamento dei valori è accuratamente registrato nel periodo appropriato	Valutazione
Tutti i deprezzamenti sono registrati nel periodo appropriato	Esistenza Valutazione Completezza
Tutte le immobilizzazioni tecniche dismesse sono registrate	Esistenza
Le immobilizzazioni tecniche dismesse sono accuratamente calcolate e registrate	Valutazione
Le immobilizzazioni tecniche dismesse sono registrate nel periodo appropriato	Valutazione
L'attività di gestione dei record delle immobilizzazioni tecniche viene mantenuta accuratamente	Completezza
L'attività di gestione dei record delle immobilizzazioni tecniche viene eseguita con cadenza regolare	Completezza
Solo le modiche valide al registro delle immobilizzazioni tecniche e/o all'archivio sono inserite ed elaborate	Completezza Esistenza
Tutte le modiche valide al registro delle immobilizzazioni tecniche e/o all'archivio sono inserite ed elaborate	Completezza Esistenza
Le modiche valide al registro delle immobilizzazioni tecniche e/o all'archivio sono accurate	Valutazione
Le modiche valide al registro delle immobilizzazioni tecniche e/o all'archivio sono prontamente elaborate	Completezza Esistenza
Il registro delle immobilizzazioni tecniche e/o l'archivio sono mantenuti aggiornati	Completezza esistenza

Figura 37 – Obiettivi di controllo per il ciclo delle risorse umane	
Obiettivi di controlli illustrati	**Dichiarazioni economiche**
Gli inserimenti all'archivio stipendi si riferiscono a dipendenti effettivi	Esistenza
Tutti i nuovi dipendenti sono inseriti nell'archivio stipendi	Completezza
I dipendenti licenziati/dimissionari sono rimossi dall'archivio stipendi	Esistenza
I dipendenti sono licenziati solo per motivi consentiti dalla legge o sindacali	Completezza
Le cancellazioni dall'archivio stipendi indicano cessazioni valide	Completezza
Tutto il temo lavorato è inserito	Completezza
Il tempo lavorato è accuratamente inserito ed elaborato	Valutazione
L'archivio stipendi è registrato nei periodi appropriati	Valutazione
Lo stipendio (incluse compensazioni e trattenute) è accuratamente calcolato e registrato	Valutazione
Lo stipendio viene versato ai dipendenti effettivi	Esistenza
Solo le modifiche valide sono effettuate all'archivio stipendi	Esistenza Completezza
Tutte le modifiche valide all'archivio stipendi sono inserite ed elaborate	Esistenza Completezza
Le modifiche all'archivio stipendi sono accurate	Valutazione
Le modifiche all'archivio stipendi sono elaborate nei tempi corretti	Esistenza Completezza
L'archivio stipendi è mantenuto aggiornato	Esistenza Completezza
Solo modifiche valide sono apportate alle tabelle delle trattenute	Esistenza completezza
Tutte le modifiche valide alle tabelle delle trattenute sono inserite ed elaborate	Esistenza Completezza
Le modifiche alle tabelle delle trattenute sono accurate	Valutazione
Le modifiche alle tabelle delle trattenute sono prontamente elaborate	Esistenza Completezza
Le tabelle delle trattenute sono mantenute aggiornate.	Esistenza Completezza

Figura 38 - Obiettivi di controllo per il ciclo degli oneri fiscali	
Descrizione degli obiettivi di controllo	**Rendiconto economico finanziario**
Sono utilizzati flussi automatizzati per il caricamento puntuale dei rimborsi.	Completezza
I pagamenti degli oneri fiscali sono correttamente calcolati e registrati nella contabilità generale.	Completezza Valutazione Esistenza
L'esposizione fiscale e gli accantonamenti sono correttamente calcolati e registrati.	Completezza Valutazione Esistenza
Le spese relative agli oneri fiscali sono registrate nel periodo corretto.	Completezza Valutazione Esistenza
Le differenze permanenti e temporanee sono identificate e accuratamente registrate.	Completezza Valutazione Esistenza
Viene utilizzato il conteggio corretto per il calcolo dei risconti fiscali	Completezza Esistenza
L'imponibile, gli oneri, le spese sono complete e correttamente calcolati e registrati.	Completezza Esistenza
Gli sgravi sono calcolati su basi appropriate, consentendo corrette imputazioni e rispettando le fasce fiscali	Completezza Esistenza
La tassa sul consumo e sulle vendite è calcolata in modo appropriato, correttamente e tempestivamente	Completezza Esistenza
L'imposta sul valore aggiunto è correttamente contabilizzata e inserita in modo appropriato.	Completezza Esistenza
Le policy per il trasferimento dei costi sono mantenute aggiornate e rappresentate accuratamente nei sistemi.	Completezza Esistenza
Tutti i pagamenti degli oneri fiscali hanno un accurato riscontro nella contabilità generale.	Valutazione
Le tasse sul patrimonio sono pagate tempestivamente e sono accurate.	Completezza Valutazione Esistenza

Appendice E - Inventario di un campione di applicazioni e dei livelli tecnologici

Figura 39 - Inventario di un campione di applicazioni e dei livelli tecnologici

Nome Applicazione	Processo di business relativo	Dettagli dell'applicazione			Database		Sistema operativo / Rete		Piattaforma hardware		Ubicazione fisica	
		Pacchetto / Applicazione sviluppata in-house	Personalizzazione	Responsabile / Proprietario	Versione	Responsabile / Proprietario	Versione	Responsabile / Proprietario	Versione	Responsabile / Proprietario	Insediamento	Responsabile / Proprietario
SAP	Gestione degli aspetti finanziari	Pacchetto	Si	Kerry M	Oracle 9i V9.2.0	Craig T	Solaris 3.2 / Novell	Ryan S	HP 9000	Doug W	Calgary	D'Arcy M
PeopleSoft	Gestione del libro paga	Pacchetto	Si	Tom M	Oracle 9i V9.2.0	Craig T	HP-UX V11.11 / Novell	Adel M	HP 9000	Doug W	Houston	Rhonda M
ACCPAC	Gestione della contabilità delle società controllate	Pacchetto	No	Esther C	Oracle 9i V9.2.0	Craig T	HP-UX V11.11 / Novell	Adel M	HP 9000	Doug W	Denver	Robert P
TIMS	Registrazione dei tempi	Pacchetto	Si	Daryl J	DB2 400	Alan S	OS400 / Novell	Reid C	AS 400	Rob K	Calgary	D'Arcy M
VIBS	Fatturazione	Personalizzata	Si	Paul Z	DB2 400	Alan S	OS400 / Novell	Ryan R	AS 400	Barb V	Calgary	D'Arcy M
SunGard	Investimenti	Elaborazione in outsourcing	No	Kerry M	Riferimento SAS 70	Craig T	Riferimento SAS 70	Ryan S	Riferimento SAS 70	Doug W	Riferimento SAS 70	Doug W

Appendice F – Strumento per la stima dei progetti

Figura 40 – Strumento per la stima dei progetti

Fase di progetto	Impegno stimato per ciascuna fase di progetto rapportato alla grandezza dell'azienda (Quanto riportato sono solo stime; i valori potrebbero risultare più bassi o più alti a causa di circostanze uniche relative a ciascuna azienda)					
	Piccola (un sito, meno di 5 applicazioni)		Media (meno di 5 siti, 5-10 applicazioni)		Grande (da 5 a 10 siti, da 10 a 15 applicazioni)	
Stima di impegno (giorni)	Estremo inferiore	Estremo superiore	Estremo inferiore	Estremo superiore	Estremo inferiore	Estremo superiore
1. Pianificazione e definizione ambito	2	5	5	10	10	20
2. Valutazione dei rischi	2	5	2	5	5	15
3. Identificazione e controllo della documentazione	5	10	10	20	20	50
4. Valutazione del progetto e dell'efficienza operativa	5	10	10	20	20	30
5. Prioritizzazione e rimedio delle debolezze	Vedere Nota 1	Vedere Nota 1	Vedere Nota 1	Vedere Nota 1	Vedere Nota 1	Vedere Nota 1
6. Predisposizione della sostenibilità	Vedere Nota 2	Vedere Nota 2	Vedere Nota 2	Vedere Nota 2	Vedere Nota 2	Vedere Nota 2

Nota 1 – L'impegno per rimediare ai problemi dipende dalla criticità della debolezza. Le aziende possono scegliere di procedere nel rimedio e affrontare i problemi di efficienza operativa, oppure implementare un nuovo processo di sviluppo dei sistemi e della gestione dei cambiamenti
Nota 2 – L'impegno per la sostenibilità include la valutazione delle opportunità di automazione e di razionalizzazione, ma non include il tempo necessario all'implementazione in quanto esso dipende da ogni singola organizzazione.

Figura 41 – Stima dell'impegno per documentare e testare (giorni)

Stima dell'impegno per documentare e testare (giorni)		
Ambiente IT (ciascuno)	Estremo inferiore	Estremo superiore
Pacchetto applicativo piccolo	1	2
Pacchetto applicativo grande	2	5
Applicazione *custom* piccola	1	2
Applicazione *custom* grande	5	10
Valutazione separazione delle responsabilità – applicazione ridotta	2	10
Valutazione separazione delle responsabilità – applicazione estesa	5	30

Figura 42 – Impegno stimato per documentare e testare (giorni)

Impegno stimato per documentare e testare (giorni)		
Ambiente IT (ciascuno)	Estremo inferiore	Estremo superiore
Foglio di calcolo – complessità bassa	0.25	1
Foglio di calcolo – complessità alta	0.5	2
Database	2	5
Sistema operativo	0.5	2
Rete	0.5	5
Centro elaborazione dati	0.5	1

Non appena la valutazione iniziale e' stata realizzata, la stima dell'impegno per effettuare i controlli può progressivamente ridursi. Le stime riportate in Figura 41 e 42 sono stime iniziali e possono variare. Per esempio, le aziende che sono fortemente decentralizzate e che hanno un numero significativo di applicazioni possono richiedere sostanzialmente più impegno. Analogamente, le aziende molto piccole con processi semplici e poche applicazioni possono richiedere meno impegno.

Appendice G - Valutazione del rischio inerente e Griglia per la Priorità dei Controlli

Considerazioni sulla valutazione del rischio

Attraverso la realizzazione della valutazione del rischio delle applicazioni appartenenti al contesto in esame e dei sottosistemi ad esse collegati, le aziende possono fissare le priorità degli sforzi concentrandosi sulle aree a maggior rischio e possono ridurre gli sforzi nelle aree a minor rischio. E' importante osservare che la valutazione del rischio e' una decisione soggettiva; tuttavia esistono fattori comuni di rischio che dovrebbero essere presi in considerazione. Le Figure dalle 43 alla 45 sono pensate per supportare la valutazione del rischio inerente.

Figura 43 – Considerazioni sul rischio inerente

Fattori di rischio di esempio	**Considerazioni che determinano un rischio più alto**	**Considerazioni che determinano un rischio più basso**
Natura della tecnologia	Complessa, unica, personalizzata (*custom*), sviluppata *in-house*	Semplice, comunemente usata, non personalizzata, prodotto in serie
Natura delle persone	Senza esperienza, mancanza di formazione, numero limitato di risorse, alto *turnover*	Con esperienza, formata e specializzata, risorse in numero sufficiente, basso *turnover*
Natura dei processi	Decentralizzata, diffusa su più siti, *ad hoc*	Centralizzata, formalizzata, consistente
Esperienza passata	Con evidenza storica di problemi relativi a errori di elaborazione, periodi di interruzione dei sistemi, corruzione di dati	Senza evidenza storica di problemi
Significato del reporting finanziario	Diretto – usato per iniziare e registrare gli importi nel reporting finanziario	Indiretto - usato per scopi analitici ma non per iniziare e registrare gli importi nel reporting finanziario

Una valutazione dovrebbe essere realizzata per ogni applicazione appartenente al contesto in esame. In alcuni casi, i sottosistemi (database, sistema operativo, rete e ambiente fisico) saranno i medesimi per molte o per tutte le applicazioni. In questo caso, i sottosistemi possono essere valutati una sola volta.

Figura 44 – Valutazione del rischio inerente per i livelli tecnologici

Fattori di rischio inerente	Livelli tecnologici				
	Applicazione	Database	Sistema Operativo	Rete	Ambiente fisico
Natura della tecnologia	A/M/B	A/M/B	A/M/B	A/M/B	A/M/B
Natura delle persone	A/M/B	A/M/B	A/M/B	A/M/B	A/M/B
Natura dei processi	A/M/B	A/M/B	A/M/B	A/M/B	A/M/B
Passata esperienza	A/M/B	A/M/B	A/M/B	A/M/B	A/M/B
Significato dei documenti economici finanziari	A/M/B	A/M/B	A/M/B	A/M/B	A/M/B
Conclusione complessiva (giudizio)	**A/M/B**	**A/M/B**	**A/M/B**	**A/M/B**	**A/M/B**

A: Alto; M: Medio; B: Basso

Nel corso della valutazione del rischio e della definizione del *rating* del rischio e' importante documentare le considerazioni o il razionale che ha condotto al *rating* del rischio. Le considerazioni illustrate in Figura 37 possono essere usate come punto di partenza, ma ulteriori analisi dovrebbero essere completate e documentate per supportare la valutazione del rischio.

La griglia che segue fornisce una guida sui controlli IT che dovrebbero essere considerati per ogni livello tecnologico. La griglia rispetta la teoria in base alla quale le applicazioni finanziarie che più direttamente supportano i controlli finanziari rappresentano un più alto rischio per il reporting finanziario e, quindi, richiedono una maggiore considerazione. Analogamente, i controlli concernenti la sicurezza fisica, che supportano un ambiente di controllo generale, ma che sono più lontani dagli ambiti di gestione finanziaria, presentano minori rischi e richiedono una minore considerazione. Come sempre, non esiste un approccio universalmente valido, e ogni azienda personalizzerà la griglia basandosi sulle proprie specifiche necessità e circostanze.

Figura 45 – Griglia per l'attribuzione della priorità dei controlli

Intestazioni PCAOB[1]	Controlli IT per la Sarbanes- Oxley	Livelli tecnologici				
		Applicazione	Database	Sistema Operativo	Rete	Ambiente fisico
Cambiamento del programma e sviluppo del programma	Acquisire e sviluppare applicazioni software	**R**	**R**	D	D	D
	Acquisire infrastruttura tecnologica	D	D	D	D	D
	Sviluppare e manutenere policy e processi	**R**	**R**	**R**	**R**	**R**
	Installare e testare applicazioni software e infrastrutture tecnologiche	**R**	**R**	D	D	D
	Gestire i cambiamenti	**R**	**R**	**R**	D	D
Accesso ai programmi, ai dati e all'operatività degli elaboratori	Definire e gestire i livelli di servizio	D	D	D	D	D
	Gestire i servizi di terze parti	**R**	**R**	**R**	D	D
	Assicurare la sicurezza dei sistemi	**R**	**R**	**R**	**R**	D
	Gestire le configurazioni	**R**	**R**	**R**	D	D
	Gestire problemi e incidenti	**R**	**R**	**R**	**R**	D
	Gestire i dati	**R**	**R**	D	D	D
	Gestire l'operatività	**R**	**R**	D	D	D

R – Raccomandato. Controlli IT dovrebbero essere considerati per ogni livello tecnologico come illustrato. L'estensione del lavoro in ciascuna area dipenderà dalla valutazione del rischio inerente
D – Discrezionale. Controlli IT dovrebbero essere considerati dove sono stati identificati dei rischi.

[1] **PCAOB** - Public Company Accounting Oversight Board

Appendice H – Esempio di documentazione di controllo e di Modello per i Test

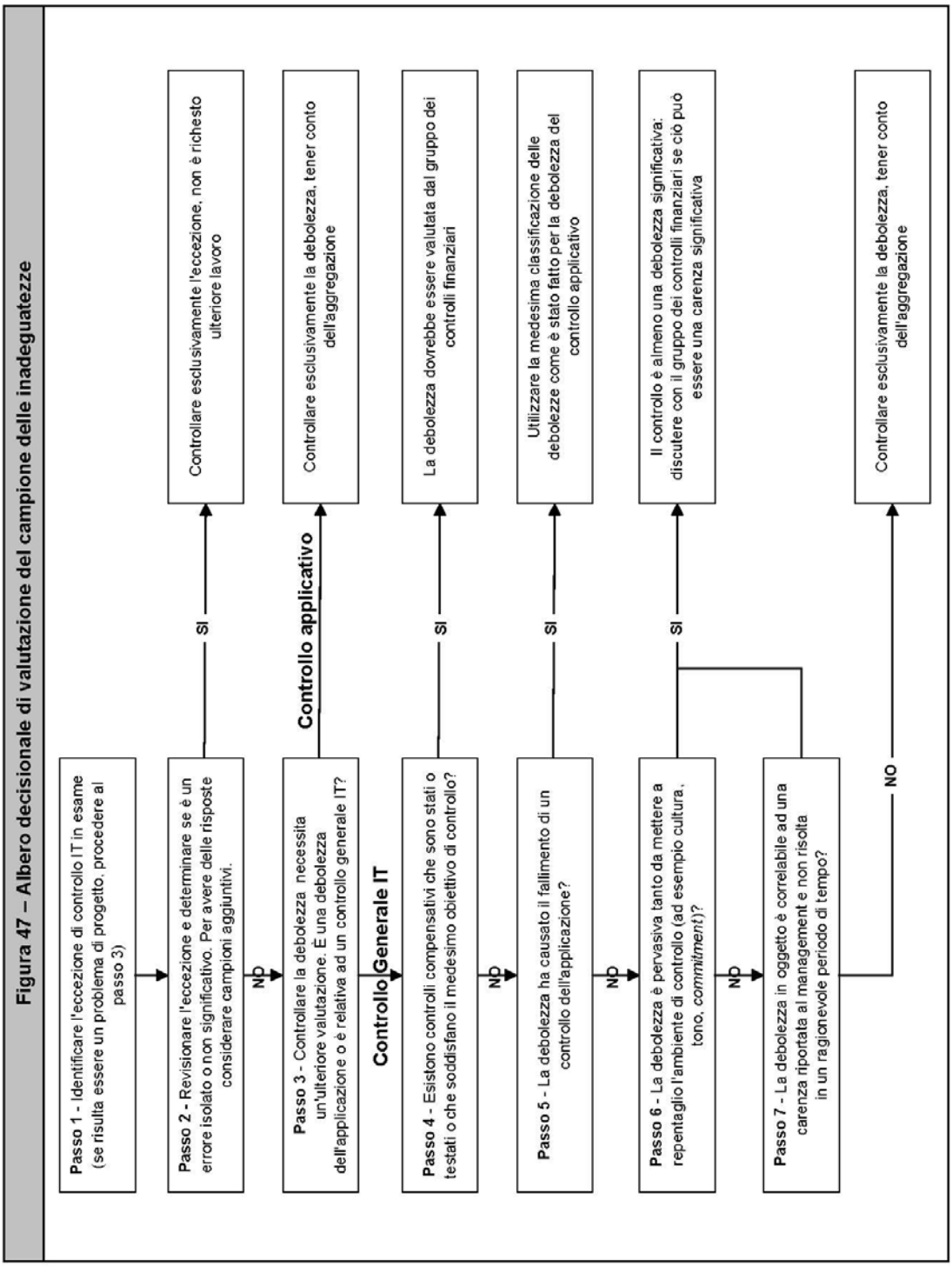
La matrice che segue fornisce una guida relativa ai tipi degli attributi di controllo che dovrebbero essere documentati e mantenuti come parte del programma di conformità. Come sempre, non esiste un approccio universalmente valido, e ogni azienda personalizzerà la matrice basandosi sulle proprie specifiche necessità e circostanze.

Figura 46 – Matrice generale dei Controlli IT

Matrice generale dei controlli IT				
Identificatore dell'obiettivo di controllo				
Conclusione: i controlli risultano operativi con efficacia sufficiente per raggiungere l'obiettivo di controllo				
Attività di controllo	**Frequenza di controllo**	**Ampiezza del campione**	**Test del Controllo**	**Risultati del test**

Appendice I – Albero decisionale di valutazione del campione delle debolezze

L'albero decisionale riportato in Figura 47 può essere utilizzato per supportare la valutazione dei problemi riguardanti la progettazione dei controlli o l'efficienza operativa. Le aziende dovrebbero consultare i propri team incaricati della conformità finanziaria e, in ultima analisi, i propri manager responsabili prima di concludere che una debolezza di controllo e' una carenza significativa o una debolezza materiale. L'albero non e' basato su dichiarazioni prescrittive, ma rispecchia un approccio comunemente seguito da molte aziende.



Appendice J – Approccio campione per i fogli elettronici

Molte aziende utilizzano i fogli elettronici come strumenti di lavoro per la realizzazione del reporting finanziario. Sfortunatamente, i fogli elettronici sono sprovvisti di quei controlli inerenti che molte applicazioni viceversa contemplano, compresi i controlli relativi all'accesso degli utenti e alla gestione delle modifiche. Di conseguenza, in tali elaborazioni sono introdotti rischi significativi.

Il medesimo approccio top-down dovrebbe essere utilizzato per determinare quali fogli elettronici si devono considerare, dal momento che non tutti i fogli elettronici presentano la stessa importanza e lo stesso rischio. L'obiettivo è identificare quali sono i fogli elettronici maggiormente rappresentativi nella elaborazione del reporting finanziario e determinare se sono attivi controlli e se tali controlli sono opportunamente testati.

Per effettuare tale attività, è stato sviluppato, usando come guida la **figura 27**, il seguente approccio in tre fasi. Come sempre, e' necessario considerare il giudizio professionale e personalizzare l'approccio per considerare le necessità specifiche di ciascuna azienda. Le tre fasi sono:

1. Inventario dei fogli elettronici – Usando come punto di partenza la documentazione relativa ai processi di business, catalogare tutti i fogli elettronici che sono coinvolti nella realizzazione del reporting finanziario e documentare il nome del foglio elettronico, il nome del processo di business connesso al foglio elettronico, le scritture contabili del foglio elettronico coinvolte, la descrizione di ciò che il foglio elettronico fa e il valore economico in esso trattato.
2. Valutazione del rischio - Per ciascun foglio elettronico inventariato, valutare l'impatto e la probabilità di errori nel reporting finanziario.
   - Impatto – Quando si valuta l'impatto dei fogli elettronici, le aziende dovrebbero considerare il valore economico trattato dal foglio elettronico e allo stesso tempo il modo in cui il foglio elettronico viene utilizzato.
   - Probabilità – Quando si valuta la probabilità che il foglio elettronico introduca un errore, le aziende dovrebbero considerare la complessità intrinseca del foglio elettronico, il numero degli utenti e la frequenza dei cambiamenti operati sul foglio elettronico stesso.

Nel valutare l'impatto e la probabilità è opportuno considerare la guida illustrata nelle **figure 48 e 49.**

Utilizzando la valutazione dell'impatto e della probabilità, calcolare una valutazione composita del rischio (vedere **figura 50**) moltiplicando i due fattori. Per esempio, un foglio elettronico che ha una valutazione dell'impatto di "2" (Moderato) e una valutazione della probabilità di "3" dovrebbe avere una valutazione composita di rischio di "6" (2*3). Una volta che tutti i fogli elettronici contengono una valutazione composita del rischio, ordinarli di conseguenza per priorità e assicurarsi di riesaminare nel complesso la loro importanza relativa.

Figura 48 – Valutazione dell'impatto			
Considerazioni per valutare l'impatto	**Basso**	**Medio**	**Alto**
Valore economico trattato dal foglio elettronico	Inferiore al 20% della significatività/materialità	Compreso tra il 20% e il 50% della significatività/materialità	Superiore al 50% della significatività/materialità
Utilizzo dei risultati del foglio elettronico	Revisioni analitiche	Comunicazione (disclosure) del rendiconto finanziario	Imputazioni in contabilità generale
Valutazione totale dell'impatto: (1 – Basso, 2 – Moderato, 3 – Alto)			

Figura 49 – Valutazione della probabilità			
Considerazioni per valutare la probabilità	**Basso**	**Medio**	**Alto**
Complessità del foglio elettronico	Bassa (usato a scopo di log o traccia dei dati)	Moderata (calcoli semplici o numero di registrazioni basso)	Alta (modellazione complessa, tabelle pivot, o altre sorgenti di dati)
Numero degli utenti del foglio elettronico	Un utente	Meno di cinque utenti	Più di cinque utenti
Frequenza dei cambiamenti al foglio elettronico	Non frequente	Occasionale	Frequente
Valutazione totale della probabilità: (1 – Basso, 2 – Moderato, 3 – Alto)			

Figura 50 – Valutazione del rischio composito			
Valutazione dell'impatto (1 - 3)	3 (Basso)	6 (Moderato)	9 (Alto)
	2 (Basso)	4 (Moderato)	6 (Moderato)
	1 (Basso)	2 (Basso)	3 (Basso)
	Valutazione della probabilità (1 – 3)		

Una volta completata la valutazione del rischio si deve stabilire il piano d'azione per i fogli elettronici. Di seguito è riportato un piano d'attività da utilizzare come linea guida:

- *Valutazione del rischio composto da 1 a 3*. Il rischio intrinseco è basso. Non è necessario intraprendere azioni.
- *Valutazione del rischio composto da 4 a 6*. Il rischio intrinseco è moderato. Sulle tabelle è necessario implementare controlli e valutazioni descritti ai successivi punti 3a-3c.
- *Valutazione del rischio composto da 7 a 9*. Il rischio intrinseco è alto. Sulle tabelle è necessario implementare controlli e valutazioni descritti ai successivi punti 3a-3g.

3. Implementazione/valutazione dei fogli elettronici - In funzione della valutazione del rischio composto (vedi punti precedenti), può essere necessario attivare ulteriori controlli sulla base delle linee guida sotto elencate. Altri controlli possono essere ritenuti necessari in funzione delle circostanze e dell'uso dei fogli elettronici:
   - a) Controlli d'accesso – Limitare l'accesso ai fogli elettronici memorizzandoli sul server e mettendo in atto le necessarie restrizioni d'accesso
   - b) Controllo delle modifiche - Definire il processo da seguire per modificare i fogli elettronici; il processo deve prevedere che i cambiamenti siano documentati in una pagina dello stesso foglio elettronico.
   - c) Documentazione – Garantire che la documentazione del foglio elettronico sia continuamente aggiornata e consenta la piena comprensione degli obiettivi di business e delle specifiche funzioni della stessa.
   - d) Test – Collaudare ufficialmente il foglio elettronico utilizzando personale non coinvolto nel processo di business. Il collaudatore deve confermare che l'elaborazione del foglio elettronico e i relativi output operino come previsto.
   - e) Controllo dei dati in entrata – Verificare e confermare che i dati sono stati inseriti completamente e accuratamente riconciliando i dati in ingresso con i documenti dai quali sono stati tratti.
   - f) Sicurezza e integrità dei dati – Prevenire accessi non autorizzati e cambiamenti involontari del foglio elettronico, bloccando o proteggendo le celle critiche che sono importanti ai fini dell'elaborazione dei dati, come formule e dati cardine.
   - g) Controlli logici – Controllare la logica del foglio elettronico ricorrendo a personale non coinvolto nello sviluppo o nell'uso del foglio elettronico. Questo controllo deve essere documentato formalmente.

Appendice K – Lezioni Apprese

Nel corso del primo e secondo anno d'implementazione della Sarbanes-Oxley si sono apprese molte cose. Nelle **figure da 51 a 56** sono elencate e illustrate, in modo non esaustivo, le esperienze maturate; l'elenco è organizzato secondo le sei fasi delineate nel percorso di conformità IT riportate in **figura 3**.

Figura 51—Lezioni Apprese—Pianificazione e Ambito	
Lezioni apprese e Vie d'uscita	
a) Strutture organizzative e di reporting inadeguati non hanno permesso di integrare completamente l'IT nello Steering Committee del Sarbanes-Oxley dell'azienda. Questo ha comportato che le comunicazioni fossero globalmente inefficaci.	Le aziende dovrebbero costituire un sottocomitato dedicato al controllo dello IT integrato nello Steering Committee del Sarbanes-Oxley. Il sottocomitato IT dovrebbe sovrintendere al processo IT della Sarbanes-Oxley, agevolare comunicazioni e l'integrazione con l'insieme del progetto Sarbanes-Oxley e rendere più agevole il compito degli auditor indipendenti coinvolti nel processo IT della Sarbanes-Oxley.
b) Non è stata chiaramente attribuita la responsabilità dei controlli IT. Le aree di confusione più ricorrenti sono state l'identificazione dei responsabili di business delle applicazioni più rilevanti e dei responsabili dei controlli applicativi e dei fogli elettronici più importanti. Quanto sopra ha comportato difficoltà nell'assicurare che i controlli IT operativi soddisfacessero i requisiti della sezione 404.	La responsabilità dei controlli IT dovrebbe essere chiaramente attribuita. I responsabili business delle applicazioni più importanti dovrebbero essere chiaramente identificati. La responsabilità dei controlli per le applicazioni e dei fogli elettronici più significativi, nonché per gli altri strumenti d'elaborazione degli utenti finali, dovrebbe essere regolata con un accordo formale.
c) In molti casi non è stato ben compreso l'ambito iniziale del processo d'implementazione della sezione 404. Applicazioni irrilevanti ai fini del processo di reporting finanziario non sono state escluse e altre che si sarebbero dovuto includere lo sono state solo su sollecitazioni degli auditor esterni. Questo ha portato a sovra-sotto stimare l'ambito dei controlli IT finalizzati a soddisfare i requisiti della sezione 404. Spesso non è stato seguito l'approccio top-down per la pianificazione dei controlli IT e la definizione del loro ambito. Sia il management sia gli auditor spesso hanno iniziato le attività di test senza prendere in considerazione l'impatto sui rischi di altri controlli COSO. Per l'attività di controllo è stata spesa una notevole quantità di lavoro che si sarebbe potuta risparmiare ricorrendo ad altri controlli meno costosi in	La disponibilità di altre line guida PCAOB nonché l'esperienza maturata negli ultimi due anni, per conformarsi ai requisiti della sezione 404, ha portato a una migliore comprensione del processo di definizione della documentazione e della reale efficacia dei controlli IT. Le aziende dovrebbero far leva sulle esperienze maturate, e fare riferimento alla sezione della road map in cui si definiscono gli ambiti, per adottare un più lineare e produttivo processo d'identificazione degli ambiti della documentazione e del test dell'efficacia dei controlli IT. Le aziende dovrebbero adottare un approccio top-down analogo a quello descritto nella sezione di definizione e pianificazione degli ambiti di questa pubblicazione, per evitare il sovra-sotto dimensionamento del test dei controlli IT e implementare un processo di definizione degli ambiti più semplice e produttivo.

Figura 51— Lezioni Apprese—Pianificazione e Ambito (*segue*)	
Lezioni apprese e suggerimenti	
grado di limitare la probabilità di non individuare carenze nei controlli. L'assenza di un approccio top-down, porta facilmente ad una sovra-sotto stima dell'ambito dei controlli IT.	
d) I piani d'implementazione non prevedevano piani di comunicazione. In assenza di piani formali di comunicazione, i nuovi controlli non sempre erano implementati in modo efficace. I piani di comunicazione sono necessari per far sì che gli interessati siano informati dei progressi e delle loro responsabilità.	I piani di comunicazione dovrebbero essere inclusi come parte dei piani di lancio dei nuovi controlli. Per esempio dovrebbe esserci un piano per comunicare al personale e fornitori le nuove linee d'indirizzo, man mano che sono sviluppate.
e) Nei piani d'implementazione non sono stati inclusi i tempi necessari agli auditor esterni. Di conseguenza alcune attività di competenza degli auditor esterni sono state eseguite più tardi di quanto desiderabile. In alcuni casi, alcune carenze significative sono state identificate solo verso la fine del progetto ed è stato possibile rimediare solo dopo la fine dell'anno.	La pianificazione degli interventi degli auditor esterni dovrebbe essere completata all'inizio dell'anno; i tempi d'esecuzione delle attività dovrebbero essere concordati contestualmente. I tempi dovrebbero essere comunicati a tutti i responsabili dei controlli IT. Questo dovrebbe garantire tempo sufficiente per rimediare, già in corso d'opera, a carenze significative e quindi permettere agli auditor l'esecuzione dei test di fine anno.
f) Sono state perse occasioni per implementare controlli standard o centralizzati, o non è stato preso in considerazione il potenziale impatto sulle strategie di test dell'attivazione di controlli standardizzati e processi/controlli centralizzati. Questo ha portato a controlli interni inefficaci e all'aumento degli sforzi connessi all'esecuzione dei test.	Le aziende dovrebbero implementare una piattaforma di controlli interni standardizzata e centralizzata per facilitare il raggiungimento di una migliore produttività progettuale e operativa. Le aziende dovrebbero anche personalizzare le strategie di collaudo per renderle compatibili con strutture di controllo interno standardizzate e centralizzate. Questo approccio permetterebbe di migliorare l'efficacia e l'efficienza del processo di controllo dei test.
g) Spesso le comunicazioni fra i team Sarbanes-Oxley finanziari/operativi e il team IT sono scarse. Entrambi i team identificano controlli che riguardano gli stessi obiettivi di controllo. In alcune occasioni è stata persa l'opportunità di basarsi su controlli automatici piuttosto che sui manuali ed è stata sbagliata la valutazione dell'affidabilità dei controlli posi in atto dagli altri team. Questo ha portato a ridondanze non desiderate.	I team Sarbanes-Oxley finanziari/operativi e IT dovrebbero collaborare per assicurare comunicazioni efficaci. I team dovrebbero integrare/condividere, ove possibile, la valutazione dei controlli, manuali e automatici, e arrivare, per ogni processo di business, a una conclusione condivisa sull'efficacia complessiva dei controlli. I due team dovrebbero collaborare, ove appropriato, per far sì che sia attribuita una maggiore affidabilità ai controlli automatici rispetto a quelli manuali.
h) Il processo di conformità era poco automatizzato e basato essenzialmente su fogli elettronici e strumenti di scrittura (word processing). Era spesso difficile seguire i progressi o identificare le cause alla base di carenze di controllo che potevano essere risolte con un approccio unificato.	Le aziende dovrebbero prendere in considerazione l'automazione del processo di conformità per aumentare la produttività, seguire più efficacemente i progressi dell'attività e identificare le cause alla base d'ogni carenza nei controlli.

Figura 51—Lezioni Apprese—Pianificazione e Ambito (*segue*)	
Lezioni apprese e Vie d'uscita	
i) L'insieme di competenze necessarie per affrontare l'implementazione è spesso risultato carente, p.es. mancavano competenze per la progettazione dei controlli, la valutazione dei rischi e la documentazione. Nell'ultimo trimestre diventava sempre più difficoltoso trovare e avere risorse d'audit competenti queste ultime erano, infatti, impegnate a soddisfare le richieste di audit obbligatori. Spesso i consulenti esperti erano più costosi di quanto inizialmente previsto. Aumentava così il rischio di non riuscire a rimediare a tutte le carenze identificate e di non soddisfare i requisiti della sezione 404.	Le aziende dovrebbero pianificare le attività in modo da garantire la disponibilità di risorse con le competenze necessarie. Per disporre dell'insieme di competenze richieste, la pianificazione potrebbe comprendere il reclutamento, la terziarizzazione delle attività o l'addestramento di risorse interne.
j) L'audit interno ha spesso contribuito all'implementazione della 404 a scapito della realizzazione dei piani interni d'audit cosicché aree di rischio al di fuori del reporting finanziario non sono state sottoposte a un adeguato audit. La partecipazione dell'audit interno genera problemi d'indipendenza di giudizio giacché l'audit e il test dei controlli non dovrebbero essere effettuati dagli stessi auditor che li hanno progettati. Questo può avere impatti sulle future attività interne di audit.	Il comitato di audit e lo Steering Committee del Sarbanes-Oxley dovrebbero coordinare e approvare con molto anticipo l'assegnazione di risorse all'audit interno e alle attività di conformità alla sezione 404. Gli auditor interni dovrebbero solo raccomandare i controlli e i responsabili di processi di business dovrebbero avere l'ultima parola nel determinare, approvare e implementare i migliori controlli. La conformità alla sezione 404 dovrebbe essere realizzata, se possibile, come parte dell'evoluzione di un processo di business piuttosto che come progetto a cadenza annuale.
k) Non è stata presa in considerazione la possibilità di inserire fra le normali funzioni dell'audit interno il test del processo di auto-valutazione dei controlli. Non è stato considerato il potenziale impatto di un processo di auto-valutazione dei controlli per ridurre i test delle attività di controllo.	Le aziende dovrebbero prendere in considerazione l'uso di processi di auto-valutazione dei controlli per limitare i test delle attività di controllo.
l) Il solo fatto che un'applicazione sia inclusa nell'ambito implica che essa necessita significativi controlli applicativi richiesti per la conformità alla Sarbanes-Oxley. Nella maggior parte dei casi è stato necessario valutare l'applicazione e i relativi sottosistemi anche se l'applicazione gestiva un numero molto limitato di controlli applicativi significativi. Questo ha comportato la documentazione e il test dei controlli per applicazioni che si sarebbero potuto escludere dall'ambito.	Per ridurre lo sforzo complessivo, se l'applicazione è soggetta a un solo controllo si dovrebbe prendere in considerazione la possibilità di eliminarlo (insieme all'applicazione stessa) identificando contemporaneamente uno specifico controllo manuale e/o aumentando l'affidabilità di un controllo manuale già esistente. Sebbene accada raramente, tale eventualità dovrebbe essere attentamente valutata dalle aziende che hanno molte applicazioni con un numero molto limitato di controlli. In queste situazioni occorre fare molta attenzione a non affidarsi incautamente ai controlli disponibili (p.es. facendo affidamento su report generati dal sistema).

Figura 52— Lezioni Apprese —Valutazione dei Rischi	
Lezioni Apprese e Vie d'uscita	
a) Spesso non sono stati considerati i rischi associati ai controlli generali IT. I livelli dei test sono stati spesso eccessivi rispetto a quanto necessario per aree a basso rischio. Al contrario, non è stato valutato che a un alto livello di rischio deve corrispondere un alto livello di test. L'incapacità di valutare il rischio nell'ambiente IT riguardo al reporting finanziario, ha comportato sovra-sotto valutazioni ai fini della conformità alla sezione 404. Spesso non sono stati valutati i rischi connessi ai controlli generali IT. L'assenza di una valutazione del rischio nell'ambiente IT in rapporto al reporting finanziario, ha comportato la sovra-sotto valutazione dell'ambito ai fini della conformità alla sezione 404.	Le aziende dovrebbero esaminare il processo descritto nella fase 2, Valutazione rischi IT, della sezione di conformità IT della Road Map, personalizzandolo per le loro specifiche necessità.

Figura 53— Lezioni Apprese —Identificare e Documentare i Controlli	
Lezioni Apprese e Vie d'uscita	
a) In un gran numero di casi gli auditor esterni non sono stati consultati in merito a natura ed estensione della documentazione richiesta. Questo ha fatto sì che alcuni processi fossero sovra documentati, e quindi che la relativa documentazione invecchiasse precocemente, oppure sotto documentati, e quindi che fosse necessario ulteriore attività per adeguarla.	Le aziende dovrebbero operare in stretta collaborazione con i loro auditor esterni fin dall'inizio dell'anno, collaborando affinché l'ambito, l'approccio utilizzato, la natura e l'estensione della documentazione e i documenti prodotti soddisfino i requisiti. Le aziende e i loro auditor esterni dovrebbero, per tutto il corso dell'anno, mantenersi in comunicazione continua affinché siano recepite al più presto le nuove richieste e linee guida di SEC e PCAOB.
b) Non è stato adottato un approccio olistico per la struttura dei controlli. Durante il processo di valutazione del rischio non è stato preso in considerazione l'impatto dell'insieme di controlli manuali, di controlli automatici delle applicazioni, di controlli generali IT, di controlli di monitoraggio (includendo i controlli svolti periodicamente dagli auditor interni) e di controllo dell'ambiente, si è così trascurata la possibilità di ridurre il rischio di svolgere test non necessari	Le aziende dovrebbero adottare un approccio olistico alla struttura dei controlli per far sì che auditor finanziari e IT lavorino insieme per valutare l'impatto dell'intero ambiente di controllo dell'azienda. Dovrebbe essere inclusa la revisione dei controlli manuali, dei controlli applicativi automatizzati, dei controlli generali IT, dei controlli di monitoraggio e la determinazione dell'approccio ottimale al collaudo dei test.

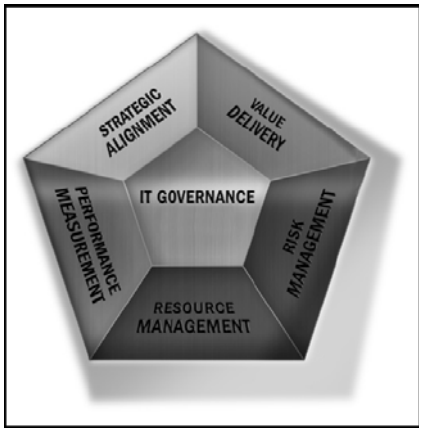
Figura 54 — Lezioni Apprese — Valutare l'Efficacia Progettuale e Operativa	
Lezioni Apprese e Vie d'uscita	
a) Spesso la documentazione dei processi è diventata l'obiettivo più importante invece che essere d'ausilio all'identificazione di controlli significativi. Questo ha fatto sì che non fossero pienamente identificati tutti i controlli significativi.	La documentazione dei processi non è il fine bensì il mezzo che mette a disposizione un ragionevole supporto per documentare i processi di business a supporto dei conti e delle transazioni aziendalmente più rilevanti. Come parte di questo processo, le aziende dovrebbero identificare i rischi che potrebbero comportare dichiarazioni inesatte e i controlli non posti in atto per evitare questi rischi. Successivamente, all'identificazione dei conti significativi, delle asserzioni e dei processi rilevanti, per identificare i controlli da testare le aziende dovrebbero tener presente i passi descritti nella terza fase della Road Map della conformità IT.
b) In alcune situazioni sono stati considerati pertinenti tutti i controlli identificati dando così luogo a test non necessari.	Le aziende dovrebbero differenziare criticamente i controlli rilevanti dagli altri controlli per garantire che sia possibile porre in essere un adeguato livello di sforzo per documentare ed eseguire i test dei controlli significativi. Come già rilevato in precedenza, le aziende per identificare i controlli da testare dovrebbero tener presente i passi descritti per la terza fase della Road Map della conformità IT.
c) Non è stata presa in considerazione la documentazione richiesta per i controlli generali IT guidati dai parametri e per quelli guidati dai processi. Questo ha comportato che la documentazione della struttura di controllo interno fosse inadeguata.	Lo sforzo di documentazione e valutazione dei controlli interni dovrebbe prendere in considerazione i controlli generali IT guidati dai parametri e quelli guidati dai processi.
d) In alcuni casi nella lista centralizzata dei gap non sono stati inclusi i gap di controllo manuale, i gap dei controlli applicativi IT e i gap dei controlli generali IT. Questo ha reso difficile misurare il potenziale compensativo dei controlli e valutare la possibilità di correggere centralmente i gap di controllo piuttosto che lasciare che più gruppi creassero soluzioni differenti per lo stesso problema.	Le aziende dovrebbero predisporre un repository centralizzato dei gap includendovi i gap dei controlli manuali, i gap del controllo delle applicazioni IT e i gap dei controlli generali. Dovrebbero anche essere identificati i possibili controlli compensativi per identificare le soluzioni correttive più adatte.
e) Nel corso della stima dell'efficacia operativa in alcuni casi sono stati rieffettuati i controlli generali IT guidati da parametri. Questo ha comportato la generazione di documentazione e test ridondanti.	Di regola le aziende non dovrebbero dar vita ad attività di documentazione e test dei controlli IT ridondanti. Questo si applica, tra l'altro, alla rivisitazione dei controlli generali IT guidati da parametri.

Figura 54— Lezioni Apprese — Valutare l'Efficacia Progettuale e Operativa (*segue*)	
Lezioni Apprese e Vie d'uscita	
f) Il report degli auditor delle società di revisione non sono stati mappati sulla matrice controllo-rischio (che dovrebbe includere anche i controlli dell'azienda). Questo ha comportato che non fossero individuati dei controlli significativi. Analogamente, spesso c'è stata incertezza sulla possibilità di prendere in considerazione i controlli documentati nella descrizione della azienda, prodotta dalla società di revisione, ma non inclusi nella relazione di audit, oppure richiedere un'ulteriore attività di test.	Le aziende dovrebbero includere nella matrice controllo- rischio i controlli e i risultati dei test riportati dagli auditor delle società di revisione. Questo permetterebbe di prendere in considerazione tutti i controlli significativi, interni o esterni, per valutare i controlli d'insieme e aggregati. I controlli descritti nei report degli auditor delle società di revisione dovrebbero essere ritenuti affidabili.

Figura 55— Lezioni Apprese — Prioritizzare e Correggere le Carenze	
Lezioni Apprese e Vie d'uscita	
a) In alcuni casi, laddove è stato il management a identificare i controlli significativi e le carenze, gli auditor esterni hanno messo in discussione le valutazioni del management. Il management ha accettato le valutazioni degli auditor esterni ed eseguito attività supplementari. Questo ha comportato che alcune carenze fossero identificate in ritardo, nell'anno. Di conseguenza il management non ha avuto tempo sufficiente per porre in atto azioni correttive.	Le aziende dovrebbero comunicare con gli auditor esterni, continuativamente e fin dall'inizio dell'attività, per garantire che i controlli significativi identificati dal management soddisfino le attese e l'ambito degli auditor esterni. Questo consentirebbe al management di evitare di svolgere attività supplementari a fine anno.

Figure 56— Lezioni Apprese — Costruire la Sostenibilità	
Lezioni Apprese e Vie d'uscita	
a) Spesso non sono stati attivati processi di revisione o valutazione del processo d'implementazione della Sarbanes-Oxley finalizzati a identificare i possibili miglioramenti che sarebbero potuti essere apportati. Al termine del processo della sezione 404 per l'anno in corso è iniziato quello dell'anno successivo. Quando le revisioni post-implementazione sono state realizzate, non sempre sono stati coinvolti tutti gli stakeholder. Questo modo d'operare può portare a perdere l'opportunità d'identificare modifiche al processo di conformità che permettono di risparmiare tempo e costi.	Le aziende dovrebbero svolgere revisioni post-implementazione finalizzate a identificare i possibili miglioramenti al processo Sarbanes-Oxley. Alla revisione dovrebbero partecipare gli stakeholder. I manager potrebbero cosi far tesoro delle lezioni apprese e implementare, per l'anno successivo, piani d'attività più efficienti.

Figure 56— Lezioni Apprese — Costruire la Sostenibilità (*segue*)	
Lezioni Apprese e Vie d'uscita	
b) Non è stata presa in considerazione l'opportunità di estendere la struttura di verifica di conformità alla Sarbanes-Oxley per verificare la conformità in altre aree e alle policy complessive della azienda. Questo ha comportato la duplicazione degli sforzi necessari per soddisfare molteplici requisiti regolamentari e di governance.	Le aziende dovrebbero prendere in considerazione l'estensione della struttura di controllo di conformità alla Sarbanes-Oxley per includervi le policy aziendali e altri requisiti regolamentari. Questo permetterebbe di ottimizzare l'insieme degli sforzi organizzativi finalizzati alle verifiche di conformità.
c) La verifica di conformità alla sezione 404 è spesso partita come progetto a se stante, finalizzato a soddisfare i requisiti regolamentari, e il processo di governance della IT non è stato integrato in quello di governance aziendale. Questo ha comportato l'incapacità di mantenere la conformità nel lungo termine.	Le aziende dovrebbero valutare l'integrazione nel processo di governance aziendale delle seguenti aree focali della governance IT: - Allineamento strategico - Sviluppo di valore - Gestione delle risorse - Gestione del rischio - Misura delle prestazioni. Per maggiori informazioni fare riferimento alla **figura 57** ed al COBIT 4.0. L'implementazione della governance IT aiuta le aziende a migliorare continuamente l'affidabilità del modello, vedi **figura 5,** e a costruire la sostenibilità del processo di conformità a lungo termine.

Figura 57— Focus sulle aree dell'IT Governance	
	• **L'allineamento strategico** (**Strategic alignment)** è focalizzato: ad assicurare il collegamento fra il business e la pianificazione IT; a definire, mantenere e validare le principali proposte IT; ad allineare le operazioni IT a quelle aziendali. • **Lo sviluppo del valore (Value delivery)** riguarda la realizzazione delle principali proposte IT attraverso il ciclo di realizzazione e rilascio; la garanzia che l'IT renda disponibili i benefici promessi rispetto alla strategia, concentrandosi sulla ottimizzazione dei costi e sulla dimostrazione del valore intrinseco dell'IT. • **La gestione delle risorse (Resource management)** riguarda l'ottimizzazione degli investimenti e la corretta gestione delle risorse IT critiche comprese le applicazioni, informazioni, infrastrutture e personale. Problemi fondamentali sono l'ottimizzazione della conoscenza e delle infrastrutture. • **La gestione del rischio (Risk management)** richiede che l'alta direzione sia cosciente dei rischi, abbia una chiara comprensione della propensione dell'azienda al rischio, la comprensione dei requisiti di conformità, la chiara comprensione dei rischi più significativi per l'azienda e l'inclusione nella organizzazione della responsabilità di gestione del rischio. • **La misura delle prestazioni (Performance measurement)** traccia e tiene sotto controllo le strategie d'implementazione, il completamento dei progetti, l'uso delle risorse, l'esecuzione del processo e la consegna del servizio, utilizzando, per esempio, tabelle ponderate di punteggio (scorecards) per tradurre la

	strategia in azioni necessarie per raggiungere gli obiettivi misurabili al di là delle tradizionali forme di contabilizzazione.

Appendice L
Problemi nell'utilizzo dei Report di verifica del SAS 70

Molte aziende spostano all'esterno parte delle loro operazioni, inclusi i sistemi informativi, per fornire i servizi alle organizzazioni. Gli standard di Auditing AICPA US alla sezione 324 "Organizzazioni di Servizio" (SAS 70), paragrafo 3 (AU 324.03), stabiliscono quanto segue:

> *I servizi resi da una società di servizi fanno parte del sistema informativo di un'azienda se influiscono su una qualsiasi delle seguenti voci:*
> • *Le classi di transazioni delle operazioni significative ai fini del bilancio dell'azienda.*
> • *Le procedure, automatizzate e manuali, tramite le quali sono avviate, registrate, elaborate e rese note le transazioni dal momento in cui iniziano fino alla loro inclusione nel bilancio.*
> • *Le registrazioni contabili correlate, automatizzate e manuali, che supportano l'informazione e le specifiche poste del bilancio delle aziende coinvolte nell'avviare, registrare, elaborare e rendere note le sue transazioni.*
> • *Il modo con cui il sistema informativo dell'azienda cattura altri eventi e condizioni significativi ai fini del bilancio.*
> • *Il processo di reporting finanziario impiegato per preparare il bilancio dell'azienda, inclusa la divulgazione e la stima di dati contabili rilevanti.*

Quando i servizi resi da una società di servizi sono parte integrante del sistema informativo dell'azienda cliente, essi entrano a far parte dei controlli interni sul reporting finanziario e quindi il management, in conformità con il PCAOB Auditing Standard No. 2, deve considerare, nella fase di valutazione dei controlli interni sui dati contabili, le attività della società di servizi.

Gli standard di auditing No. 2 consentono al management, e alle società di auditing, di fare affidamento, se la relazione SAS 70 è ritenuta sufficiente, sulle relazioni degli auditor delle società di servizi relative ai controlli in essere e ai test d'efficacia operativa (relazione SAS 70) a supporto della valutazione e del giudizio (opinion).

La parte restante di quest'appendice identifica i problemi connessi agli argomenti della SAS 70 che possono esistere o emergere quando si valuta se la relazione SAS 70 è soddisfacente.

Ambito

Diversi argomenti possono portare alla conclusione che l'ambito della reportistica SAS 70 è insufficiente per provare l'efficacia dei controlli svolti dalle società che forniscono servizi; alcuni degli argomenti sono riportati qui di seguito:

- La descrizione dei controlli non è pertinente o lo è solo per una parte dei servizi esternalizzati che fanno parte dei sistemi informativi.

- La descrizione dei controlli non copre a sufficienza le sedi della società di servizi che erogano servizi agli utenti dell'azienda.
- La società di servizi a sua volta subappalta dei servizi e quest'ultimi sono stati esclusi dall'ambito dei report SAS 70 e quindi non sono disponibili i relativi report.
-
- In questi casi il management e gli auditor dovrebbero considerare di:
- Pervenire alla comprensione dei controlli in essere sulle operazioni svolte dalle società di servizi che non sono coperti nei report SAS 70, ma sono rilevanti ai fini delle dichiarazioni finanziarie dell'azienda.
- Ottenere evidenza, tramite test diretti o con altri mezzi, che i controlli funzionano correttamente.

Nell'esecuzione di queste procedure, il management e gli auditor dovrebbero essere consapevoli che le procedure da eseguire possano cambiare in funzione dell'importanza dei controlli presso le società di servizi per le valutazioni del management e in funzione del livello d'interazione fra i controlli dell'azienda e i controlli delle società di servizi.

Descrizione dei Controlli

Il paragrafo 20 degli "PCAOB Auditing Standard No. 2" stabilisce che la descrizione dei controlli stabilita dalle società di servizi è progettata per permettere alle aziende utenti e agli auditor di ottenere:

> *… la comprensione dei controlli, attuati presso le società di servizi, rilevanti ai fini dei controlli interni dell'azienda e dei controlli da svolgere presso l'azienda sulle attività delle società di servizi.*

Mentre la società di servizi è responsabile della correttezza della descrizione dei controlli e il suo auditor valuta la correttezza della descrizione, aspetti specifici dei processi dell'azienda utente e affermazioni presenti nel reporting finanziario possono far sì che la descrizione dei controlli della società di servizi possa non soddisfare le necessità dell'azienda utente e dei suoi auditor.

Problema: La descrizione dei controlli non è sufficientemente dettagliata per permettere al management o all'auditor di:

- Identificare quali tipi d'affermazioni presenti nel reporting finanziario possono essere influenzati dai controlli e da fonti di dichiarazioni inesatti.
- Prendere in considerazione i fattori che influiscono sui rischi d'errore sostanziale (material).
- Supportare le valutazioni del management sui controlli svolti internamente.
- Supportare l'opinion degli auditor sui controlli interni.

Problema: gli obiettivi di controllo specificati dal management della società di servizi, non contemplano tutti i rischi, presenti nel reporting finanziario, identificati dal management dell'azienda utente o non sono sufficientemente descritti per capire se i rischi sono stati presi in considerazione.

Problema: I controlli identificati dal management sono insufficienti, a giudizio del management o degli auditor dell'azienda utente, per soddisfare gli specifici obiettivi di controllo collegati alle affermazioni contenute nel reporting finanziario dell'azienda utente.

Problema: La descrizione dei controlli non riporta informazioni sufficienti sui controlli IT ad alto livello per consentire all'azienda e ai propri auditor, di valutare la loro efficacia operativa nello stabilire, migliorare o mitigare l'efficacia dei controlli IT a livello attività.

Questi problemi spesso possono essere risolti aggiungendo alla descrizione dei controlli presenti nei report SAS 70 le informazioni disponibili nei manuali utente, nel sistema, nei manuali tecnici, nei contratti fra aziende utente e società di servizi, nei rapporti degli auditor interni e le autorità che disciplinano le società di servizi. Può essere necessario integrare queste informazioni con altre ottenute, oralmente o in forma scritta, direttamente dalle società di servizi.

Problema: La descrizione dei controlli non riporta quelli che dovrebbero esistere presso l'azienda utente che sono contemplati nel progetto dei controlli della società di servizi.

Normalmente i controlli delle società di servizi sono progettati in modo da coinvolgere nei controlli interni le aziende utenti del servizio. Se nella descrizione dei controlli non sono identificati quelli da svolgere a cura dell'azienda utente, le aziende utenti e i loro auditor dovrebbero valutare se sia o no necessario identificarli. Nello svolgere la valutazione, gli utenti dei servizi dovrebbero mettere a confronto, e riportarle nei controlli del rapporto SAS 70, le potenziali fonti di dichiarazioni inesatte da loro identificate.

Tempificazione

Esiste un compromesso, insito tra la necessità del management e dell'auditor, di ottenere la valutazione più aggiornata possibile sui controlli della società di servizi e il bisogno di ricevere il report SAS 70 con una tempestività sufficiente a consentire che qualsiasi eccezione di controllo od opinion qualificata sull'obiettivo del controllo possano essere valutate e il relativo rischio possa essere mitigato. Questo compromesso spesso comporta che la data del report SAS 70 preceda quella del bilancio dell'azienda utente, e ciò genera due problemi che potrebbe essere necessario affrontare.

Primo, sono sopravvenuti cambiamenti rilevanti nel periodo intercorso fra l'esecuzione dei test d'efficacia operativa e la data in cui è stata svolta la valutazione del management.

Se ci sono stati cambiamenti significativi ai controlli operanti presso la società di servizi, allora il management e l'auditor dovrebbero prendere in considerazione la necessità di:

- Capire quali controlli, rilevanti ai fini del reporting finanziario dell'azienda, sono cambiati
- Ottenere l'evidenza che i controlli che sono cambiati operino in modo efficace.

Notifiche delle modifiche, aggiornamenti dei manuali tecnici, materiale didattico e altri tipi di comunicazione della società di servizi spesso bastano al management e all'auditor per capire l'effetto dei cambiamenti su quanto dichiarato nel reporting finanziario Potrebbe tuttavia essere necessario rivolgere delle richieste aggiuntive al personale della società di servizi e ricevere documentazione supplementare.

L'evidenza che i controlli, che sono cambiati, operano in modo efficace può essere più difficile da ottenere. Se la società di servizi mantiene l'efficacia dei controlli generali IT, allora il management e l'auditor potranno essere in grado di aver la prova, presso il sito dell'azienda stessa, del funzionamento dei cambiamenti attraverso il test diretto dei controlli applicativi o la partecipazione ai test di accettazione utente e l'esame dei relativi risultati.

In altri casi, i controlli che sono cambiati possono essere ridondanti rispetto altri controlli posti in essere presso l'azienda. In casi come questi, il management e l'auditor potrebbero scegliere di testare i controlli ridondanti. Gli stessi potrebbero infine giungere alla determinazione che i controlli possono essere testati soltanto presso il sito della società di servizi e in questi casi aver bisogno di recarsi presso la società di servizi o di prendere accordi affinché l'auditor della società di servizi proceda al test dei controlli che sono cambiati e rilasci un rapporto contenente il risultato delle procedure concordate o un attestato.

La natura e l'ampiezza delle procedure seguite dal management e dall'auditor varieranno con l'importanza attribuita ai controlli nelle valutazioni dal management stesso, e con il livello di interazione tra i controlli dell'azienda utente e i controlli attuati presso la società di servizi.

Il secondo problema riguardante la tempificazione è quella relativo a quando è intercorso un lasso significativo di tempo tra il periodo coperto dai test di efficacia operativa e la data delle asserzioni del management.

In un caso come questo, sussiste un rischio che i controlli presso la società di servizi siano cambiati o abbiano cessato di operare con efficacia. Il management dovrebbe eseguire delle procedure per identificare tutti i casi in cui siano avvenuti cambiamenti del genere. Le procedure da seguire sono discusse nell'Auditing Standard n. 2 del PCAOB, dal paragrafo B25 al B27, e se un cambiamento è intervenuto nei controlli della società di servizi, allora esso dovrebbe essere valutato secondo quanto sopra descritto.

Natura e Ampiezza dei Test

Quando la natura e l'ampiezza dell'attività di test eseguita dall'auditor della società di servizi non sono per il management aziendale un supporto sufficiente alla valutazione dei controlli in funzione del reporting finanziario, occorre che management e l'auditor dell'azienda stessa intraprendano procedure aggiuntive.

Problema: Il report comprende i controlli messi in atto, ma non include i test di efficacia operativa.

Problema: I test di efficacia operativa dei controlli specificati dalla società di servizi non mettono a disposizione sufficienti evidenze a supporto di una conclusione sui rischi di controllo per le asserzioni del reporting finanziario dell'azienda.

L'Audit Standard n. 2 del PCAOB, al paragrafo B21, riporta:

> *Un rapporto dell'auditor di una società di servizi che non includa i test dei controlli, i risultati degli stessi e la sua opinion sull'efficacia operativa (in altre parole, i report sui controlli messi in atto descritti nel paragrafo .24a della sezione 324 di AU) non forniscono evidenza di efficacia operativa.*

Esiste un problema simile se i controlli specificati nel report non sono stati testati a sufficienza per capire se hanno influenza sui rischi relativi al reporting finanziario identificati dal management. Il SAS 70 stabilisce che in questi casi:

> *L'evidenza che i controlli rilevanti ai fini della valutazione del management e dell'opinion dell'auditor, operano in modo efficace, può essere acquisita seguendo le procedure descritte nel paragrafo .12 della sezione 324 dell'AU. Tali procedure includono:*
>
> *a. Eseguire alcuni test dei controlli che l'azienda effettua sulle attività della società di servizi (per esempio, testare la riesecuzione indipendente da parte dell'azienda di alcune elaborazioni eseguite dalla società di servizi o testare la riconciliazione che l'azienda effettua tra gli output e i documenti di origine).*
>
> *b. Eseguire test dei controlli presso la società di servizi.*

Se la società di servizi mette a disposizione il report relativo a procedure concordate, che riporta i risultati delle procedure eseguite per testare l'efficacia operativa dei controlli illustrati nella descrizione dei controlli, il management e l'auditor dovrebbero valutare se il test effettuato è sufficiente, secondo criteri simili a quelli adottati per valutare i report sui controlli resi operativi.

Problema: La descrizione dei test sui controlli non è presentata con un dettaglio sufficiente, in merito alla natura, la tempificazione e l'ampiezza dell'attività di test, tale da consentire al management dell'azienda o al suo auditor di valutare il rischio di controllo per le asserzioni relative al reporting finanziario.

In questo caso, il management e l'auditor dovrebbero discuterne con la società di servizi e i suoi auditor per ottenere più informazioni sulla descrizione dei test. Questo genere di richieste, e le risposte, dovrebbero essere documentate secondo gli standard, e la descrizione dei test valutata in base alla sufficienza delle risposte ottenute.

Se non si può arrivare a una discussione del genere, allora lo specifico test dovrebbe essere considerato come fonte di materiale insufficiente a costituire evidenza per una conclusione.

Problema: La descrizione dei test effettuati sugli aspetti rilevanti dell'ambiente di controllo, informazione e comunicazione, valutazione del rischio, e monitoraggio relativi ai servizi forniti non è sufficiente per permettere al management dell'azienda o all'auditor di valutare la loro efficacia operativa, nello stabilire, migliorare l'efficacia o attenuare la debolezza dei controlli dichiarati.

Secondo il SAS 70, se la descrizione dei test effettuati non include il test degli "aspetti rilevanti dell'ambiente di controllo, informazione e comunicazione, valutazione del rischio, e monitoraggio relativi

ai servizi forniti“, il management dell’azienda e l’auditor dovrebbero considerare l’importanza di questi controlli ai fini della valutazione e del livello di interazione tra i controlli aziendali e i controlli della società di servizi. Il management aziendale e l’auditor dovrebbero quindi considerare l’esecuzione di procedure limitate per testare questi controlli chiedendo di visionare ed esaminare le dichiarazioni depositate a norma di legge e altri documenti.

Problema: Descrivendo i risultati dei test di efficacia operativa effettuati, la descrizione delle eccezioni (es. ampiezza del campione, numero di eccezioni rilevate, natura delle eccezioni, fattori causali, azioni correttive o altre informazioni qualitativamente rilevanti) non è sufficiente per permettere al management o all’auditor di valutarne l’impatto sul rischio di controllo per le asserzioni del reporting finanziario.

In questo caso, il management e l’auditor dovrebbero essere in grado di discutere con la società di servizi e i suoi auditor per ottenere più informazioni sulla descrizione della(e) eccezione(i). Questo genere di richieste, e le risposte, andrebbero documentate secondo gli standard, e il controllo valutato in base alla sufficienza delle risposte ottenute.

Se non si può pervenire a una discussione del genere, allora il management e l’auditor dovrebbero considerare il controllo come non operante in modo efficace e dovrebbero valutarne l’impatto sulle asserzioni del reporting finanziario.

Qualifiche ed Eccezioni

Problema: L’opinion dell’auditor della società di servizi o le eccezioni riferite nell’ambito della sezione del report “Informazioni fornite dall’auditor della società di servizi” portano alla conclusione che gli aspetti del controllo interno in carico alla società di servizi sono inefficaci.

Quando l’opinion dell’auditor della società di servizi contiene una qualifica dell’opinion stessa o viene annotata un’eccezione nella descrizione dei risultati del test, il management dovrebbe identificare la qualifica o l’eccezione come una carenza di controllo, e individuare tutti i controlli implementati che la compensano o che, altrimenti, mitigano il rischio associato alla carenza. La carenza dovrebbe quindi essere valutata secondo la metodologia di valutazione delle carenze adottata dall’azienda.

Problema: Le qualifiche contenute nell’opinion dell’auditor della società di servizi non sono descritte in maniera sufficiente tale da permettere al management dell’azienda o all’auditor di valutarne l’impatto sul rischio di controllo per le asserzioni del reporting finanziario.

In questo caso, il management e l’auditor dovrebbero discuterne con la società di servizi e i suoi auditor per ottenere più informazioni sulla descrizione della qualifica. Questo genere di richieste, e le risposte, andrebbero documentate secondo gli standard, e sia l’obiettivo di controllo sia i controlli relativi andrebbero valutati in base alle risposte ottenute.

Se non si riuscisse a organizzare una discussione del genere, allora il management e l'auditor dovrebbero considerare gli obiettivi di controllo come non raggiunti, e valutarne l'impatto sulle asserzioni del reporting finanziario.

Auditor della società di servizi

Problema: la reputazione, competenza, indipendenza e professionalità dell'auditor della società di servizi non sono a un livello sufficiente da costituire un supporto alla valutazione del management aziendale e all'opinion dell'auditor.

Lo Standard di Auditingn.2 del PCAOB,ne paragrafo B24, prescrive:

> *Nel determinare se il rapporto dell'auditor della società di servizi fornisca un'evidenza sufficiente a supportare la valutazione del management e l'opinion dell'auditor, management e auditor dovrebbero informarsi sulla reputazione, la competenza e l'indipendenza dell'auditor della società di servizi. Le fonti più appropriate d'informazione sulla reputazione professionale dell'auditor della società di servizi sono oggetto del paragrafo 10° dell'AU sezione 543, intitolato "Part of Audit Performed by Other Independent Auditors".*

Laddove reputazione, competenza, indipendenza o professionalità dell'auditor della società di servizi non fossero sufficienti, il management e l'auditor dovrebbero giudicare come non sufficienti la natura e l'ampiezza delle procedure adottate, e procedere secondo le modalità descritte nei casi precedenti.

Appendice M - Separazione dei compiti nelle principali applicazioni contabili

L'adeguata separazione dei compiti è un aspetto importante da considerare nel determinare se le attività di controllo di un'azienda sono efficaci per conseguire gli obiettivi del controllo interno. Il concetto alla base delle separazioni dei compiti è che nessun dipendente o gruppo di dipendenti dovrebbe essere in una posizione tale da poter commettere e contemporaneamente nascondere errori o frodi nel normale svolgimento dei propri compiti. In generale, i principali compiti incompatibili da separare sono:

- Autorizzazione o approvazione delle transazioni relative ai beni aziendali
- Custodia dei beni
- Registrazione o reporting delle relative transazioni

I sistemi tradizionali di controllo interno hanno fatto affidamento sull'assegnare questi compiti a individui diversi, o nel separare funzioni incompatibili. Tale separazione dei compiti è intesa a impedire che un addetto abbia sia l'accesso ai beni sia la responsabilità di mantenere l'assegnazione della titolarità sui beni stessi. Nell'ambiente IT la separazione dei compiti è storicamente ritenuto e comprovato come fattore critico dei controlli generali. Per esempio, le aziende implementano controlli che limitano ai soli addetti autorizzati la possibilità di passare programmi in produzione. Allo stesso modo, le aziende normalmente separano il compito di richiedere l'accesso ai sistemi e ai dati da quello di concederlo.

E' comunque altrettanto critica un'adeguata separazione dei compiti anche a livello di applicazione/processo di business. In un sistema di gestione dell'inventario, per esempio, differenti addetti sono responsabili per mansioni quali:

- Attivare o richiedere un acquisto
- Porre o immettere ordini d'acquisto
- Ricevere merci
- Assicurare la tenuta degli inventari
- Mantenere le registrazioni inventariali e/o autorizzare la rettifica ai costi o alle quantità, compresa l'autorizzazione all'eliminazione o allo scarto
- Effettuare modifiche agli archivi dell'inventario
- Eseguire conteggi indipendenti d'inventario
- Fare il follow-up a fronte di discrepanze rilevate durante il conteggio d'inventario
- Autorizzare richieste di produzione e/o trasferimenti di materiali
- Ricevere/trasferire merci in/dalla produzione
- Spedire merci.

Per molte aziende identificare, a livello di applicazione, queste mansioni incompatibili o in conflitto costituisce una difficoltà. Gli ambienti basati su sistemi legacy comportavano necessariamente e facilitavano la separazione dei compiti a causa della struttura di controllo prevalentemente manuale che li circondava. Anche la frammentazione dei sistemi legacy facilitava la separazione dei compiti, perché i sistemi per gli acquisti, per l'inventario e per la contabilità generale erano separati. Questa concezione tradizionale della separazione dei compiti necessita di essere ridefinita nel caso di ambienti ERP totalmente automatizzati. I sistemi ERP hanno riposizionato l'enfasi sulla responsabilizzazione degli utenti, abilitandoli ad avere accesso alle funzioni di business o anche a gestire i beni fisici e registrarne la movimentazione direttamente all'interno dei sistemi informatici e contabili. La nozione di controllo sulla

separazione dei compiti va quindi ampliata affinché includa una prospettiva di gestione del rischio e un bilanciamento delle contromisure.

Ci sono vari approcci all'identificazione di conflitti relativi alla separazione dei compiti a livello di processo aziendale. Quelli di seguito sono due esempi di strumenti/schemi che le aziende potrebbero utilizzare/adattare per i loro ambienti. Il primo in f**igura 58** può essere più applicabile ai sistemi legacy, e il secondo in f**igura 59** ai sistemi integrati.

La **figura 58** è l'illustrazione di un approccio, adottato in relazione a un'applicazione vendite, mirato a mettere in evidenza compiti tra loro in conflitto. Si potrebbero creare documenti dello stesso genere anche per altre applicazioni significative coinvolte nel reporting finanziario. Lo schema si compila indicando il nome, o i nomi, di chi è responsabile di ciascuna delle funzioni nell'ambito delle applicazioni elencate. Se una delle funzioni è svolta da un'applicazione informatica, allora come individuo si può inserire "computer" oppure "IT".

Figura 58 - Applicazione Vendite

	Autorizzazione	Custodia dei Beni	Registrazione	Attività di Controllo
Emette ordini d'acquisto				
Approva il credito e I suoi termini				
Approva l'accesso agli archivi correlati al credito				
Autorizza le spedizioni				
Imposta i documenti di spedizione				
Gestisce l'elenco delle merci in attesa di spedizione				
Imposta la fatturazione				
Verifica l'accuratezza della fatturazione				
Approva l'accesso agli archivi correlati ai prezzi				
Approva le deroghe ai prezzi standard				
Verifica la completezza della fatturazione				
Gestisce il conto vendite				
Gestisce la contabilità clienti				
Provvede alla quadratura tra spedizioni e fatturazioni				
Provvede alla quadratura tra la contabilità clienti e la contabilità generale				

Una volta compilati i moduli per ognuna delle applicazioni significative, questi vanno rivisti per tutti i casi in cui un singolo addetto esegue compiti che dovrebbero essere considerati incompatibili. Esistono compiti potenzialmente incompatibili se un singolo addetto esegue compiti di più di una categoria (autorizzazione o approvazione, custodia, o registrazione/reporting) o se un singolo addetto è responsabile dell'effettuazione di un controllo sulla stessa transazione per la quale egli stesso è responsabile della registrazione/reporting. Inoltre, quando nessuno esegue un compito questo può indicare una carenza nei controlli. Tenete presente che non in tutti i casi, in cui un singolo addetto esegue compiti in più d'una colonna, ciò debba significare mancanza di separazione dei compiti. Occorre che le aziende, poi, prendano in considerazione la possibilità della mancanza di separazione dei compiti nell'ambito della stessa categoria (p.es. il singolo addetto che autorizza il credito approva anche la cancellazione dei crediti inesigibili).

Una volta identificato il caso di un addetto che esegue compiti incompatibili, si dovranno riconsiderare tutti i compiti da lui svolti per capire se l'efficacia di quei compiti sia ridotta o annullata a causa della mancanza di separazione tra loro. Se è così, il passo successivo è quello di occuparsi degli effetti sui controlli esercitati sull'applicazione e del rischio di errore o di frode. Se si identifica un incremento di rischio, le aziende dovranno cercare altri controlli in grado di prevenire o annullare tale rischio e di questi valutare l'efficacia. Se non si trovassero altri controlli, il rischio di errore sul reporting finanziario sarebbe maggiore, e questo a causa della mancanza di separazione dei compiti.

Un secondo approccio alla valutazione della separazione dei compiti consiste nell'utilizzo di una matrice che elenca le funzioni del business aziendale. Nell'ambito della conformità alla sezione 404 della Sarbanes-Oxley, molte aziende hanno sviluppato matrici di questo genere che rispecchiano la loro ottica di gestione del rischio e il bilanciamento tra accesso funzionale e sicurezza. Bisognerà modellare questi schemi su ognuno dei processi di business aziendali all'interno dell'azienda e realizzare il giusto equilibrio tra le potenzialità attribuite e il bisogno di minimizzare il rischio di frode o di transazioni non autorizzate.

La **figura 59** è un esempio dell'applicazione di questo concetto alla funzione aziendale di acquisto-pagamento. Come illustrato nell'esempio, una "x" indicherebbe una funzione incompatibile in base alla definizione di compiti incompatibili fissata dal management.

Figura 59 - Matrice Separazione dei Compiti Acquisti-Pagamenti

Funzioni	Creare e mantenere la lista fornitori	Approvare / rilasciare ordini di acquisto	Trattare la ricezione della merce	Trattare le fatture dei fornitori	Trattare i pagamenti in contanti	Sbloccare le fatture bloccate	Inserire le note di debito verso fornitori
Creare e mantenere la lista fornitori		X	X	X			
Approvare / rilasciare ordini di acquisto			X	X			
Trattare la ricezione della merce				X			
Trattare le fatture dei fornitori						X	X
Trattare i pagamenti in contanti							X
Sbloccare le fatture bloccate							
Inserire le note di debito verso fornitori							

Le tecniche specifiche per automatizzare il test di separazione dei compiti vanno oltre gli argomenti trattati in questa sede. E' tuttavia un punto di partenza il prendere in considerazione quei report che potrebbero essere già disponibili all'interno del sistema stesso. Si dovrebbe inoltre prendere anche in considerazione il software di audit per automatizzare quanto più possibile il processo di revisione e di test.

Appendice N - Indice delle Figure

Riferimenti

Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Guidance for Smaller Public Companies Reporting on Internal Control over Financial Reporting*, USA, July 2006, *www.coso.org*

Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Enterprise Risk Management Framework*, USA, September 2004, *www.coso.org*

Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Internal Control—Integrated Framework*, USA, 1992, *www.coso.org*

CSE (Canada), SCSSI (France), BSII (Germany), NLNCSA (Netherlands), CESG (UK), NIST (USA) and NSA (USA), *Common Criteria and Methodology for Information Technology Security Evaluation*, 1999

Deloitte & Touche LLP, "Moving Forward–A Guide to Improving Corporate Governance Through Effective Internal Control," 2003

Deloitte & Touche LLP, "Taking Control, A Guide to Compliance with Section 404 of the Sarbanes-Oxley Act of 2002," 2003

Dewitt, Ron; "Managing Change is Managing People," 30 April 2004, *www.cioupdate.com*

Ernst & Young LLP, "The Sarbanes-Oxley Act of 2002, The Current Landscape—Rules, Updates and Business Trends," 2003

International Organization for Standardization (ISO), *Code of Practice for Information Security Management*, ISO/IEC 17799, Switzerland, 2005

IT Governance Institute, COBIT 4.0, USA, 2005, *www.itgi.org*

IT Governance Institute, *Board Briefing on IT Governance, 2nd Edition*, USA, 2003, *www.itgi.org*

IT Governance Institute, *IT Governance Implementation Guide*, USA, 2003, *www.itgi.org*

KPMG, "The Defining Issues—Implications of Proposed Auditing Standard on Internal Control," 2003

LaMarsh & Associates Inc., Managed ChangeTM Model, USA

Office of Government Commerce (OGC), Central Computer and Telecommunications Agency (CCTA), IT Infrastructure Library (ITIL), UK, 1989

Public Company Accounting Oversight Board, "Report on the Initial Implementation of Auditing Standard No. 2," Standard: Release No. 2005-023, USA, 30 November 2005

Public Company Accounting Oversight Board, Staff Questions and

Answers on Auditing Internal Control Over Financial Reporting, USA, 16 May, 21 January 2005

Public Company Accounting Oversight Board, Staff Questions and Answers on Auditing Internal Control Over Financial Reporting, USA, 22 November, 6 October 2004

Public Company Accounting Oversight Board, Staff Questions and Answers on Auditing Internal Control Over Financial Reporting, USA, 23 June 2004, revised 27 July 2004

Public Company Accounting Oversight Board, "An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements," Final Auditing Standard: Release No. 2004-00 1, USA, 9 March 2004

PricewaterhouseCoopers LLP, "The Sarbanes-Oxley Act of 2002, Strategies for Meeting New Internal Control Reporting Challenges," 2003

PricewaterhouseCoopers LLP, "Understanding the Independent Auditor's Role in Building Trust," 2003

Securities and Exchange Commission, Concept Release Concerning Management's Reports on Internal Control Over Financial Reporting (Release No. 34-54122, File No. 57-11-06), USA, 11 June 2006

Securities and Exchange Commission, SEC Announces Next Steps for Sarbanes-Oxley Implementation, USA, 17 May 2006

Securities and Exchange Commission, Commission Statement on Implementation of Internal Control Reporting Requirements, USA, 16 May 2005

Securities and Exchange Commission, Office of the Chief Accountant, "Division of Corporation Finance: Staff Statement on Management's Report on Internal Control Over Financial Reporting," USA, 16 May 2005

Securities and Exchange Commission, Office of the Chief Accountant, "Division of Corporation Finance: Management's Report on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports-Frequently Asked Questions," USA, revised October 6, 2004

Securities and Exchange Commission, "Final Rule: Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports," Release Nos. 33-8238; 34-47986; IC-26068; File Nos. S7-40-02; S7-06-03, USA, June 2003, *www.sec.gov/rules/final/33-8238.htm*

Attribuzioni

Le Figure 2, 3, 4, 30, 31, 32, 33 e 34 in questo documento sono state fornite da Deloitte & Touche LLP.