Sarbanes-Oxley Act
Sezione 404 (Internal Control over Financial Reporting)

Relatori: Marco Bozzola, Ilaria Faedo

22 novembre 2010

ERNST & YOUNG
Quality In Everything We Do

Agenda

- Introduzione al Sarbanes-Oxley Act
- Le sezioni della SOX – 302 e 404
- La sezione 404
- Fasi di un progetto SOX
  - Process mapping
  - Assessment
  - Remediate and report
- Esempio di un progetto SOX
- Attività dell'External Auditor
- La SOX all'italiana: Legge sul Risparmio (262/2005)

ERNST & YOUNG
Quality In Everything We Do

Introduzione al Sarbanes-Oxley Act

- Il Sarbanes-Oxley Act diventa legge il 30 luglio 2002
- Rappresenta la risposta del legislatore statunitense ai noti scandali finanziari che hanno scosso il mercato americano a partire dal 2001 (fra i quali Enron e WorldCom) ed è considerata la riforma più significativa in questo ambito dal 1930.
- Riforma la contabilità delle società quotate ai mercati finanziari statunitensi.
- Si pone come obiettivo il ripristino della fiducia degli investitori e la protezione degli azionisti contro possibili frodi attraverso:
  - ✓ il rafforzamento dei principi di corporate responsibility;
  - ✓ l'introduzione di nuovi obblighi di informativa societaria in capo alle società;
  - ✓ il miglioramento della qualità e trasparenza del financial reporting e dell'attività di auditing;
  - ✓ l'aggravio delle sanzioni applicabili a fronte di accertate violazioni della legge e comportamenti fraudolenti da parte del Management della società.

►***Il provvedimento persegue obiettivi di credibilità e trasparenza dell'amministrazione societaria e contabile e si traduce in un'importante riforma strutturale della Corporate Governance***

=

TRASPARENZA e CONTROLLO NEI PROCESSI CONTABILI

Introduzione al Sarbanes-Oxley Act - *segue*

Gli aspetti maggiormente innovati introdotti sono:

Le sezioni della SOX – 302 e 404

Sezione 302

I CEO e i CFO devono personalmente certificare che sono responsabili, ed hanno valutato l'efficacia, delle cosiddette *disclosure controls and procedures*

Sezione 404

MANAGEMENT

Valuta l'efficacia dell'*internal control over finacial reporting* e include nell'*annual report* le conclusioni ad esso relative

EXTERNAL AUDITORS

Attesta e riferisce sulla valutazione del management dell'efficacia dell'internal control over financial reporting

- **analisi** del processo di valutazione adottato dal management;
- **raccolta delle evidenze** relative al disegno e all'operatività dei controlli;
- **valutazione** sulla bontà delle conclusioni del management

La sezione 404

OBBLIGHI DEL MANAGEMENT:

- è **responsabile** dei controlli interni e deve valutarne periodicamente l'efficacia e l'operatività;
- i controlli interni devono essere **documentati**;
- la valutazione deve essere fatta secondo un **modello di controllo idoneo e riconosciuto** (es. *COSO Framework*[1]);
- la valutazione dell'efficacia e idoneità dei controlli deve essere supportata da **idonea evidenza**;
- i revisori esterni non possono, per motivi di indipendenza, sostituirsi al management nello svolgimento di tale attività;
- il management non può certificare che i controlli interni sono efficaci se esiste una ***material weakness*** alla data di attestazione.

Il management deve istituire un processo strutturato e periodico per la valutazione degli *internal controls over financial reporting* (il cosiddetto **MANAGEMENT ASSESSMENT PROCESS**)

[1] *Committee of Sponsoring Organizations of the Tradway Commission*

ERNST & YOUNG
Quality In Everything We Do

La sezione 404 - *segue*

Sulla base di quanto stabilito dal Public Company Accounting Oversight Board (PCAOB), il **Management Assessment Process** dovrà, come minimo, coprire le seguenti attività:

SCOPE:

- ✓ Identificazione dei controlli da valutare
- ✓ Valutazione della rilevanza dei controlli identificati rispetto alla probabilità che il mancato funzionamento di tali controlli si traduca in un errore

ASSESS:

- ✓ Valutazione dell'efficacia del disegno dei controlli (design effectiveness);
- ✓ Valutazione dell'operatività dei controlli (*operating effectiveness);*
- ✓ Identificazione delle carenze del sistema di controllo interno che, in relazione alla loro significatività/probabilità, possano essere qualificate come "Significant Defincencies" e/o "Material Weaknesses"

COMMUNICATE:

- ✓ Comunicazione dei risultati dell'assessment agli adeguati livelli (External Auditors, Audit Committe)

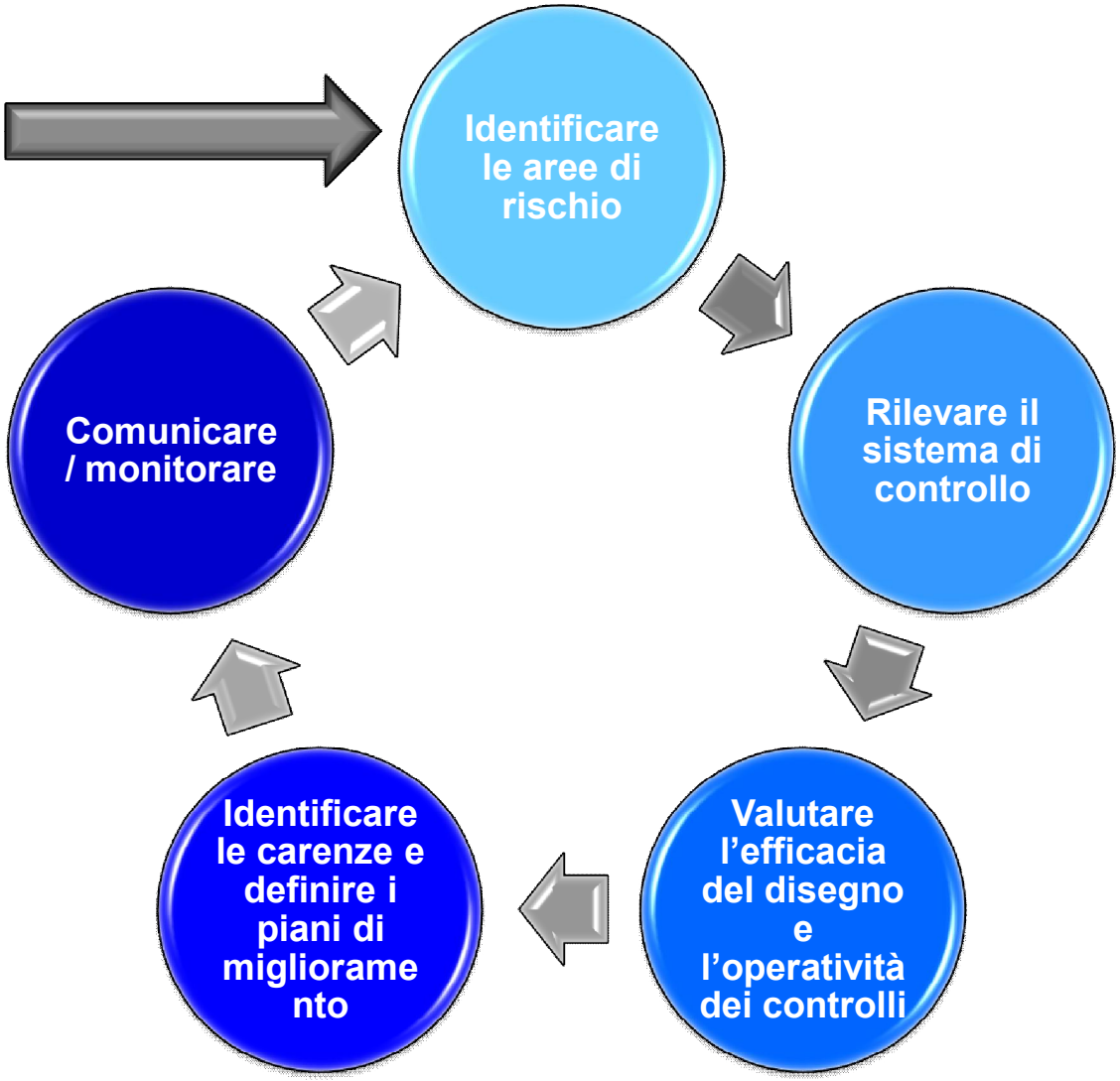
ERNST & YOUNG
Quality In Everything We Do

La sezione 404 - *segue*

DEFINIRE IL PROCESSO

DOCUMENTAZIONE:

- Disegno dei controlli interni (con identificazione dei 5 componenti del SCI);
- Descrizione delle modalità con cui le transazioni significative sono identificate, registrate, elaborate ed identificate;
- Descrizione dei controlli disegnati per prevenire / identificare frodi o errori (responsabilità del controllo e segregazione delle funzioni);
- Risultati dell'attività di verifica



Fasi di un progetto SOX –
Process mapping

- → Definire lo schema generale di classificazione dei processi;
- → Legare i processi alle voci di bilancio;
- → Classificare i processi in base alla loro rilevanza e rischiosità;
- → Centralità del processo di financial reporting;
- → Definire la documentazione a seconda della criticità del processo.

NARRATIVE: descrizione generale del processo con identificazione dei principali ruoli/responsabilità e delle modalità operative e di controllo

RISK and CONTROL MATRIX: identificazione e valutazione delle singole attività di controllo attraverso la compilazione di una matrice

Fasi di un progetto SOX –
Assessment

1) Identificazione rischi / obiettivi di controllo
2) Rilevazione dei controlli
3) Valutare i controlli di alto livello (entity level control – IT general control)
4) Valutazione dei controlli
5) Validazione controlli / testing

CoSo Framework – Sistema di Controllo Interno:

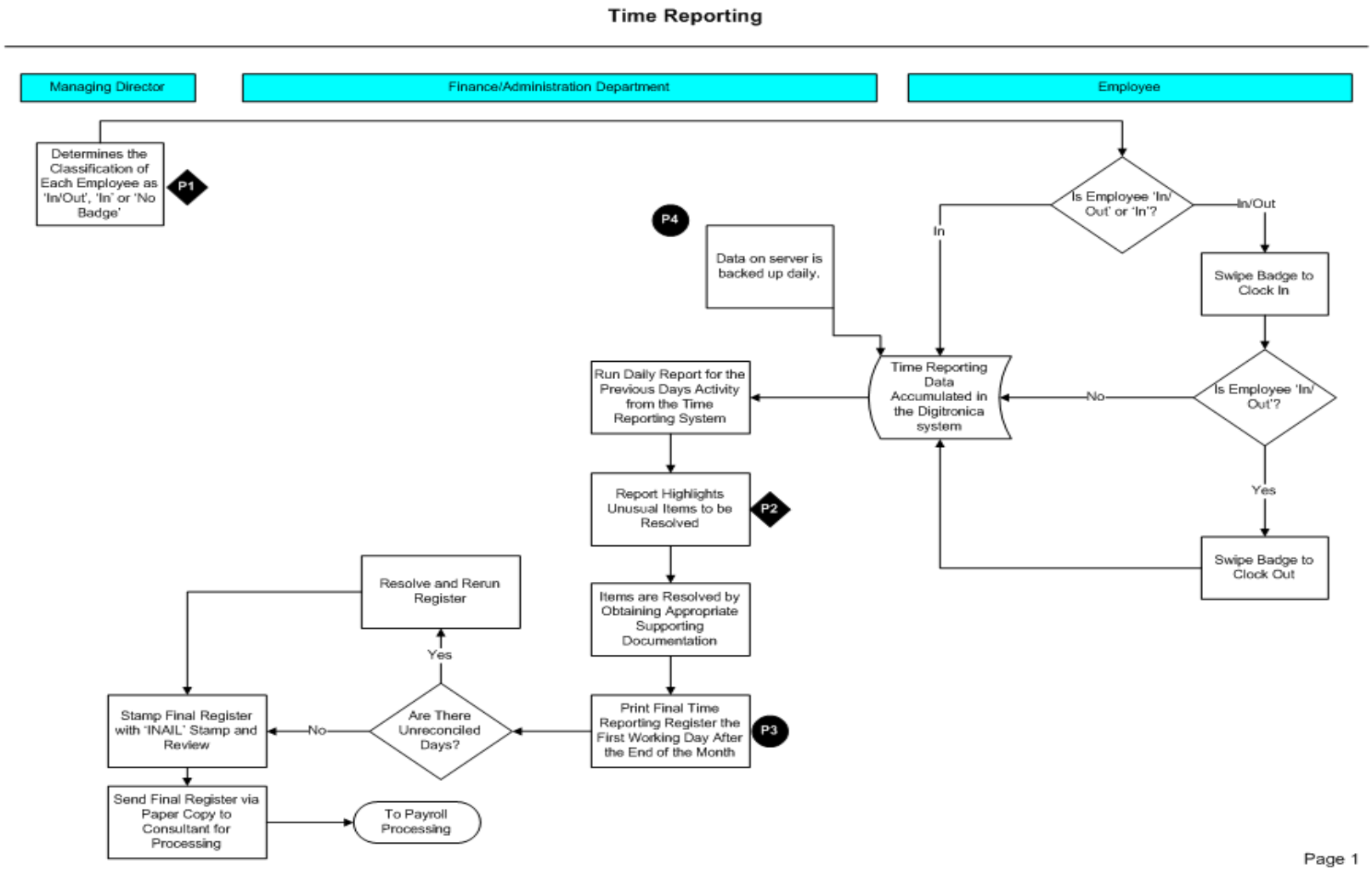
- **MONITORING**: insieme delle attività necessarie per verificare e valutare periodicamente adeguatezza, operatività ed efficacia dei controlli interni
- **INFORMATION and COMMUNICATION**: processo istituito per assicurare la l'accurata e tempestiva raccolta e comunicazione delle informazioni
- **CONTROL ACTIVITIES**: procedure di controllo definite per consentire la riduzione dei rischi ad un livello accettabile e garantire il raggiungimento degli obiettivi aziendali
- **RISK ASSESSMENT**: processo volto ad assicurare l'individuazione, l'analisi e la gestione dei rischi aziendali
- **CONTROL ENVIRONMENT**: ambiente nel quale gli individui operano ("cultura aziendale" in relazione al controllo)

ERNST & YOUNG
Quality In Everything We Do

Fasi di un progetto SOX –
Remediate and Report

- ✓ Valutazione dell'adeguatezza del sistema dei controlli nel suo complesso;
- ✓ Identificazione delle azioni correttive;
- ✓ Definizione di un sistema di monitoraggio;
- ✓ Attestazione del management

Esempio di un progetto SOX –
Procedura del personale (flowchart)



Esempio di un progetto SOX – *segue*
Procedura del personale (Segregation of duties matrix)

Function	Authorization	Record Keeping	Control Procedure
Establish and Maintain Personnel Information (Master Data) Function:			
Authorizes new employees	Managing Director		
Authorizes pay rates/salaries	Managing Director		
Updates employee master file (HR)		Finance Clerk	
Reviews master file changes (HR)			Finance Manager
Payroll Processing Function:			
Updates employee master file (Payroll)		Finance Clerk	
Reviews master file changes (Payroll)			Finance Manager
Accumulates labor hours worked		Finance Clerk	
Approves labor hours worked	Finance Manager		
Generates payroll register		Finance Clerk	
Reviews payroll for propriety			Finance Manager
Disbursing Payroll Function:			
Reconciles payroll bank accounts			Finance Clerk
Approves payroll checks	N/A		
Prepares funds transfer instructions		Finance Clerk	
Authorizes funds transfer instructions	Finance Manager /BoD		
Benefits Processing Function:			
Provides enrollment data to Plan Administrator.		Finance Clerk	
Reviews claims paid & eligibility reports.			Finance Manager
System access administration:			
Authorizes system access (HR)	Finance Manager		
Authorizes system access (Payroll)	Finance Manager		
Grants system access			IT Department
Reviews changes to system access			IT Department

ERNST & YOUNG
Quality In Everything We Do

Esempio di un progetto SOX – *segue*
Procedura del personale (Risk-control matrix)

CONTROL	Time reporting for employees identified as 'In/Out' and 'In' is performed through a automatic system in which badges are scanned	A report from the time tracking system is generated by the Finance Clerk daily for the previous day with unusual items being highlighted	The Finance Clerk generates a final time reporting register on the first working day after each month. Each employee must have the appropriate hours for each day identified	The server in which payroll data is maintained is backed up daily.
RISK	**P1 (IT)**	**P2**	**P3**	**P4 (IT)**
Hours are incorrectly charged between capital projects and expense accounts.		D	D	
Discrepancy between hours worked and hours reported.	P	D	D	
Employees may be paid for hours not worked, resulting in excessive labor costs.	P	D	D	
Lack or loss of information or documents.	P			P
Employee time and attendance information may not be authorized resulting in input of fictitious time and attendance information.		P	D	
Time and attendance data recorded may not reflect actual time worked because of (unintentional or deliberate) errors on employee time cards or time records.	P	D	D	
Payroll records may not be backed-up making it difficult to support disbursements paid to employees.				P

Significant Accounts Affected: Cash, General and Administrative Expense, Sales & Marketing Expense, and Cost of Goods Sold

ERNST & YOUNG
Quality In Everything We Do

Esempio di un progetto SOX – *segue*
Procedura del personale (Testing)

- **Controls**: The Finance Clerk generates a final time reporting register on the first working day after each month. Each employee must have the appropriate hours for each day identified (normal, overtime, holiday, etc.). Finance Manager reviews and signs.

- **Procedures**: Obtain the final time reporting register for 3 months and ensure it has been reviewed and signed by the finance manager.

- **Results**: Obtained the February, April and June final time reporting register noting they were approved by Finance Director.
- **Assessment**: Based upon the testing performed, these controls exist and are effective.
-
- **Review Assessment**: Based on the review of testing, the control is in place and operating effectively.

ERNST & YOUNG
Quality In Everything We Do

Attività dell'*External Auditor*

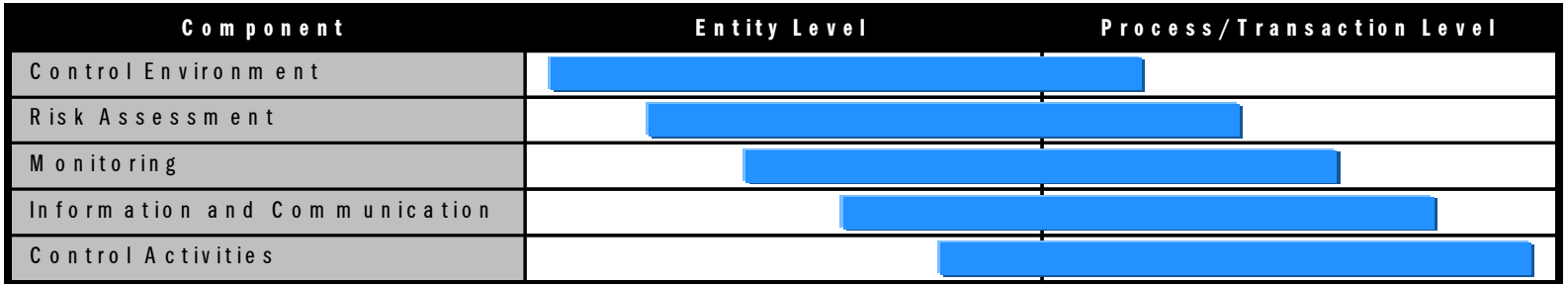
Evaluating Management's Assessment Process

Il management deve:

- Accettare la responsabilità per l'efficacia del controllo interno della società sul financial reporting;
- Valutare l'efficacia del controllo interno della società sul financial reporting in base a criteri adeguati;
- Suppportare la sua valutazione con sufficienti elementi di prova, compresa la documentazione;
- Presentare una valutazione scritta della efficacia dei controlli interni della società rispetto alla rendicontazione finanziaria di fine esercizio della società

Individuare gli Entity Level Controls

"I controlli che esistono a livello aziendale, spesso hanno un impatto pervasivo sui controlli a livello di transazione, di processo o di applicazione. Per tale ragione può essere opportuno per il revisore testare e valutare, prima di tutto, l'efficacia dei controlli a livello aziendale, perché i risultati di tale lavoro potrebbe influenzare il modo in cui il revisore valuta gli altri aspetti dell'*internal control over financial reporting."*



Attività dell'*External Auditor -* *segue*

Fraud Considerations for the Integrated Audit

"Il Management ha la responsabilità di progettare e realizzare programmi e controlli per prevenire, scoraggiare e individuare frodi; la documentazione predisposta dal Management in tale ambito dovrebbe includere i controlli volti a prevenire o individuare le frodi, tra cui:
- che svolge il lavoro;
- relativa segregazione dei ruoli e delle responsabilità."

I revisori hanno la responsabilità di valutare tutti i controlli specificamente destinati a contrastare ("mitigare") il rischio di frode individuati e attuati dalla società.

Identifying Significant Flows of Transactions and Key Controls

Identificare i conti significativi:

- Considerare sia fattori quantitativi e qualitativi (dimensione e la composizione del conto);
- Volume di attività, complessità ed omogeneità
- La natura del conto
- Complessità della contabilità e del reporting associati all'account
- Probabilità (o possibilità) di significative passività potenziali derivanti da attività rappresentata dal conto
- Modifiche rispetto al periodo precedente in considerazione le caratteristiche

ERNST & YOUNG
Quality In Everything We Do

Attività dell'*External Auditor -* *segue*

Identificare le asserzioni significative:

Le asserzioni significative sono asserzioni che hanno un impatto significativo sulla questione se il conto è correttamente iscritto sotto il profilo di: esistenza, presenza, valutazione (e allocazione), misura, completezza, diritti ed obblighi, presentazione e pubblicazione.

Per ogni processo significativo, il revisore deve:

- **Comprendere il flusso delle operazioni**, incluso come le operazioni sono avviate, autorizzate, registrate, elaborate e riportate
- **Individuare i rischi**, cioè i punti all'interno del processo da cui potrebbe derivare una dichiarazione errata – anche a causa di frodi - relativi a ciascuna asserzione
- **Identificare i controlli** che il management ha messo in atto per affrontare questi errori potenziali

► Test of Controls

Natura, tempistica ed estensione dei test sui controlli.

Non si considerano le procedure eseguite da terzi come prova principale, ma si testano a campione per valutare la qualità e l'efficacia del lavoro.

I risultati dei test condotti dal revisore esterno hanno un impatto diretto sulle sue valutazioni circa il Combined Risk Assessments e il livello di affidiabilità dei test condotti dalla società. E' facile intuire che l'inefficacia di alcuni test sui controlli conduce all'aumento del livello di rischiosità (e quindi all'ampiezza delle attività che devono essere svolte dal revisore).

ERNST & YOUNG
Quality In Everything We Do

Attività dell'*External Auditor -* *segue*

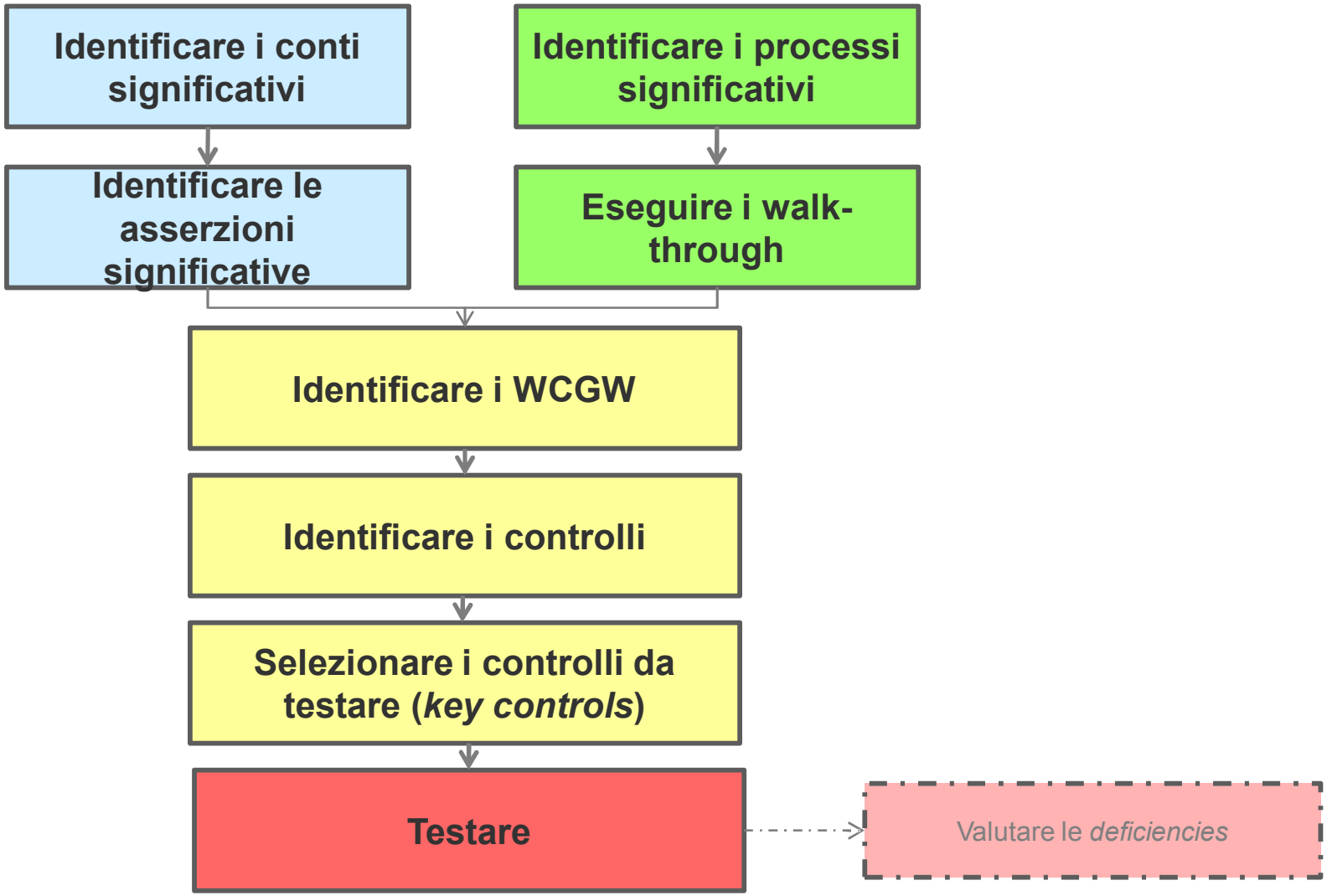
Evaluating Deficiencies

Type	Rischio di errori potenziali	Significatività del potenziale errore
Deficiency	Remoto	Senza conseguenze
Significant Deficiency	Più che remoto	Con conseguenze (non materiali)
Material Weakness	Più che remoto	Conseguenze significative

Il revisore esterno deve valutare se il *management* ha individuato e concluso correttamente circa le eventuali carenze constatate ("carenze significative" o "debolezze materiali"). Se il management non ha svolto completato il proprio *assessment* , il revisore non ha facoltà di esprimere un'opinione sull'efficacia del *internal control over financial reporting*.

ERNST & YOUNG
Quality In Everything We Do

Attività dell'*External Auditor* - *segue*



La SOX all'italiana: Legge sul Risparmio (262/2005)

- Le vicende del mercato nazionale (oltre che i casi internazionali già noti) degli ultimi anni hanno evidenziato una crescente attenzione degli operatori sul tema dell'identificazione e gestione dei rischi aziendali (caso ***Parmalat***).
- I **Governi** e gli **Organismi di Vigilanza** hanno ulteriormente innalzato la sensibilità degli operatori emanando disposizioni e regolamenti che rendono sempre più stringente il binomio **rischi – controlli**, enfatizzando l'importanza ed il ruolo del **Sistema di Controllo Interno.**

SCENARIO NORMATIVO IN ITALIA:

Banca d'Italia e Consob	Prescrivono la predisposizione di un sistema di rilevazione, valutazione, misurazione dei rischi che minacciano il corretto funzionamento ed il raggiungimento degli obiettivi aziendali al fine di rendere più efficienti ed efficaci i processi aziendali
Codice di autodisciplina della Borsa (Preda)	Suggerisce l'istituzione di un Comitato per il Controllo Interno, composto da un numero adeguato di amministratori non esecutivi. Tale comitato ha il compito di analizzare le problematiche ed istruire le pratiche rilevanti per il controllo delle attività aziendali
Principio di comportamento e Guida Operativa del Collegio Sindacale	Attribuiscono al Collegio Sindacale il compito di vigilare sul controllo interno, sull'osservanza della legge, sulla corretta amministrazione e di valutare l'adeguatezza della struttura organizzativa e del sistema amministrativo contabile. Disciplina inoltre i flussi informativi tra il CS e i soggetti preposti al controllo
D.Lgs.58/98 Draghi	Ha introdotto in Italia i principi della "Corporate Governance" ponendo enfasi sulla rilevanza del sistema di controllo interno e sul ruolo dei soggetti che devono assicurare e vigilare sulla sua adeguatezza
D.Lgs.231/01	Ha introdotto la responsabilità amministrativa degli enti e la figura dell'Organismo di Vigilanza quale soggetto deputato al controllo sull'applicazione del Modello di Organizzazione, Gestione e Controllo
Riforma del Diritto Societario	Modifica le norme sul Collegio Sindacale allineandosi alla disciplina del TUF (coerentemente con le disposizioni circa i modelli dualistico e monistico) e pone l'accento sui requisiti soggettivi degli organi di controllo e sull'attività di vigilanza sui principi di corretta amministrazione e sul SCI
Legge sul Risparmio	Interviene direttamente sulla "governance aziendale" introducendo la figura del "Dirigente preposto alla redazione dei documenti finanziari" con responsabilità, tra l'altro, sulla veridicità dei documenti pubblicati, sulla redazione di apposite procedure e sull'applicazione delle stesse.

ERNST & YOUNG
Quality In Everything We Do

La SOX all'italiana: Legge sul Risparmio (262/2005) - *segue*

L. 262/05 (Legge sul Risparmio): l'art. 14, che *modifica l'Art 154-bis del D.Lgs 58/ 98 (TUF),* prevede l'introduzione di un "***dirigente preposto alla redazione dei documenti contabili societari***".

Tale dirigente deve:

- **predisporre adeguate procedure amministrativo contabili** per la predisposizione del bilancio d'esercizio e consolidato e di ogni altra comunicazione diffusa al mercato contenente informazioni e dati sulla situazione economica, patrimoniale e finanziaria. Tali comunicazioni sono accompagnate da una dichiarazione scritta del *Direttore Generale* e del *Dirigente Preposto* che ne attestino la corrispondenza al vero;
- **attestare con apposita relazione** (*) allegata al bilancio sia la **corrispondenza del bilancio** alle risultanze dei libri e delle scritture contabili, sia l'**adeguatezza e l'effettiva applicazione delle procedure amministrativo-contabili** predisposte dal Dirigente stesso

COSA FARE

Documentazione del Sistema di Controllo Interno

- Identificare i processi che alimentano e generano l'informativa di natura patrimoniale, economica e finanziaria
- Formalizzare adeguate procedure amministrativo contabili

Start-up Presidio Governance Amministrativo-Contabile

Valutazione del SCI e Test of Controls

- Fornire alle figure responsabili gli elementi necessari e valutarne ed attestarne periodicamente l'adeguatezza e l'effettiva operatività

(*) Potrebbe essere assimilata al "Management Report on Internal Control", richiesta dalla Section 404 del Sarbanes-Oxley Act

ERNST & YOUNG
Quality In Everything We Do

La SOX all'italiana: Legge sul Risparmio (262/2005) - *segue*

Di seguito è data evidenza dei documenti nei quali si sostanziano tali analisi unitamente alle componenti del SCI impattate.

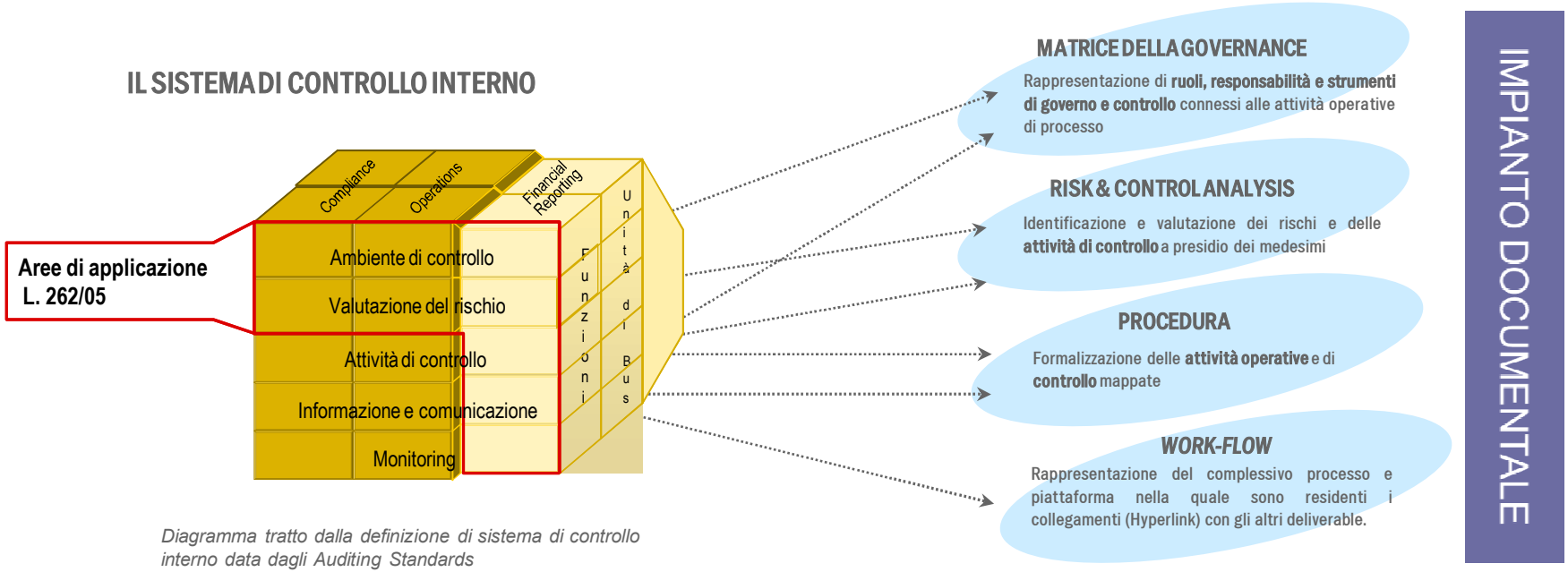


Diagramma tratto dalla definizione di sistema di controllo interno data dagli Auditing Standards

ERNST & YOUNG
Quality In Everything We Do

La SOX all'italiana: Legge sul Risparmio (262/2005) - *segue*

In merito all'adeguatezza delle procedure si rileva che, non prevedendo la normativa italiana specifici standard di riferimento, è naturale attingere alla ormai consolidata esperienza maturata sul mercato statunitense. **Il Dirigente preposto deve predisporre adeguate procedure amministrative e contabili per la formazione del bilancio di esercizio, del bilancio consolidato nonché di ogni altra comunicazione di carattere finanziario**. In tal senso il CoSO Report costituisce la più efficace e testata *best practice* di riferimento per la valutazione del Sistema di Controllo Interno.

Con l'intento di conseguire un'attestazione consapevole e ottemperante al disposto normativo e regolamentare, il Dirigente Preposto è chiamato ad esperire specifiche verifiche (*Test of Controls*), finalizzate ad acclarare la corretta esecuzione da parte delle strutture aziendali responsabili (cd. *Process Owner*) dei controlli, previsti dalle procedure, a garanzia dell'informativa contabile e finanziaria.

L'esecuzione dei *Test of Controls* prevede la definizione di un piano periodico di verifiche che consenta, lungo tutto il periodo di riferimento, di testare estensivamente i controlli previsti dalle procedure amministrative e contabili al fine di pervenire ad una valutazione circa l'effettiva applicazione, nel tempo, delle procedure stesse.

ERNST & YOUNG
Quality In Everything We Do

Grazie.