Sarbanes Oxley Act

Erfahrungsbericht

ENI Group - AGIP Deutschland GmbH

Dipl. Kfm. Dr. Stefan Gros

3.Finance-Gipfel am 09./10. Mai 2005 in Berlin

Einleitung

- ENI Group hat die Wirtschaftsprüfungsgesellschaft Deloitte als Berater im Hinblick auf die Anpassung der internen Kontrollstrukturen and die Anforderungen von Sarbannes Oxley Acts mandatiert..
- Internal Control Readiness und Compliance soll am 30.06.2005 erreicht sein. Die Abschlußprüfung für den Konzernabschluß zum 31.12.2005 soll auch die internen Kontrollstrukturen gemäß SOA beinhalten. Die offizielle deadline wurde von der SEC auf den 31.12.2006 verschoben.
- Die im Folgenden angestellten Betrachtungen stellen die persönlichen Einschätzungen von Herrn Dr. Stefan Gros, CFO AGIP Deutschland GmbH dar und sind nicht die offizielle Auffassung von AGIP Deutschland GmbH, der ENI Group oder von Deloitte!
- Die Betrachtungen erstrecken sich auf erste Erfahrungen der ENI Group, AGIP Deutschland, aber auch auf Erfahrungen von Deloitte.

Agenda

1. Was ist der Sarbanes Oxley Act – was ist neu?

2. Vorgehensweise bei dem SOX –Readyness Projekt

3. Erwartungen des Abschlussprüfers / wiederkehrende Arbeiten

4. Erfahrungen aus der Praxis

5. Chancen in Sarbanes Oxley - Was kommt als nächstes?

Chronologie des Sarbanes-Oxley Act (SOX)

30. Juli 2002	Präsident Bush unterzeichnet den SOX
29. August 2002	SEC erlässt Anwendungsbestimmungen zur Umsetzung von SOX 302
Okt. 2002 – Jan. 2003	SEC schlägt Anwendungsbestimmungen zur Implementierung verschiedener Bestimmungen des SOX
Januar - Juli 2003	SEC veröffentlicht Anwendungsbestimmungen zur Umsetzung der zentralen Bestimmungen des SOX
26. April 2003	Gründung des Public Company Accounting Oversight Board (PCAOB)
22. Oktober 2003	Registrierungszeitpunkt für alle US-WP-Gesellschaften beim PCAOB
19. April 2004	Registrierungszeitpunkt für ausländische WP-Gesellschaften beim PCAOB
15. November 2004	Erstmalige Anwendbarkeit SOX 404 auf US-Unternehmen
15. Juli 2005	Erstmalige Anwendbarkeit SOX 404 auf ausländische Unternehmen

Entwicklung bedeutender US-Kapitalmarktgesetze …

Securities Act (1933)

Ziel:

Schutz der Investoren durch Registrierung von Wertpapieren (FK/EK) sowie Festlegung von Mindestinformationsanforderungen bei der Emission von Wertpapieren

Fokus:

1. Definition der Wertpapiere, die bei der SEC registriert werden müssen
2. Definition der Prospektinformation
3. Definition der SEC Emissionsinformationen

Securities Act (1934)

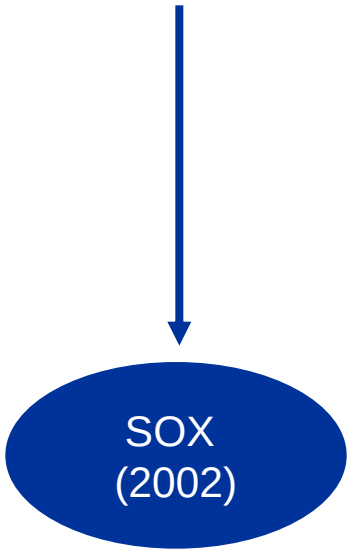
Ziel:

Schutz der Investoren durch Registrierung der Wertpapieremittenten und periodische Berichterstattung

Fokus:

1. Definition relevanter Emittenten sowie der Berichterstattung (10-K, 10-Q, 8-K, etc.)
2. Anti-Fraud-Bestimmungen für Käufer und Verkäufer von Wertpapieren (Insidergeschäfte)
3. Regelungen zur Übertragung von Stimmrechten
4. Offenlegungspflichten bei Aktienübernahmen

… Sarbannes Oxlex Act



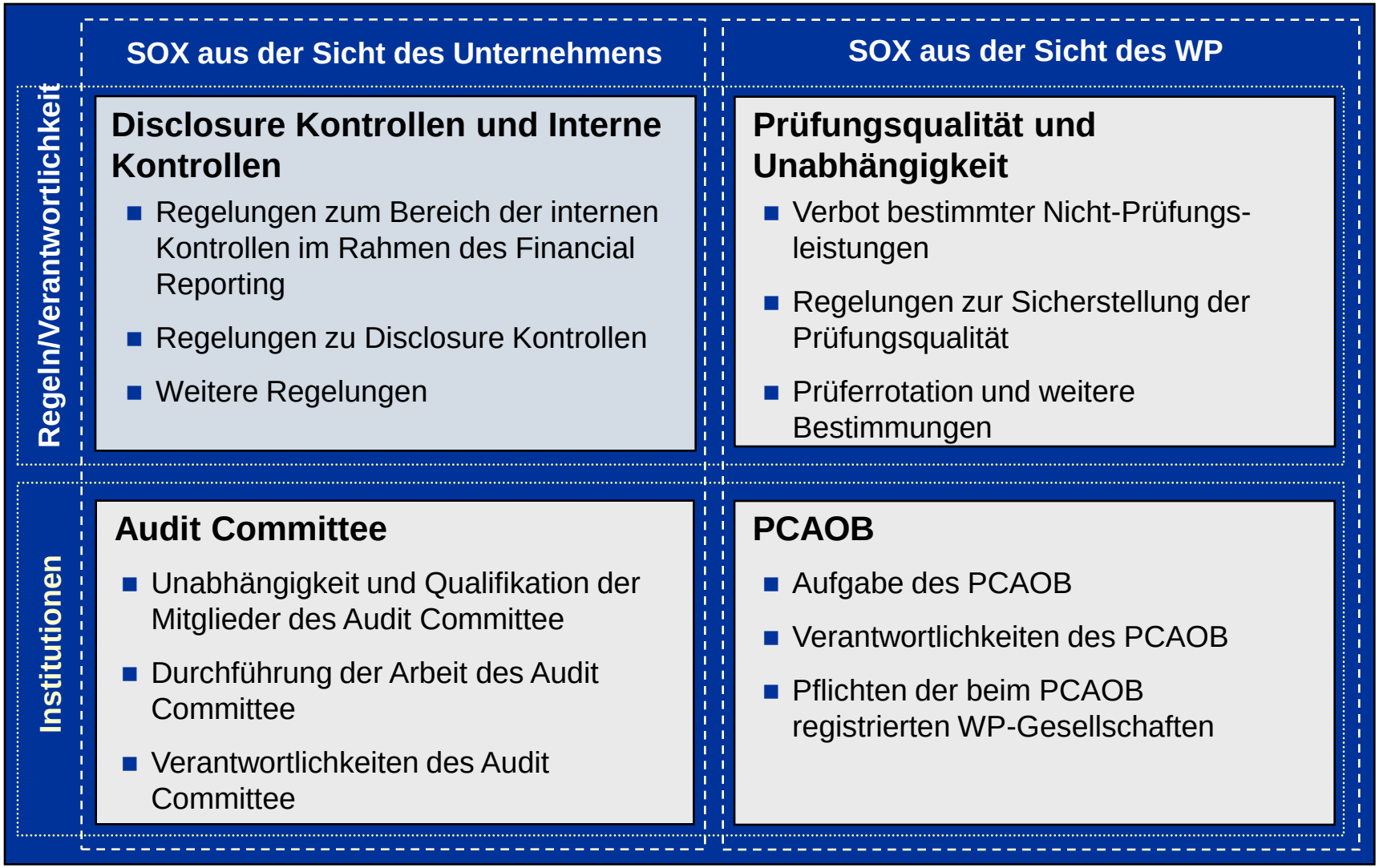
Ziel:

Wiederherstellung des Vertrauens der Investoren (Wolrdcom-Skandalen) durch neue Regelungen zu **Disclosures** und **Corporate Governance**

Fokus:

1. Disclosure Kontrollen und Interne Kontrollen
2. Audit Committee
3. Public Accounting Oversight Board
4. Prüfungsqualität und Unabhängigkeit

Die vier Eckpunkte des SOX



SOX 302 – Anforderungen hinsichtlich der Disclosure Kontrollen (1 / 2)

Sektion 302 fordert vom CEO und CFO der Gesellschaft, quartalsweise sowie jährlich zu bestätigen, dass sie:

- hinsichtlich aller wesentlichen Sachverhalte keine falschen Aussagen getroffen haben oder einen wesentlichen Sachverhalt nicht erwähnt haben
- die im Abschluss sowie in sonstigen veröffentlichten Unterlagen enthaltenen Angaben in allen wesentlichen Aspekten richtig dargestellt haben
- für die Prozesse und Kontrollen hinsichtlich des Zustandekommens der Angaben verantwortlich sind
- die Kontrollverfahren so aufgebaut haben, dass ihnen alle wesentlichen Informationen bekannt geworden sind

Gültig ab:
29. August 2002

SOX 302 – Anforderungen hinsichtlich der Disclosure Kontrollen (2 / 2)

- die Beurteilung der Wirksamkeit der Disclosure Kontrollen am Ende der jeweiligen Periode durchgeführt haben
- gegenüber dem Audit Committee sowie dem WP alle Fälle wesentlicher Kontroll-Defizite sowie Fraud-Fälle (Unterschlagungen etc.) dargelegt haben
- in den zu veröffentlichenden Unterlagen die wesentlichen Änderungen in den internen Kontrollverfahren beschrieben haben

Gültig ab:
29. August 2002

SOX 404 – Anforderungen hinsichtlich der Kontrollen über das Financial Reporting

Jeder Financial Report muss einen Bericht über die vorhandenen internen Kontrollen mit folgenden Punkten enthalten:

- Erklärung über die Verantwortung des Managements hinsichtlich der Einrichtung und Aufrechterhaltung angemessener interner Kontrollstrukturen und -aktivitäten für das Financial Reporting
- Erklärung zu den Ergebnissen der vom Management durchgeführten Wirksamkeitsprüfung
- WP-Bericht über die Prüfung der Erklärungen des Managements

Gültig ab:

US-Unternehmen:

15. November 2004

US-Kleinunternehmen / Nicht-US-Unternehmen:

15. Juli 2005

SOX 404 – Anforderungen hinsichtlich der Kontrollen über das Financial Reporting

Ziel der Sektion 404 ist die Verpflichtung der Unternehmen, Prozesse zu implementieren, die folgende zentralen Elemente abdecken:

- angemessene Genehmigungsverfahren für Geschäftsvorfälle
- Schutz des Gesellschaftsvermögens gegen unerlaubte Vermögensschädigungen
- Korrekte Erfassung der Geschäftsvorfälle der Gesellschaft und Berichterstattung in Übereinstimmung mit den geltenden Rechnungslegungsvorschriften

Gültig ab:

US-Unternehmen:

15. November 2004

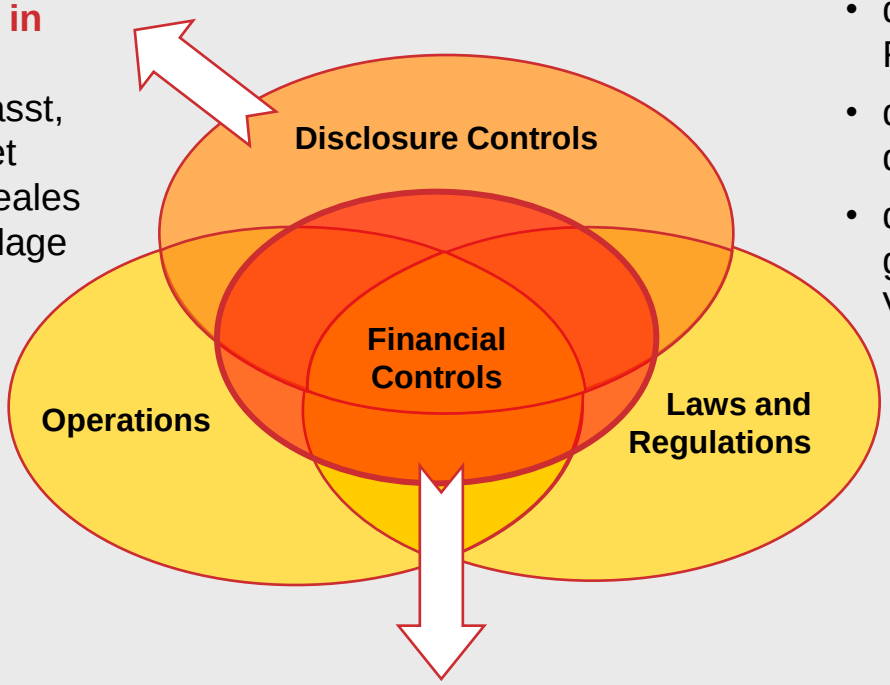
US-Kleinunternehmen / Nicht-US-Unternehmen:

15. Juli 2005

Zusammenspiel von SOX 302 und 404

Anforderungen aus SOX 302

Kontrollen, die sicherstellen, dass **Reportinginhalte in Übereinstimmung mit SEC -Vorschriften** erfasst, verarbeitet und berichtet werden, um somit ein reales Bild der Unternehmenslage zu liefern



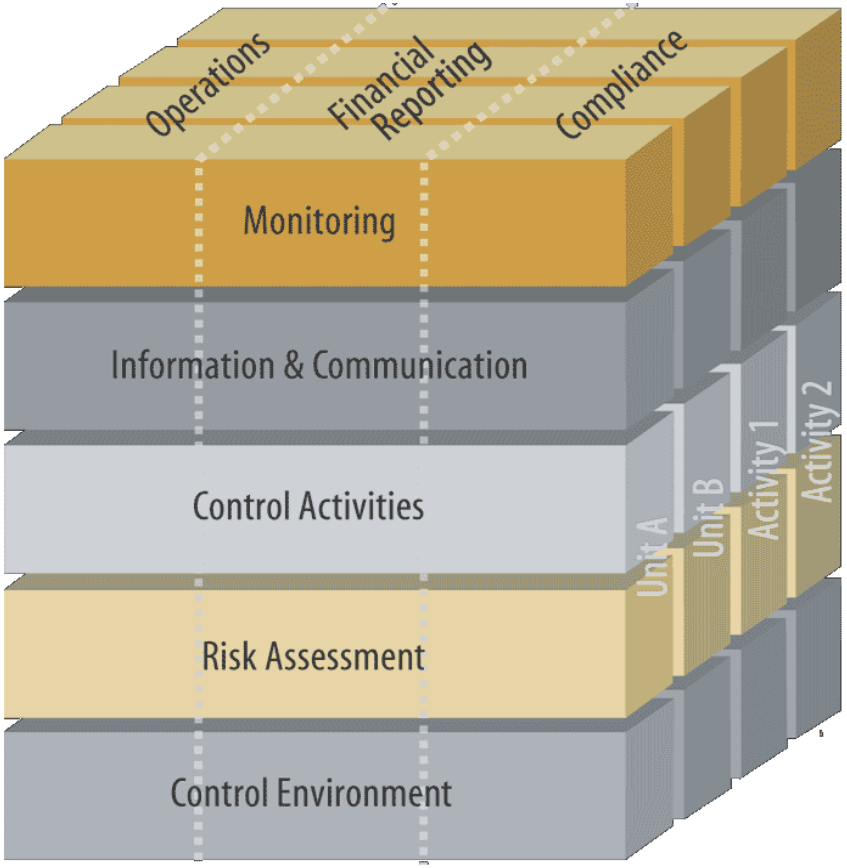
COSO Framework
Interne Kontrollen zur Sicherstellung:

- der Zuverlässigkeit des Financial Reporting
- der Effektivität und Effizienz der betrieblichen Prozesse
- der Übereinstimmung mit geltenden Gesetzen und Vorschriften

Anforderungen aus SOX 404 Alle Kontrollen, die im Zusammenhang mit der Erstellung des **Financial Reporting** dazu beitragen, ein den tatsächlichen Verhältnissen entsprechendes Bild des Unternehmens im Einklang mit US-GAAP zu vermitteln

Der Rahmen für das interne Kontrollsystem: COSO

Die Verpflichtung auf Rahmenvorgaben für das interne Kontrollsystem ist ein neuer Aspekt



Agenda

1. Was ist der Sarbanes Oxley Act – was ist neu?

2. Vorgehensweise beim SOX Readyness-Projekt

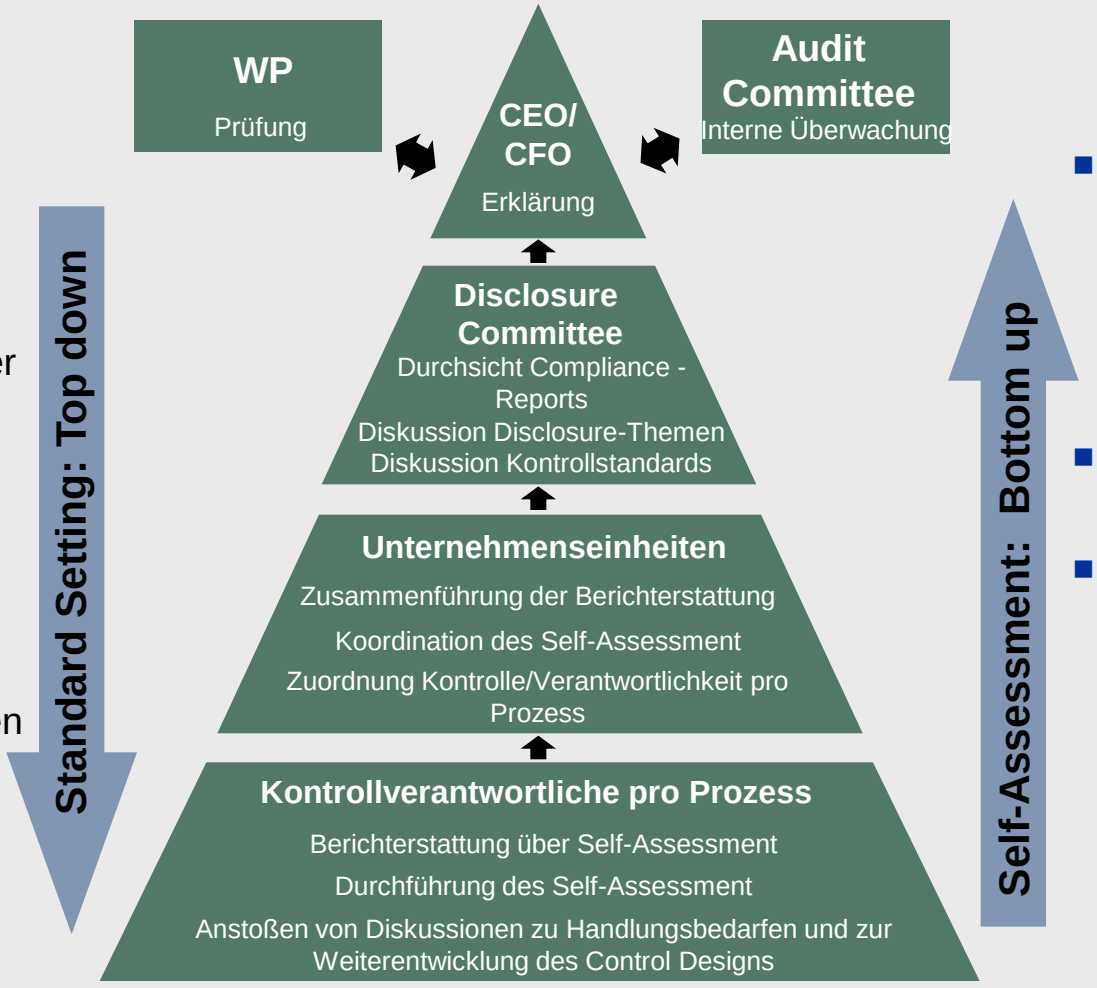
3. Erwartungen des Abschlussprüfers / wiederkehrende Arbeiten

4. Erfahrungen aus der Praxis

5. Chancen in Sarbanes Oxley - Was kommt als nächstes?

Sarbanes Oxley Readyness Projekt: Top Down / Bottom Up Approach

- Definition der internen Kontroll-umgebung/des Kontrollkonzeptes
- Auswahl relevanter Unternehmens-einheiten
- Definition der wesentlichen Prozesse
- Definition von Referenzprozessen und -kontrollen
- Festlegung des Self-Assessment-Prozesses



- Zusammenführen der Ergebnisse des Self-Assessment und regelmäßige Berichterstattung
- Durchführung der Self-Assessment
- Übernahme des des „Top-down-Ansatzes“ und ggf. Anpassung an spezifische Gegebenheiten

Agenda

1. Was ist der Sarbanes Oxley Act – was ist neu?

2. Vorgehensweise beim SOX Readyness-Projekt

3. Erwartungen des Abschlussprüfers / wiederkehrende Arbeiten

4. Erfahrungen aus der Praxis

5. Chancen in Sarbanes Oxley - Was kommt als nächstes?

Erwartungen des Abschlußprüfers (1 / 3)
PCAOB Regeln

- Der Prüfer muß für wichtige Prozesse einen Walkthrough durchführen um den Prozessfluß verstehen und das Kontrolldesign sowie die Wirksamkeit der Kontrollen beurteilen zu können – dies schließt auch die IT-Kontrollen mit ein.
- Durchführung von Tests zur Feststellung der operativen Wirksamkeit von Kontrollen und deren Fähigkeit die Risiken hinsichtlich möglicher Fehler im Ausweis von Finanzdaten zur Verringern (sog. Assertions).
- Es sind beide Arten von Kontrollen, sowohl vorbeugende (oft automatisierte Anwendungskontrollen) als auch nachgelagerte Kontrollen (preventive and detective controls) einzubeziehen.

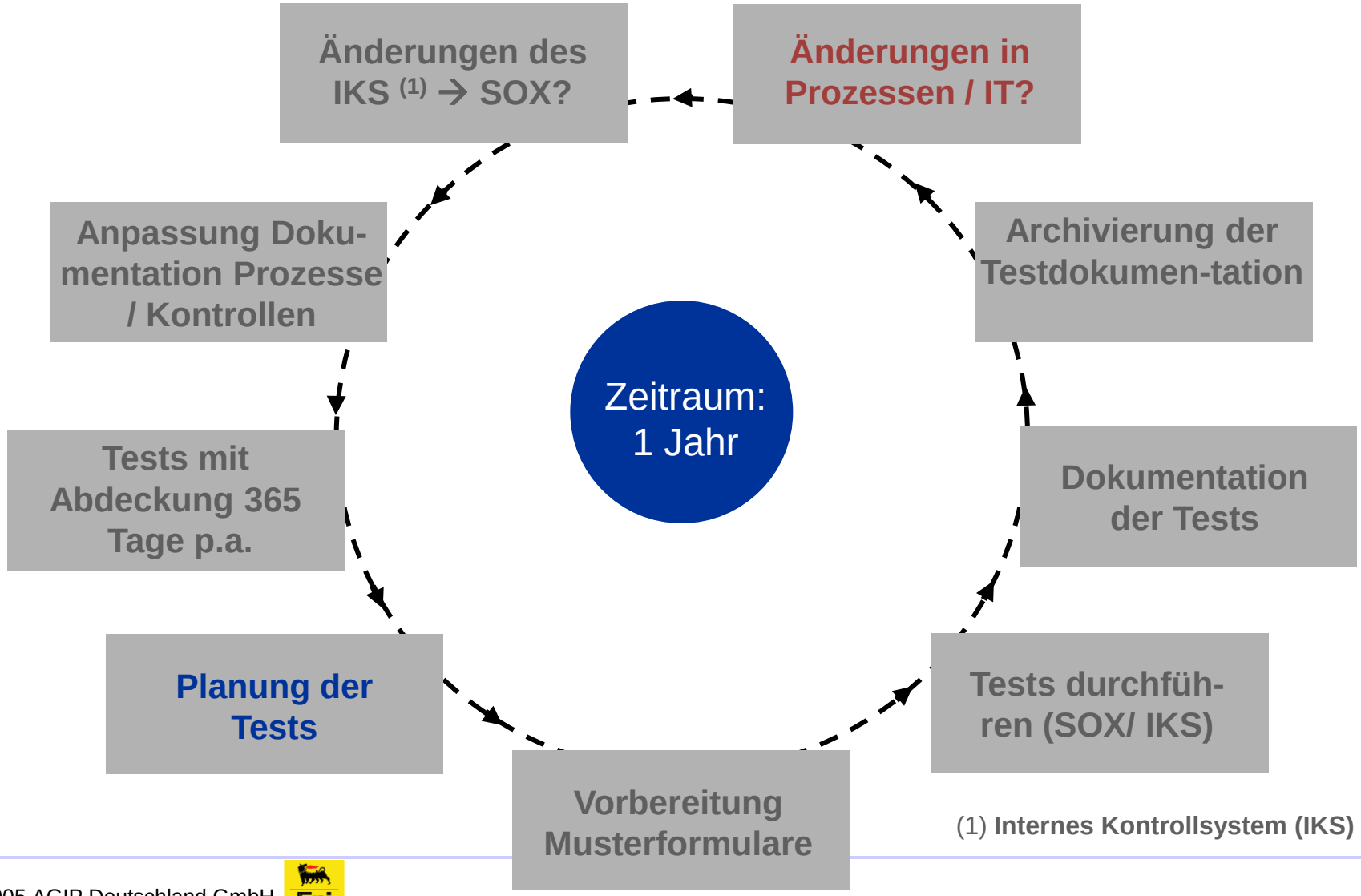
Erwartungen des Abschlußprüfers (2 / 3)
Wichtige Aufgaben im Rahmen von SOX-Prüfungen

- Der Abschlußprüfer hat zu bestätigen (wenn möglich), dass angemessene Kontrollen für das Finanzberichtswesen vorhanden sind und diese funktionieren
- Der Abschlußprüfer hat zu bestätigen, dass das Unternehmen seine Kontrollen getestet und bei Schwachstellen Gegenmaßnahmen eingeleitet hat
- Der Abschlußprüfer wird folgende Schritte durchführen
  - Walkthrough Test von Prozessen und Kontrollen (einschl. Dokumentation)
  - Die Tests des Unternehmens nachvollziehen (einschließlich einer Prüfung der Testdokumentation des Unternehmens)
  - Eigene Tests durchführen

Erwartungen des Abschlußprüfers (3 / 3)
Wichtige Aufgaben im Rahmen von SOX-Prüfungen

- IT-Anwendungen werden auf Prozessebene berücksichtigt – als wichtige Ergänzung hierzu ist eine Prüfung der sog. General Computer Controls (GCC) erforderlich
- Er wird sog. Entity Level Controls überprüfen und ausgelagerte Einheiten / Prozesse (z.B. Rechenzentrumsbetrieb)
- Er wird das sog. Control Environment (tone from the top) überprüfen

Sarbanes Oxley – regelmäßig wiederkehrende Aufgaben



(1) **Internes Kontrollsystem (IKS)**

Agenda

1. Was ist der Sarbanes Oxley Act – was ist neu?

2. Vorgehensweise beim SOX Readyness-Projekt

3. Erwartungen des Abschlussprüfers / wiederkehrende Arbeiten

4. Erfahrungen aus der Praxis

5. Chancen in Sarbanes Oxley - Was kommt als nächstes?

Erfahrungen aus der Praxis

Wishful Thinking in den meisten Unternehmen:

➔ Das vorhandene Risikomanagement erfüllt die SOX Anforderungen

Lessons Learned

➔ Bestehende Risikomanagementsysteme erfüllen nicht die SOX Anforderungen

Am häufigsten **fehlen** in Unternehmen:

➔ Eine Definition der „Significant Controls“

➔ Definition und Anwendung eines zugelassenen Standards (z.B. COSO)

➔ Vorkehrungen / Möglichkeiten zur jährlichen Überprüfung aller Significant Controls

➔ Vollständige Dokumentation von Kontrollzielen und Kontrollaktivitäten für die betroffenen Prozesse

Typische Herausforderungen für das Unternehmen und den Abschlußprüfer

- Änderungen in den Prozessstrukturen oder der Risikostruktur werden nicht nachvollzogen
- Dokumentation von durchgeführten Kontrollen und durchgeführten Tests der Kontrollen Tests ist nicht ausreichend
- Anzahl der Stichproben ist zu gering
- Anwendungskontrollen werden nicht einbezogen
- General Computer Controls werden nicht berücksichtigt
- Die Einschätzung der Schwere / Bedeutung von Feststellungen ist nicht konsistent im Konzern
- Erzielung von Konsistenz zwischen Prozesssdokumentation, gewählten Key-Controls, Assertions und durchgeführten Tests

Typische Potentiale bei SOX-Projekten (1/2)

Einzelner Faktoren fördern die Verlässlichkeit und Effizienz des Projekts und späteren Betriebs entscheidend.

- Langfristige Planung von Projekt und Betrieb

- Zentrale vs. dezentrale Zuordnung der Verantwortung für die Prüfung von Kontrollen

- Zentrale vs. dezentrale Zuordnung der Verantwortung für das Management von SOX

- Einbindung von Abschlussprüfer und Revision

Typische Potentiale bei SOX-Projekten (2/2)

- Formelle vs. Informelle Kommunikationsstrukturen

- Formelle vs. Informelle Berichtswege

- Integration in bestehende Überwachungs-, Controlling- und Berichtssysteme

- Fehlende Unterstützung durch spezielle Software

Agenda

1. Was ist der Sarbanes Oxley Act – was ist neu?

2. Vorgehensweise beim SOX Readyness-Projekt

3. Erwartungen des Abschlussprüfers / wiederkehrende Arbeiten

4. Erfahrungen aus der Praxis

5. Chancen in Sarbanes Oxley - Was kommt als nächstes?

Chancen im Sarbanes Oxley Prozess

- Sarbanes Oxley zu befolgen ist **keine einmalige Aktivität** – es ist vielmehr ein Prozess
- Sarbanes Oxley kann dauerhafte Verbesserungen in der Unternehmensüberwachung und der Transparenz von Geschäftsprozessen sowie de Zahlenwerks von Unternehmen bewirken
  - Verbesserung der Zuverlässigkeit von Prozessen und Erweiterung des Verantwortungsbereichs für Prozessverantwortliche
  - Verbesserungen der Informationsqualität führen zu fundierteren Entscheidungen
  - Verbesserung bei der Nutzung von IT-Anwendungen in den betroffenen Prozessen
  - Sarbanes Oxley leistet einen Beitrag zur Befolgung anderer Corporate Governance Codes sowie zur Vorbereitung auf Basel II
  - Verhindert den Abfluss von Mitteln durch oder den Verlust von Vermögen durch Fokussierung von Kontrollen auf Risikobereiche

Was kommt nach Sarbanes Oxley?

Die Zeit nach dem Sarbanes Oxley Readyness Projekt ist geprägt durch Verbesserungen im Sarbanes Oxley Prozess, der Integration mit anderen Corporate Governance Anforderungen sowie der Implementierung eine chancenorientierten Sicht

- ➔ Stärkere Fokussierung von Kontrollen auf Risiken
- ➔ Verbesserungen in der Dokumentation
- ➔ Integration mit IT zur Effizienzsteigerung bei den Kontrollprüfungen
- ➔ Der risikominimierenden Sicht muß die **chancenmaximierende Sicht** hinzugefügt werden bzw. im Unternehmen implementiert werden!

  Die Prozessaufnahme und –gestaltung sowie die Dokumentation dieser können so **Optimierungspotentiale für das Unternehmen** aufdecken!!

Vielen DANK für Ihre Aufmerksamkeit!

Kontaktdaten:

Dipl. Kfm. Dr. Stefan Gros

AGIP Deutschland GmbH, München

drgros@yahoo.de oder stefan.gros@agip.de

Literatur

Reed, Sinnett, Why should private companies implement Sarbannes-Oxley?, Financial Executive Magazin, April 2005

PWC, Sarbannes-Oxley remains a force to be reckoned within the Boardroom, Survey November 2004.

COSO, Internal Control – Integrated Framework, Volume 2, Jersey City 1994

BACKUP

Ergänzung COSO (1/5)

Die **SEC** verweist in Ihrer Final Rule **nicht** auf ein **bestimmtes internes Kontrollssystem der Finanzberichterstattung gemäß Sec. 404 SOX**. Die SEC bezieht sich auf ein **Rahmenwerk**!

In dem Rahmenwerk werden Eckpunkte definiert, damit **Spielraum** gegeben ist, das verschiedene Ausprägungen des Rahmenwerkes angewendet werden können. So wird Rücksicht genommen, dass in anderen Ländern und in Zukunft andere Rahmenwerke angewendet werden können.

Solch ein Rahmenwerk muß jedoch folgende **4 Eckpunkte** erfüllen:

1. Unvoreingenommenheit
2. Qualitativ und Quantitativ konstante Bewertung
3. Angemessene Vollständigkeit, sodaß Faktoren, die die Wirksamkeit interner Kontrollen beeinflussen, nicht vergessen bzw. Außen vor gelassen werden.
4. Gewährleistung einer Evaluation des internen Kontrollsystem.

Ergänzung COSO (2/5)

=> Die SEC weist ausdrücklich darauf hin ,daß das **COSO- Rahmenwerk diese Anforderungen erfüllt** und von den Unternehmen angewendet werden kann.

Die **nationalen** und **internationalen** Standards nehmen ebenfalls Bezug auf das COSO Rahmenwerk. So greift der IDW Prüfungsstandard 260 ebenso wie der International Standard on Auditing (ISA) 400 auf das Rahmenwerk zurück. Beide stimmen im Wesentlichen mit diesem überein.

⇒ Aufgrund dieser hervorgehobenen, zentralen Stellung des COSO möchte ich nun kurz erläutern:

⇒ **Was sind die Elemente des COSO?**

COSO Ergänzung (3/5)

Ziel des COSO: a) Vielzahl verschiedener Sichtweisen und Ansätze zu integrieren

b) Interne Kontrollen sollen Sicherheit im Hinblick auf **3 Dinge** erbringen:

1.Effectiveness and efficiency of operations (Effektivität u. Effizienz)

2.Reliability of financial Reporting (Verläßlichkeit)

3.Compliance with laws and regulations..

Bei den internen Kontrollen handelt es sich nicht um eine zeitpunktbezogene Aktion, sondern um einen fortlaufenden Prozess! Mitarbeiter in jeder Stufe des Unternehmens sind betroffen.

- Die 1. **Zielkategorie „operations“** bezieht sich auf die effektive und effiziente Nutzung der Ressourcen eines Unternehmens. In diesem Ziel wird der Hauptgeschäftszweck eines Unternehmens angesprochen, einschließlich der Sicherung der Vermögenswerte.
- Die **2. Zielkategorie „Financial Reporting“** greift die Verläßlichkeit und die Ordnungsmäßigkeit der Finanzberichterstattung auf.z.B. korrekte Jahresabschlußerstellung
- In der **3. bzw. letzten Zielkategorie** COMPLIANCE wird die Erfüllung der maßgeblichen Gesetze und Vorschriften thematisiert. i.e. Sarbannes Oxley.

COSO Ergänzung (4/5)

Neben diesen Zielen nennt das COSO-Rahmenwerk **5** miteinander in Verbindung stehende Komponenten:

1. Control Environment (Kontrollumfeld):

- Unternehmenskultur spielt hier eine Rolle (Ethische Werte, Integrität und fachliche Kompetenz der Mitarbeiter)

2. Risk Assessment (Risikobeurteilung)

- Unternehmen muss sich der Risiken des Geschäftsmodells bewusst sein. Dieses Risiko lässt sich auf die Ziele die sich ein Unternehmen setzt und die Aktionen, die daraus entstehen zurückführen.
- Mittels Kontrollen sollen die hieraus entstandenen Risiken, die die Zielerreichung gefährden, identifiziert, analysiert und entsprechend gehandhabt werden.

3. Controll Activities (Kontrollaktivitäten):

- Gegenmaßnahmen zur Bewältigung der o.g. Risiken sind durch die Kontrollaktvitäten zu überprüfen.
- diese bestehen aus: a) Verfahren und b) Kontrollgrunudsätzen, die sicherstellen, daß notwendige Managemententscheidungen effizient durchgeführt werden.

4. Information and Communication

- Ein Info – und Ksystem stellt die Grundlage dar, die die Mitarbeiter zur Entscheidungsfindung benötigen.
- Werkzeug

COSO_Ergänzung (5/5)

5. Monitoring (Überwachung des Kontrollsystems)

- Interne Kontrollen sind als andauernde Prozesse definiert worden.
- Die Prozesse müssen einer Überwachung unterliegen
- Dies kann fortlaufend und prozessintegriert gestaltet werden oder einmalig separat erfolgen
- Monitoring soll gewährleisten, das das gesamte System auf Veränderungen reagieren kann und notwendige Anderungen vorgenommen werden können.

⇒ **Zusätzlich:** Anforderungen an das interne Kontrollsystem ergeben sich jedoch auch aus der **Branche**, **Größe** und Kultur des Unternehmens.

Es daher verwundert es auch nicht dass die Ausgestaltung von internen Kontrollsystemen von Unternehmen zu Unternehmen teilweise von Tochterunterunternehmen zu Tochterunternehmen sehr unterschiedlich ausfallen kann.

Fazit: Das hier vorgestellte System folgt – aufgrund der Eingangs geschilderten Ereignisse dem PRINZIP der RISIKOMINIMIERUNG.

CEO & CFO‘s haben jedoch nicht nur dieses Ziel vor Augen. Zwar haben sie grundsätzlich ein Interesse an verlässlichen Daten, an einer guten Informationsverarbeitung und an einer zutreffenden Risikobeurteilung. Doch ist es für eine Unternehmensführung ebenso wichtig und notwendig mit einem internen Kontrollsystem die **vorhandenen Chancen zu maximieren**!! Diese Anforderung muss einfließen.