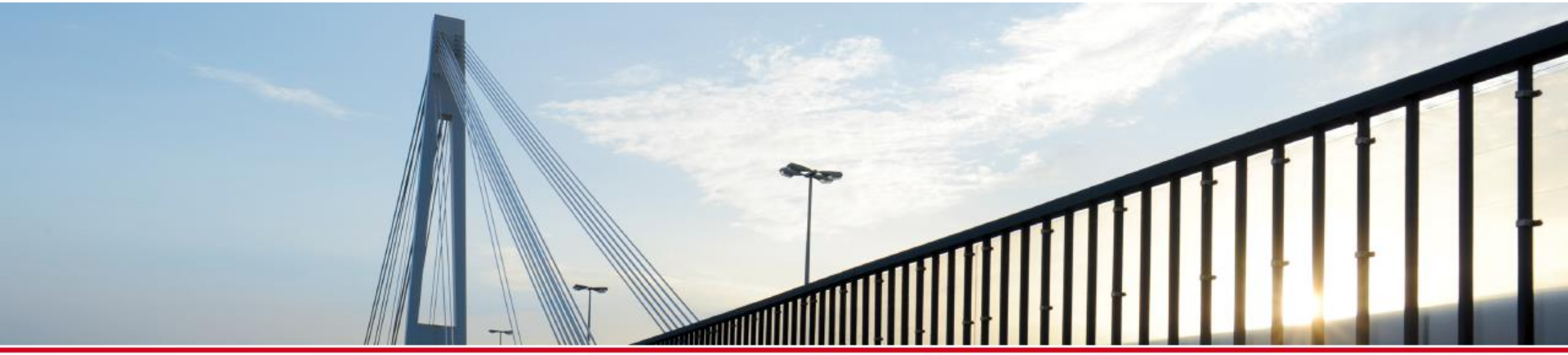
the Bridge

we make your accounting international



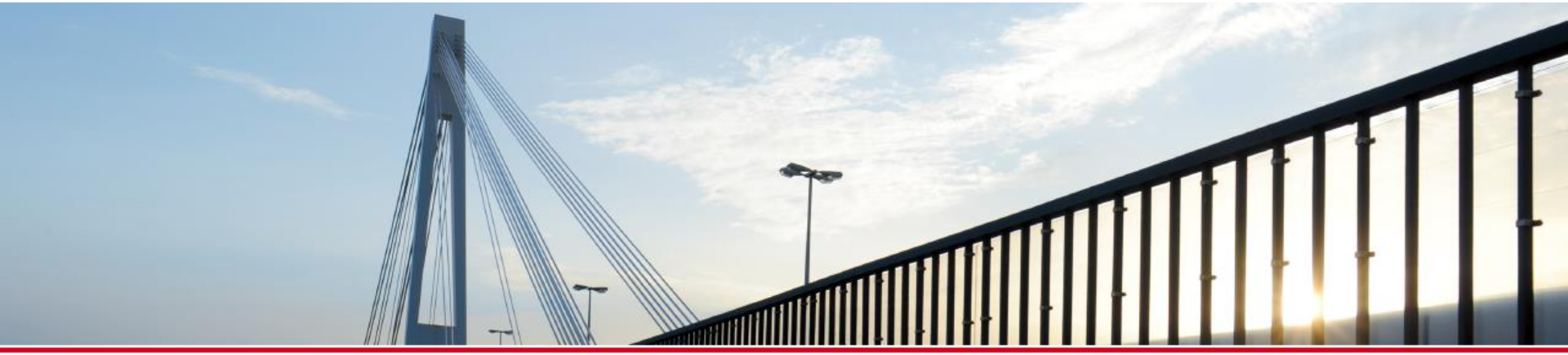
Workshop

„SOX-Implementierung als Chance begreifen! – Say what you do and do what you say"

Judith Geiß, Inhaberin von the Bridge · Consulting & Training

the Bridge

we make your accounting international



SOX-Implementierung als Chance begreifen - Say what you do and do what you say“

Ein Workshop mit Judith Geiß, the Bridge - Consulting & Training

In diesem Workshop bringen wir Ihnen die Chancen einer SOX-Implementierung anhand eines Praxisbeispiels nahe.

Nutzen Sie diese gezielt um Unternehmensprozesse zu optimieren und die Kommunikation innerhalb des Unternehmens zu verbessern

Eine Übersicht, welche Punkte in dieser Präsentation behandelt werden

1. Verfasser und Entstehung
2. SOX – die vier Grundpfeiler
3. SOX Sektion 302 – Disclosure Kontrollen
4. SOX Sektion 404 – Kontrollanforderung über das Financial Reporting
5. Zusammenspiel von SOX 302 und SOX 404
6. Der Rahmen für das Kontrollsystem - COSO
8. Sarbanes Oxley Readiness Project
9. Erwartungen des Abschlussprüfers
10. Wiederkehrende Aufgaben
11. SOX – Erfahrungen aus der Praxis
12. SOX – Chancen
13. SOX – was kommt danach?

Abkürzungen bezüglich SOX in einer kleinen Übersicht:

Abkürzungen:

- SOX: Sarbanes Oxley Act
- WP: Wirtschaftsprüfer
- PCAOB: Public Accounting Oversight
- CEO/CFO: Chief Executive/Financial Officer
- COSO: Committee of Sponsoring Organizations of the Treadway Commission
- SA: Self-Assessment
- GCC: General Computer Controls
- IKS: Internes Kontrollsystem
- SC: Significant Controls

Quellen:

"Auswirkungen des Sarbanes-Oxley-Acts auf deutsche Unternehmen", Katja Moritz/Marco Gesse, Heft 49 Beiträge zum Transnationalen Wirtschaftsrecht der Martin-Luther-Universität Halle-Wittenberg

und

„Erfahrungsbericht ENI Group - AGIP Deutschland GmbH", Dipl. Kfm. Dr. Stefan Gros, 3.Finance-Gipfel am 09./10. Mai 2005 in Berlin

Wie kam SOX zu seinem Namen und warum entstand es?

- **Namensgeber** und **Verfasser** des **Bundesgesetzes Sarbanes-Oxley-Act (SOX) aus dem Jahre 2002** sind **Paul Sarbanes** in seiner Funktion als Vorsitzender des Ausschusses für Bankwesen, Wohnungs- und Städtebau des Senats der USA und **Michael Oxley** als Vorsitzender des Ausschusses für Finanzdienstleistungen des Repräsentantenhauses der USA.
- Hierbei liegt der Fokus auf **Wiederherstellung des Vertrauens der Investoren** nach den **vorangegangen Bilanzskandalen** von Unternehmen wie Worldcom und Enron durch Neuregelungen zu **Disclosures** und **Corporate Governance.**

→ Ziel ist die **Verbesserung der Verlässlichkeit von Berichterstattung** der Unternehmen

Wen betrifft es: Vor allem **börsennotierte Unternehmen**, deren Wertpapiere an den US-Börsen gehandelt werden, ebenso auch **Tochterunternehmen von US-Konzernen**

Die vier Eckpunkte bei SOX – Grundlage zur Verbesserung

	SOX aus Unternehmenssicht	SOX aus Sicht des WP
Regeln / Verantwortlichkeit	**Disclosure Kontrollen und Interne Kontrollen** ▪ Regelungen zum Bereich der internen Kontrollen im Rahmen des Financial Reporting ▪ Regelungen zu Disclosure Kontrollen ▪ Weitere Regelungen	**Prüfungsqualität und Unabhängigkeit** ▪ Verbot bestimmter Nicht-Prüfungsleistung ▪ Regelungen zur Sicherstellung der Prüfungsqualität ▪ Prüferrotation und weitere Bestimmungen
Institutionen	**Audit Committee** ▪ Unabhängigkeit und Qualifikation der Mitglieder des Audit Committee ▪ Durchführung der Arbeit des Audit Committee ▪ Verantwortlichkeiten des Audit Committee	**PCAOB (Public Accounting Oversight Board)** ▪ Aufgabe des PCAOB ▪ Verantwortlichkeiten des PCAOB ▪ Pflichten der beim PCAOB registrierten WP-Gesellschaften

Anforderung von quartalsweiser und jährlicher Bestätigung der CEO /CFO, dass:

- hinsichtlich aller wesentlichen Sachverhalte **weder falsche Aussagen** gemacht noch irgendwelche wichtigen **Sachverhalte verschwiegen** wurden
- alle Angaben im Abschluss und sonstiger veröffentlichten Unterlagen **in allen Aspekten korrekt dargestellt** wurden
- eine **Verantwortlichkeit für die Prozesse und Kontrollen** hinsichtlich des Zustandekommens der Angaben besteht

Anforderung von quartalsweiser und jährlicher Bestätigung der CEO /CFO, dass:

- die Kontrollverfahren so aufgebaut wurden, dass **alle erforderlichen Informationen bekannt** geworden sind
- die Beurteilung der **Wirksamkeit der Disclosure Kontrollen** am Ende der jeweiligen Periode durchgeführt wurde
- alle wesentlichen **Kontroll-Defizite sowie Fraud-Fälle** (Unterschlagungen etc.) dem Audit Committee und dem WP dargelegt wurden
- notwendige **Änderungen in den internen Kontrollverfahren** in den veröffentlichten Unterlagen beschrieben wurden

Anforderung eines Berichts über die vorhandenen internen Kontrollen für jeden Financial Report mit folgenden Punkten:

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

Verpflichtung zur Prozessimplementierung für folgende zentrale Elemente:

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

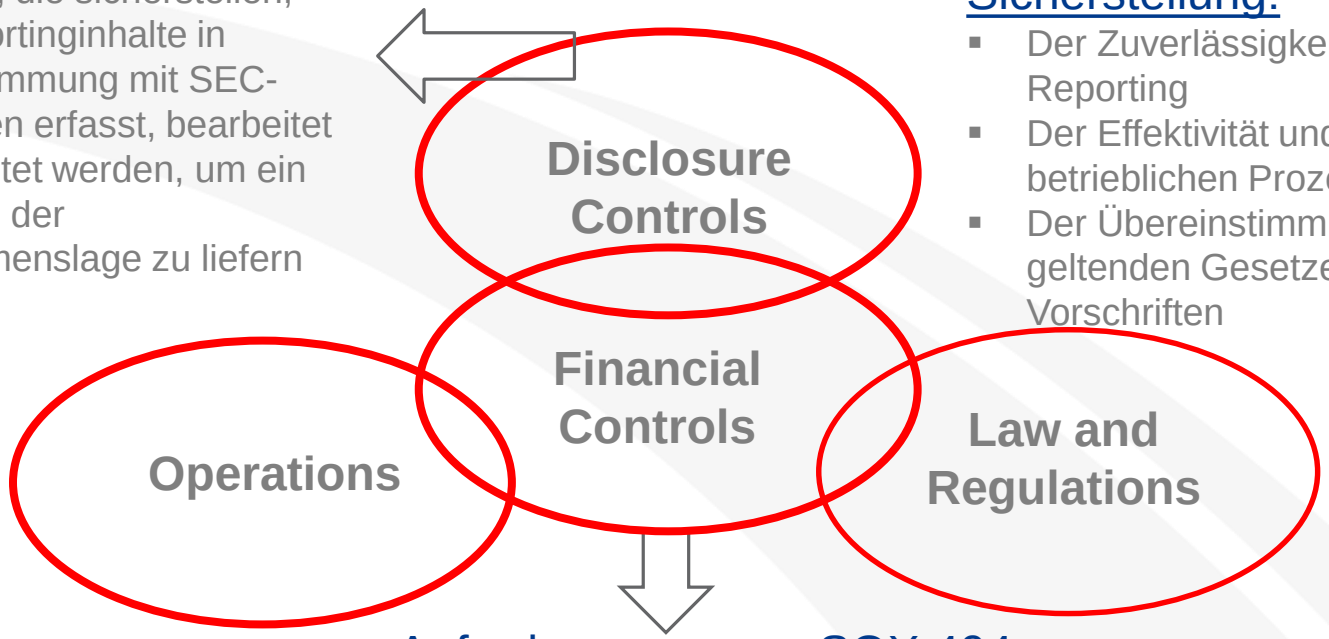
Anforderung eines Berichts über die vorhandenen internen Kontrollen für jeden Financial Report mit folgenden Punkten:

Anforderungen aus SOX 302:

Kontrollen, die sicherstellen, dass Reportinginhalte in Übereinstimmung mit SEC-Vorschriften erfasst, bearbeitet und berichtet werden, um 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:

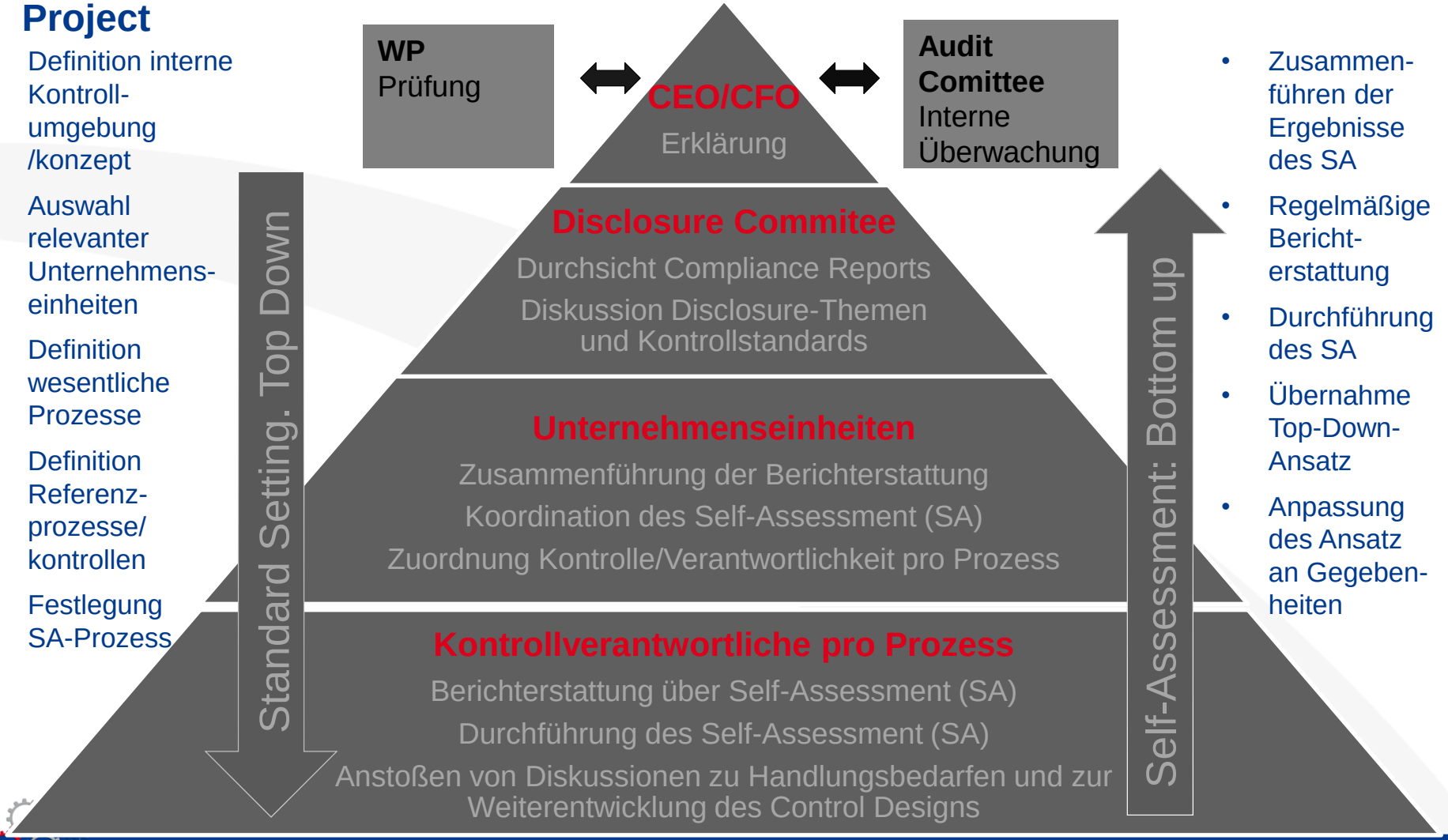
Alle Kontrollen, die im Zusammenhang mit der Erstellung des Financial Reporting dazu beitragen, ein den tatsächlichen Verhältnissen entsprechendes Bild im Einklang mit US-GAAP zu vermitteln

the Bridge
we make your accounting international

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

Top Down / Bottom Up Approach – Vorgehensweise beim SOX Readyness Project

- Definition interne Kontroll-umgebung /konzept
- Auswahl relevanter Unternehmens-einheiten
- Definition wesentliche Prozesse
- Definition Referenz-prozesse/ kontrollen
- Festlegung SA-Prozess



- Zusammen-führen der Ergebnisse des SA
- Regelmäßige Bericht-erstattung
- Durchführung des SA
- Übernahme Top-Down-Ansatz
- Anpassung des Ansatz an Gegeben-heiten

Das erwartet der Prüfer – PCAOB Regeln

- Es muss für wichtige Prozesse ein **Walkthrough** durchgeführt werden, um das Kontrolldesign sowie die Kontrollwirksamkeit beurteilen zu können; dies schließt IT-Kontrollen ein.
- Durchführung von **Tests zur Feststellung der operativen Kontrollwirksamkeit** und der **Fähigkeit von Risikominimierung** hinsichtlich möglicher Fehler im Ausweis von Finanzdaten
- **Vorbeugende Kontrollen** (automatisierte Anwendungskontrollen) und **nachgelagerte Kontrollen** (preventive and detective controls) sind notwendig.

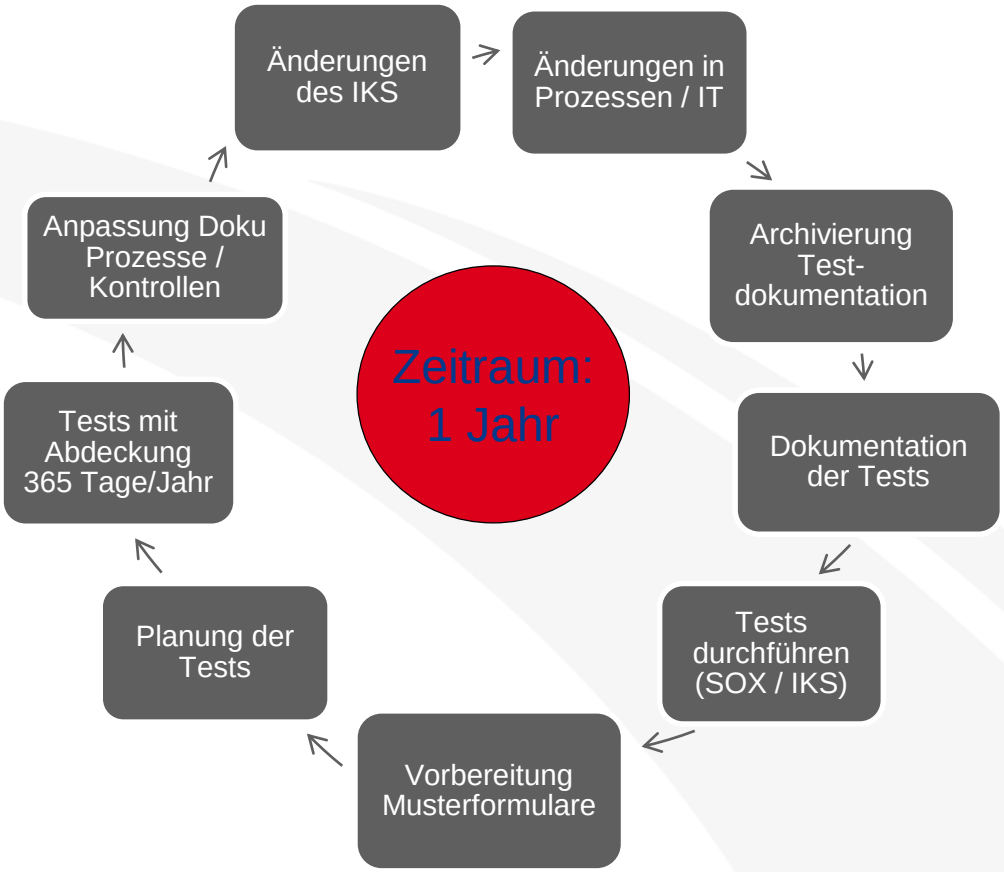
Das erwartet der Prüfer – wichtige Aufgaben im Rahmen der SOX-Prüfung

- Bestätigung durch den Abschlussprüfer für das Vorhandensein von angemessenen, funktionierenden **Kontrollen für das Finanzberichtswesen**
- Nachweis über **Test der Kontrolle**n und ggf. durchgeführte Verbesserung (Schwachstellen)
- Der Abschlussprüfer geht vor mit:
  - **Walkthrough-Tests** von Prozessen und Kontrollen (inkl. Dokumentation)
  - Nachvollziehbarkeit der **Unternehmenstest**s (inkl. Prüfung der Testdokumentation)
  - Durchführung **eigener Tests**

Das erwartet der Prüfer – wichtige Aufgaben im Rahmen der SOX-Prüfung

- Berücksichtigung der **IT-Anwendungen** auf Prozessebene einschliesslich Prüfung der **General Computer Controls (GCC)**
- **Entity Level Controls** und **Kontrolle ausgelagerter Einheiten** (z.B. Rechenzentrum)
- Untersuchung des **Control Environments** (tone from the top)

Wiederkehrende Aufgaben im Zeitraum 1 Jahr



Durch Praxiserfahrungen lernen und gut vorbereitet sein!

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” (SC)

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

→Vorkehrungen / Möglichkeiten zur jährlichen Überprüfung der SC

→Vollständige Dokumentation von Kontrollzielen und – aktivitäten für die betroffenen Prozesse

Herausforderungen und Probleme für Unternehmen und Abschlussprüfer

- Änderungen in den Prozess-Strukturen oder der Risikostruktur werden nicht vollzogen
- Dokumentation der Kontrollen und Test ist unzureichend
- Anzahl der Stichproben ist zu gering
- Anwendungskontrollen nicht einbezogen
- GCC (General Computer Controls) werden nicht berücksichtigt
- Bedeutungseinschätzung von Feststellungen ist nicht konsistent

Erzielung von Konsistenz zwischen Prozess-Dokumentation, gewählten Key-Controls, Assertions und durchgeführten Tests

Chancen zur Verbesserung durch SOX nutzen!

- SOX Richtlinien zu befolgen ist **keine einmalige** Aktivität – es ist vielmehr ein **kontinuierlicher** Prozess
- SOX kann dauerhafte **Verbesserungen in der Unternehmensüberwachung** und der **Transparenz von Geschäftsprozessen** bewirken

→Verbesserung der **Zuverlässigkeit von Prozessen** und **Erweiterung des Verantwortungsbereichs** für Prozessverantwortliche

→Verbesserung der **Informationsqualität** führen zur fundierten Entscheidungen

→Verbesserung bei der **Nutzung von IT-Anwendungen** in den betroffenen Prozessen

→Verhinderung des Verlusts von Mitteln durch **Fokussierung von Kontrollen auf Risikobereiche**

Die Zukunft durch Verbesserungen, Integration und Implementierung gestalten!

Die Zeit nach dem Sarbanes Oxley Readyness Project ist geprägt durch **Verbesserungen** im SOX-Prozess, **Integration** mit anderen Corporate Governance Anforderungen sowie der **Implementierung** einer chancenorientierten Sicht

→Stärkere Fokussierung von Kontrollen und Risiken

→Verbesserung der Dokumentation

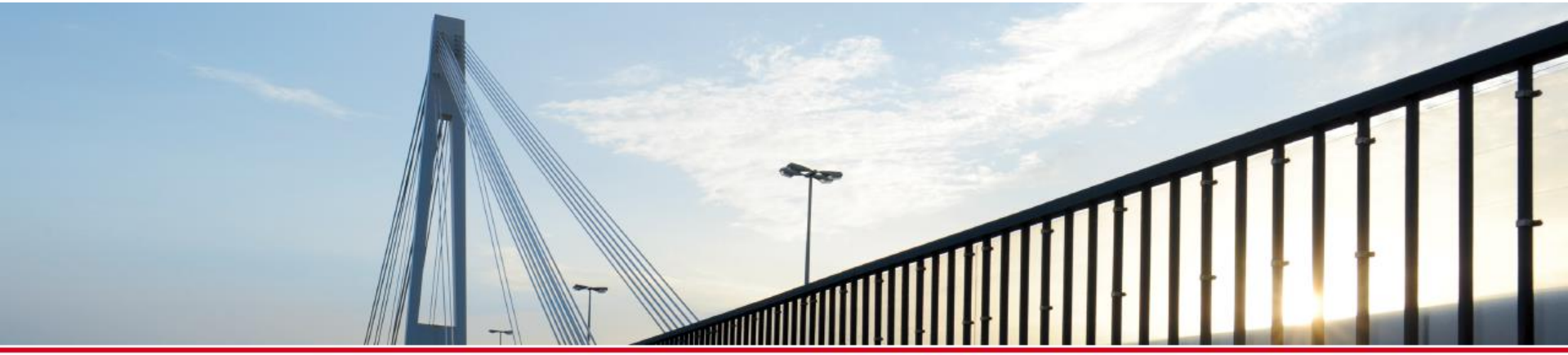
→Integration mit IT zur Effizienzsteigerung bei Kontrollprüfungen

→Implementierung der chancenmaximierenden Sicht im Unternehmen

Die Prozessaufnahmen, - gestaltung und –dokumentation können Optimierungspotentiale für das Unternehmen aufdecken

the Bridge

we make your accounting international



Vielen Dank für Ihre Aufmerksamkeit!

Ihre Judith Geiß

mannheim@thebridge-online.com · www.thebridge-online.com