

PricewaterhouseCoopers IT-Sicherheit – ihre Rolle in Compliance-Projekten

10th Symposium on Privacy and Security
Zürich, 31.8.2005

Stephan Teiwes

*connectedthinking

PRICEWATERHOUSECOOPERS 

Übersicht

1. Kosten von Compliance
2. Neuregelungen zur Compliance
3. Bedeutung von Compliance
4. Compliance-Projekte
5. Compliance-Anforderungen durch den Sarbanes-Oxley Act
 - COSO Risk Modell
 - Bereiche des IKS
 - IT-Risiken und Mächtige Kontrollen
 - Kontrollgebiete zur IT-Sicherheit
 - Prüfung von Kontrollen
 - Beurteilung von Mängeln
6. Schlussfolgerungen

Kosten von Compliance

168 Wörter für \$ 10 – 20 Mrd. !

SEC. 404. MANAGEMENT ASSESSMENT OF INTERNAL CONTROLS.

(a) **RULES REQUIRED.**—The Commission shall prescribe rules requiring each annual report required by section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m or 78o(d)) to contain an internal control report, which shall—

(1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and

(2) contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.

(b) **INTERNAL CONTROL EVALUATION AND REPORTING.**—With respect to the internal control assessment required by subsection (a), each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this subsection shall be made in accordance with standards for attestation engagements issued or adopted by the Board. Any such attestation shall not be the subject of a separate engagement.

- Die jährlichen Kosten für Unternehmen durch den SEC. 404, Sarbanes-Oxley Act werden auf ca. \$ 10 – 20 Mrd. geschätzt.
- Eine Studie der Financial Executives International (FEI) von März 2005 ergab:

Für 217 Unternehmen mit durchschnittlichem Umsatz von \$ 5 Mrd. betragen die durchschnittlichen Kosten für SEC. 404: \$ 4.36 Mio, d.h. ca. 0.1 % des Umsatzes.

Quelle: CFO Magazine, 11.5.2005, „Is Sarbanes-Oxley worth the Cost?“

Kosten von Compliance

Ausgaben für SOX in 2004

Firmen Umsatz	< \$5 Mrd.	\$5 Mrd. - \$10 Mrd.	\$10 Mrd. – \$50 Mrd.	> \$50 Mrd.
Durchschnittliche Anzahl zusätzlicher Audit Stunden	6'285	20'756	11'540	19'000
Durchschnittliche Kosten für Compliance pro \$ Mrd. Umsatz	\$1.9 Mio	\$1.1 Mio	\$0.6 Mio	\$0.3 Mio

Quelle: Roundtable Survey, December 2004
www.tlr.executiveboard.com



Trend: Kosten für (SOX-)Compliance treffen kleinere Unternehmen härter!

Kosten von Compliance

Standpunkte zur Diskussion

Investors don't necessarily agree.
"Obviously, to the extent 404 impacts earnings negatively, it's a concern," says Cynthia L. Richson, corporate governance officer for the \$64.5 billion Ohio Public Employees Retirement System (OPERS).
"On the other hand, who is measuring the cost of corruption and accounting scandals we've been through? Some cite that as contributing to a \$7 trillion, even as high as \$9 trillion, collapse in the capital markets."

Indeed, observes the PCAOB's McDonough, "the reason this legislation is so tough is because the American people rose in fury. They believed corporate leadership in America had let them down, which I believe [is true]." Sarbox, he points out, passed the Senate unanimously, and missed unanimous House passage by just three votes.

Quelle: CFO Magazine, 11.5.2005, „Is Sarbanes-Oxley Worth the Cost?“

- Kosten durch Korruption: im Billionenbereich (?)
- Misstrauen, Wut und Empörung der Bevölkerung über Führung von Unternehmen (Bsp. Rentenfonds)
- SOX wurde vom US Senat einstimmig angenommen

Neuregelungen zur Compliance

Neue Richtlinien in Europa zur Stärkung der Corporate Governance

Europäische Union

- Richtlinie des Europäischen Parlamentes über die Prüfung des Jahresabschlusses (8. EU-Richtlinie; in parlamentarischer Behandlung)

Deutschland

- 10-Punkte Plan der Deutschen Bundesregierung:
 - Verbesserung der Unternehmensintegrität und Anlegerschutz
 - Prävention von Falschinformationen des Kapitalmarktes
- Bilanzreform- und Bilanzkontrollgesetz
- Deutscher Corporate Governance Kodex

Schweiz

- Gesellschaftsrecht (OR, ZGB),
- Revisionsaufsichtsgesetz (Schweiz)

Neuregelungen zur Compliance

Einige branchenspezifische Vorschriften

Basel II

- Erhöhte Anforderungen an das operationelle Risikomanagement und Kontrollen für Banken führen zu Forderungen nach besserer Transparenz bei deren Kreditoren

EBK

- Richtlinien der Eidgenössische Bankenkommission

FDA

- Die US Food and Drug Administration Title 21 CFR Part 11 schreibt elektronische Akten, Belege und Unterschriften vor.

HIPAA

- Health Insurance Portability and Accountability Act (HIPAA): Krankenkassen etablieren den Schutz von persönlichen Patientendaten und setzen Patienten über ihre Datenschutz-Policies in Kenntnis.

Rolle der IT-Sicherheit zur Compliance
PricewaterhouseCoopers

Seite 7
September 05

Bedeutung von Compliance

Compliance: Handeln im Einklang mit geltenden Regeln

Compliance: An independent function that identifies, assesses, advises on monitors and reports on the bank's compliance risk, that is, the risk of legal or regulatory sanctions, financial loss, or loss to repudiation a bank may suffer as a result of its failure to comply with all applicable laws, regulations, codes of conduct and standards of good practice (together "law, rules and standards").

Quelle: Basel Committee on Banking Supervision
The compliance function in banks, S. 9

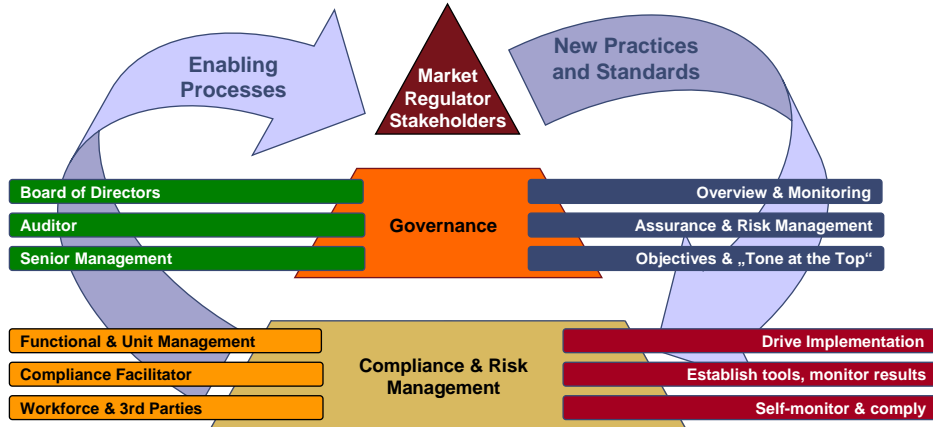
- Compliance beinhaltet das organisatorische Modell, die Prozesse und Systeme, um
 - Die Einhaltung von Gesetzen, Vorschriften, internen Standards und Policies zu gewährleisten
 - Die Erwartungen der „Key Stakeholder“ zu erfüllen
 - Die Geschäftsmodelle, das Ansehen und die finanziellen Rahmenbedingungen zu entwickeln
- Compliance erfordert diverse Aktivitäten mit Berührungspunkten zum Linien-Management und die Verdichtung von Informationen mit Folgerichtigkeit und Messbarkeit.

Rolle der IT-Sicherheit zur Compliance
PricewaterhouseCoopers

Seite 8
September 05

Bedeutung von Compliance

Compliance Rollen und Verantwortlichkeiten



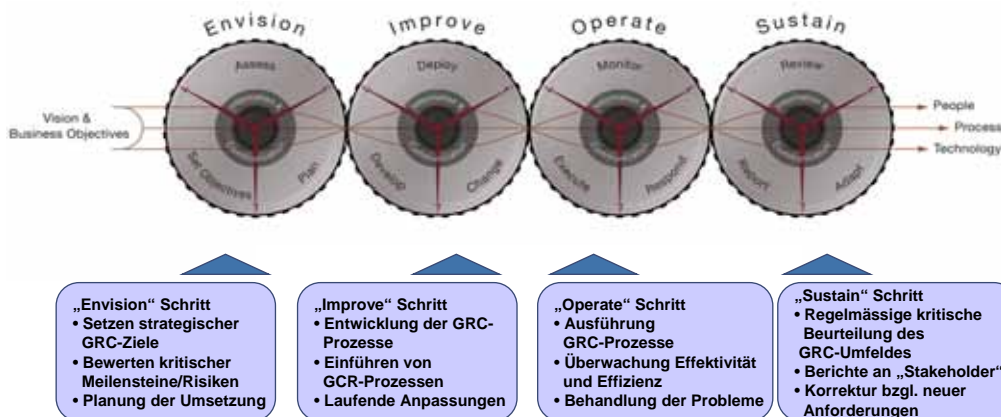
Die Compliance-Funktion sollte von ordentlichen Geschäftsbereichen unabhängig sein.

Rolle der IT-Sicherheit zur Compliance
PricewaterhouseCoopers

Seite 9
September 05

Compliance-Projekte

Governance, Risk & Compliance* (GRC) Projekte



*PwC Governance, Risk and Compliance Operating Model

Rolle der IT-Sicherheit zur Compliance
PricewaterhouseCoopers

Seite 10
September 05

Compliance-Projekte: aktuelles Beispiel Sarbanes-Oxley Act

Aktuell: Sarbanes-Oxley Compliance

Auch wenn es heute (noch) nicht jedes Unternehmen unmittelbar betrifft, kann anhand von SOX/IKS-Projekten Wichtiges gelernt werden:

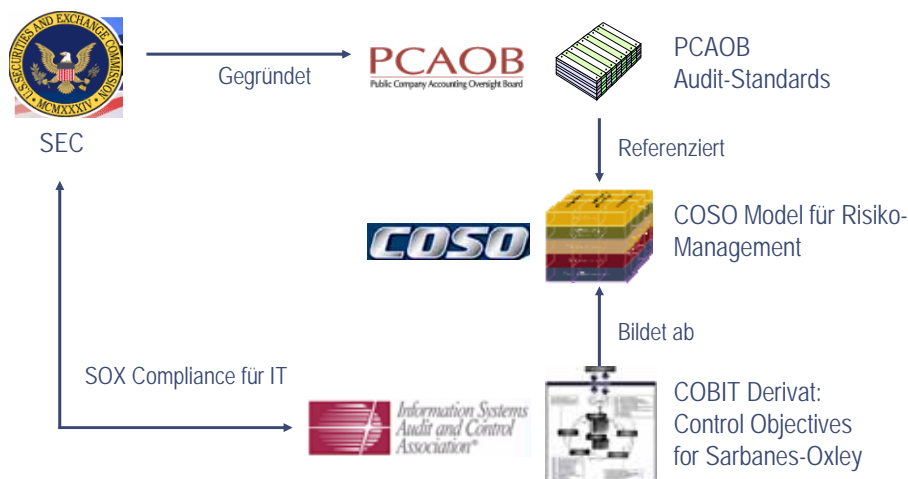
- Was es für ein Unternehmen bedeuten kann, in kurzer Zeit ein globales Kontrollumfeld materiell verbessern oder aufbauen zu müssen
- Ob Chancen einer solchen Situation wirklich genutzt und Risiken erkannt werden
- Wie Synergien zwischen Kontroll- und Steuerfunktionen genutzt werden können
- Wie Kontrollumfelder systematisch in Design und Umsetzung verbessert werden können
- Wie Kontrollumfelder auf deren Effektivität geprüft werden
- Dass diese Thematik heute schon mehr Unternehmen in Europa direkt betrifft, als zunächst angenommen wird
 - Unternehmen, die US-börsenkotiert sind, und deren Tochterunternehmen, sowie Unternehmen, deren Konkurrenz SOX-konform sind, und die im internationalen Vergleich der Anschluss nicht verpassen werden möchte
 - Obligationenrecht (OR Art. 727): „Wirtschaftlich bedeutende Unternehmen“ (gemäss Bilanzsumme, Umsatz oder Anzahl Vollzeitstellen)

Rolle der IT-Sicherheit zur Compliance
PricewaterhouseCoopers

Seite 11
September 05

Compliance-Anforderungen durch den Sarbanes-Oxley Act, 2002

Von SEC Compliance-Anforderungen zu COBIT

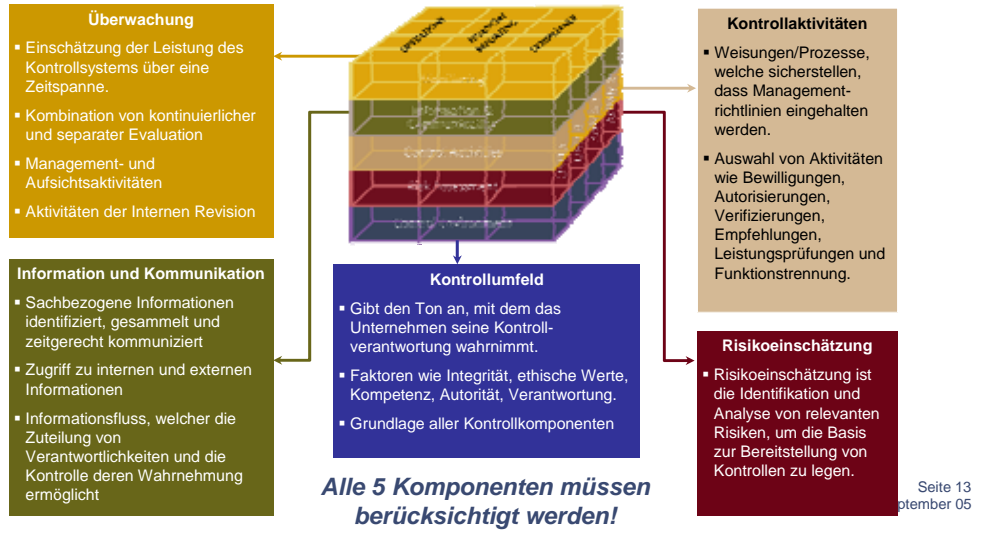


Rolle der IT-Sicherheit zur Compliance
PricewaterhouseCoopers

Seite 12
September 05

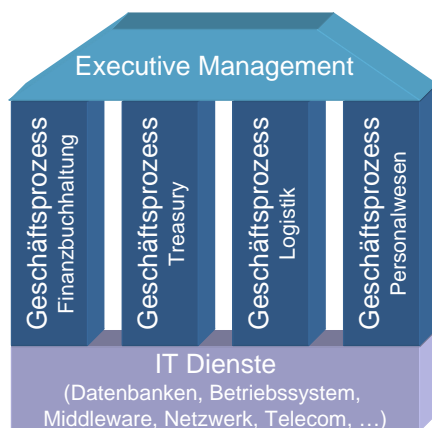
Compliance-Anforderungen durch den Sarbanes-Oxley Act

COSO-Modell eines Internen Kontrollsystems



Compliance-Anforderungen durch den Sarbanes-Oxley Act

Bereiche des Internen Kontrollsystems im Unternehmen



Unternehmenskontrollen:
Ethik, Leitbild, Politik, Governance

IT-Applikationskontrollen:
Kontrollen in IT-Applikationen,
die in Geschäftsprozessen
eingesetzt werden.

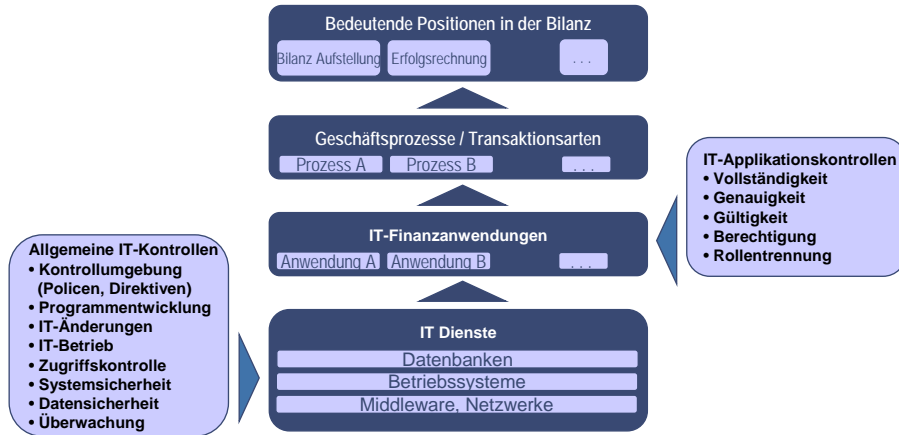
Allgemeine IT-Kontrollen:
Kontrollen, die in IT-Prozessen
und IT-Diensten integriert sind,
auf welchen IT-Applikationen
aufsetzen.

Rolle der IT-Sicherheit zur Compliance
PricewaterhouseCoopers

Seite 14
September 05

Compliance-Anforderungen durch den Sarbanes-Oxley Act

Risikoorientierung: Konzentration auf das „Wesentliche“

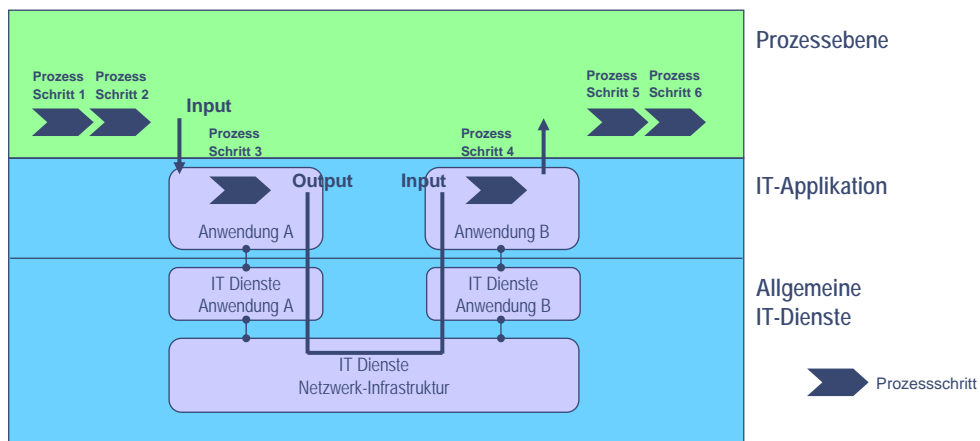


Rolle der IT-Sicherheit zur Compliance
PricewaterhouseCoopers

Seite 15
September 05

Compliance-Anforderungen durch den Sarbanes-Oxley Act

Geschäftsprozess mit Informationsfluss

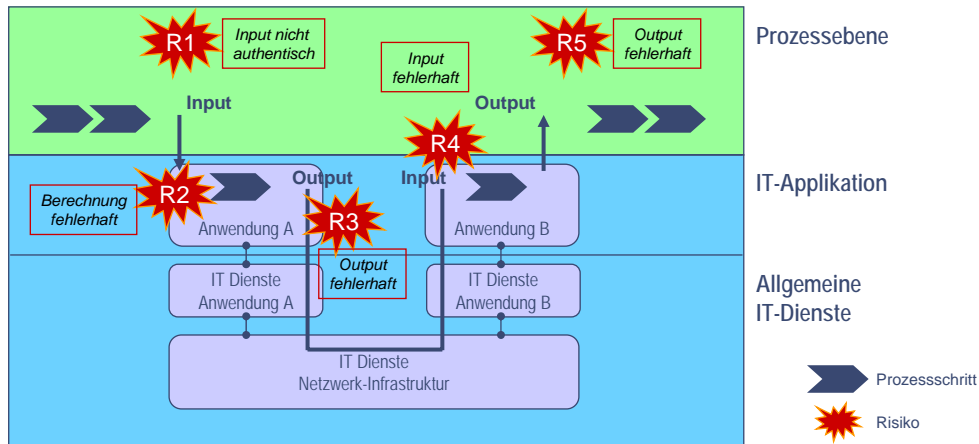


Rolle der IT-Sicherheit zur Compliance
PricewaterhouseCoopers

Seite 16
September 05

Compliance-Anforderungen durch den Sarbanes-Oxley Act

IT-Risiken im Geschäftsprozess

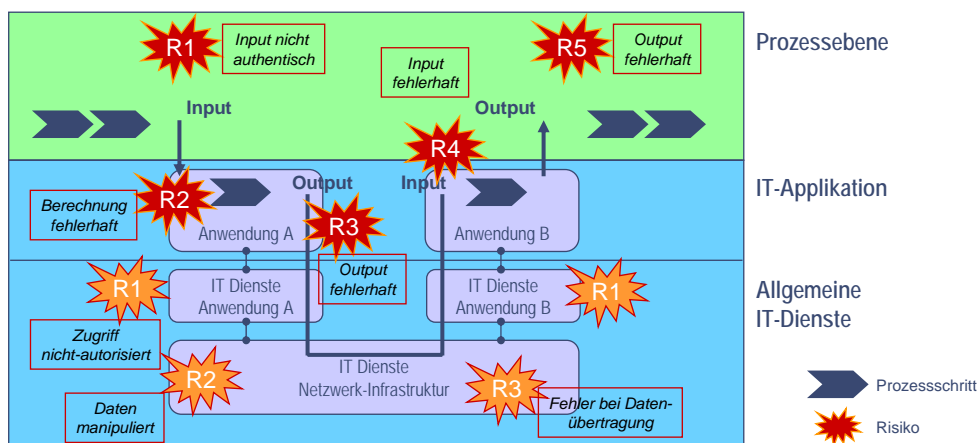


Rolle der IT-Sicherheit zur Compliance
PricewaterhouseCoopers

Seite 17
September 05

Compliance-Anforderungen durch den Sarbanes-Oxley Act

IT-Risiken im Geschäftsprozess (Fortsetzung)

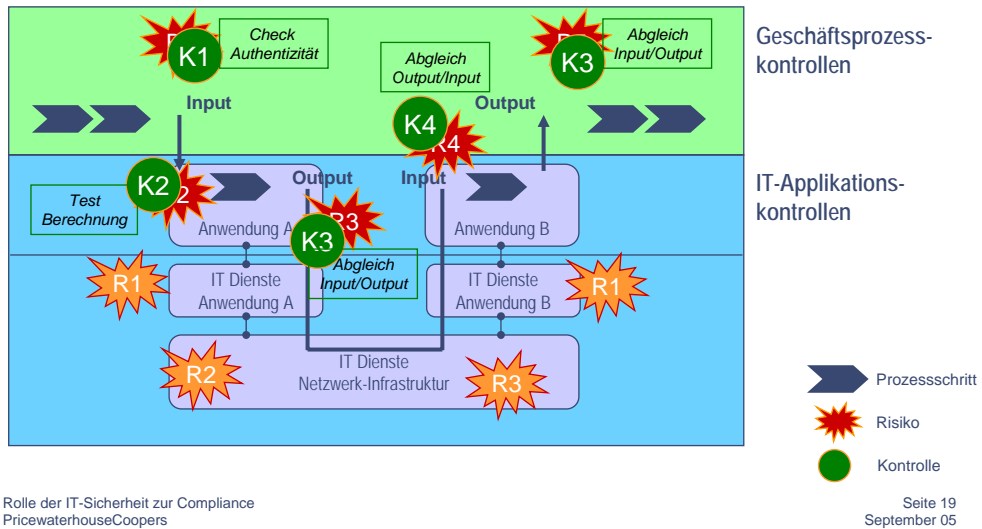


Rolle der IT-Sicherheit zur Compliance
PricewaterhouseCoopers

Seite 18
September 05

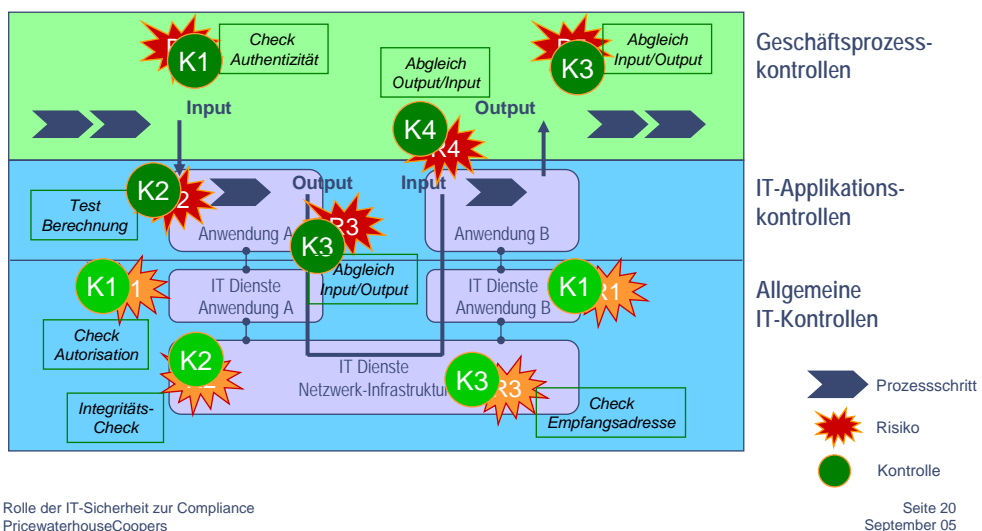
Compliance-Anforderungen durch den Sarbanes-Oxley Act

IT-Kontrollen im Geschäftsprozess



Compliance-Anforderungen durch den Sarbanes-Oxley Act

IT-Kontrollen im Geschäftsprozess (Fortsetzung)



Compliance-Anforderungen durch den Sarbanes-Oxley Act

Dokumentation für SOX: Kontrollen + Prozess

Typische Prozessdokumentation:



- Prozessbeschreibung auf operativer Ebene
- Keine detaillierte Dokumentation von Kontrollen

SOX Prozessdokumentation (Dokumentationspflicht!):



- High-level Prozessdokumentation (Basis z.B. ITIL)
- Detaillierte Dokumentation von Kontrollen (Basis z.B. COBIT)

Rolle der IT-Sicherheit zur Compliance
PricewaterhouseCoopers

Seite 21
September 05

Compliance-Anforderungen durch den Sarbanes-Oxley Act

Bedeutung mächtiger (pervasive) IT-Kontrollen

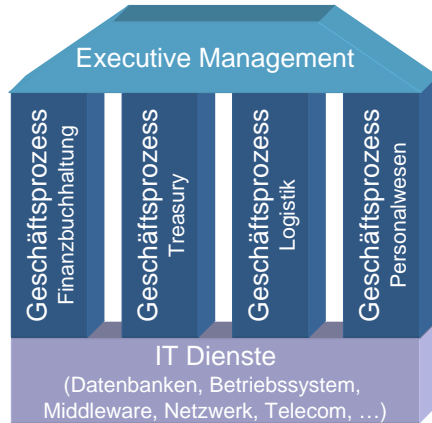
- Unternehmenskontrollen (Company-level controls) gelten als besonders wichtig und mächtig, denn
 - ohne angemessene Ethik, Leitbild und Risikobewusstsein wird es kein effektives internes Risiko- und Kontrollsystem geben
 - Allgemeine IT-Kontrollen (IT General Controls) gelten als besonders wichtig und mächtig, denn
 - sie beeinflussen umfassend die operative Effektivität aller automatisierten Applikationskontrollen
 - effektive allgemeine IT-Kontrollen ermöglichen erst das Testen der Effektivität von Applikationskontrollen
- !** Kontrollen zur IT-Sicherheit sind hier i.a. sehr starke IT-Kontrollen

Rolle der IT-Sicherheit zur Compliance
PricewaterhouseCoopers

Seite 22
September 05

Compliance-Anforderungen durch den Sarbanes-Oxley Act

Kontrollen zur IT-Sicherheit



Unternehmenskontrollen:
Direktiven/Richtlinien zur IT-Sicherheit;
Governance in IT-Sicherheit

IT-Applikationskontrollen:
Zugriffskontrollkonzepte,
Input/Output-Kontrollen,
Verarbeitungskontrollen.

Allgemeine IT-Kontrollen:
Kontrollen der IT-Sicherheit, die in
IT-Prozessen und IT-Diensten
integriert sind.

Rolle der IT-Sicherheit zur Compliance
PricewaterhouseCoopers

Seite 23
September 05

Compliance-Anforderungen durch den Sarbanes-Oxley Act

Kontrollgebiete zur IT-Sicherheit nach COBIT

IT Architektur

IT Organisation

Compliance

Weisungen/Prozesse zur SW-Entwicklung

IT Systemsicherheit

Behandlung von Problemen / Störungen

Datenmanagement

Rechenzentrumsicherheit

Überwachung

Rolle der IT-Sicherheit zur Compliance
PricewaterhouseCoopers

Seite 24
September 05

Compliance-Anforderungen durch den Sarbanes-Oxley Act

Prozess: IT Systemsicherheit

Nr.	Kontrollziel	COSO Komponente	Kontrollbeschreibung	Schlüsselkontrollen
1	Ein IT Sicherheitsplan existiert und ist mit der gesamten strategischen IT Planung abgestimmt.	Kontrollaktivitäten	Vom Unternehmen zu definieren	Vom Unternehmen zu definieren
2	Der IT Sicherheitsplan ist aktuell und reflektiert Änderungen im IT Umfeld und Sicherheitsanforderungen von speziellen Systemen.	Kontrollaktivitäten		
3	Prozesse werden befolgt um sicherzustellen, dass alle Benutzer auf dem Systemen zugelassen sind und die Transaktionen gültig sind.	Kontrollaktivitäten		
4	Prozesse werden befolgt, um die Effektivität der Zulassungs- und Zugangsmechanismen zu unterhalten (z.B. regelmässige Passwortwechsel)	Kontrollaktivitäten		
5	Prozesse werden befolgt, damit die zeitgerechte Aufbereitung, Ausgabe, Ausserkraftsetzung und Schliessung von Benutzerkonten gewährleistet ist.	Kontrollaktivitäten		

Rolle der IT-Sicherheit zur Compliance
PricewaterhouseCoopers

Seite 25
September 05

Compliance-Anforderungen durch den Sarbanes-Oxley Act

Prozess: IT Systemsicherheit (Fortsetzung)

Nr.	Kontrollziel	COSO Komponente	Kontrollbeschreibung	Schlüsselkontrollen
6	Ein formalisierter Genehmigungsprozess existiert, um Zugangsprivilegien zum System und den Daten zu gewähren.	Kontrollaktivitäten	Vom Unternehmen zu definieren	Vom Unternehmen zu definieren
7	Ein Kontrollprozess existiert und wird befolgt, um periodische Kontrollen und Bestätigungen von Zugangsrechten durchzuführen.	Kontrollaktivitäten		
8	Wo Netzwerkverbindungen eingesetzt werden, müssen geeignete Kontrollmassnahmen wie Firewalls, Intrusion Detection und Sicherheitsprüfungen unbefugten Zugang verhindern.	Kontrollaktivitäten		
9	Der IT Sicherheitsplan und die dazu gehörigen Aktivitäten und Prioritäten sind an die aktuelle Sicherheitseinschätzung angepasst.	Information und Kommunikation		
10	Der IT Sicherheitsadministrator überwacht und registriert die Sicherheitsaktivitäten. Er deckt Missbräuche auf und berichtet sie an die Geschäftsleitung	Überwachung		

Rolle der IT-Sicherheit zur Compliance
PricewaterhouseCoopers

Seite 26
September 05

Compliance-Anforderungen durch den Sarbanes-Oxley Act

Testen der Effektivität von Prozess und Kontrollen

- Beurteilung der Effektivität der Prozess- und Kontrollentwürfs
 - Prüfung von
 - Prozess
 - Schlüsselkontrollen
 - Prüfungsmethode: Schrittweise Analyse
- Beurteilung der Effektivität von Kontrollen im Betrieb
 - Prüfung von
 - Schlüsselkontrollen
 - Prüfungsmethode:
 - Kontrollschritt-wiederholung (nicht immer möglich)
 - Überprüfung von Stichproben
 - Beobachtung
- Die Rolle des Testers/Prüfers muss von Prozess- und Kontrollentwicklung und Kontrollausführung unabhängig sein

Rolle der IT-Sicherheit zur Compliance
PricewaterhouseCoopers

Seite 27
September 05

Compliance-Anforderungen durch den Sarbanes-Oxley Act

Beurteilung von Mängeln

An (inconsequential) *control deficiency* exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis.

A significant deficiency is an internal control deficiency in a significant control or an aggregation of such deficiencies that could result in a misstatement of the financial statements that is more than inconsequential.

A material weakness is a significant deficiency or an aggregation of significant deficiencies that preclude the entity's internal control from providing reasonable assurance that material misstatements in the financial statements will be prevented or detected on a timely basis by employees in the normal course of performing their assigned functions.

Quelle: PCAOB, AS2, p. 143ff.

- Die Beurteilung, ob ein Mangel belanglos ist oder nicht, erfordert ein **beachtliches Mass an professionellen Wissen und Erfahrung** und beruht auf Faktoren wie:
 - Eigenart und Bedeutung des Mangels
 - Nähe zu Finanzanwendungen und wichtigen Konten
 - Anfälligkeit für Wirtschaftskriminalität
 - Ursache und Häufigkeit des Mangels

Rolle der IT-Sicherheit zur Compliance
PricewaterhouseCoopers

Seite 28
September 05

Compliance-Anforderungen durch den Sarbanes-Oxley Act

Allgemeine IT-Kontrollen – „Substantielle Mängel“?

- Mängel bei allgemeinen IT-Kontrollen müssen nicht unweigerlich zu einer Falschaussage in der Finanzberichterstattung führen und werden daher im Zusammenhang mit den zugehörigen Anwendungskontrollen betrachtet
- Falschaussagen in der Finanzberichterstattung können eher durch schlecht programmierte Kontrollen oder ineffektive halbautomatische Kontrollen auf Anwendungsebene entstehen
- Dennoch: die grundsätzliche, weitreichende Vernachlässigung der allgemeinen IT-Kontrollen oder die nicht termingerechte Beseitigung von identifizierten Schwächen kann leicht zu substantiellen Mängeln führen

Rolle der IT-Sicherheit zur Compliance
PricewaterhouseCoopers

Seite 29
September 05

Zusammenfassung und Fazit

Schlussfolgerungen I

- Zunehmende Gleichrichtung von Compliance-Anforderungen durch Gesetze. Gefordert sind ein
 - Formales System zum Management Operationeller Risiken
 - Internes Kontrollsystem zur Sicherung der ordnungsmässigen Geschäftsführung
- Der Sarbanes-Oxley Act (SOX) geht weit über die bisherigen Anforderungen und Sanktionen hinaus
 - Aufgrund der wirtschaftlichen Bedeutung der US-Börse hat SOX Auswirkungen weltweit
 - Schweizerische und Europäische Unternehmen sind betroffen
 - SOX hat eine „Sogwirkung“ für hiesige Gesetze
 - Weitreichende Mängel bei IT-/IT-Sicherheitskontrollen können als substantielle Mängel identifiziert werden
- Anhand von SOX-Projekten kann man lernen
 - Grundsätzliche Richtung und Massnahmen; Stärken, Schwächen, Chancen und Risiken

Rolle der IT-Sicherheit zur Compliance
PricewaterhouseCoopers

Seite 30
September 05

Zusammenfassung und Fazit

Schlussfolgerungen II

- **Kosten von Compliance:**
 - Die Debatte läuft
 - Kleine Unternehmen zahlen im Durchschnitt (deutlich) mehr als grosse Unternehmen
 - Darum erfordert es dringend eine Orientierung der Compliance-Massnahmen and Grösse und Materialität des Unternehmens (wie im neuen Schweizerischen Revisionsgesetz geregelt):
 - Grosse Gesellschaften:
 - Sind „nach allen Regeln der Kunst“ zu prüfen
 - Als Basis gelten immer internationale Standards
 - Kleine Gesellschaften:
 - Vernünftig reduzierte Anforderungen
 - Verdichtung von Dokumentation und Kontrollen
- Kombination von **Governance, Risk & Compliance** verspricht Optimierung von Wertschöpfung und Werterhalt

Rolle der IT-Sicherheit zur Compliance
PricewaterhouseCoopers

Seite 31
September 05

Ihr Kontakt

Dr.-Ing. Stephan Teiwes
CISA, CISM, CISSP
Senior Manager, Advisory Services
Nordstrasse 15, CH-8035 Zürich
Office: +41 1 630 27 96 Mobile: +41 79 752 63 73
mailto: stephan.teiwes@ch.pwc.com

© 2005 PricewaterhouseCoopers AG/SA. All rights reserved. PricewaterhouseCoopers AG/SA refers to the Swiss firm of PricewaterhouseCoopers AG/SA and the other member firms of PricewaterhouseCoopers International Limited, each of which is a separate and independent legal entity.

PRICEWATERHOUSECOOPERS 