
Herstellung gesetzlicher Konformität der IT-Prozesse bei einem verzweigten globalen Konzern

Xionet: Identity Management

Bochum, 20. Oktober 2005

Prof. Dr. Thomas Wolf



Agenda

§ Hintergrund

§ Der Sarbanes Oxley Act und seine Konsequenzen

§ Praxisbericht: Sox Konformität der IT

§ Resümee

Mit dem Computereinsatz entstanden neuartige Probleme im Hinblick auf die Nachvollziehbarkeit und Sicherheit von Informationen

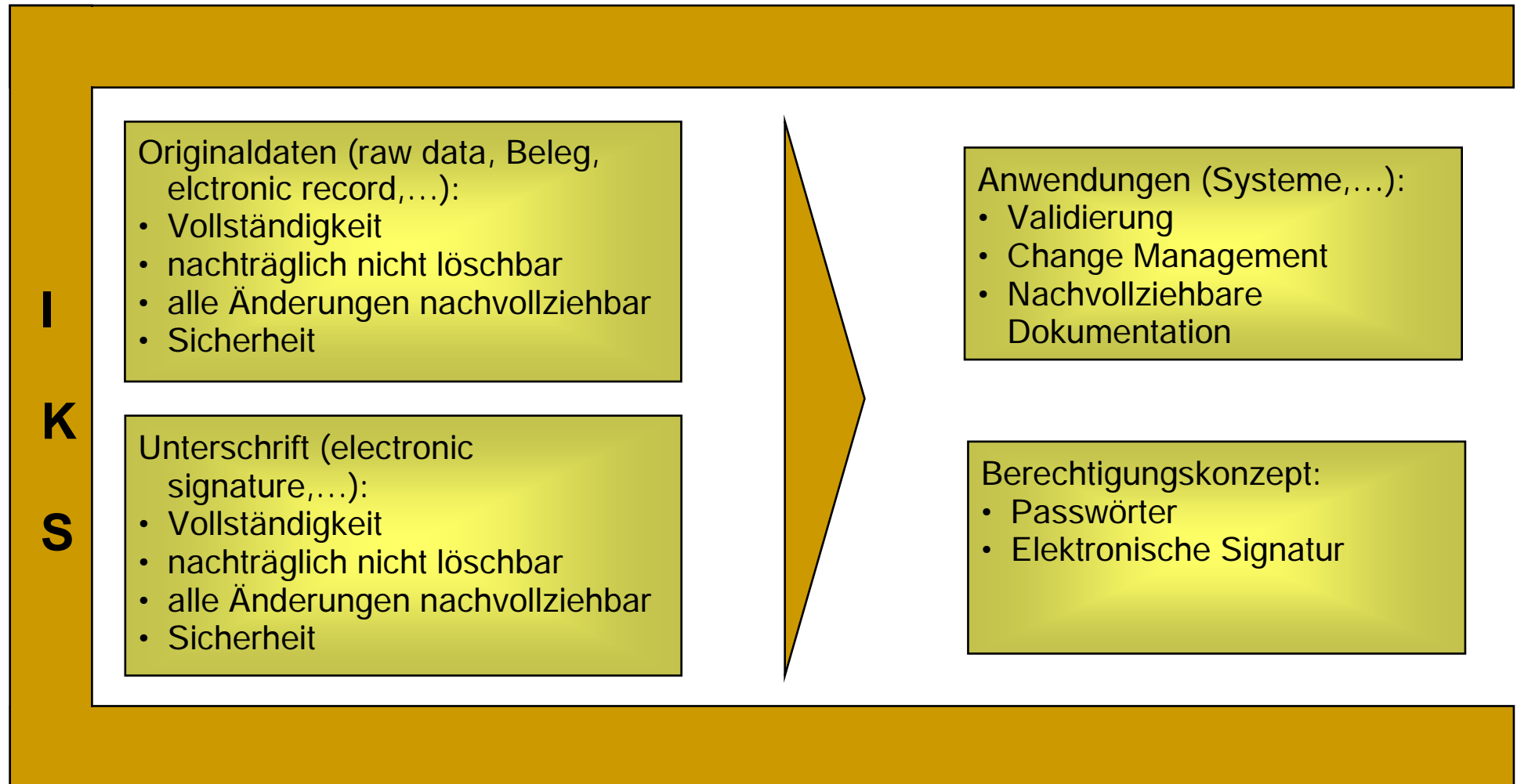
- n Daten können geändert werden, ohne dass Spuren entstehen
- n Die Ergebnisse automatisierter Verarbeitung werden nicht im Einzelfall verifiziert
- n Kontrollen werden ganz oder teilweise in die Systeme verlagert:
 - Automatische Überprüfung von Kompetenzgrenzen
 - Plausibilitäten (z.B.: Verhalten eines Kunden)
 - Kontrollschritte in Arbeitsanweisungen („workflows“)

Regulatorische Anforderungen an die Nachvollziehbarkeit von Informationen an sich gibt es schon viel länger (Wirtschaftsprüfung seit dem 19. Jahrhundert; GxP seit 1968)

Je nach inhaltlicher Anforderung wurden ganz unterschiedliche Regelwerke entwickelt

Zweck der Regulierung	Regelwerk
Arzneimittelsicherheit	GxP (Good manufacturing/ laboratory/ clinical Practices) (FDA seit 1969), 21 CFR Part 11 (FDA 1997)
Anlegerschutz, Gläubigerschutz	GoS (Grundsätze ordnungsmäßiger Speicherbuchführung) (BMF 1978)
Anlegerschutz	GoBS (Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (BMF 1995)
Anlegerschutz, persönliche Verantwortlichkeit der Unternehmensführung	Sox (Sarbanes Oxley Act) (US Kongress 2002)
Gläubigerschutz, Kreditwürdigkeit	Basel II
Informationssicherheit	BS 7799 (1993), seit 2000 ISO 17799
Steuerehrlichkeit	GDPdU (Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen) (Steuersenkungsgesetz 2002)

Die IT- spezifischen Anforderungen in den verschiedenen Regelwerken gleichen sich weitgehend, setzen unterschiedliche Schwerpunkte



Agenda

§ Hintergrund

§ Der Sarbanes Oxley Act und seine Konsequenzen

§ Praxisbericht: Sox Konformität der IT

§ Resümee

Der SOA regelt die Verantwortlichkeiten der Unternehmensführung und der Wirtschaftsprüfer grundlegend neu

Hintergrund:

Vorausgegangen waren Zusammenbrüche/ **Bilanzskandale** (z.B. Enron, Tyco, MCI,...), die nicht nur in der US-amerikanischen Öffentlichkeit, sondern auch weltweit in einer bislang nicht gekannten Intensität diskutiert wurden.

Reichweite:

Die Regelungen des Sarbanes-Oxley Acts beschränken sich nicht auf den amerikanischen Raum. Sie betreffen vielmehr **alle Unternehmen, die an einer US-amerikanischen Wertpapierbörse notiert sind, sowie deren IT- und BPO- Zulieferer.**

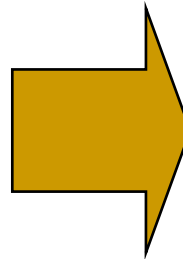
Ausblick:

Parmalat und Royal Ahold zeigen, dass die Kapitalmärkte im europäischen Raum vor Finanzskandalen wie in den USA keineswegs gefeit sind. Daher sind auch **in Europa Bestrebungen** in Form von Gesetzesvorlagen erkennbar, die Transparenz entsprechend klarer Richtlinien zu steigern und damit ein Corporate Governance zu verbessern.

- **Der Sarbanes-Oxley Act sieht Maßnahmen mit Auswirkungen auf verschiedene Zielgruppen vor. (CEO, CFO und deren Wirtschaftsprüfer)**
- **Kontrollorgan ist die SEC (U.S. Securities and Exchange Commission)**

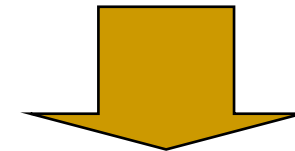
Er bezieht sich direkt nur auf die Finanzprozesse eines Unternehmens, indirekt damit auch auf Applikationen und die IT-Umgebung

- Finanz- und Rechnungswesen
- Bilanzwesen
- Einkauf und Kreditorenbuchhaltung
- Inventarmanagement
- Projekte
- Personal, Personalbuchhaltung
- Umsätze und Debitorenbuchhaltung
- Investitionsmanagement
- Cash Management
- Unternehmensfinanzierung
- ...



Finanzprozesse werden durch Applikationen unterstützt:

- Applikationserstellung muss einbezogen werden
- Applikationsänderungen müssen einbezogen werden



Applikationen laufen auf Systemen:

- Prozesse des IT- Betriebs müssen betrachtet werden
- Infrastruktur muss betrachtet werden

Deshalb haben eine Reihe von Artikeln des Sarbanes-Oxley Act Auswirkungen auf die IT

Section 103: Internal audit must, and therefore businesses should, maintain all audit-related records, including electronic ones, for seven years.

Section 201: Firms that audit the company's books can no longer also provide IT-related services.

Section 301: Must provide systems or procedures that let whistle-blowers communicate confidentially with the company's audit function.

Sections 302: Certification of Financial Reports - CEO and CFO must sign statements verifying completeness and accuracy of financial reports. Criminal penalties.

Section 404: Certification of Internal Controls - CEO, CFO and outside auditors must attest to the effectiveness of internal controls for financial reporting.

Section 409: Material Event Reporting - Companies must report material changes in financial conditions "on a rapid and current basis." The act calls for "real-time disclosure" but doesn't yet define what that means.

Die umfassendsten Konsequenzen für Entwicklung, Wartung und Betrieb von Systemen hat Artikel 404

- § Artikel 404 fordert die Einrichtung und Pflege eines internen Kontrollsystems für die Finanzberichterstattung (Internal Control Over Financial Reporting).
- § Die SEC definiert den „*Internal Control Over Financial Reporting*“ als einen von CEO und CFO eingerichteten Prozess, der die Ordnungsmäßigkeit der Finanzberichterstattung und damit die Erstellung der Abschlüsse gemäß der anzuwendenden Rechnungslegungsvorschriften sicherstellt.
- § Hierdurch ist das Management aufgefordert, ein adäquates internes Kontrollsystem:
 - einzurichten,
 - kontinuierlich anzuwenden,
 - zu überwachen und
 - Anwendung und Überwachung zu dokumentieren
- § Ein Bericht über dessen Wirksamkeit ist jährlich bei der SEC einzureichen. Zusätzlich muss der Wirtschaftsprüfer die Richtigkeit des Berichts testieren. Letzteres setzt voraus, dass dieser eine eigenständige Bewertung des internen Kontrollsystems der Finanzberichterstattung durchführt.

Die Verantwortung für SOX Konformität lässt sich nicht outsourcen: deshalb sind viele IT- Service Unternehmen betroffen

....Nonetheless, it is clear that **the responsibility to maintain effective internal control over financial reporting is not delegable** by public company management.

Robert Gareis and Michael S. Mensik, Partners, Baker & McKenzie, Chicago, Illinois

<http://accounting.smartpros.com/x43338.xml>

"**The use of a service organization does not reduce management's responsibility** to maintain effective internal control over financial reporting. Rather, user management should evaluate controls at the service organization, as well as related controls at the user company when making its assessment about internal control over financial reporting."

"If the service organization is part of a user company's information **system—they are part of the company's internal control** over financial reporting..."

Management should evaluate controls at the service organization as well as related controls at the user company when assessing internal controls over financial reporting. From the IT perspective, if the services provided are significant, it will require both management and its independent auditors to evaluate the service organization's controls

By Lily Shue, CISA, CISM, CCP; Volume 5, 2004

<http://www.isaca.org/Template.cfm?Section=Home&Template=/MembersOnly.cfm&ContentID=14611>

Kontrolle des Serviceunternehmens ist ein Muss, für die Art der Kontrolle gibt es zwei unterschiedliche Möglichkeiten

Voraussetzungen:

- § Ein Unternehmen, das IT Services erbringt, unterliegt dann den Sox Kontrollanforderungen, wenn die IT Services finanzrelevante Daten betreffen (speichern, verarbeiten, transportieren,...)

Kontrollerfordernisse:

- § Grundsätzlich sind jene Kontrollen einer Service Organisation zu prüfen, welche einen Einfluss auf das interne Kontrollsystem mit Bezug auf den Jahresabschlußbericht einer User Organisation haben oder haben können.
- § Die Prüfung dieser Kontrollen basiert auf der Beschreibung der Kontrollen der Service Organisation.
- § Diese Beschreibung ist durch die Service Organisation zu erstellen.

Durchführung der Kontrollen:

- § Kontrolle auf Basis eines SAS 70 Reports
- § Eigene Kontrollen

SAS 70 beschreibt selbst keine geforderten Kontrollen, diese sind jeweils spezifisch festzulegen

Inhalt:

SAS 70 schreibt keine Kontrollen vor, die durch eine Service Unternehmen zu erfüllen sind. Die Kontrollziele sind immer als spezifisch für eine Service Organisation und deren Kunden zu betrachten

Als Grundlagen für Kontrollen können u.a. folgende Standards genutzt werden:

- § [BS7799 / ISO 17799](#)
- § Cobit
- § SysTrust Principles and Criteria
- § WebTrust Principles and Criteria
- § IT Control Objectives for Sarbanes-Oxley

Durchführender:

- Ein SAS 70 Audit kann nur von einem unabhängigen certified public accountant (CPA) durchgeführt werden.
- Das Unternehmen dem der CPA angehört, muss den „specific professional standards“ des American Institute of Certified Public Accountants (AICPA) verpflichtet sein.
- Ein SAS 70 Audit kann auch außerhalb der USA durchgeführt werden. Wichtig ist lediglich, dass die Anforderungen des AICPA erfüllt sind.
- Das Unternehmen kann zur Leistungserbringung auch nicht CPAs einsetzen. Allerdings muss der finale Report durch einen CPA inhaltlich qualitätsgesichert werden und darf nur von ihm herausgegeben werden.

Auch mit SAS 70 Bericht bleibt dem Management noch einiges zu tun

Analyse:

- § Zeitperiode, die der Bericht abdeckt
- § Ist die Reichweite des SAS 70 Berichts klar definiert und deckt die Anforderungen ab
- § Geprüfte Tests, Ergebnisse und Einschätzung des Prüfers
- § Abschätzung, ob die Prüfereneinschätzung gerechtfertigt ist.
- § Abschätzung, ob der Prüfer unabhängig ist
- § Gab es Auffälligkeiten in der Vergangenheit, die nicht abgedeckt sind

Ergänzende Untersuchungen, falls der Bericht nicht sehr zeitnah:

- § Änderungen in der Organisation oder beim Personal
- § Änderungen bei den Kontrollprozessen
- § Änderungen in SLAs oder Verträgen
- § Auffälligkeiten bei Kontrollen

Die Aufgabe des Managements ist größer, wenn kein SAS 70 Bericht des IT Service Unternehmens vorliegt

Zu klärende Fragen:

- § Gibt es klar vereinbarte Service Level?
- § Sind die wesentlichen IT-Controls vertraglich vereinbart? Speziell für:
 - § Anwendungsentwicklung
 - § Change Management
 - § Zugangskontrolle
 - § IT Betrieb
- § Gab es je eine unabhängige Prüfung? Ergebnisse hinsichtlich:
 - § Reichweite
 - § Ergebnisse
 - § Konsequenzen aus erkannten Problemen
- § Weitere Vorgehensweise definieren, um hinreichende Sicherheit zu erlangen

Agenda

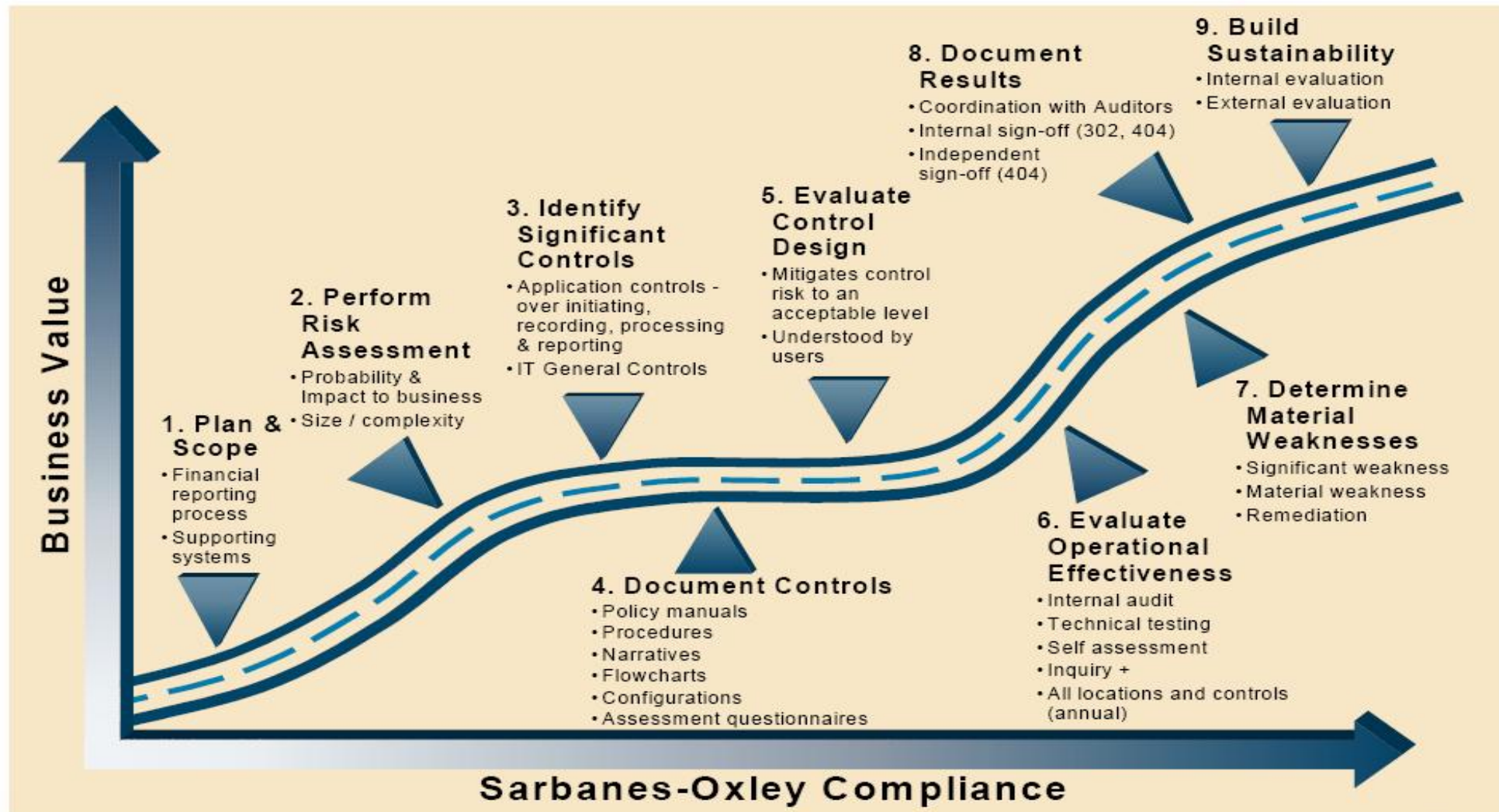
§ Hintergrund

§ Der Sarbanes Oxley Act und seine Konsequenzen

§ Praxisbericht: Sox Konformität der IT

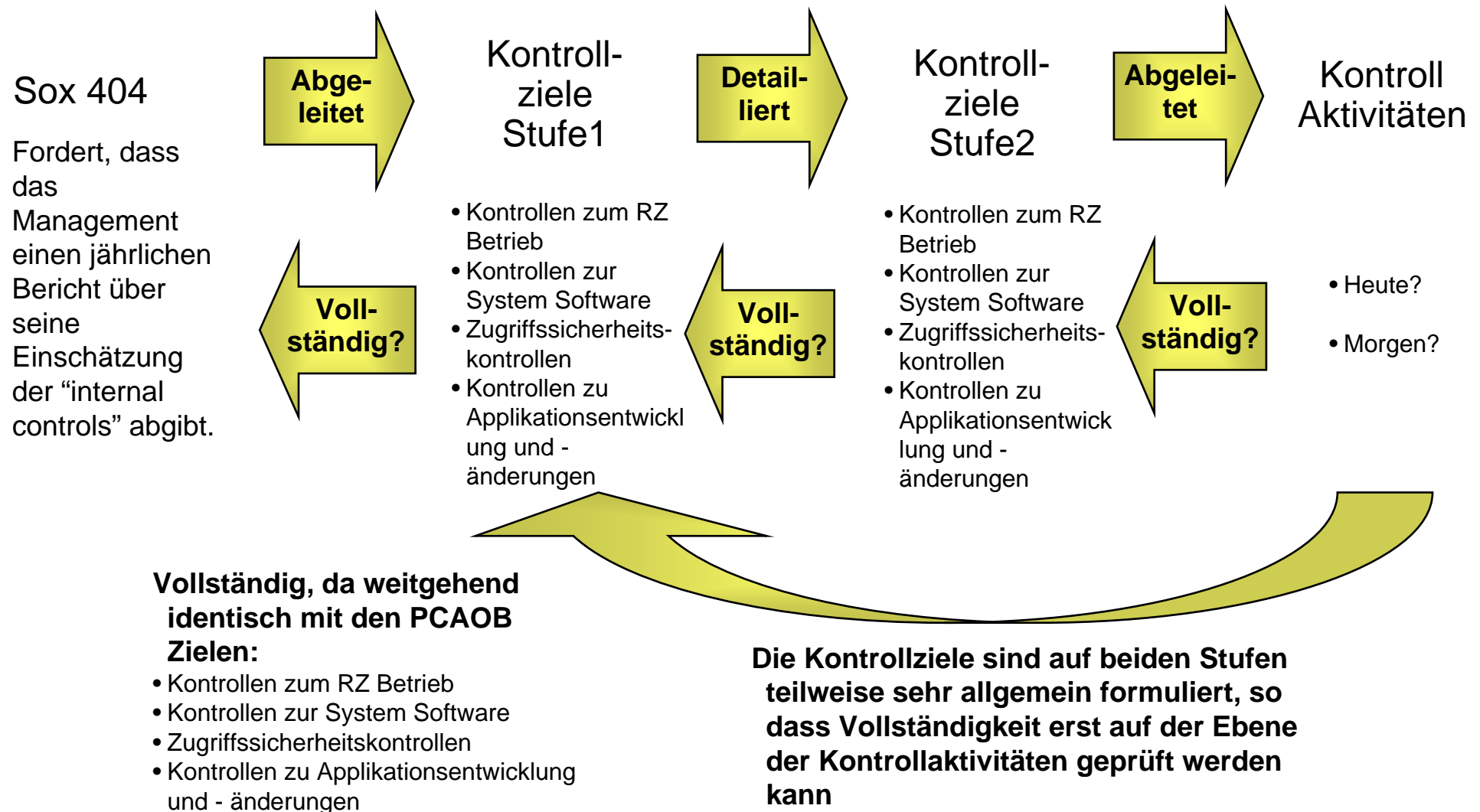
§ Resümee

Der klassische Weg zur Konformität zielt dann darauf ab, SOX Prüfbarkeit herzustellen und die Prüfung zu „bestehen“

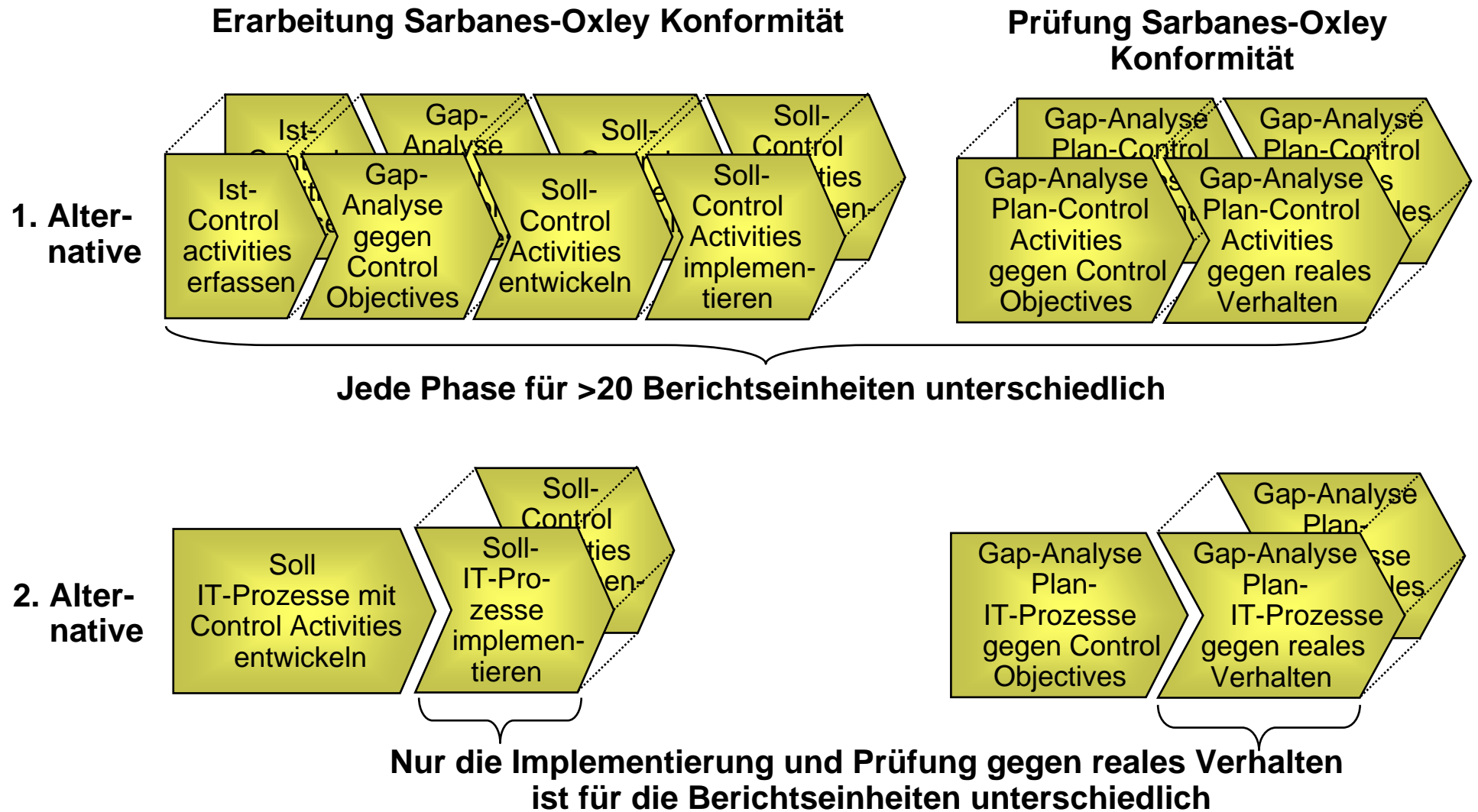


©2003 IT Governance Institute

Der Konzernansatz folgte dem klassische Weg SOX Konformität in jedem Konzernunternehmen einzeln prüfbar zu machen



Statt für mehr als 20 Berichtseinheiten individuell Sox Konformität sicherzustellen, entwickelten wir standardisierte, konforme Prozesse

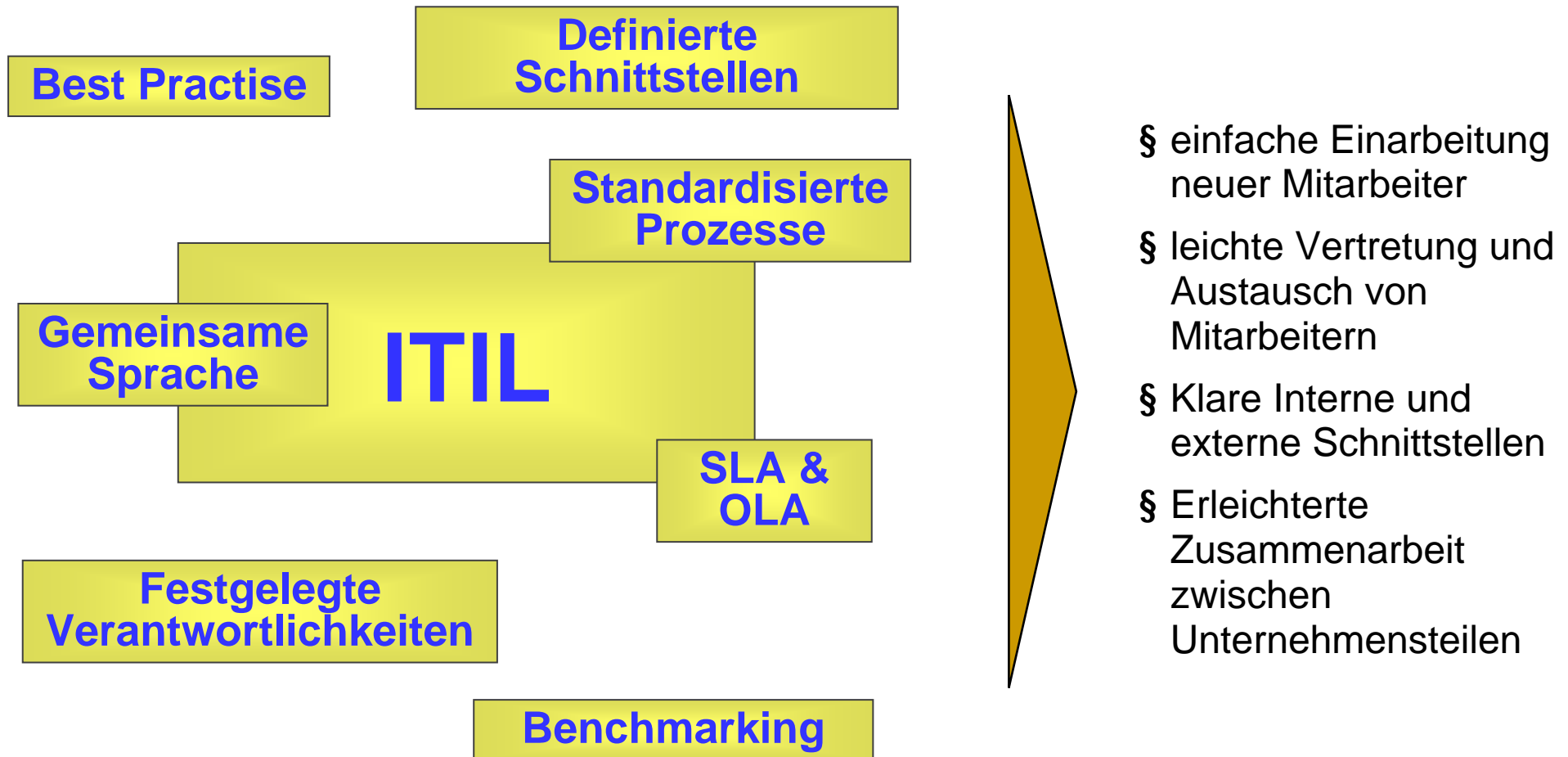


Wir verwenden ITIL, den weltweiten de- facto Standard im IT Service Management

ITIL

- § ist die Abkürzung von „IT Infrastructure Library“
- § Ist eine Architektur zur Etablierung und zum Betrieb des IT Service Managements
- § wurde im Auftrag der britischen Regierung durch die CCTA (heute OGC) in Norwich (England) entwickelt
- § entstand in Zusammenarbeit mit IT- Dienstleistern, Mitarbeitern aus Rechenzentren, Lieferanten, Beratern und Ausbildern
- § hat sich als weltweiter De-facto-Standard im Service Management etabliert
- § kann als der „Best Practice“ Leitfaden im IT Management bezeichnet werden
- § regelt das „Was“ und nicht das „Wie“

Als Ergebnis haben wir nicht nur Sox Konformität erreicht, sondern auch Service Excellence bei der Leistungserbringung



Agenda

§ Hintergrund

§ Der Sarbanes Oxley Act und seine Konsequenzen

§ Praxisbericht: Sox Konformität der IT

§ Resümee

Die Prüfbereiche des Sarbanes – Oxley Acts fordern eine klare Rollentrennung: als Modell und in der täglichen Unternehmenspraxis

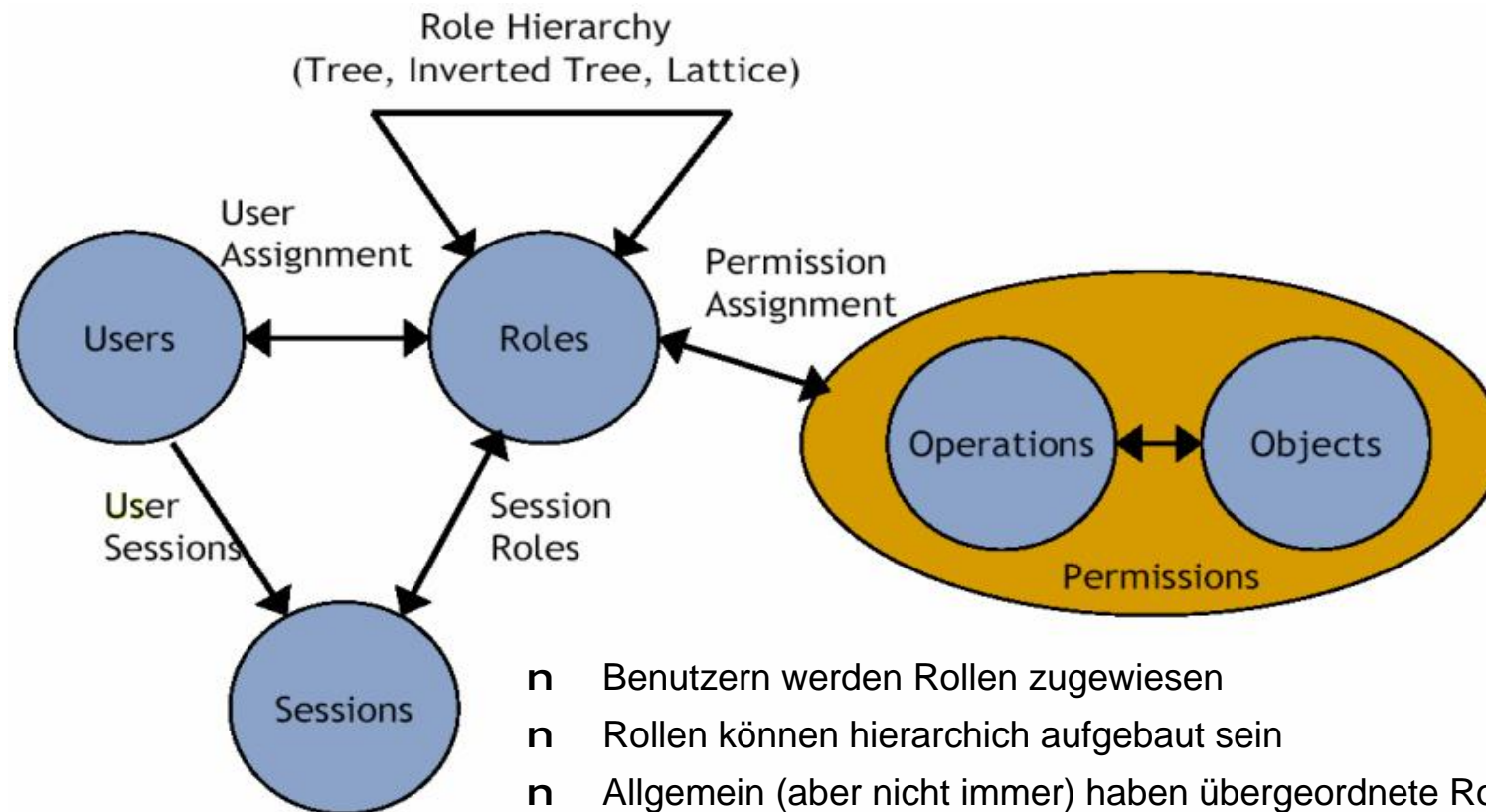
SOX- Prüfungsbereiche

- § Control environment & organisational controls
- § Controls on application development and maintenance
- § Controls on logical security
- § Controls on physical access & environmental security
- § Application controls and monitoring
- .

Verantwortlich

- § IT-Leiter
- .
- § Entwickler – Betreiber
- .
- § Security- Beauftragter
- § Security- Beauftragter
- .
- § Anforderer – Genehmiger (z. B. im Einkauf)

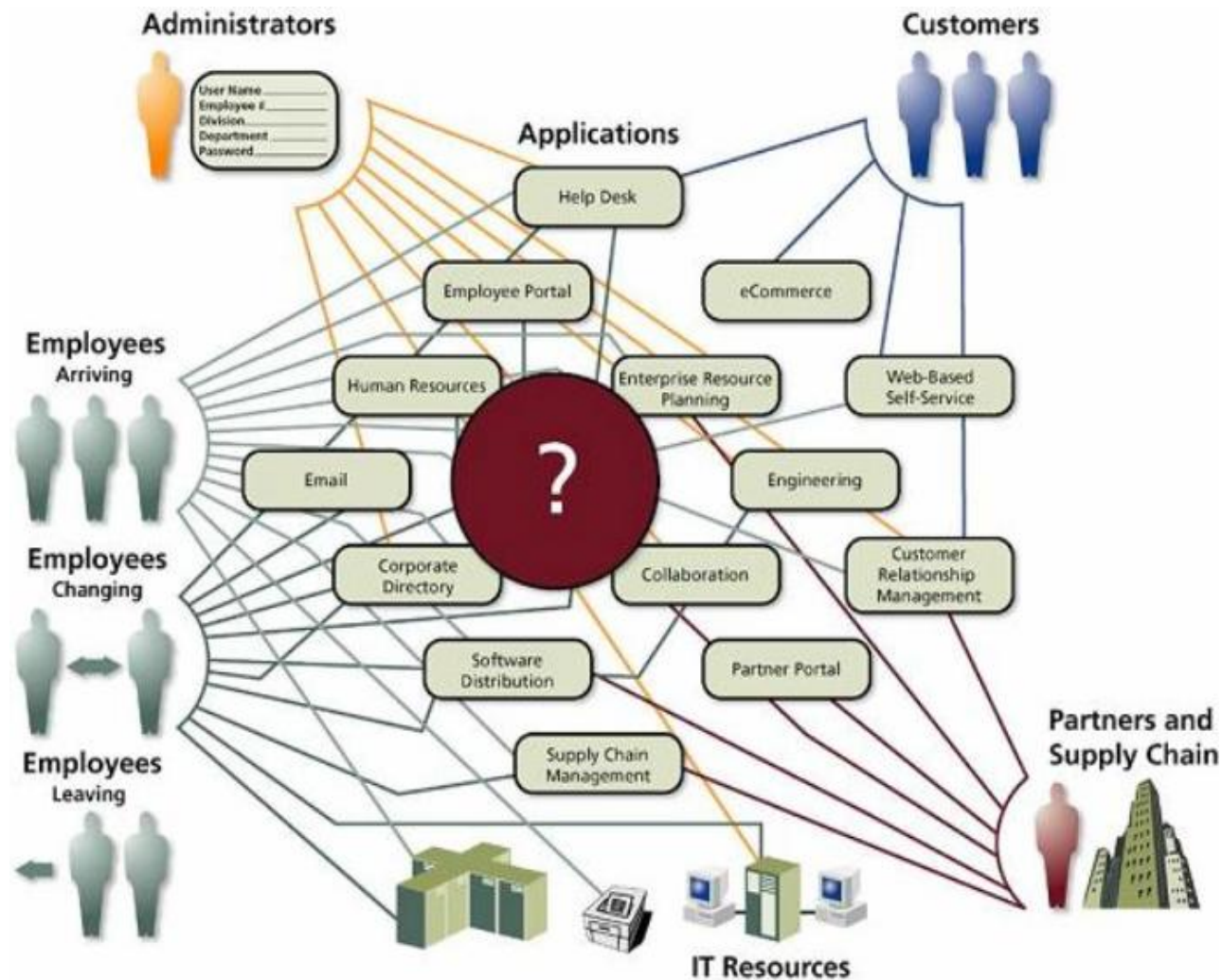
Im Modell ist das meist noch relativ einfach zu beschreiben



- n Benutzern werden Rollen zugewiesen
- n Rollen können hierarchisch aufgebaut sein
- n Allgemein (aber nicht immer) haben übergeordnete Rollen alle Berechtigungen der untergeordneten Rollen.
- n Permissions sind Operationen auf Objekte.
- n Permissions können + (additiv) oder - (subtraktiv) zugewiesen werden.
- n Rollen können auch temporär pro Sitzung zugewiesen werden.

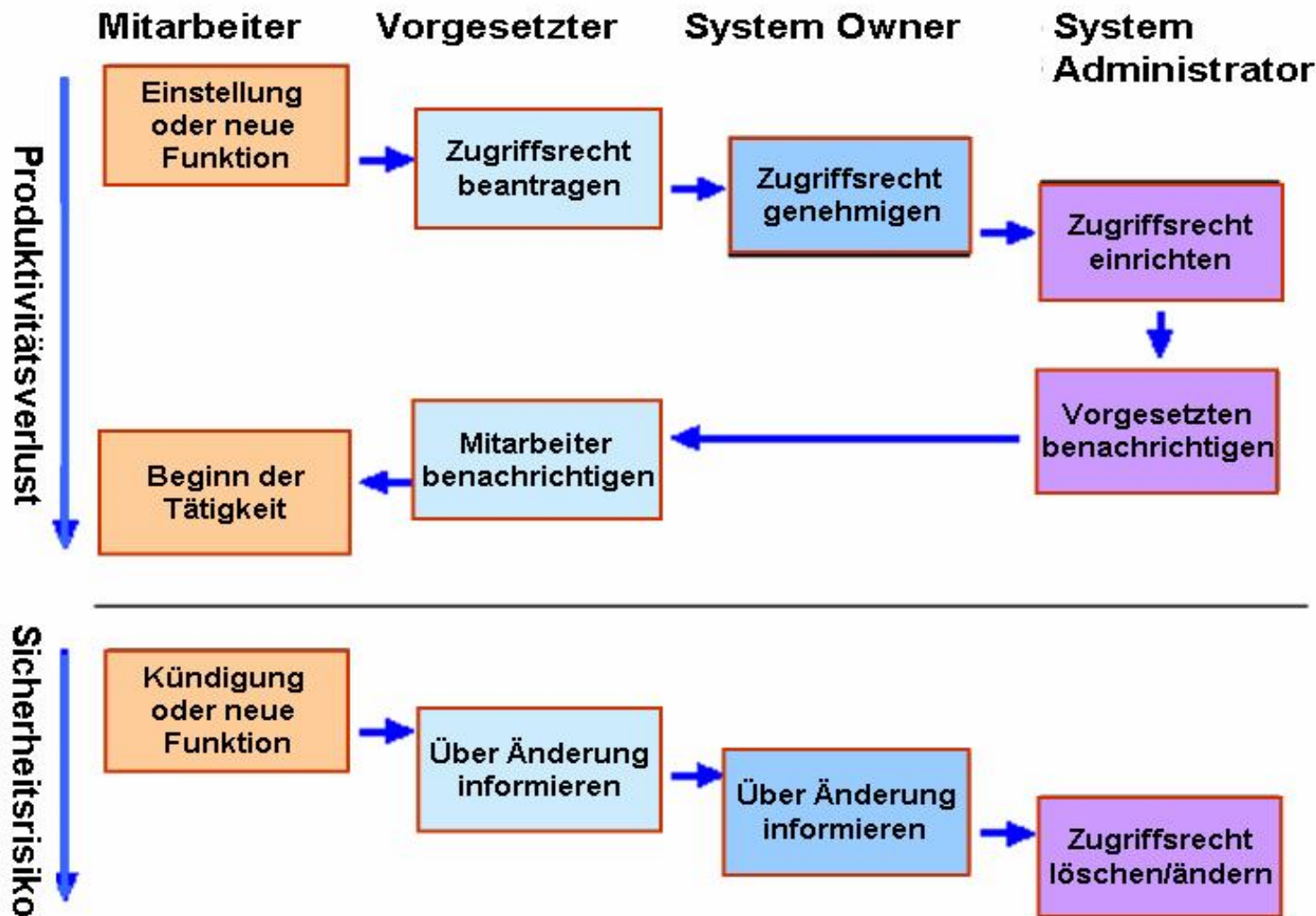
Quelle: Ferraiolo, Sandhu, Gavrila: A Proposed Standard for Role-Based Access Control, 2000.

Die Umsetzung in die gelebte Unternehmenspraxis ohne konsistentes Identity Management wird dagegen zum Problem



User Informationen sind oft fragmentiert, mehrfach vorhanden oder überholt: es gibt weder konsistente Prozesse noch Prüfbarkeit.

SOX erhöht den Druck auf ein umfassendes Identity Management – aus Produktivitäts- und Sicherheitsgründen



Quelle: Dr. Horst Walther, SiG Software Integration GmbH

Der Sarbanes Oxley Act unterscheidet sich dabei im Anspruch von anderen Regulierungen inhaltlich nur unwesentlich

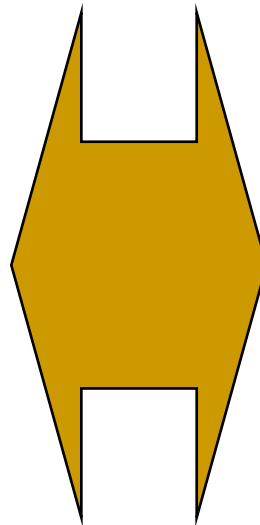
Sox für IT:

- n „arbeite ordentlich“ und
- n „dokumentiere, dass Du ordentlich gearbeitet hast“



Druck auf Prozessintegration:

- n HR (Berechtigungskonzept,...)
- n Asset Management
- n ...



Bleibt die Frage:

Was ist anders als bei anderen Regelwerken?

Die Antwort: Manche Regelwerke (SOA, Part 11,...) werden einfach ernster genommen als andere

