

Governance, Risk, Compliance (GRC) & SOA Identity Management

14.02.2008

Sebastian Rohr, KCP
sr@kuppingercole.de

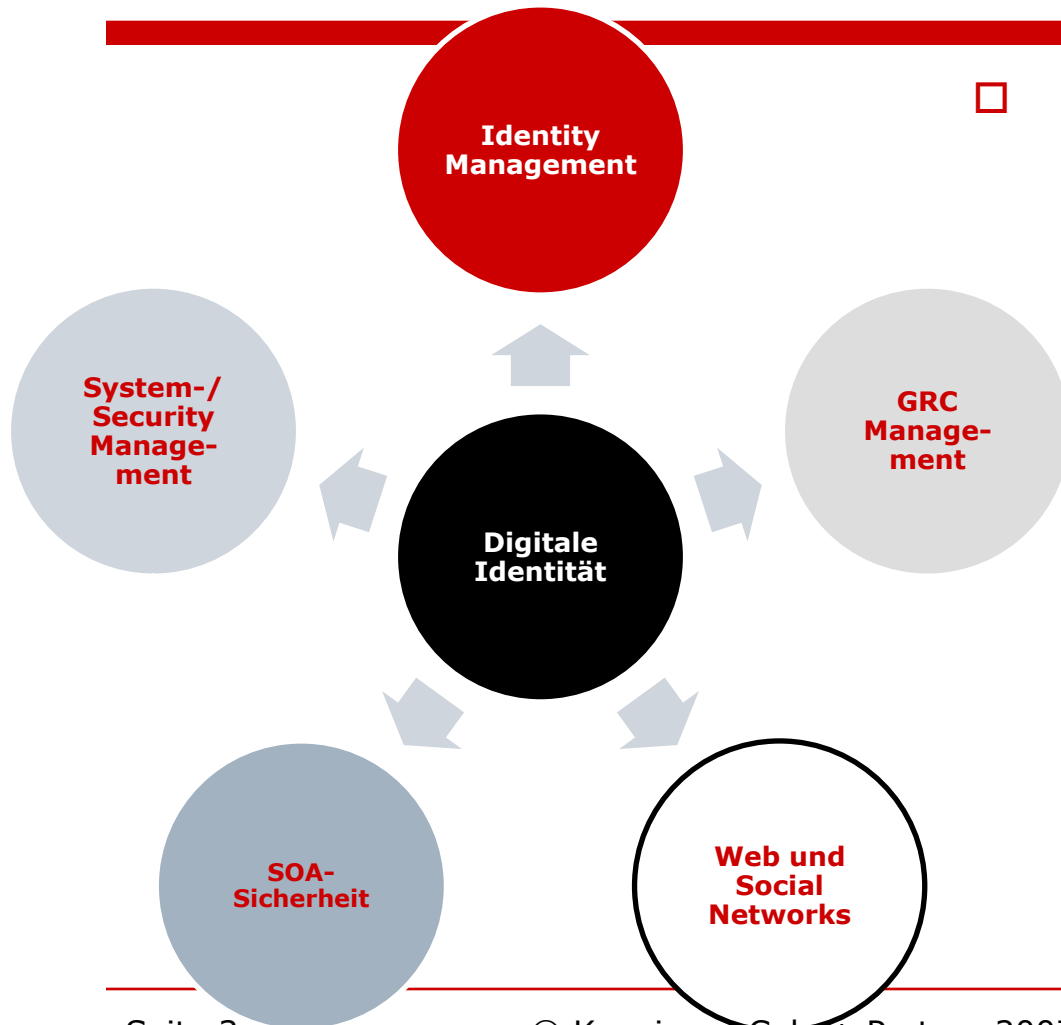
Agenda

Management von Identitäten

IAM, GRC – was ist das?

SOA – wo ist der Bezug?

Die Identität im Mittelpunkt



- Die digitale Identität und ihre Wirkungen
 - Identity & Access Management
 - Das Management digitaler Identitäten
 - Compliance, Governance, Risk Management:
 - Das Risiko der Nichtbeherrschung digitaler Identitäten
 - SOA, Anwendungssicherheit:
 - Digitale Identitäten richtig nutzen

Identity Management + IT-Sicherheit: Henne oder Ei?

**Keine Sicherheit
ohne Identitäten**

- WER darf was machen?
- WER hat was gemacht?
- WER hat es erlaubt?

**Identity
Management:**

Corporate Governance

IT Governance

Compliance-Support

Identitätsmanagement

Keine Compliance ohne Identity Management!

Die Grundfragen

Wer darf was machen?

- Klare Regelungen für das Handeln von Benutzern

Wer hat was wann gemacht?

- Klare Nachvollziehbarkeit des Handelns von Benutzern

Warum durfte **wer** was machen?

- Klare Nachvollziehbarkeit der administrativen Handlungen

Das WER, also die Identität, spielt eine zentrale Rolle

- Auditing ohne eine einheitliche Sicht auf die Identität funktioniert nicht
- Für den Zugriff auf archivierte Daten müssen Identitäten auch langfristig nachvollziehbar sein

Die Rolle des Identity Managements für Compliance

Identity Management ist eine unverzichtbare Basis für Compliance

- Basis für Authentifizierung und Autorisierung
- Basis für zentrale, anwendungsübergreifende Sicherheitskonzepte
- Basis für Auditing

Keine Compliance ohne Identity Management!

Keine SOA ohne Identity Management!

Die Rolle der SoDs

SoD: Segregation of Duties

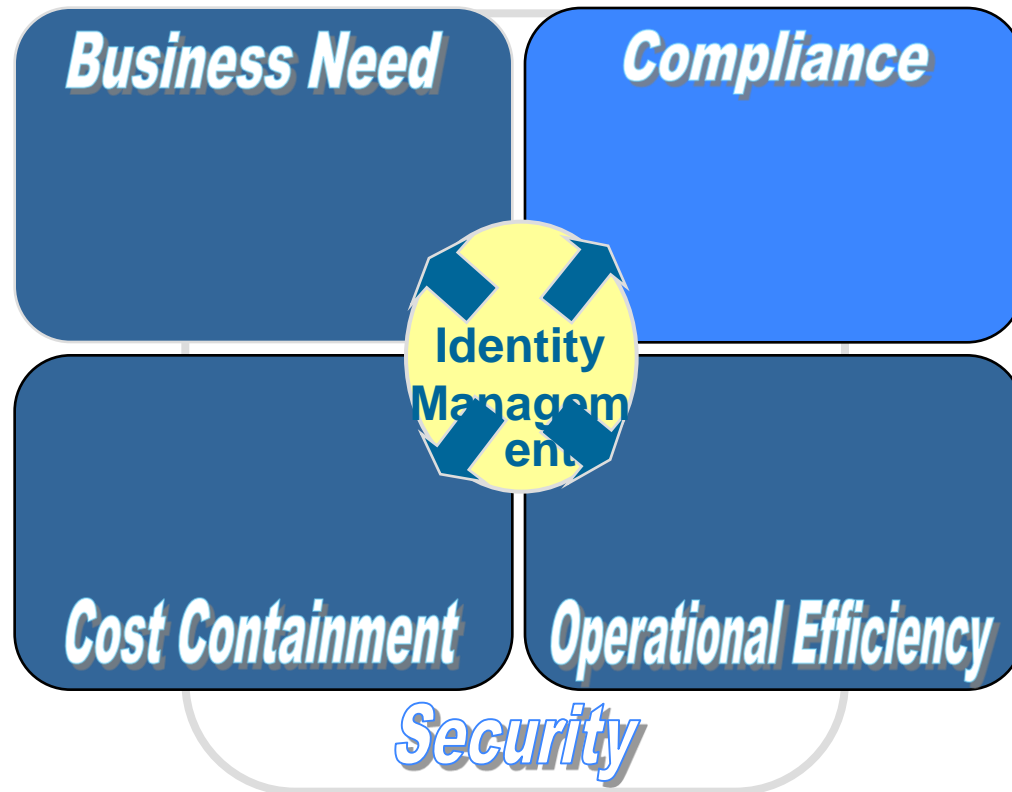
Definierte Konflikte

Müssen von Systemen unterstützt werden

- Vordefiniert
- Definierbar

Mit Optionen für zulässige Konflikte und deren explizite Überwachung

Compliance



Vermeidung von Kosten und anderen Nachteilen durch Nichteinhaltung der Compliance (Bußgelder, persönliche Strafen für Führungskräfte, Image,...)

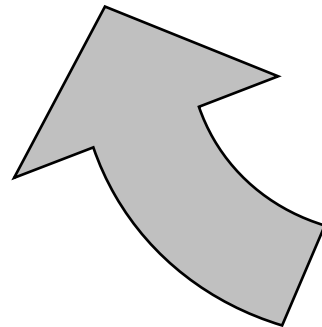
Die Voraussetzungen für Compliance

Auditing

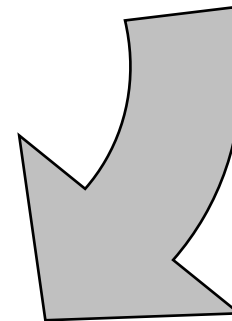
WANN

WER

Identitäts-
management



WAS



Archivierung

Compliance wird zum Kernthema

67% sehen die Trennung von Zuständigkeiten („Segregation-of-Duties“) als wichtigsten Aspekt*

57% beklagen, dass es für Compliance Management derzeit noch keine zentrale Struktur gibt*

87% bezeichnen IAM als kritischen Erfolgsfaktor für Compliance*

94 % der CIOs geben an, zunehmend für die Compliance-Umsetzung in ihren Abteilungen rechenschaftspflichtig zu sein**

69 % wollen auch andere Bereiche ihrer Compliance-Anforderungen an die IT herantragen**

Quellen: *Forrester Research, 03/2005, 152 US-Unternehmen

** Iluma Research, 04/2005, 100 Unternehmen D, GB, F, NL

Beteiligte

CEO
CFO

- Compliance/Governance
- Extended Enterprise
- Kostentransparenz

IT-Admin

- „Benutzer“freundlichkeit
- Sicherheit

CIO

- Compliance/Governance
- Kostentransparenz
- Sicherheit

Anwender

- Benutzerfreundlichkeit

Sales
Marketing

- Extended Enterprise
- Total Customer Experience

Kunde

- Total Customer Experience

Betriebsrat

- Einsichtnahme in Prozesse
- Übereinstimmung mit betrieblichen Regelungen

Revision
Prüfer

- Compliance/Governance

Herausforderung GRC

Sehr viele verschiedene Vorschriften, ständig weitere Vorschriften

Viele Regelungen sind vergleichsweise unscharf

- Risikomanagement im § 91 Abs. 2 AG und § 43 Abs. 1 und 2 GmbHG:
...Etablierung eines angemessenen Risikomanagements und internen Überwachungssystems...

Viele der Regelungen sind in hohem Maße strafbewehrt:

- SOX (SarbanesOxleyAct) Bis zu 25 Jahre Freiheitsstrafe
- 72 % der CIOs befürchten nicht, persönlich zur Verantwortung gezogen zu werden (Iluma Research) – eine Fehleinschätzung:
 - Persönliche Haftung
 - Potenzielle Freiheitsstrafen

Was wird gefordert?

Transparenz über Unternehmensrisiken/Risiko-Management

Dokumentationserfordernisse, auch für eMail

Sicherheit des Unternehmens und der IT-Systeme und –Prozesse

- Verstärkte Systemprüfungen

Definierte Delegation von Verantwortlichkeiten auf allen Ebenen

Nachvollziehbarkeit/Revisionsfähigkeit

- Aufbereitung der Daten

Und wo ist die SOA?

Es geht um Identitäten! Früher Menschen, jetzt Services!

Services können sehr leistungsfähig sein – und mächtig!

Macht bedarf entsprechender Kontrolle

IAM ist ein Werkzeug für die Umsetzung der Kontrolle!

GRC bildet den Rahmen der Kontrollobjekte

Alle anderen Herausforderungen (Nachvollziehbare Archivierung, Revisionsfähigkeit, DRM,...) sind ohne IDM nicht lösbar!

Die Ebene der Services

Neuerungen:

- Definition einer Schicht von Identity Services

Bewertung:

- Form der SAP NetWeaver Identity Services noch unklar
- Virtual Directory Services als wichtiges Element

SOA Sicherheit

Ähnlichkeit:

- Früher griff ein Mensch auf einen Dienst zu
- Jetzt greift ein Dienst auf einen anderen Dienst zu

Problem:

- Eindeutige Identifikation
- Eindeutige Authentisierung
- Zurechenbarkeit
- Verkettung + Verschleierung

Backup

Compliance – der Begriff

- (Corporate) Compliance
 - Wörtlich: „Befolgung, Entsprechung“
 - Wortsinn: „In Übereinstimmung mit geltenden Vorgaben handeln“
 - BaFin: „Einhaltung von gesetzlichen, aufsichtsbehördlichen und internen Vorschriften, Regelungen, Richtlinien, u.ä.“
- Compliance umfasst also generell die Einhaltung von Regelungen für Unternehmen im weitesten Sinne
- Ein breit gefasster Begriff!
 - Was genau ist gemeint?
 - Warum gewinnt Compliance so an Bedeutung?
 - Was hat die IT damit zu tun?

Compliance-Vorschriften

Ein Ausschnitt...

International

- Sarbanes-Oxley Act
- Consumer Privacy Protection Act
- Börsenregelungen (SEC 17a-3, 17a-4)
- „Winter-Report“ (Report of the High Level Group of Company Law Experts on an Modern Regulatory Framework for Company Law in Europe)

National

- KonTraG
- BDSG
- HGB, GoBS
- BVerfG
- SigG (Signaturgesetz)
- Corporate Governance Kodex

Branchenspezifisch

- HIPAA (Gesundheitswesen)
- FDA 21 CFR (Pharma)
- Basel II (Kreditwesen)
- Gramm-Leach-Bliley Act (Kreditwesen)
- MaH/MaK (Kreditwesen)

Funktionspezifisch

- US Patriot Act (eMail-Verkehr)
- EU-Richtlinie über den elektronischen Geschäftsverkehr (eCommerce-Richtlinie)
- European Privacy Act (Kundendaten)

Beispiel KonTraG – wenig konkret

- ❑ Nachweis von Maßnahmen zur Risikofrüherkennung und -abwehr
- ❑ Nachweis von objektiv und subjektiv pflichtgemäßem Handeln
- ❑ Setzt Auditing voraus – der Nachweis kann nur erbracht werden, wenn man aufgezeichnet hat, was man getan hat
- ❑ Setzt (auch) sichere IT-Systeme voraus

Beispiel HIPAA – sehr konkret

- Anforderungen durch HIPAA:
 - Physikalischer Schutz aller Netzwerkkomponenten und IT-Anwendungen, unter anderem durch lückenlose Zugriffskontrolle
 - Authentifizierung aller Nutzer über persistente Identitätsverzeichnisse
 - Autorisierung des Zugriffs auf Ressourcen
 - Wirksame Verschlüsselung und nachweisbarer Schutz vor Datenmanipulation
 - Überwachung und Reporting
 - Verbindliche Regeln für die Administration