

Schutz kritischer Daten im SAP-Umfeld

Access Management &
Compliance - Schrecken ohne
Ende?

IT-SA, Nürnberg
7. Oktober 2015

Agenda

Ein Startpunkt

Regulatorische Anforderungen

Themen & Lösungen

Access Compliance Maßnahmen

Ein Startpunkt

Präzisierung des Themengebietes

Identity, Access & Governance Management (kurz IAGM)

beschreibt Gesamtlösungen, die Anwender mit allem versorgen, was sie im Rahmen Ihrer Aufgaben für ein Unternehmen an Zugängen zu IT-Ressourcen benötigen. Und das auch noch schnell, effizient, nachhaltig und regelkonform.

Identity steht für die Anwender, die über Ihre Benutzerkonten mit Rechten versorgt werden sollen. ***Access*** bezeichnet Rollen und Berechtigungen, die den Anwendern Zugang zu den IT-Ressourcen verschaffen. ***Governance*** beschreibt die Organisation und Prozesse sowie die Anforderungen, die hierbei aus internen oder externen Gründen eingehalten werden müssen.

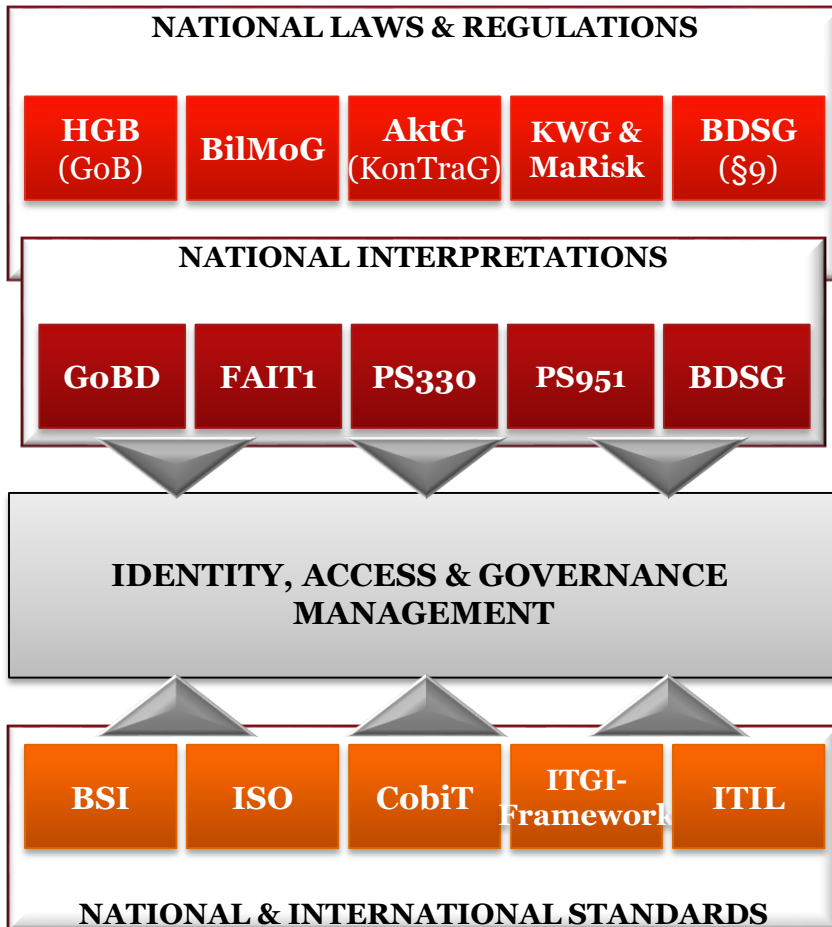
Ein Startpunkt

Aktuelle Herausforderungen

- Verschmelzung von funktionsgleichen Systemen (z.B. ERP-Transformationsprojekte) **ohne** angemessene **Berechtigungs-Harmonisierung**
- Zeitgleich **Zunahme von Anwendungen** und insbesondere Kleinst-/EUA- & Workflow-Lösungen mit uneinheitlichen Berechtigungen
- **Fehlende Komplexitätsreduktion** auch bei Anwendungen innerhalb des SAP-Kosmos (ECC, BW, SCM, BO, S/4)
- Zunehmende **Verknappung** erfahrener Access Management **Experten** bei gleichzeitiger Verlagerung in SSC oder Outsourcing
- **Ansteigende regulatorische Anforderungen** insb. in spez. Branchen (Banken / Versicherungen, Pharma und Energieversorger)
- **Uneinheitliche IAGM und GRC-Lösungen** oft von unterschiedlichen Unternehmensbereichen ausgewählt und betrieben

Regulatorische Anforderungen

Überblick



- IAGM sollte Bestandteil eines dokumentierten **Informationssicherheits-Managements-Systems** sein, das wiederum in die IT-Governance & Compliance eingebunden ist.
- IAGM ist darüber hinaus ein essentieller Bestandteil des **Steuerungs- und Überwachungssystems** eines Unternehmens.
- Insofern unterliegt IAGM einer Reihe komplexer gesetzlicher und freiwilliger **Regelungen und Standards**.

Regulatorische Anforderungen

Komprimierte Version

Minimalprinzip

.. jeder Mitarbeiter verfügt nur über die Rechte, die er für seine Tätigkeit benötigt

Vgl. MaRisk (BA) AT 7.2, Tz. 2

Funktionstrennungsprinzip

... miteinander unvereinbare Tätigkeiten werden durch unterschiedliche Mitarbeiter durchgeführt ..

Vgl. MaRisk (BA) AT 4.3.1, Tz. 1

Themen & Lösungen

Im Überblick

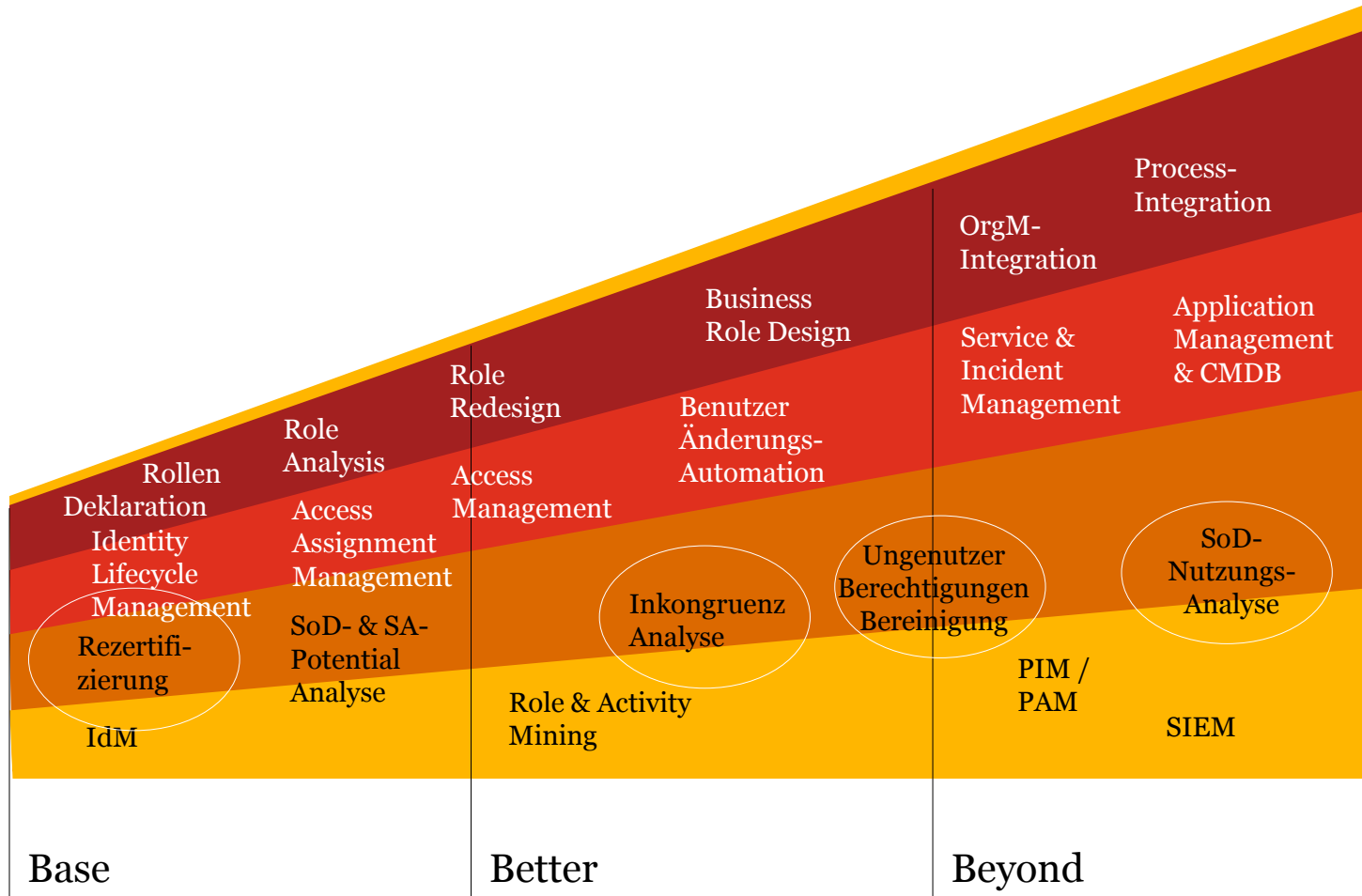
Access

Modelling

Governance

Compliance

Automation



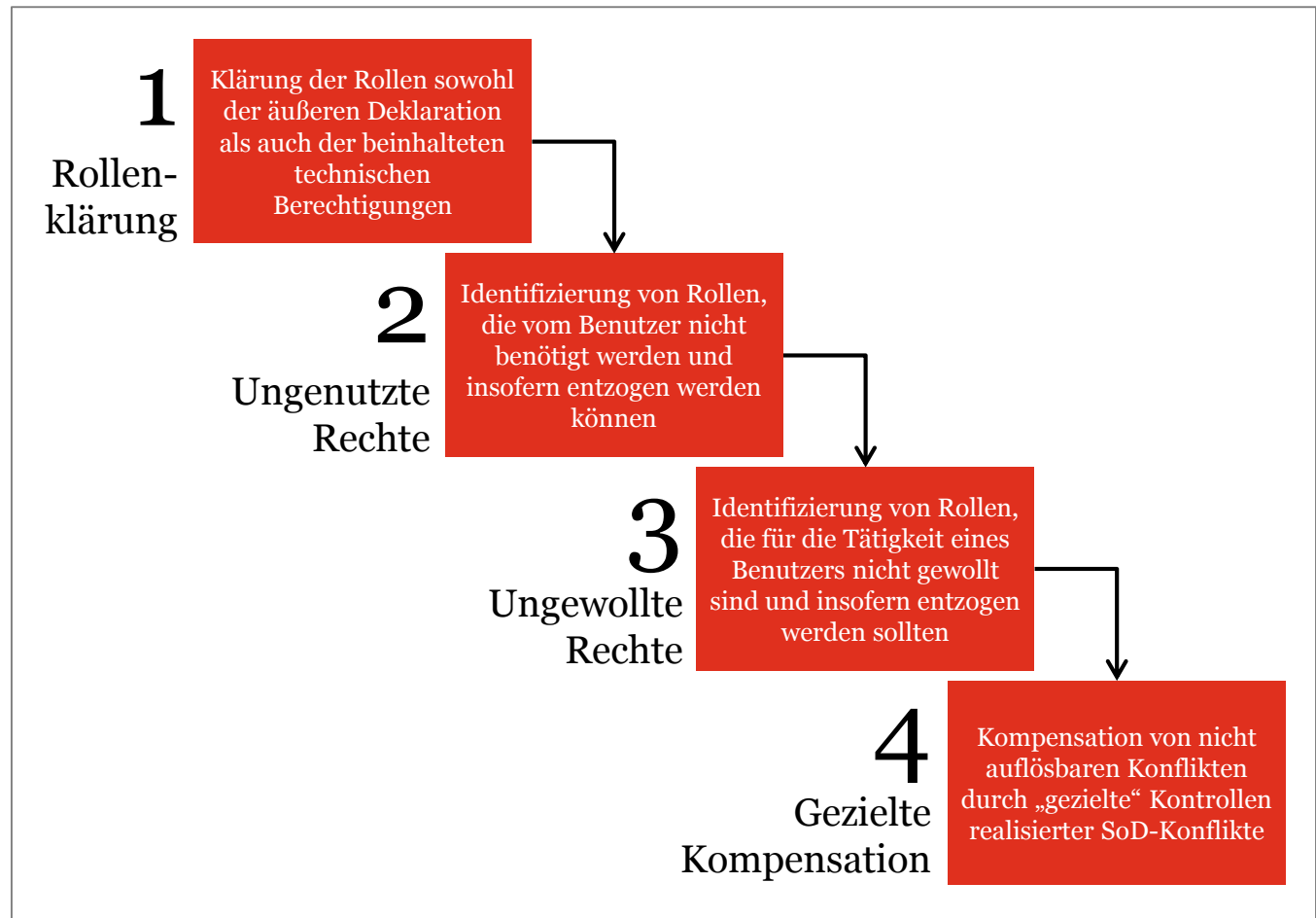
Themen & Lösungen

Am Beispiel von Maßnahmen der SoD-Klärung

Das Spektrum der Maßnahmen zur Gestaltung des Benutzer- und Berechtigungsmanagements ist vielfältig.

Wir wählen hieraus den Ausschnitt des **Access Compliance Managements**.

Und hier wiederum ausgesuchte Maßnahmen zur **Klärung von SoD-Konflikten**, die dazu beitragen können, dem IAGM-Thema den „Schrecken“ zu nehmen.



Access Compliance Maßnahmen (Base)

Rollenklärung (Deklaration & Strukturgebung)

Benutzer

(=natürliche Person)



- Benutzer-ID
- Vorname
- Nachname
- Abteilung
- OrgEinheit
- Kostenstelle
- Standort

Businessrolle

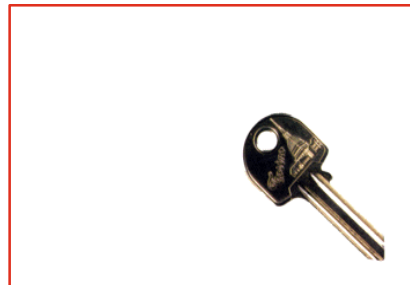
(= Tätigkeit)



- BR-Name
- BR-Text
- BR-Beschreibung
- OrgEinheit & Teileinheit
- Differenzierungstyp & -wert
- Risikotyp & -klasse

Applikationsrecht

(= Prozessschritt)



- AR-Name
- AR-Text
- AR-Beschreibung
- Applikation & -typ
- Prozess/Teilprozess
- Differenzierungstyp & -wert
- Risikotyp & -klasse

Access Compliance Maßnahmen (Better)

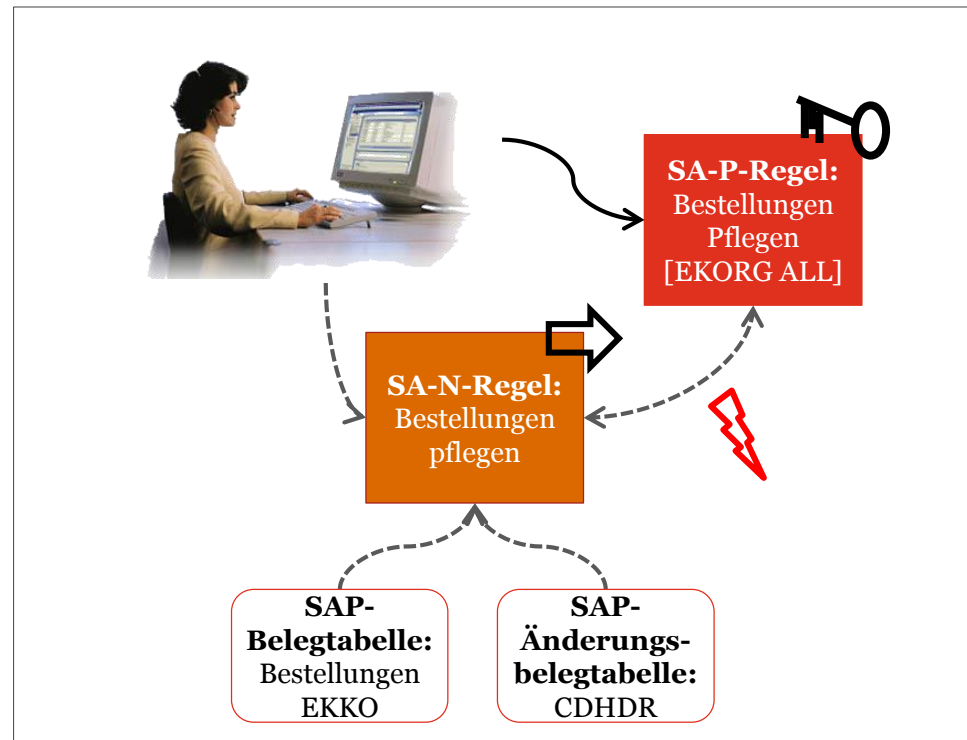
Bereinigung ungenutzter Berechtigungen

Viele Benutzer verfügen über Berechtigungen mit Zugriff auf Funktionen, die sie für die Ausführung ihrer übertragenen Verantwortung überhaupt **nicht benötigen**. Wir nennen dies „ungenutzte Berechtigungen“ oder „**Berechtigungs-Überhänge**“.

Die Ursachen sind u.a. zu weitreichende initiale Berechtigungsvergaben, fehlende Anpassungen an Wechsel der Tätigkeiten oder das Fehlen angemessener Rollen.

Mit Auswertungen der Nutzungsanalyse kann die reale Nutzung von Funktionen über SAP-Beleg- & -Änderungsbelegtabellen ausgewertet werden. So können in Kombination mit der Berechtigungsanalyse von Funktionen **Lösch-Vorschlagslisten** erstellen.

Dies gewährleistet, dass mit dem Entzug der Funktionen grundsätzlich **keine Einschränkung** der Mitarbeiter in ihren ausgeübten Funktionen entsteht.



Access Compliance Maßnahmen (Better)

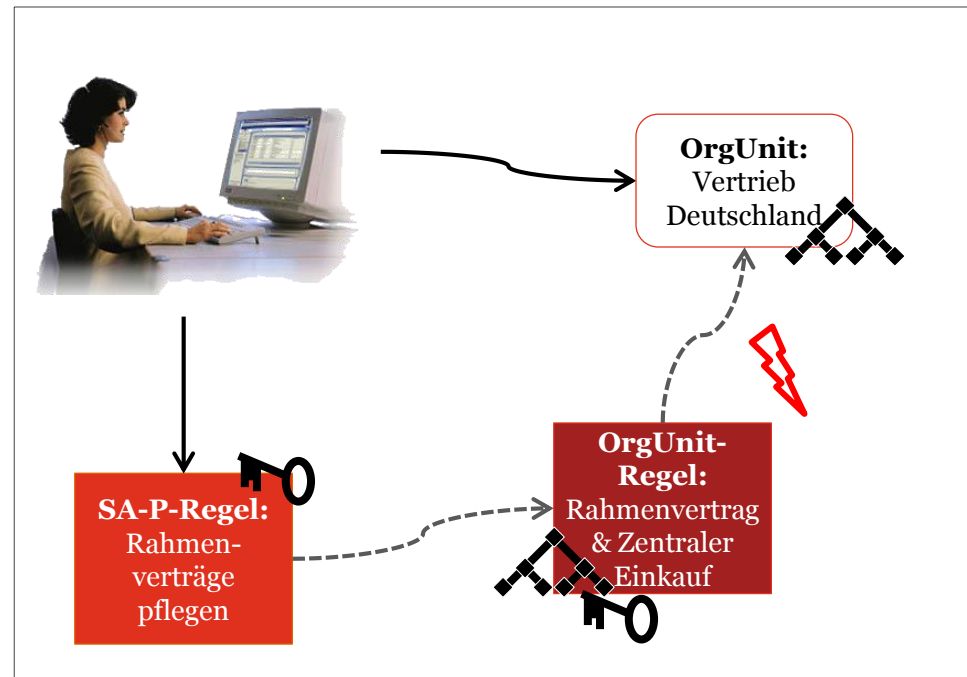
Bereinigung ungewollter Berechtigungen

Die Zuordnung der Benutzer im GRC AC zur Organisationshierarchie und damit zu einem **OrgUnit-Knoten** (einer Planstelle in SAP HCM) ermöglicht grundsätzlich eine **organisatorische Einordnung**.

Hierzu sollte die Organisationshierarchie/Planstellen nicht nur primär für die Gehaltseinstufung verwendet werden, sondern eine prozessuale und organisatorische Einordnung ermöglicht, aus der eine Verknüpfung mit den Aufgaben eines Mitarbeiters möglich sind.

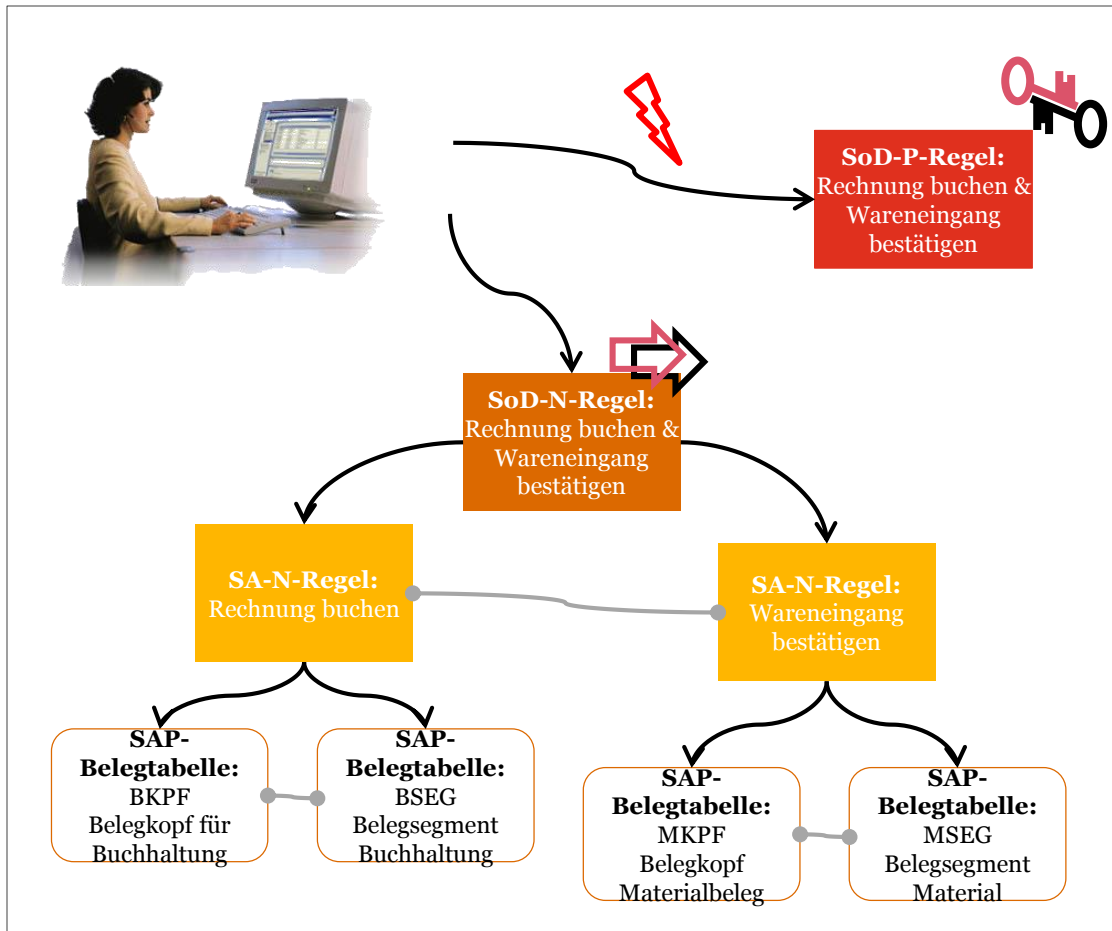
Wenn dies vorliegt, kann eine **Verknüpfung** zwischen sensiblen Funktionen und OrgUnits hergestellt werden.

Dadurch können signifikante Abweichungen zwischen Erwartungshaltung und tatsächlicher Zuordnung von Berechtigungen ermittelt werden. Selbst wenn ein Benutzer eine Funktion unberechtigter Weise genutzt hat.



Access Compliance Maßnahmen (Beyond)

Kompensierende Kontrollen & SoD-Realisierung



Sind bei kleineren Einheiten SoD-Konflikte unvermeidbar, schlägt die Stunde der kompensierenden Kontrollen.

Hierbei kristallisiert sich in der Praxis zunehmend die fehlende Eignung „normaler“ Kontrollen des Internen Kontrollsystems zur Deckung der Risiken aus SoD-Konflikten heraus.

Lösung hierfür kann die Identifizierung konkreter, vollzogener SoD-Konflikte von Benutzern und deren Kontrolle nach dem 4-Augen-Prinzip sein.

Ihre Ansprechpartner

Johannes Liffers

Kapelle-Ufer 4
10117 Berlin
Tel.: +49 30 2636-1658
email: johannes.liffers
@de.pwc.com



Björn Schmidt

PricewaterhouseCoopers AG
Bernhard-Wicki-Str. 8
80636 München
Phone: +49 89 5790-6058
bjoern.schmidt@de.pwc.com

