www.pwc.de

Professionelles SoD-Resolution Management

Beispiele aus der Praxis
DSAG AK GRC
6. November 2015

pwc

Agenda

A	Ein Startpunkt
B	Regulatorische Anforderungen
C	SoD-Resolution / Klärung
1	Rollenklärung
2	Ungenutzte Rechte
3	Ungewollte Rechte
4	Gezielte Kompensation
F	SoD-Fazit

A-C

Startpunkt bis SoD-Resolution

A) Ein Startpunkt
Präzisierung des Themengebietes

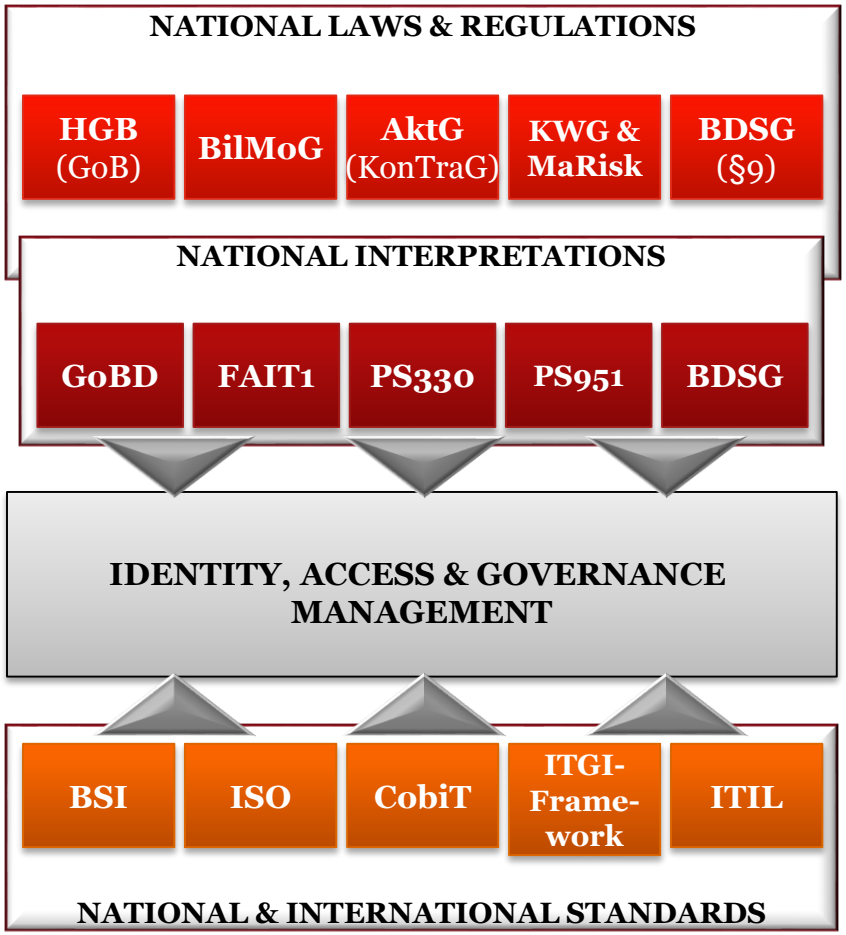
Identity, Access & Governance Management (kurz IAGM) beschreibt Gesamtlösungen, die Anwender mit allem versorgen, was sie im Rahmen ihrer Aufgaben für ein Unternehmen an Zugängen zu IT-Ressourcen benötigen. Und das auch noch schnell, effizient, nachhaltig und regelkonform.

Identity steht für die Anwender, die über 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.

A) Ein Startpunkt
Aktuelle Herausforderungen

- Verschmelzung von funktionsgleichen Systemen (z.B. ERP-Transformation-Projekte) **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, Native HANA, 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

B) Regulatorische Anforderungen
Überblick



- IAGM sollte Bestandteil eines dokumentierten **Informationssicherheits-Management-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**.

B) 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

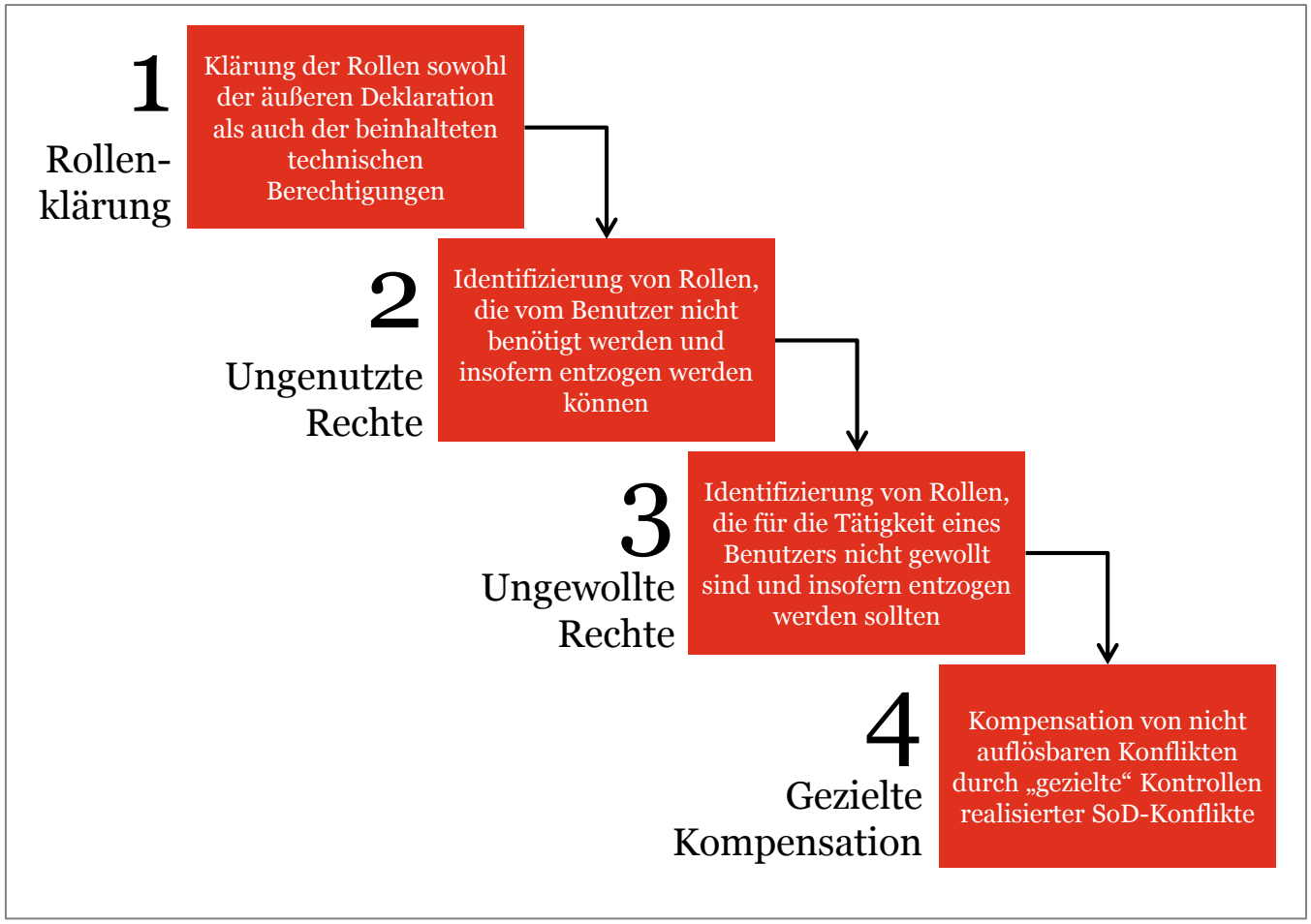
... miteinander unvereinbare Tätigkeiten werden durch unterschiedliche Mitarbeiter durchgeführt ..

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

C) SoD-Resolution
Am Beispiel ausgewählter Maßnahmen

Das Spektrum der Maßnahmen zur Gestaltung des Benutzer- und Berechtigungs-managements 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.



1-4

Einzelne SoD-Klärungs-Maßnahmen

1) 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

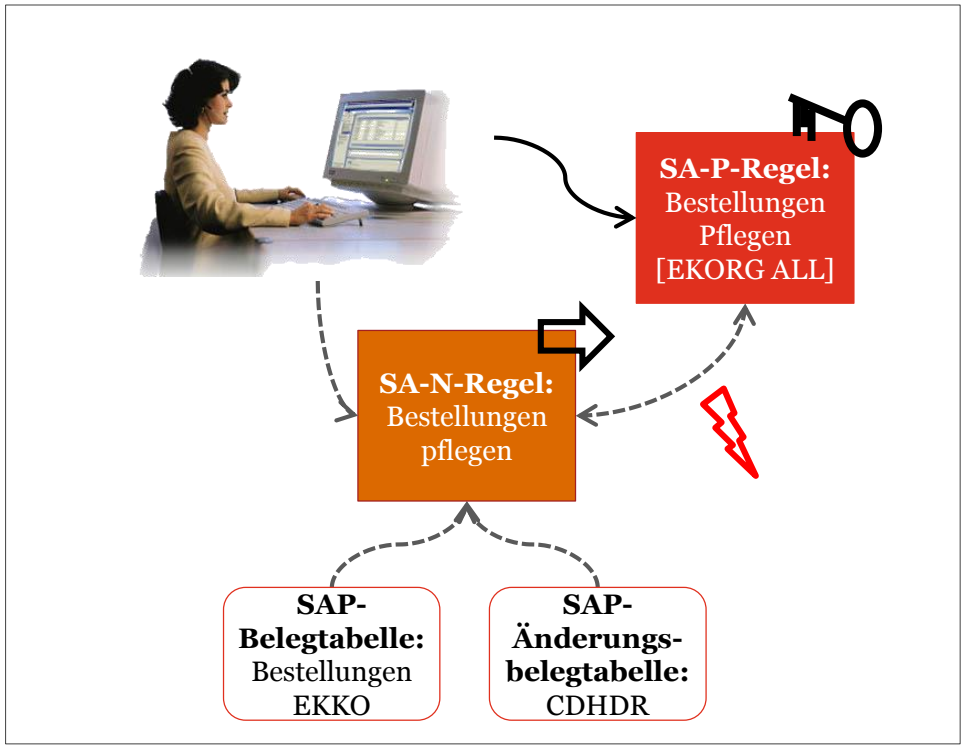
2) Ungenutzte Berechtigungen
Am Beispiel

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- & -Änderungsbeleg-tabellen ausgewertet werden. So können in Kombination mit der Berechtigungs-analyse von Funktionen **Lösch-Vorschlagslisten** erstellt werden.

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



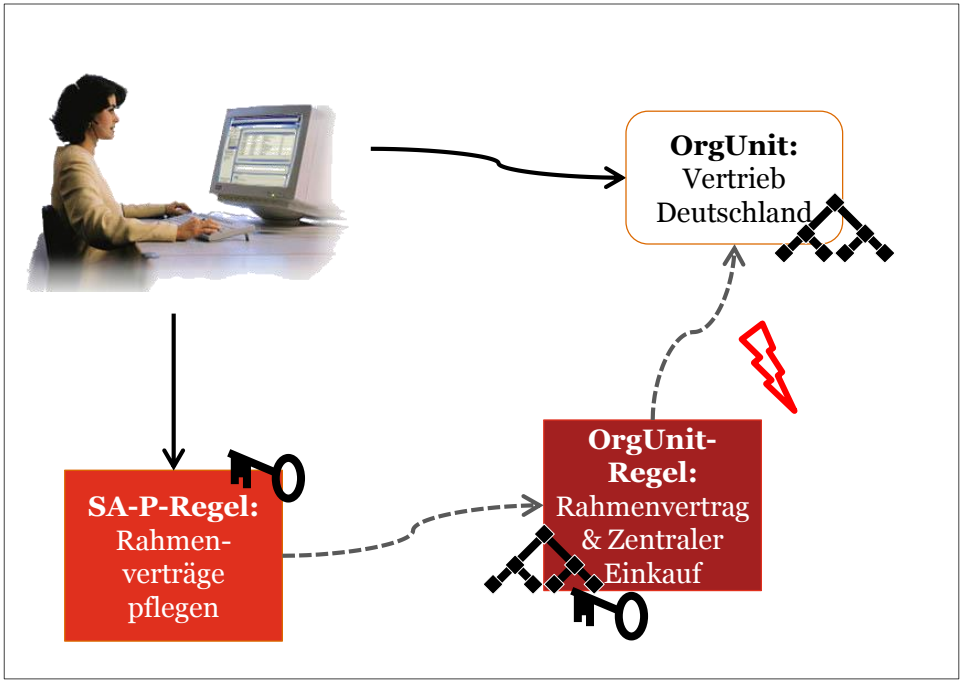
3) Ungewollte Berechtigungen
Am Beispiel

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**.

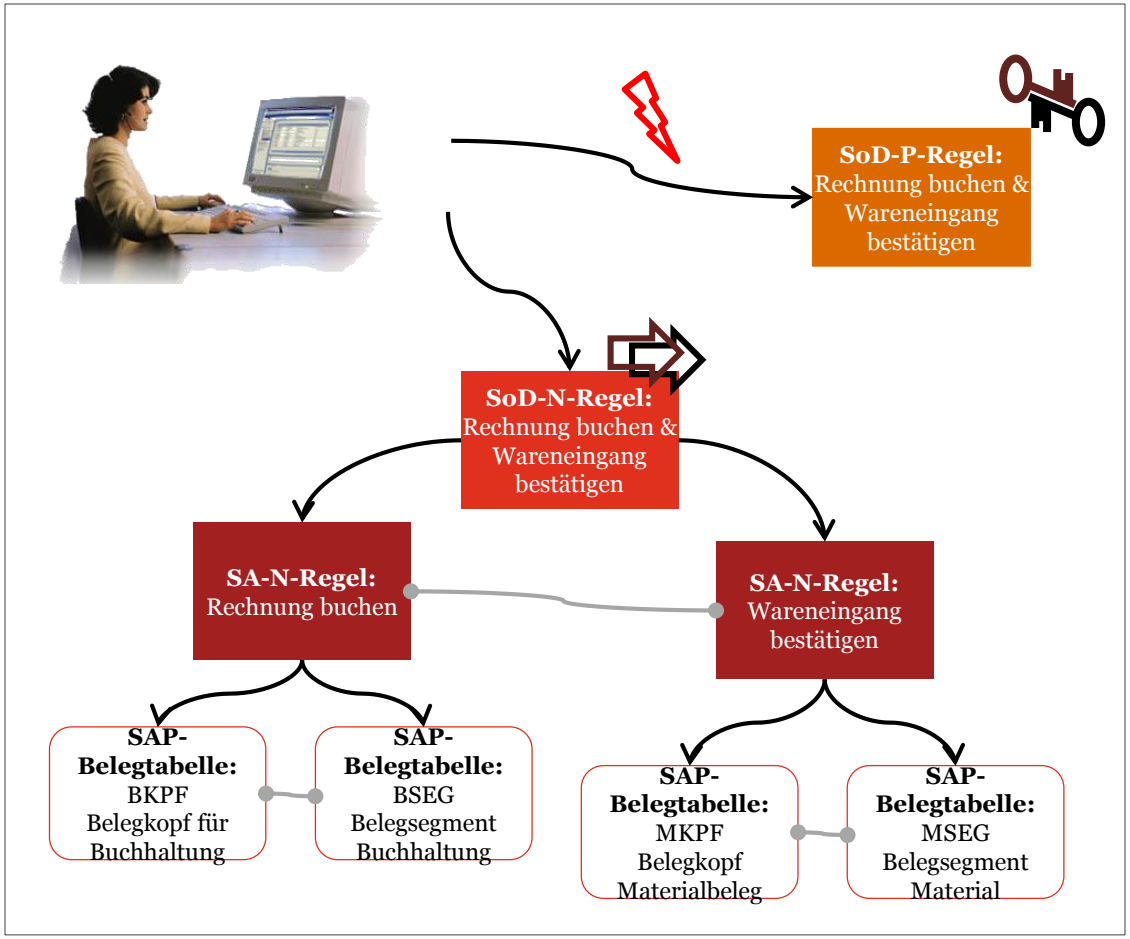
Hierzu sollte/n die Organisations-hierarchie/Planstellen nicht nur primär für die Gehaltseinstufung verwendet werden, sondern eine prozessuale und organisatorische Einordnung ermöglicht, aus der eine Verknüpfung mit den Aufgaben eines Mitarbeiters möglich ist.

Wenn dies vorliegt, kann eine **Verknüpfung** zwischen sensitiven 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.



4) Gezielte Kompensation
Am Beispiel



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.

F

SoD-Fazit

A) SoD-Fazit

- Neben der klassischen SoD-Potenzial-Analyse bieten SAP- und auch Non-SAP-Systeme eine Vielzahl von Nutzungs-Informationen, um die Klärung von Funktionstrennungskonflikten (Segregation of Duties - SoD) erheblich **vereinfachen** zu können.
- Voraussetzung ist ein **transparentes Rollenkonzept**, mindestens mit sensitiven Funktionen (Sensitive Access – SA) in eigenständigen Einzelrollen, ein sinnvolles und **verständliches Regelwerk** (SoD und SA) als Bestandteil einer Lösung zur **SoD- und SA-Potenzialanalyse** (z. B. SAP GRC AC ARA).
- Ebenfalls ist eine Lösung zur **Nutzungsanalyse** von Sensitiven Funktionen und Funktionstrennungen auf Belegebene und ein auf das Potenzial-Analyse-Regelwerk abgestimmter **Content für die Nutzungsanalyse** erforderlich. Diese Lösung sollte sinnvoll in die bestehende IAM-/GRC-Landschaft integriert sein.
- So kann die Analyse unter Nutzung von Standardanwendungen wie Fraud Management, SAP GRC AC (& AVM), GRC PC oder anderen Marktlösungen z. B. für Identity, Access und Governance Management oder Data Warehousing erfolgen.
- Die Beleganalysemaßnahmen sollten hierbei nahtlos in die übrigen **SoD-Klärungsmaßnahmen** sowie insgesamt in das **interne Kontrollsystem** für Access Controls und weiter für Process Controls eingebunden sein.

Ihre Ansprechpartner

Johannes Liffers

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

Timm Schwarz

Moskauer Str. 19
40227 Düsseldorf
Tel.: +49 211 981 - 2956
email: timm.schwarz
@de.pwc.com