

*Enabling & Accelerating  
Identity, Access & Governance Management*

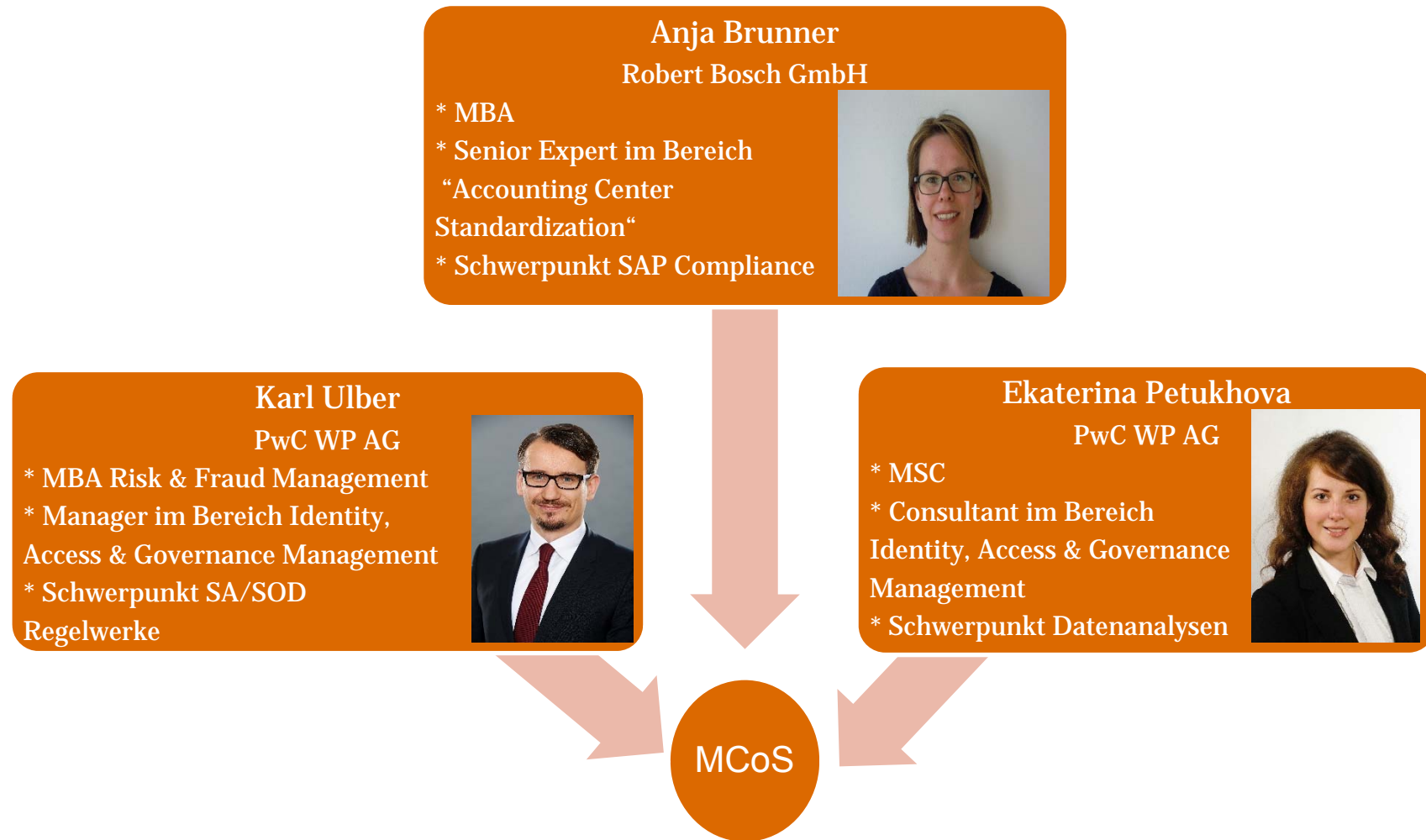
# **Belegbasierte SAP-Nutzungsanalyse**

*Von „hätte tun können“  
Zu „hat getan“*

DSAG Jahreskongress 2016



# Vorstellung der Referenten



---

# ***Einführung***

Die im Folgenden vorgestellte ***belegbasierte SAP Nutzungsanalyse*** folgt aus konkreten Problemen der Wirtschaft\* sowie aus rechtlichen Anforderungen\*\*.

Ausgehend von der konkreten Herausforderung bei unseren Mandanten, nicht nur zu prüfen wer über sensitive Funktionen verfügt, sondern ebenso zu prüfen, ob diese sensitiven Funktionen ***tatsächlich genutzt*** wurden, ist die Idee entstanden, dieser Anforderung unter Verwendung der in SAP vorhandenen ***Log- und Protokolldateien*** nachzukommen.

Ausgehend von einer Darstellung der ***Bedarfsauslöser*** werden wir die ***fachliche Lösung*** deren ***technische Umsetzung*** sowie den ***Projektablauf*** am Beispiel eines Projektes bei der Robert Bosch GmbH erläutern.

\* ca. 57% der Unternehmen sind von Wirtschaftskriminalität (z.B. Diebstahl vertraulicher Daten, Manipulation von Konto- und Finanzdaten) betroffen

\*\* Forderung des Minimalprinzips bei der Berechtigungsvergabe im Rahmen des IKS gemäß GoBD u.w.

# Über Bosch und den bisherigen Status Quo

**4 Unternehmensbereiche:**  
Mobility Solutions, Industrial  
Technology, Consumer Goods,  
Energy and Building Technology

**Umsatz von 70,6 Milliarden  
Euro** im Geschäftsjahr 2015

Robert Bosch Gruppe besteht aus  
rund **440 Tochter- sowie  
Regionalgesellschaften** in rund  
**60 Ländern**

Weltweit rund **375 000  
Mitarbeiter** (Stand: 31.12.2015)

**IKS** umfasst verschiedene  
**Berechtigungskontrollen** (z.B.  
Potenzialanalyse sowie  
Nutzungsanalysen)

**IKS Kontrollen** werden tool-  
gestützt geprüft (Nutzungsanalyse  
mit **MCoS**). MCoS bisher nicht  
umfassend aufgrund Logik und  
Performance Probleme im Einsatz



# 1

---

## *Warum Nutzungsanalyse?*

# Warum Nutzungsanalyse?

## Bedarfsauslöser



# Warum Nutzungsanalyse?

## Nutzen



**Entfernung  
überflüssiger  
Rollen-  
zuordnungen**

Identifizierung von Rollen,  
die nicht dem Tätigkeitsprofil  
des Mitarbeiters entsprechen.



**Gezielte  
Kompensation  
von SoD-Konflikten**

Identifizierung von Belegen,  
welche unter Anwendung von  
Funktionstrennungs-  
konflikten erzeugt wurden.



**Identifikation  
von Prozess-  
abweichungen**

Erstellung einer klaren  
Prozesslandschaft, welche  
Funktion für welche  
Gesellschaft pro System in  
einem bestimmten Zeitraum  
ausgeführt wurde.



**Optimierung und  
Flexibilisierung  
des Funktions-  
trennungs-  
Regelwerks**

Review & Benchmarking des  
Risiko-Katalogs gegen Best-  
Practice Regelwerken  
vergleichbarer Unternehmen.  
Flexible Anpassung der  
systemseitigen Abfragen.



# 2

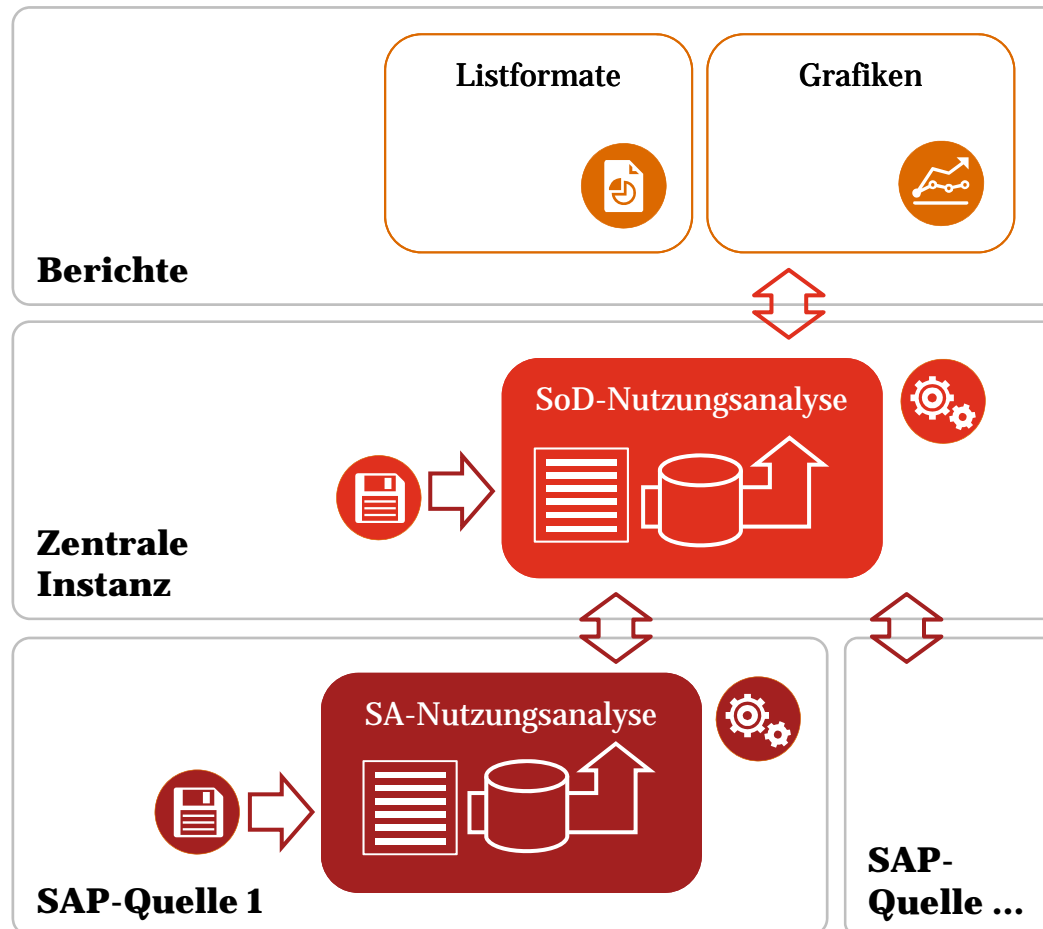
---

## *Wie funktioniert die Nutzungsanalyse?*



# Wie funktioniert die Nutzungsanalyse?

## Technische Umsetzung



Unsere beiden Programme zur Unterstützung der **Nutzungsanalyse** für **Einzelfunktionen (SA)** und **Funktionstrennungen (SoD)** werden jeweils auf den Zielsystemen und ggf. auf einem Zentralsystem eingespielt.

Die **Algorithmen** zur Analyse der SoD- und SA-Regeln können per **Flatfiles** eingespielt oder direkt in den Programmen erfasst werden.

Nun werden die Daten **in** den Zielsystemen auf Benutzer mit **Einzelfunktionen ausgewertet** und die Ergebnisse in der Zentralen Instanz zu Informationen für **Benutzer mit Funktionstrennungsverletzungen** kombiniert.

Die Datenergebnisse beider Analysen können dann mit **Reporting-Tools** oder klassischen Anzeigefunktionen in SAP zur Verfügung gestellt werden.



# 3

***Wie lief das Projekt ab?***

# Wie lief das Projekt ab?

## Projektschritte



- Review des bestehenden **Risiko-Kataloges**
- Konkretisierung der **Risikobeschreibung** (z.B. Bankdatenänderungen)
- Identifikation **Log- & Protokollierungstabellen**
- Definition **Filtertypen** zur Ergebnisabgrenzung
- Umsetzung **Abfragelogik** in Tool (ABAP)
- Prüfung auf abweichende **Filterwerte**
- Lokalisierung **systemspezifischer Filterwerte**
- **Datenauswertung** mit Filtern (z.B. Zeitraum...)
- **Ergebnisverteilung** gemäß Zuständigkeit
- **Überwachung** der Analyse



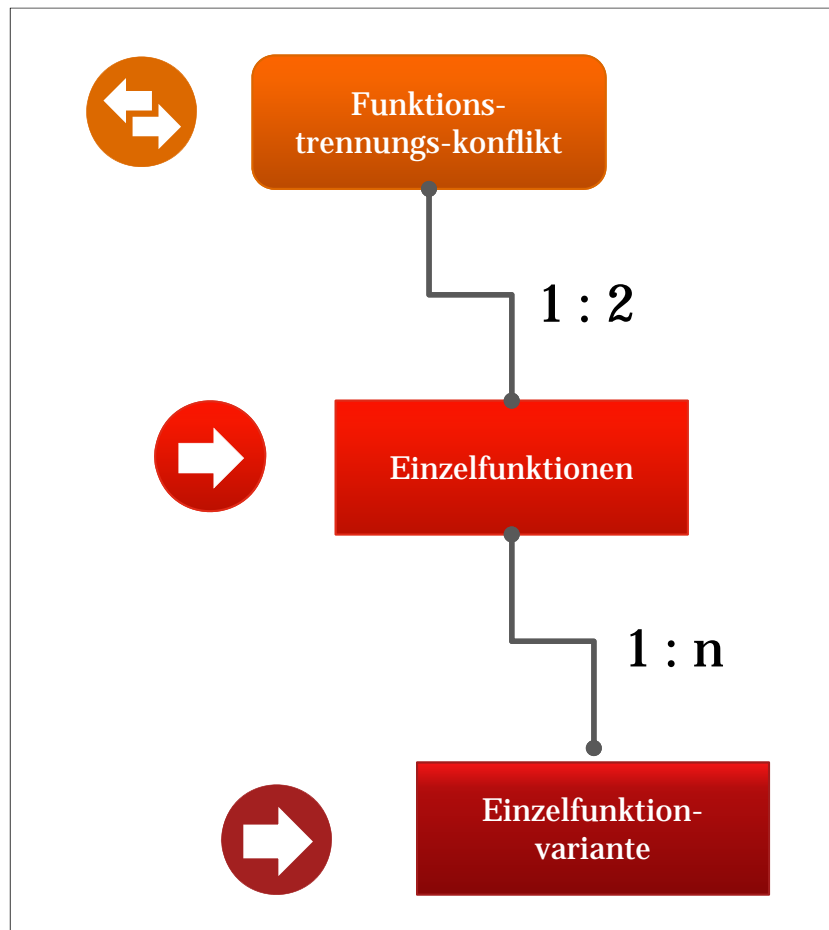
4

---

*Showcase*

# Showcase

## Ebenen der Auswertungen



Mit Hilfe der Nutzungsanalyse können sowohl sensitive **Einzelfunktionen** sowie **Funktions-trennungs-konflikte** in Bezug auf deren Nutzung analysiert werden.

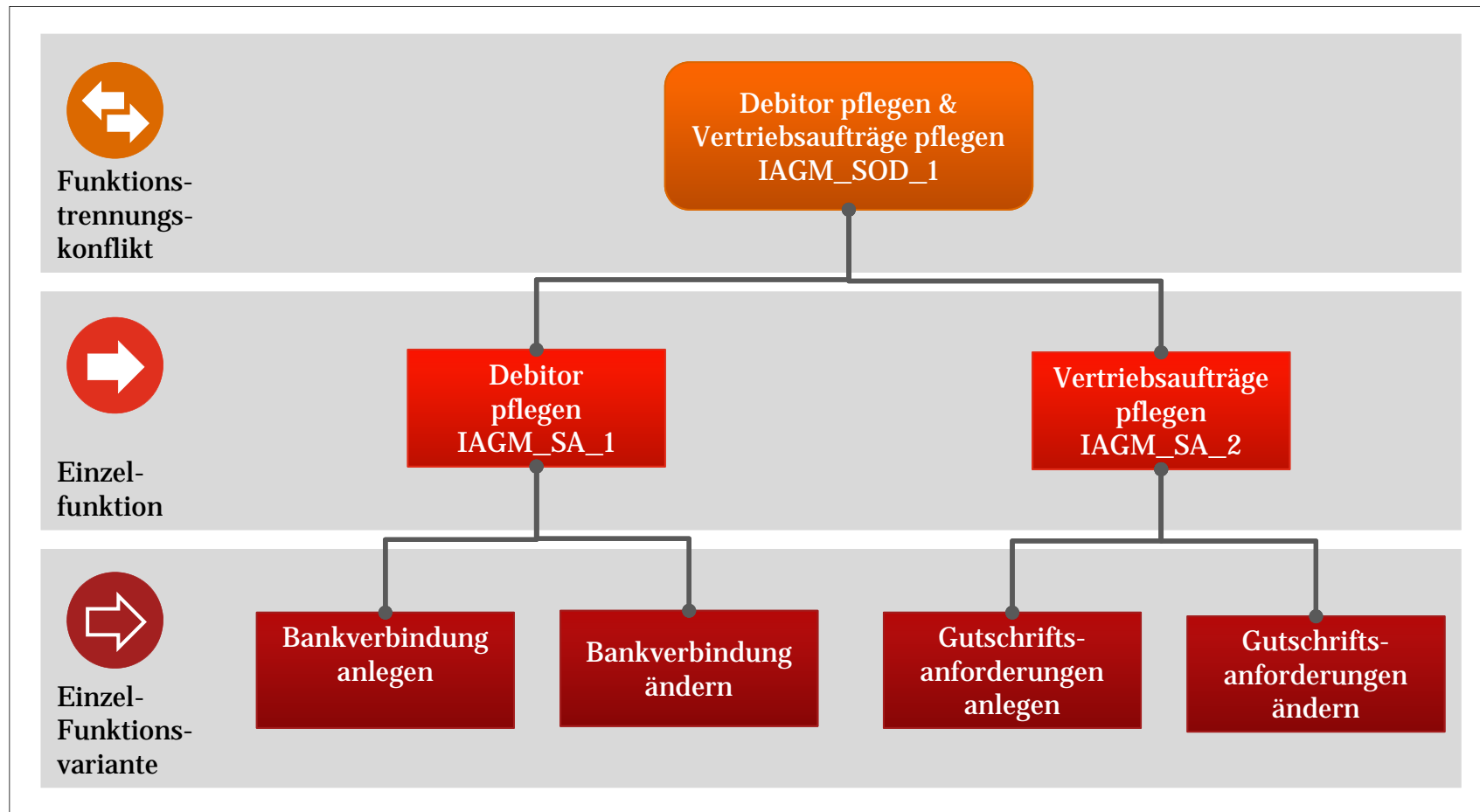
Ein Funktions-trennungs-konflikt setzt sich dabei aus zwei Einzelfunktionen zusammen.

In Abhängigkeit der zu analysierenden Einzelfunktionen ist es mitunter sinnvoll sogenannte **Varianten** für Einzelfunktionen zu definieren. Dies ist z.B. notwendig, wenn zwischen der **Anlage** und der **Änderung** eines betriebswirtschaftlichen Objektes in der Analyse unterschieden werden soll und sich die relevanten Informationen jeweils in unterschiedlichen Tabellen befinden (z.B. wird die Anlage eines Hauptbuchbeleges in der BKPF gespeichert während dessen Änderungen in der CDHDR erfasst wird).

Auf Ebene des **Ergebnis-Präsentation** kann dabei flexibel ausgewählt werden, ob die Ergebnisse pro Variante oder **konsolidiert** auf Einzelfunktionsebene angezeigt werden sollen.

# Showcase

## Funktionsstrennungskonflikt





# 5

---

## *Zusammenfassung*

# **Zusammenfassung**

## **Projektergebnisse**





# ***Nutzungsanalyse Ansprechpartner***

**Anja Brunner**  
**Robert Bosch GmbH**  
Siemensstraße 33A  
71254 Ditzingen  
Tel.: +49 711-8111-1724  
email: [anja.brunner@de.bosch.com](mailto:anja.brunner@de.bosch.com)

**Karl Ulber**  
**PwC**  
Käthe-Kollwitz-Str. 21  
04109 Leipzig  
Tel.: +49 341 9856 257  
email: [karl.ulber@de.pwc.com](mailto:karl.ulber@de.pwc.com)

**Ekaterina Petukhova**  
**PwC**  
Kapelle-Ufer 4  
19117 Berlin  
Tel.: +49 30 2636 1301  
email: [ekaterina.petukhova@de.pwc.com](mailto:ekaterina.petukhova@de.pwc.com)