Machbarkeit globaler Business-Rollen Modelle

DSAG Arbeitsgruppe GRC
Potsdam, November 2013

pwc

Agenda

IAGM & Businessrollen

Das Rollenmodell

IAGM-Automation

Herausforderungen

Fragen & Antworten

IAGM & Business-rollen

IAGM & Businessrollen

IAGM – IA-was?

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.

Interne und externe regulatorische Anforderungen (***Governance & Compliance***) verlangen, dass diese Zugänge aber auch nicht mehr umfassen als wirklich notwendig ist (least privilege-, need to know- oder Minimalprinzip). Ergänzend sollen bei der Vergabe besondere Risiken z. B. aus kritischen Funktionen oder Funktionstrennungsaspekten vermieden werden (Segregation of Duties – SoD und Sensitive Access – SA).

IAGM & Businessrollen
Businessrollen definiert!

Businessrollen sind Elemente eines Rollenkonzeptes, die typische Arbeitsplätze/Funktionen eines Unternehmens abbilden (z. B. Einkäufer/in).

Unter einem typischen oder typisierten ***Arbeitsplatz*** verstehen wir eine identische oder zumindest sehr ähnliche Kombination aus Aufgaben mit Bezug zu IT-Anwendungen, die von mehreren Mitarbeitern aufgrund ähnlicher Funktionen wahrgenommen werden.

Unter einer ***Aufgabe*** verstehen wir eine spezifische Kombination einer Aktivität in Bezug auf ein betriebswirtschaftliches Objekt (z. B. Bestellanforderungen pflegen), der im Idealfall passende Berechtigungen in einer Zielanwendung entsprechen.

Die Businessrollen kombinieren insofern alle Berechtigungen, die zur Ausführung der Aufgaben eines Arbeitsplatzes erforderlich sind, unabhängig von den ***Plattformen & Systemen,*** auf denen die Aufgaben abgebildet sind.

IAGM & Businessrollen
Warum Businessrollen?

- Businessrollen als Abbild von typischen Arbeitsplätzen sind ein probates Element zur ***systemübergreifenden*** Definition und Bündelung der IT-Zugänge.
- Businessrollen und Aufgaben (und ggfs. Programme) können von Fachbereichen definiert und verstanden werden. Aufgaben können von den IT-Experten verstanden und in technische Berechtigungen umgesetzt werden. Sie sind insofern ein ideales ***Bindeglied*** zur Bedarfskommunikation ***zwischen Fachbereich und IT***.
- Die Anzahl der einzeln durch Genehmiger zu entscheidenden Elemente bei der Beantragung kann im Vergleich zur Einzelrollen-Beantragung massiv reduziert werden. Dadurch erhöht sich die ***Akzeptanz*** und reduziert sich der Aufwand der ***Genehmiger***.
- Enthalten Businessrollen ***Applikationsrollen fremder Rollen-Eigner,*** können diese ihre Zustimmung einmal zur Businessrolle geben. Eine Genehmigung bei der Vergabe der Businessrolle entfällt dadurch.
- Wird bei der Gestaltung von Businessrollen darauf geachtet, dass nur unvermeidbare, gewollte SoD-Konflikte in Businessrollen enthalten sind, kann die ***Zahl der Konflikte*** in Benutzern drastisch reduziert werden.
- ***Änderungen in Arbeitsplätzen*** können durch Anpassungen der zugeordneten Applikationsrollen angepasst werden. Die Synchronisation erfolgt automatisch über die IAGM-Anwendung.

IAGM & Businessrollen
Was sind Voraussetzungen?

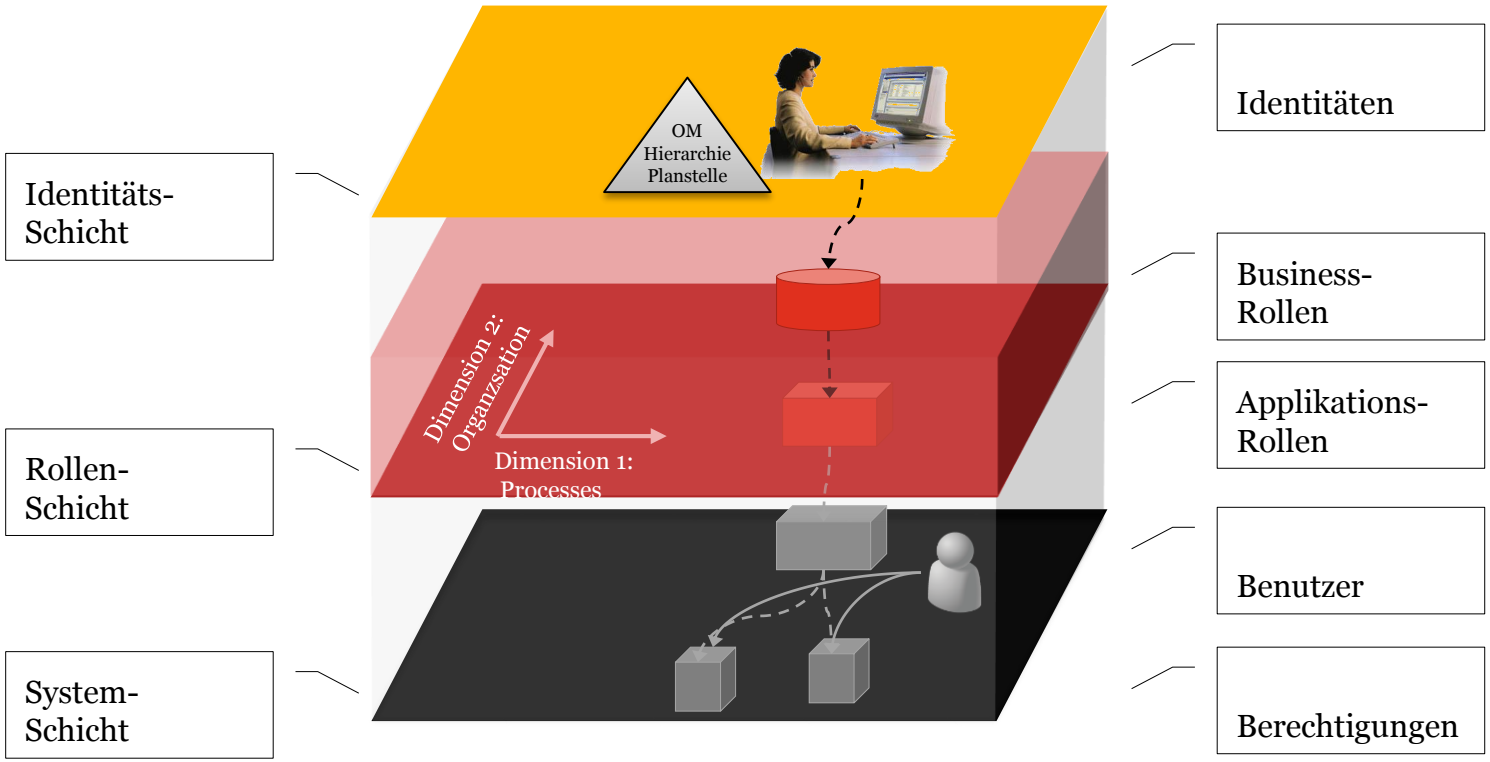
- Die Ziel-Anwendungen verfügen über ein ***angemessenes Berechtigungskonzept***, das die IT-Aufgaben der abzubildenden typischen Arbeitsplätze als Gruppierung von Rollen/Berechtigungen abbilden kann.
- Das Unternehmen verfügt über eine transparente und strukturierte ***Prozesshierarchie*** und ***Organisationshierarchie*****,** die den realen Prozessen, Aufgaben und Organisationsstrukturen des Unternehmens entsprechen.
- Das Unternehmen verfügt über ein qualifiziertes ***Netzwerk von Prozessexperten*** im IT-Bereich und Prozesskoordinatoren in den Fachbereichen, die Auskunft geben können über die Kombination von Aufgaben in Arbeitsplätzen.
- Das Rollenmodell, das Regelwerk, die Prozesse und organisatorischen Rollen werden unterstützt durch eine ***IAGM-IT-Lösung***, die der allgemeinen Komplexität des Themas und den spezifischen Anforderungen des Kunden gerecht wird.

Das Rollen-Modell

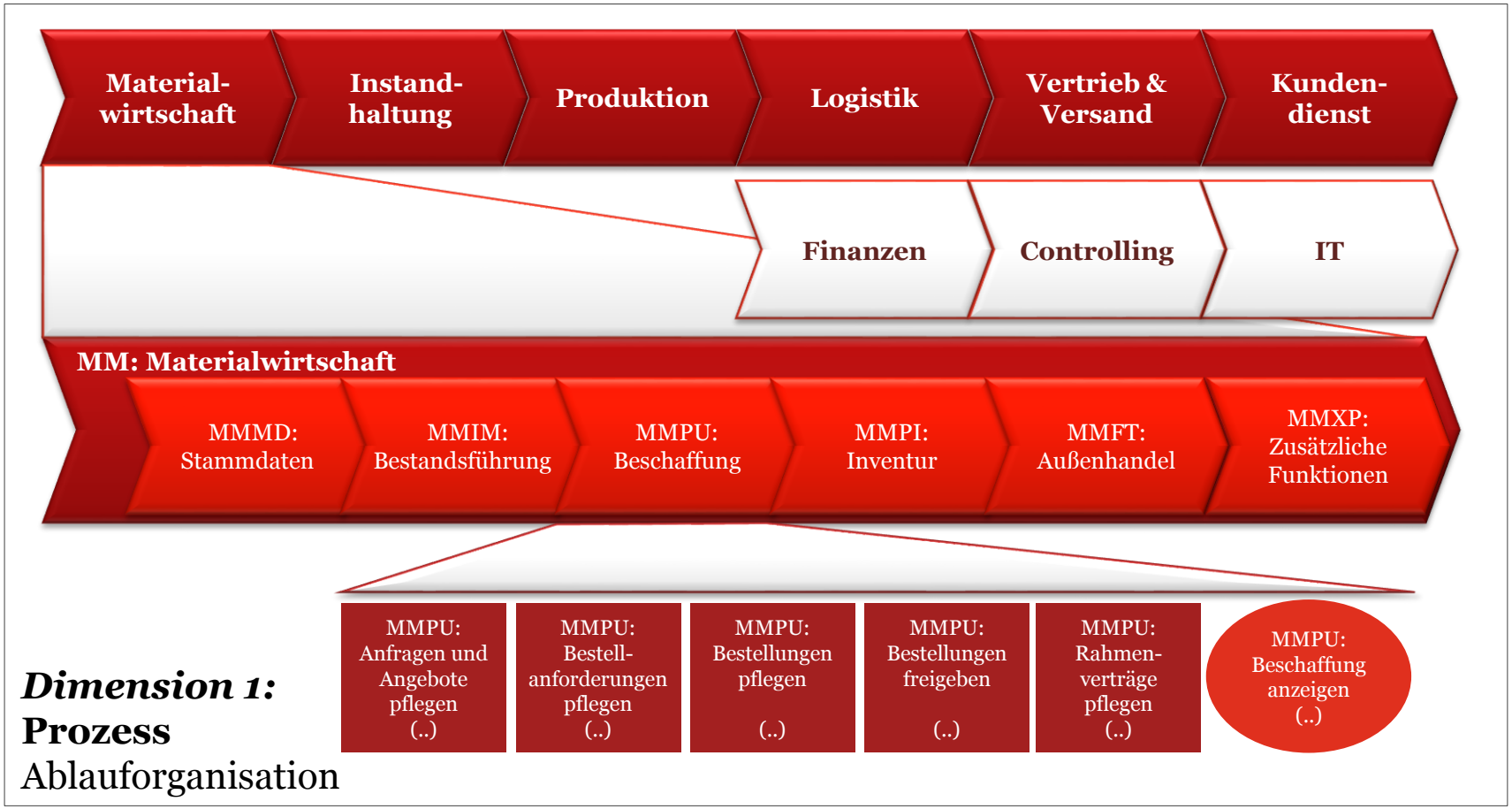
Das PwC Rollenmodell
Die 4 PwC-Anforderungen an angemessene Rollen

Außen-Beurteilung	Rollen-Klarheit	Jede Business- und Applikationsrolle ist über die Rollenattribute eindeutig in die zwei Hauptdimensionen eingeordnet. Dies heißt, dass die Rollen einem Haupt- / Teilprozess sowie einem Differenzierungstyp und –wert zugeordnet sind.
	Rollen-Transparenz	Die Business- und Applikationsrollen sind in ihrer Granularität sowie über den Rollennamen und die Rollenbeschreibung so definiert, dass ein sachkundiger Dritter innerhalb angemessener Zeit die Funktion der Rolle nachvollziehen kann.
Innen-Beurteilung	Rollen-Kongruenz	Die Applikationsrollen sind frei von inhärenten Funktionstrennungskonflikten des SoD-Regelwerks. Applikationsrollen beinhalten grundsätzlich jeweils nur eine sensitive Funktion des SA-Regelwerks.
	Regel-Konformität	Die Business- und Applikationsrollen beinhalten nur die Applikationsrollen bzw. technischen Berechtigungen, die mit dem Rollennamen und den Rollenattributen übereinstimmen.

Das PwC Rollenmodell
Schichten & Dimensionen

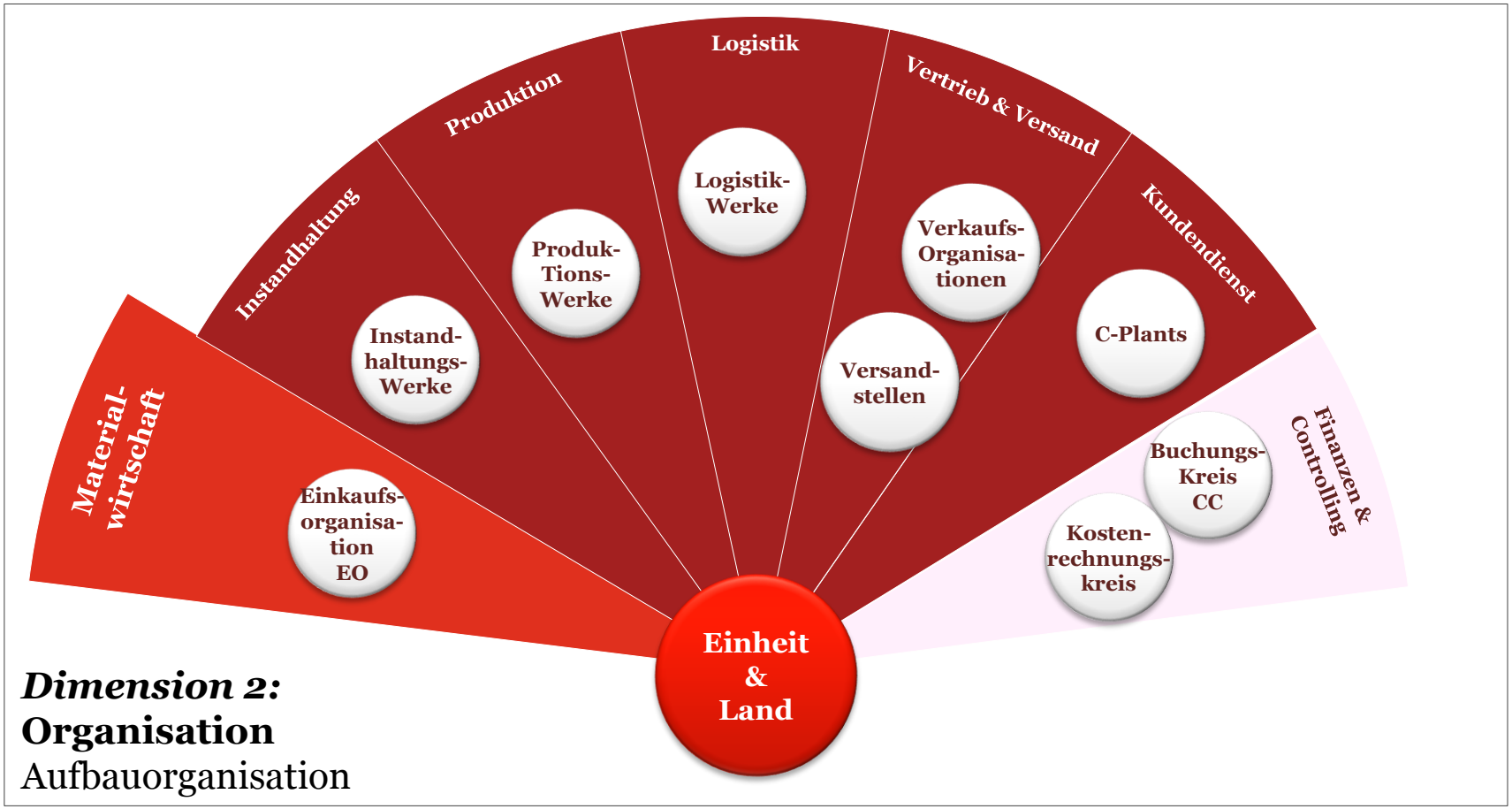


Das PwC Rollenmodell
Die Prozessuale Dimension



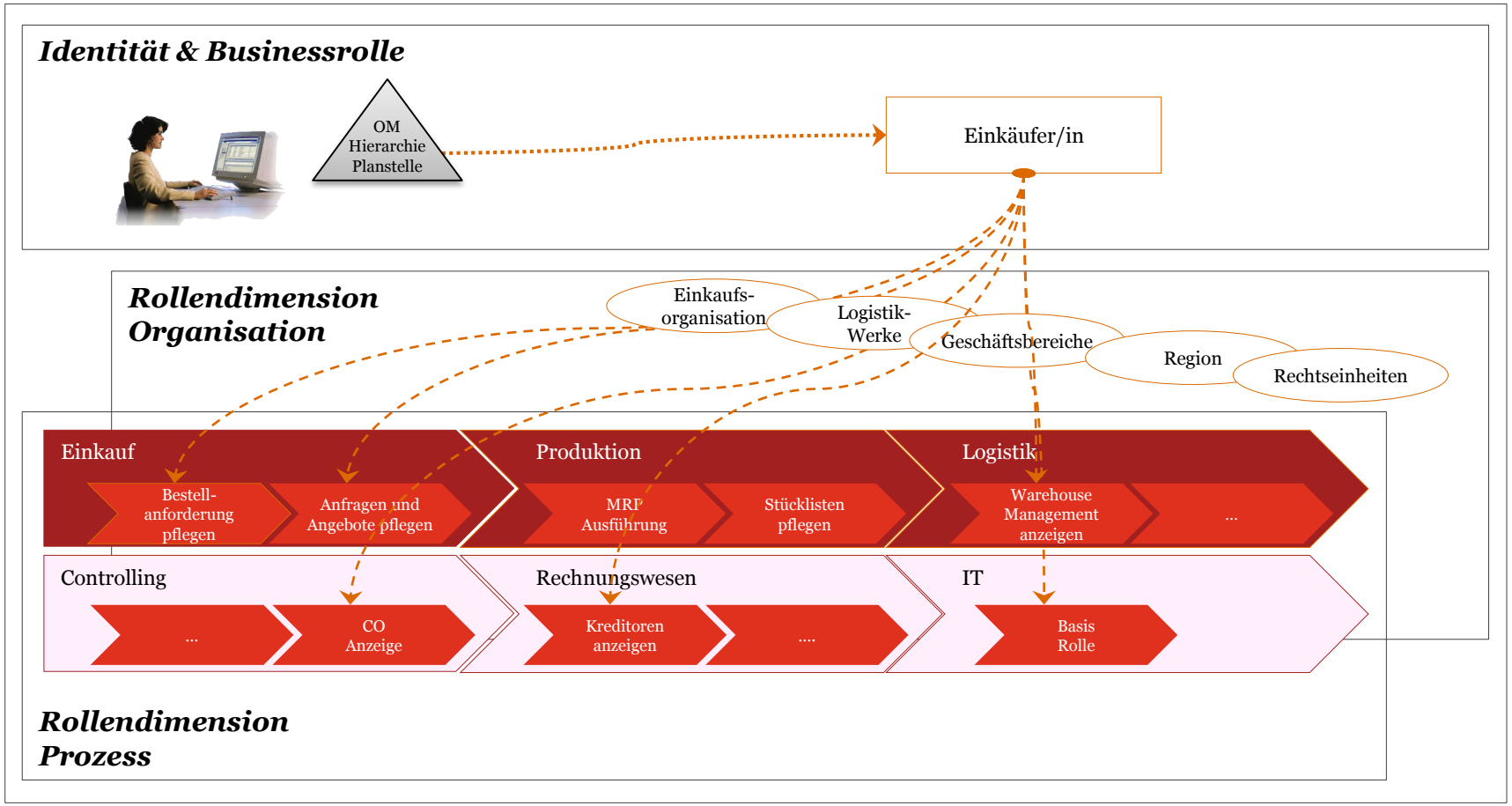
Dimension 1:
Prozess
Ablauforganisation

Das PwC Rollenmodell
Die Organisatorische Dimension

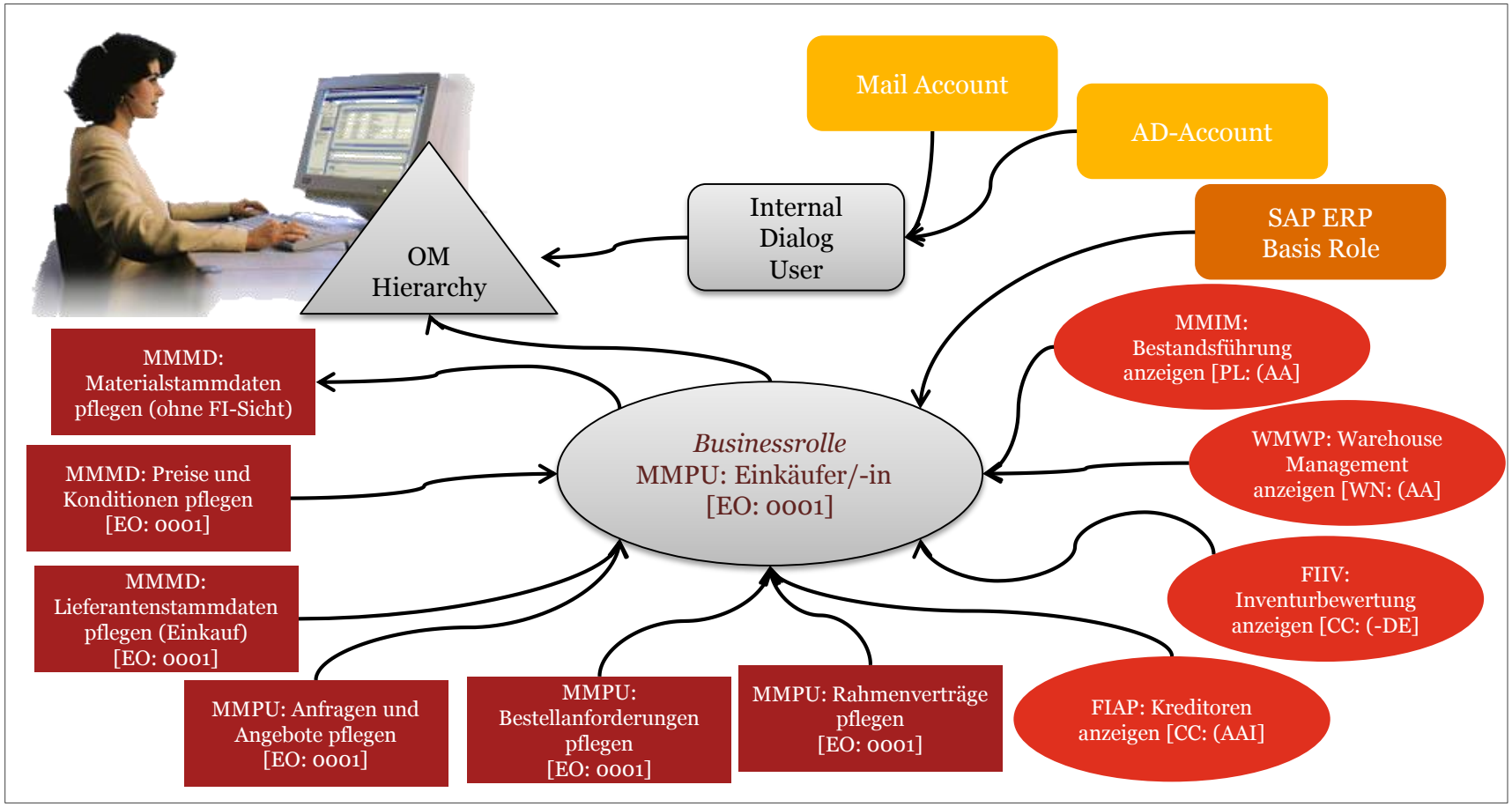


Dimension 2:
Organisation
Aufbauorganisation

Das PwC Rollenmodell
Identität – Prozess – Organisation

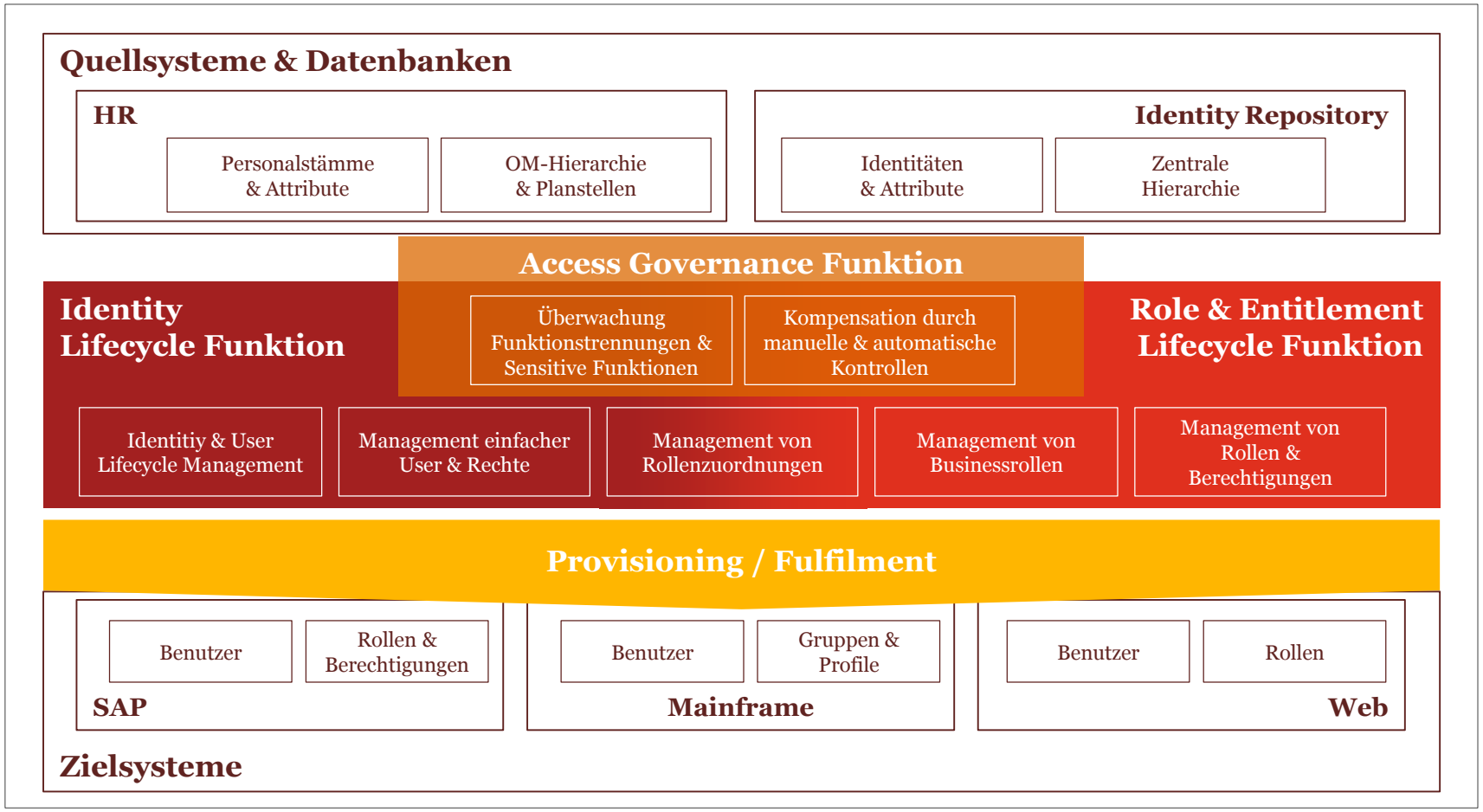


Das PwC Rollenmodell
Ein Beispiel



IAGM Automation

IAGM Automation
System- & Funktions-Landschaft



IAGM Automation
Selektionskriterien

BASICS

- Einfach ***Bekanntmachung der Applikationsrollen*** in der IAGM-Anwendung. Im Idealfall automatische Delta-Synchronisation und Attributierung.
- ***Pflege von Businessrollen*** mit Hinterlegung von Pflicht- und Wahl-Attributen. Einfache Selektion/Zuordnung von Applikationsrollen.
- ***Freie Attributierung*** von Applikations- und Businessrollen unabhängig von den Ziel-Applikationen.

ADVANCED

- Pflege eines ***Differenzierungsmodells*** mit Differenzierungstypen und –werten als Grundlage für Tochterrollen für Businessrollen (und ggfs. Applikationsrollen).
- Vorschläge für die ***Zuordnung von Applikationsrollen*** zu Businessrollen in Abhängigkeit des gewählten Differenzierungstyps und -werts der Businessrolle
- Anlage von Mutter- Applikationsrollen und ***Ableitung von Tochter-Applikationsrollen*** in SAP auf Basis des Differenzierungsmodells

Heraus-forderungen

Herausforderungen
Fragestellungen Allgemein

- Wie beherrscht man die ***Rollenanzahl*** aus der Multiplikation aus Mutter-Prozessrollen und Mutter-Businessrollen mit Differenzierungstypen und -werten?
- Wie geht man mit der Notwendigkeit der ***Zuordnung von Tochter-Applikationsrollen*** mit anderen Differenzierungstypen/-werten als denen der Tochter-Businessrollen um?
- Wie ***modelliert man Businessrollen*** bei einer Gruppe von Personen mit ähnlichen Funktionen:
  - Kleinster gemeinsamer Nenner mit zusätzlichen Einzel-Applikationsrollen
  - Vereinigungsmenge aller Aufgaben der Personen
  - Aufspaltung in zwei eigenständige Businessrollen jeweils entweder mit vollem Aufgabenumfang oder Basis- und Add On-Businessrolle

Fragen & Antworten

Ihr Ansprechpartner

Martin Krause
Alsterufer 1
20354 Hamburg
Tel.: +49 40 6378 1520
email: martin.krause@de.pwc.com

Johannes Liffers
Kapelle-Ufer 4
10117 Berlin
Tel.: +49 30 26 36 16 58
email: johannes.liffers@de.pwc.com