

# Access Governance

## Identity Management aus dem Business für das Business

Detlef Sturm  
Senior System Architect  
Beta Systems Software

Christian Himmer  
Abteilungsleiter Identity Management  
Finanz Informatik Technologie Service

22.11.2011

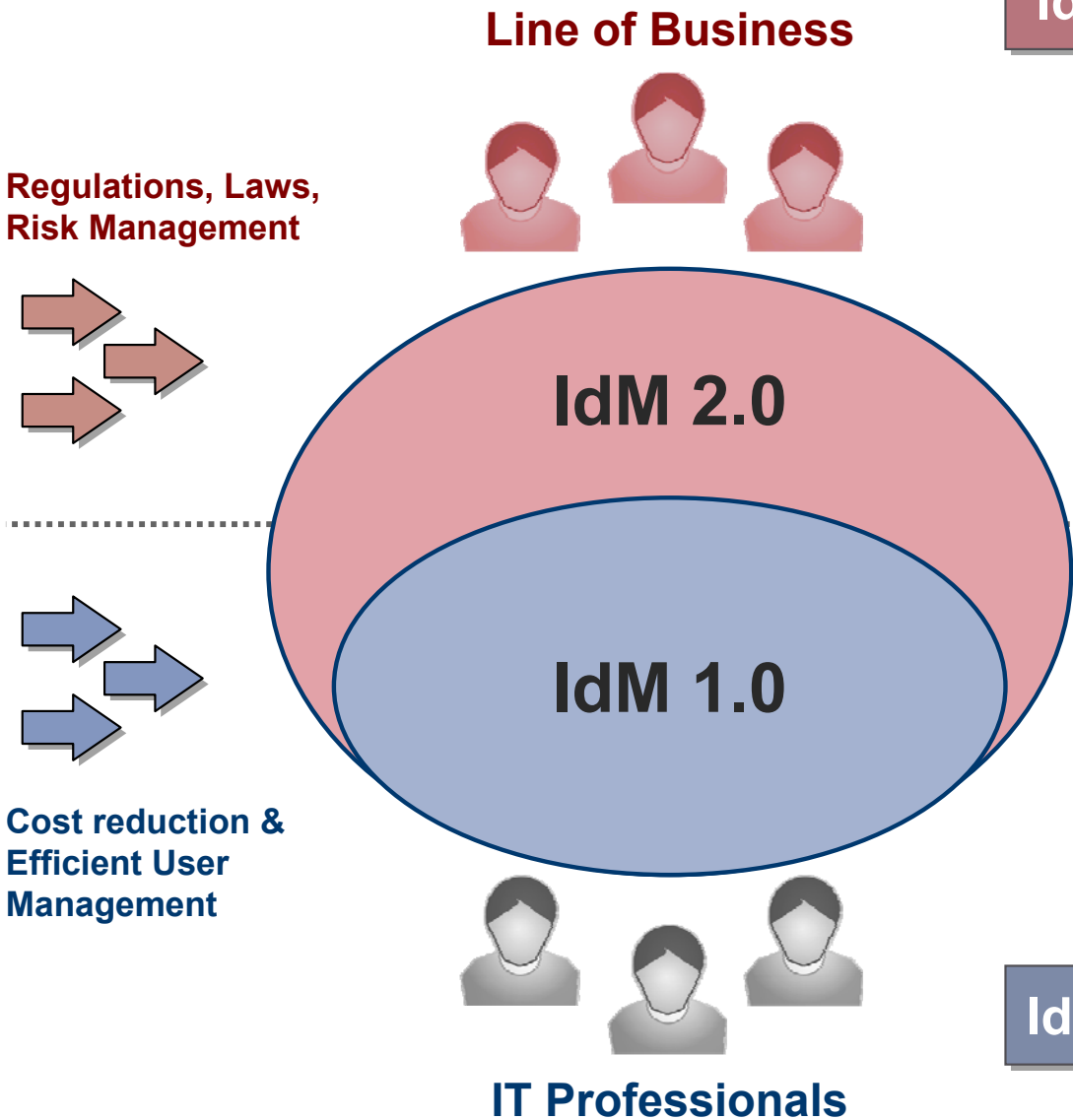
**Webinar**  
**KuppingerCole**

## Agenda

- **IdM im Wandel**
  - Von Access Management zu Access Governance
  
- **Access Governance**
  - Grundlegende Funktionsbausteine
  
- **Technologie vs. Best Practices**
  - Berechtigungsvergabe
  - Funktionstrennung (SoD-Richtlinien)
  - Business-orientierte Rollenmodellierung
  - Antrags- und Genehmigungsverfahren
  - Zertifizierung von Berechtigungen



# Identity Management im Wandel



## Access Governance (IAG)

Identity & Access Management (IAM)

- „Business-Kollaboration“
  - Veränderte Nutzung und Wahrnehmung des IdM
  - Business-getriebene Rollen
  - Self-Services
- 
- IT-lastig und Administrator-orientiert
  - Single-Point of Administration
  - HR-driven Provisioning
  - Role-based Access Control

## Identity & Access Management (IAM)

# Access Governance: Business für das Business

## Funktionsbausteine von Access Governance

- **Antrags- und Genehmigungsverfahren für Berechtigungen**  
(Access Request & Approval)
- **Transparenz und Zertifizierung von Berechtigungen**  
(Access Review & Certification)
- **Business-orientierte Rollenmodellierung**  
(Business Role Modeling)
- **Definition und Überprüfung von Richtlinien (Funktionstrennung)**  
(Policy Definition and Validation - SoD)
- **Risikobewertung und Risikoanalysen für Berechtigungen**  
(Access Risk Rating & Analysis)
- **Historisierung von Berechtigungen und Prozessinformationen**  
(Access & Process History)
- **Überwachung von Benutzeraktivitäten**  
(User Activity Monitoring)
- **Überprüfung und Nachweis von Compliance Anforderungen**  
(Compliance Audit & Reports)



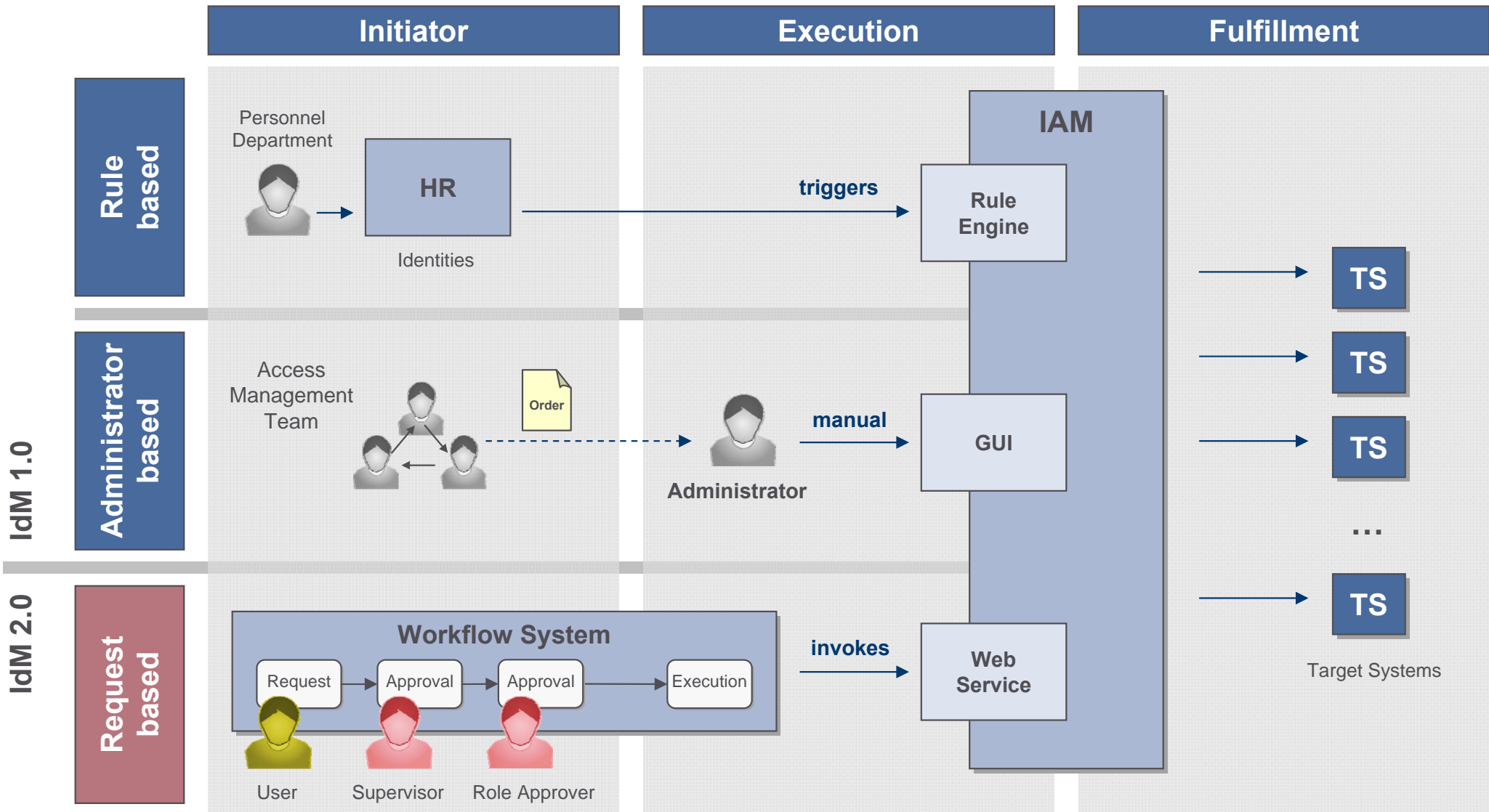
# Access Governance: Business für das Business

## Unsere Themen des Webinars:

- 1. Möglichkeiten der Berechtigungsvergabe**  
(Role Assignment)
- 2. Punkte für die Funktionstrennung**  
(Policy Definition and Validation - SoD)
- 3. Aspekte der Rollenmodellierung**  
(Business Role Modeling)
- 4. Antrags- und Genehmigungsverfahren**  
(Access Request & Approval)
- 5. Zertifizierung von Berechtigungen**  
(Access Certification)

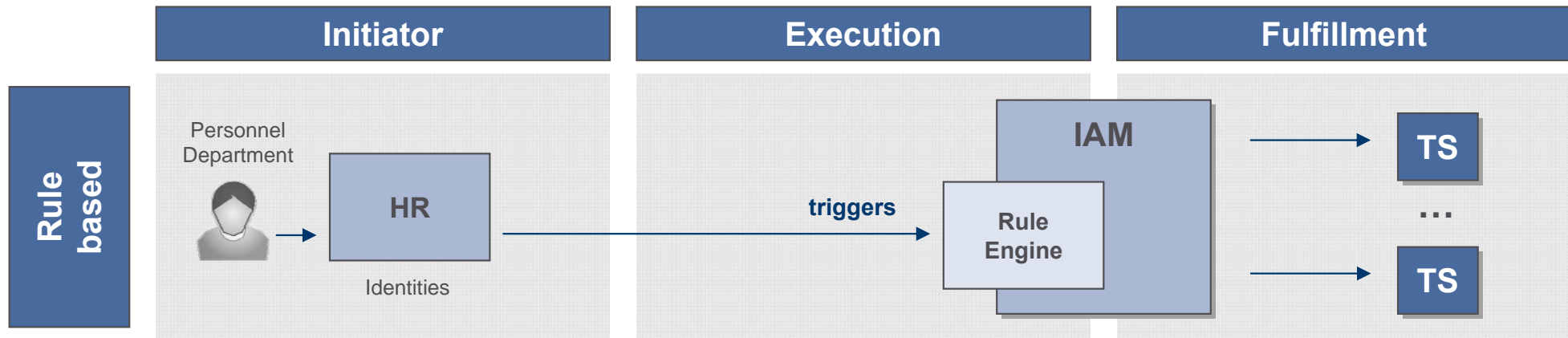


# Möglichkeiten für die Berechtigungsvergabe sind sehr vielseitig !



- Werden die IdM 1.0 Ansätze von den Antrags-und Genehmigungsverfahren verdrängt?

# Hohe Automatisierung ist ein Servicefaktor



## Provisionierung und Deprovisionierung

- Bei Eintritt:
  - Anlage von Accounts
  - Vergabe von Berechtigungen
- Bei Versetzung:
  - Entzug von alten Berechtigungen
  - Vergabe von neuen Berechtigungen
- Bei Austritt:
  - Sperrung und Löschung der Accounts

### Best Practice:

- automatischer Entzug oder manuelle Befristung aller „alten“ Berechtigungen



**Provisionierung ist wichtig!**

**Deprovisionierung ist compliance-relevant!**

# Funktionsstrennung (SoD) ist mehr als die Definition von Kriterien

## Elemente von Policy Management

### Policy Definition

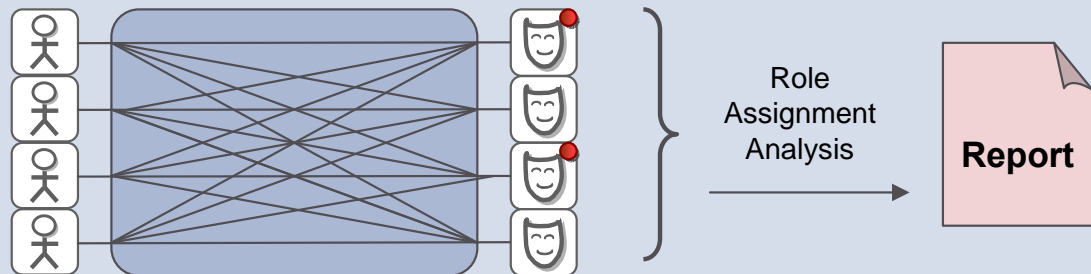
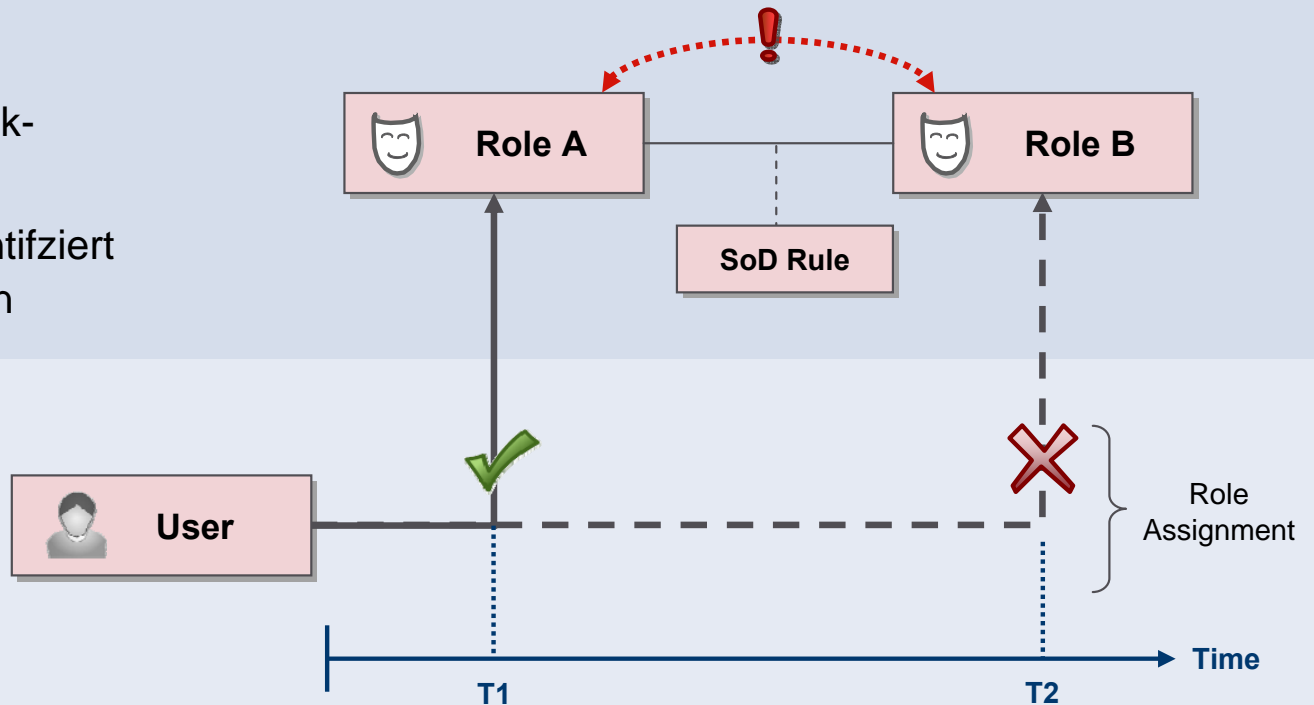
- Für kritische Aktivitäten ist eine Funktionsstrennung erforderlich (MaRisk)
- Die betroffenen Rollen müssen identifiziert und der Ausschluss definiert werden

### Policy Enforcement

- Bei der Rollenvergabe sind die SoD-Regeln zu berücksichtigen
- Ausnahmen müssen besonders behandelt werden

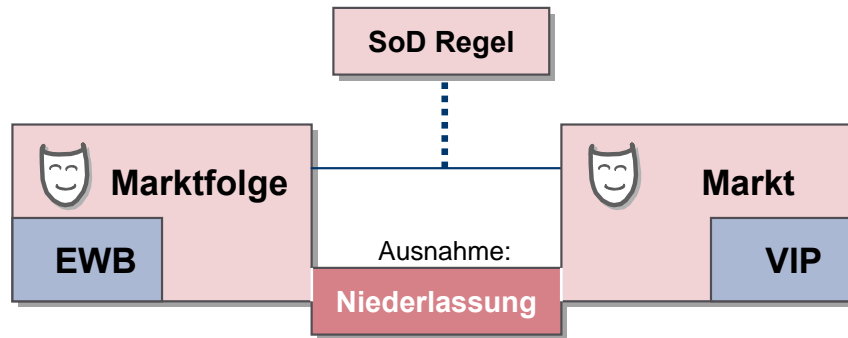
### Policy Validation

- Compliance erfordert zusätzlich einen Nachweis bzgl. der Einhaltung der Regeln und den Ausnahmen



## Erfahrungen bei der Umsetzung von SoD

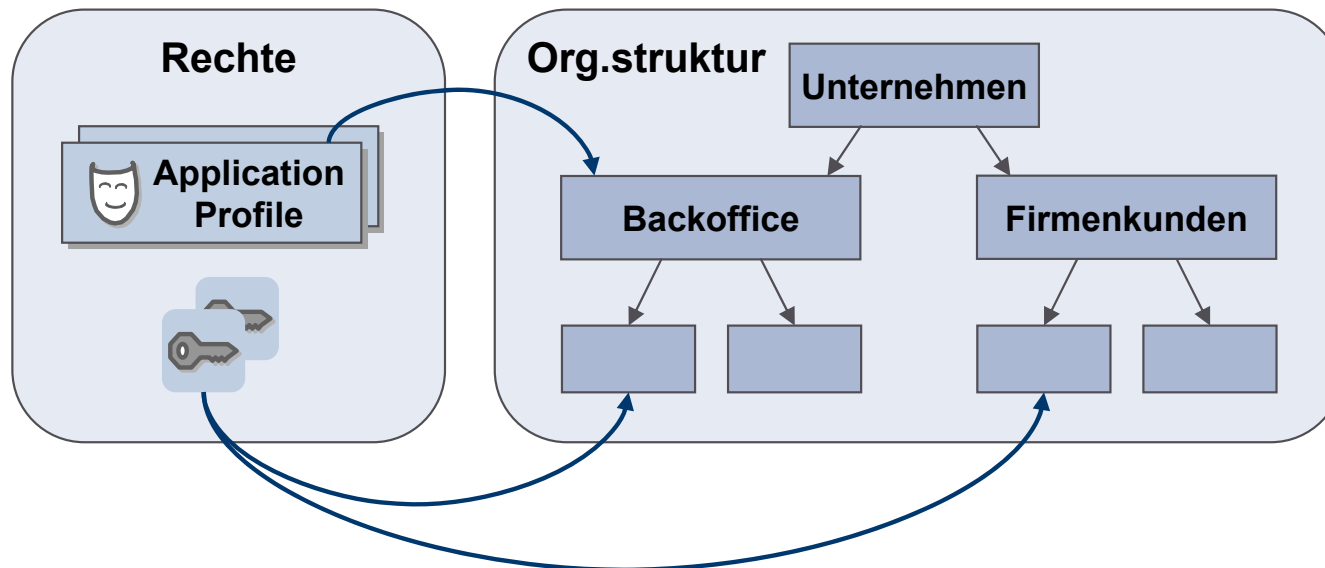
- Die Anforderungen aus dem Lehrbuch vs. Praxis



► Fachliche Regeldefinition wird sehr komplex !

(EWB – Einzelwertberichtigung, VIP – VIP-Betreuung)

- Eine Lösung aus der Praxis: Zuordnung der Rechte zu zulässigen Org.einheiten

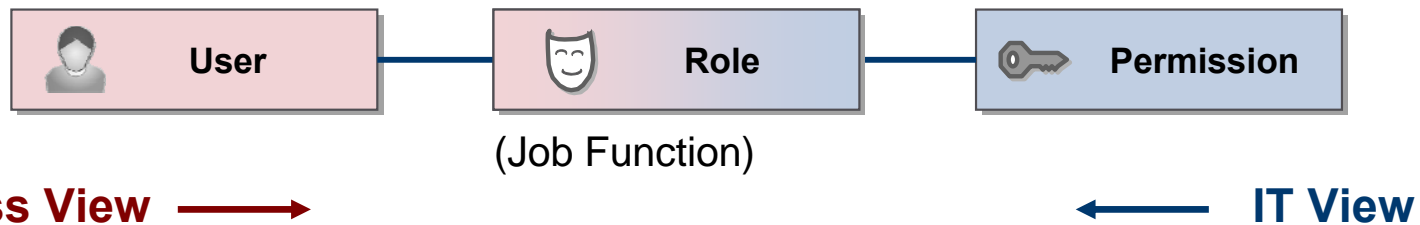


### Best Practice:

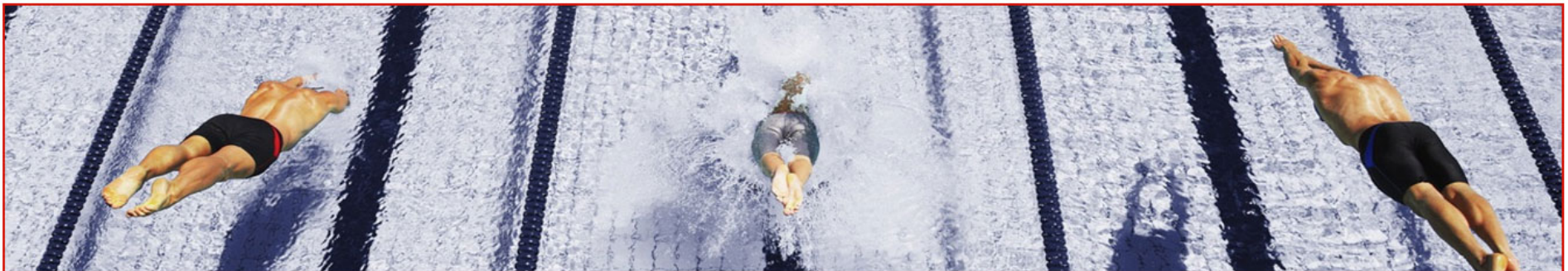
- Recht zu OrgEinheit bei Verwendung der Org.struktur
- ergänzt im Vertragsart (Externer, Mitarbeiter, Azubi u.ä.)

# Rolle – Business-verständliche Fassade der Berechtigungen

## Grundsätzliches Rollenmodell

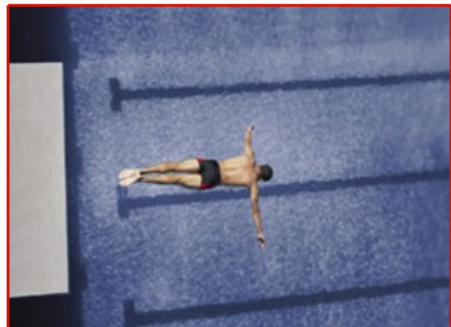
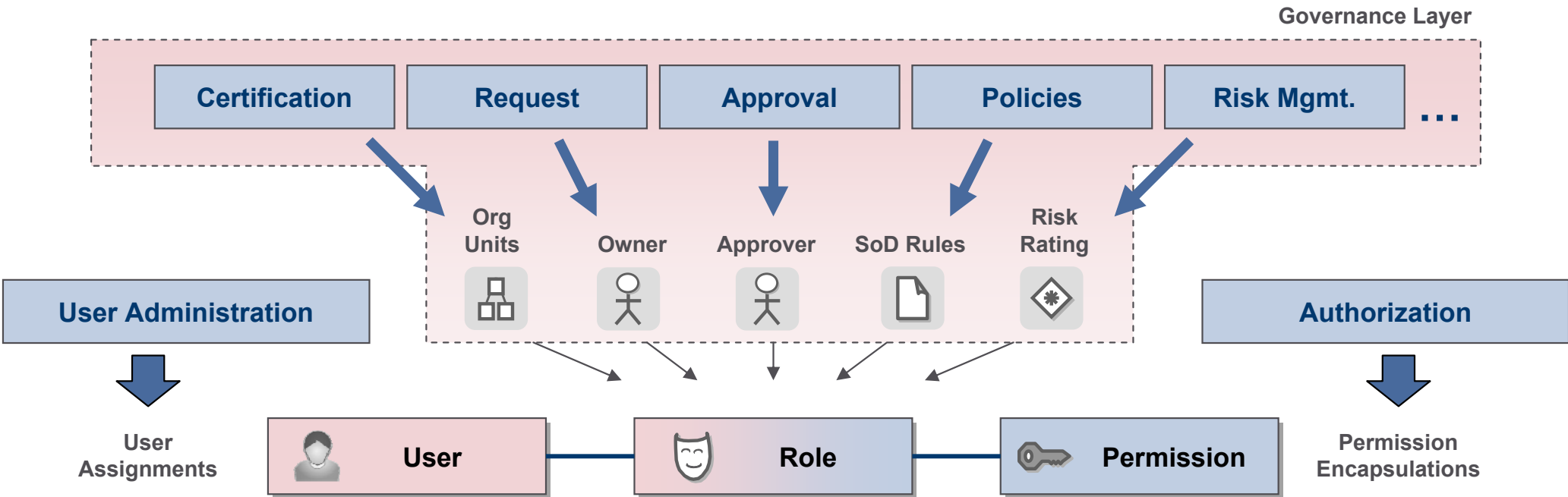


- Kapselt die Berechtigungen in eine abstrakteren Form
- Zuweisung der Rolle zu Benutzern
- Semantik der Rolle soll der Job-Aufgabe entsprechen  
→ Rolle wird zur Business-verständlichen Fassade der technischen Berechtigungen
- Diese Sicht wurde maßgeblich geprägt durch RBAC



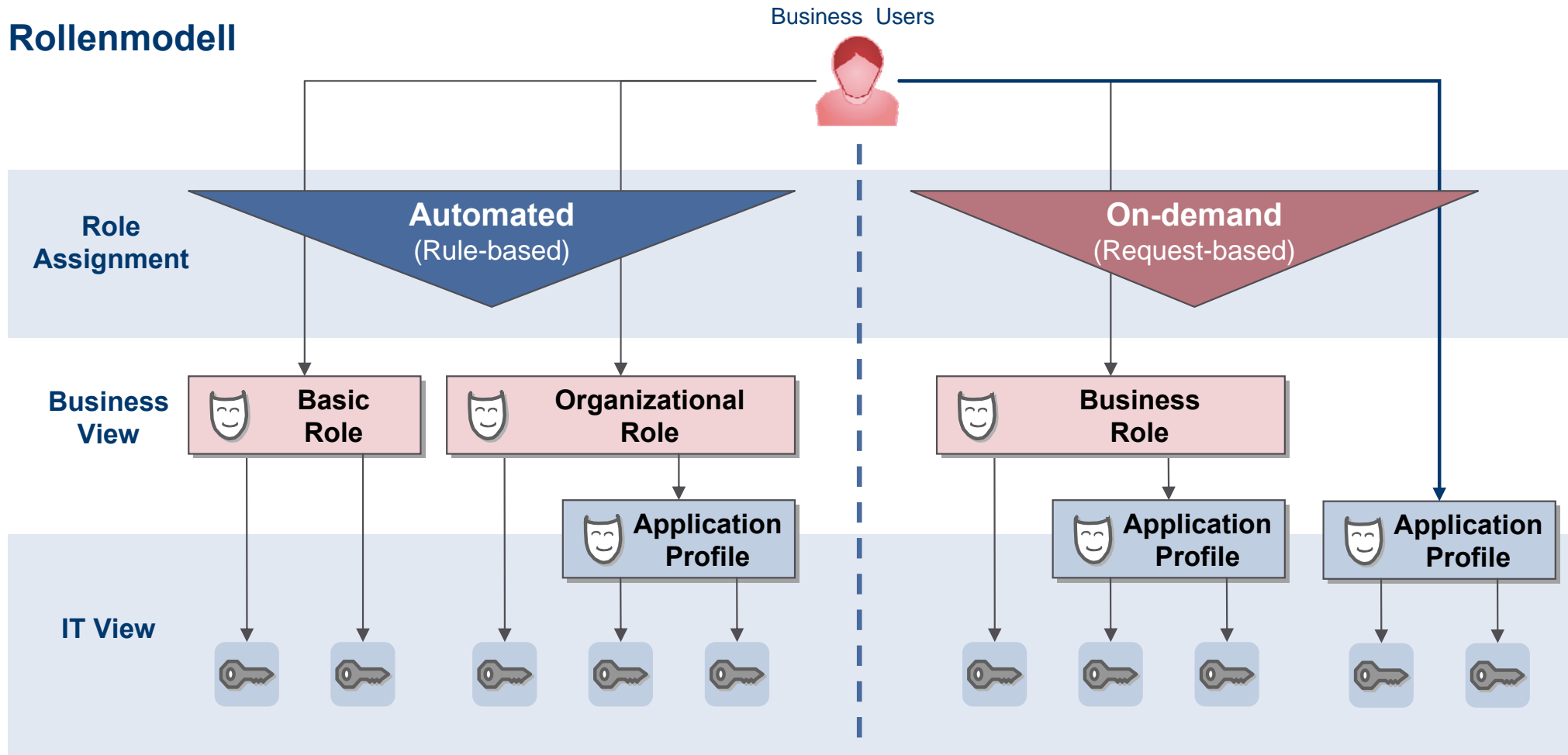
# Aspekte von Access Governance erzeugen weitere Anforderungen

## Vom traditionellen Rollenansatz zu Governance-supported Rollen



# Ein flexibles Rollenmodell kann dem Business helfen

## Rollenmodell



### Best Practice 1:

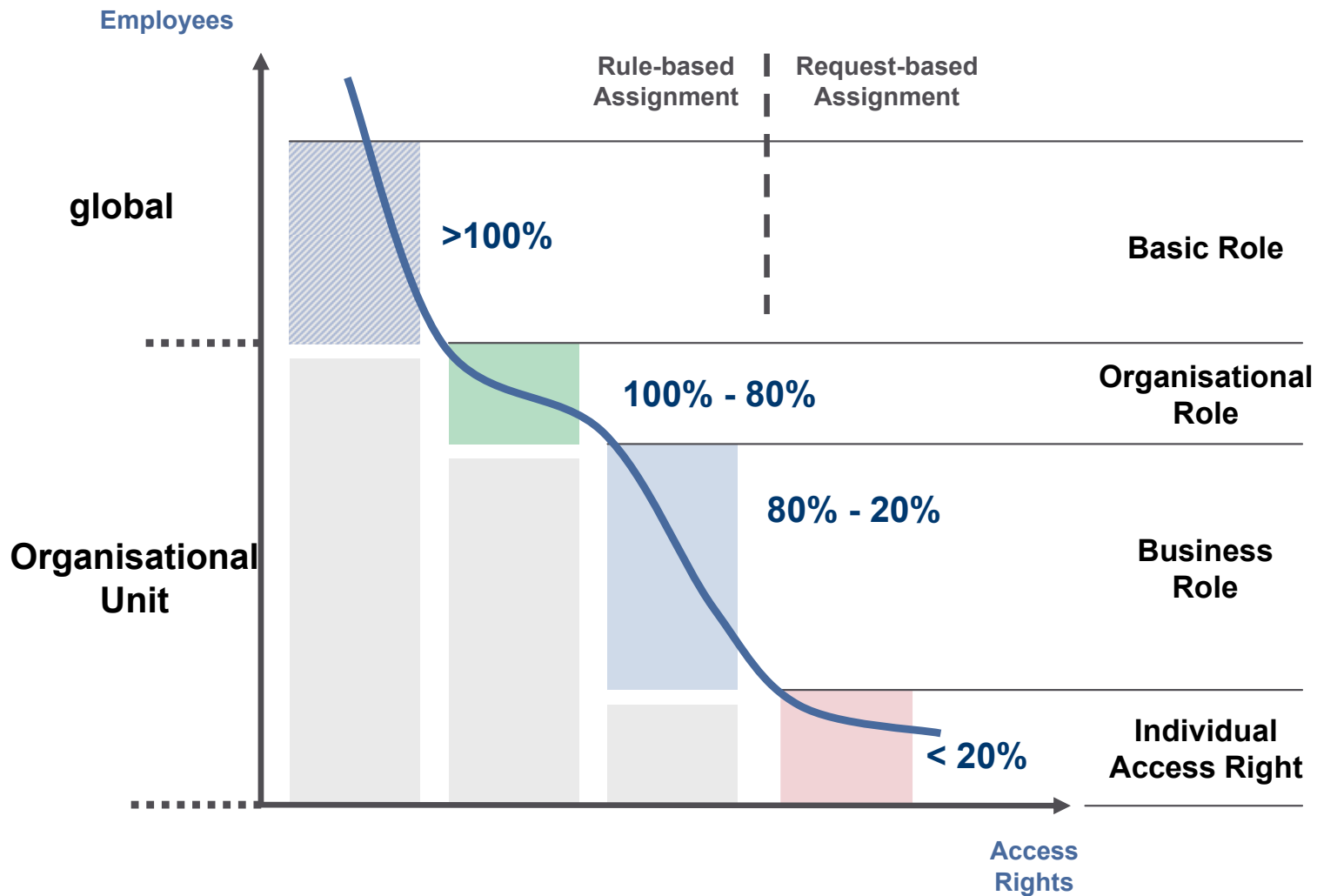
- Transparenz schaffen mit Anwendungsprofilen

### Best Practice 2:

- Individuell bleiben Kompetenzen und kritische Rechte

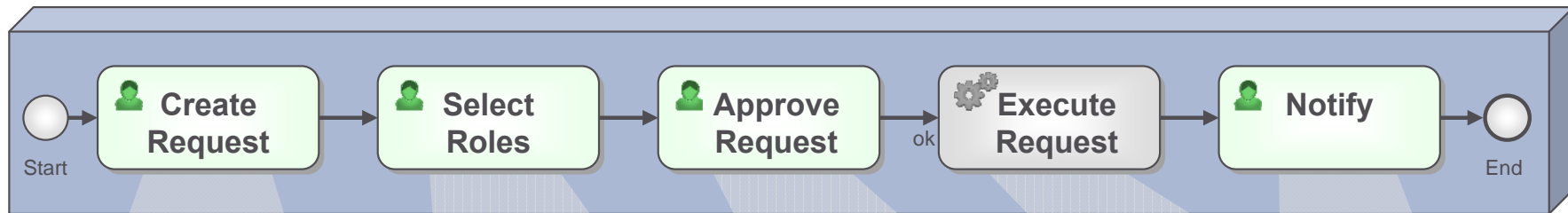
# Rollenart ist abhängig von der Mitarbeiteranzahl

## Schematische Verteilung $\Sigma$ Mitarbeiter und $\Sigma$ Rechte



# Antragsverfahren bringen neue Fragestellungen in die IdM-Welt

## Grundsätzlicher Prozess und technologische Anforderungen



**Antragsteller**

- ▶ **Wer** kann Rollen beantragen?
- ▶ **Für wen** wird beantragt?
- ▶ Können Rollen **für mehrere** Benutzer gleichzeitig beantragt werden?

**Rollen**

- ▶ **Welche Rollen** können und dürfen beantragt werden?
- ▶ Können **mehrere Rollen** gleichzeitig beantragt werden?

**Genehmiger**

- ▶ **Wer** genehmigt?
- ▶ **Wer** definiert die Genehmiger?
- ▶ Wie **viele Genehmigungen** sind erforderlich?
- ▶ Was passiert bei einer **Ablehnung**?

**Ausführung**

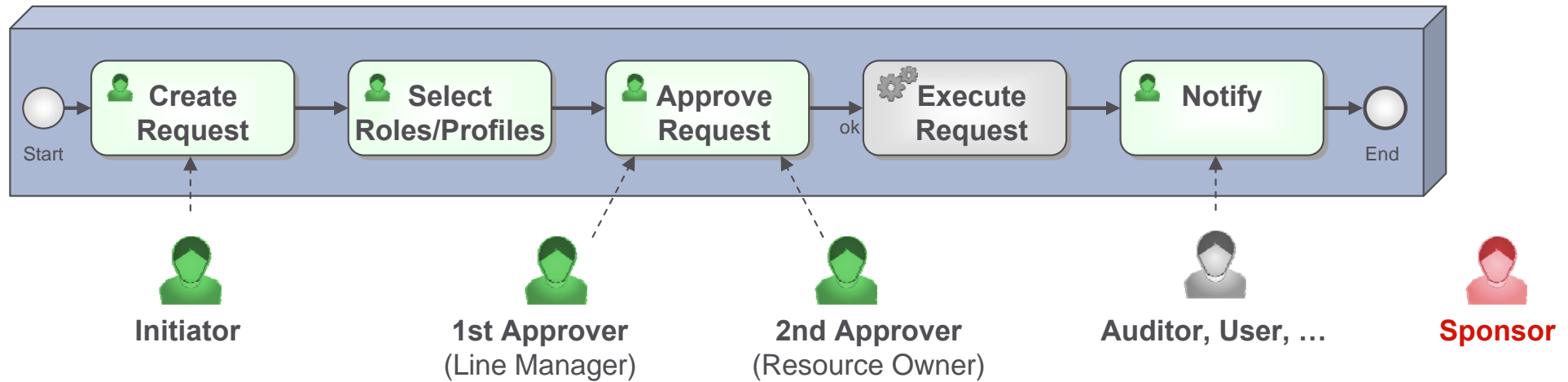
- ▶ **Wie** wird der Antrag ausgeführt?

**Benachrichtigung**

- ▶ **Wer** wird benachrichtigt?
- ▶ **Wie** wird benachrichtigt

# Business-Orientierung ist mehr als nur Technologie

## Stakeholder und ihre wichtigsten Anforderungen



### Sicht der Antragsteller

- ▶ Intuitive GUI
- ▶ Suchmöglichkeiten
- ▶ Verständliche Objekte
- ▶ Statusrückmeldung
- ▶ Prozess-Geschwindigkeit

### Sicht der Genehmiger

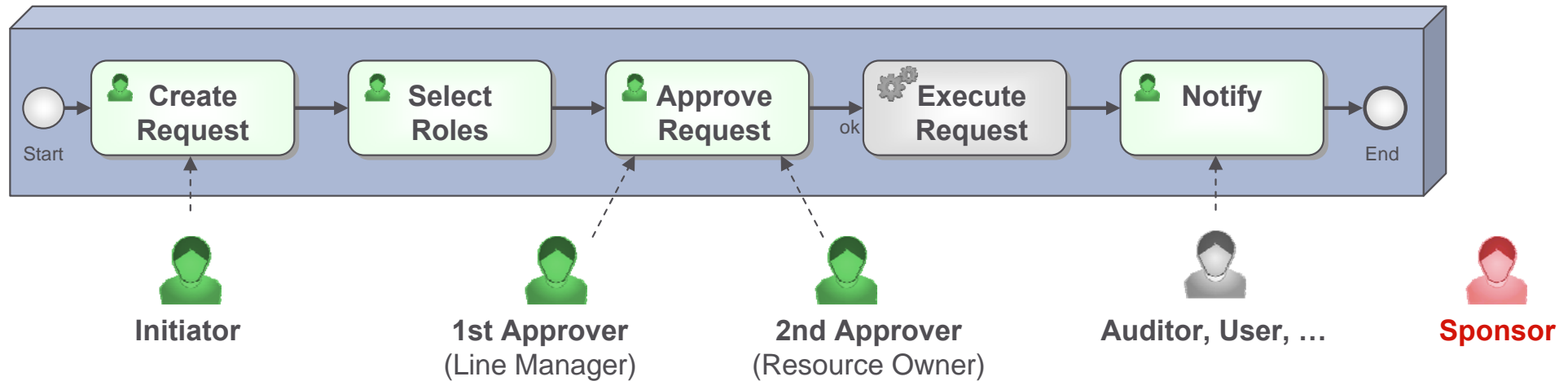
- ▶ Noch intuitivere GUI
- ▶ Aktive Information
- ▶ Stellvertreterregelung
- ▶ Dynamische Einbindung
- ▶ Prozess-Transparenz

### Sicht des Sponsors

- ▶ Abbildung der Prozesse
- ▶ Integration in die IT-Landschaft
- ▶ Kosten
- ▶ Monitoring

# Business-Orientierung ist mehr als nur Technologie

## Stakeholder und ihre Anforderungen



### Best Practice:

- Ausfiltern unzulässiger Rechte erhöht die Übersicht
- Selektionslisten erhöhen die Qualität und machen das Ausfüllen leichter
- Vorbefüllung von Feldern
- So wenig Genehmigungen wie möglich:
  - Keine Line Manager bei unkritischen Rechten
  - Ressource Owner nur bei Bedarf
- Anzeige der relevanten Daten auf einer Seite
- Genehmigung / Ablehnung mit einem Klick

# Access Governance: Auch für die bestehende Berechtigungen

## Zertifizierungsphasen und Optionen:

### Definition & Initiierung

- **Zertifizierungsobjekte**
  - Benutzer, Rollen, Ressourcen, Regeln, ...
- **Initiierung**
  - Periodisch, ereignis-gesteuert, on-demand, pro-active
- **Verantwortlicher**
  - Vorgesetzter, Rollen-Owner, ...

### Ausführung

- **Transparenz über die Berechtigungen**
  - Ausführliche und verständliche Informationen
- **Ausführung**
  - Im Bulk, objekt-individuell
  - Stichprobenartig
- **Zertifizierungszeitraum**
  - Grundsatz: je älter, desto höher das Risiko

### Maßnahmen

- **Positive Zertifizierung**
  - Anpassung der Risikobewertung
  - Reporting
- **Negative Zertifizierung**
  - Entzug der Berechtigung (automatisch, per Antrag)
  - Reporting



# Zertifizierungen müssen praxistauglich sein

## Ausgangsbasis:

- Interpretation von „angemessen“ in der schriftlich fixierten Ordnung.
- Damit Festlegung von „regelmäßig“ und „nachweisbar“.

## Zertifizierung:

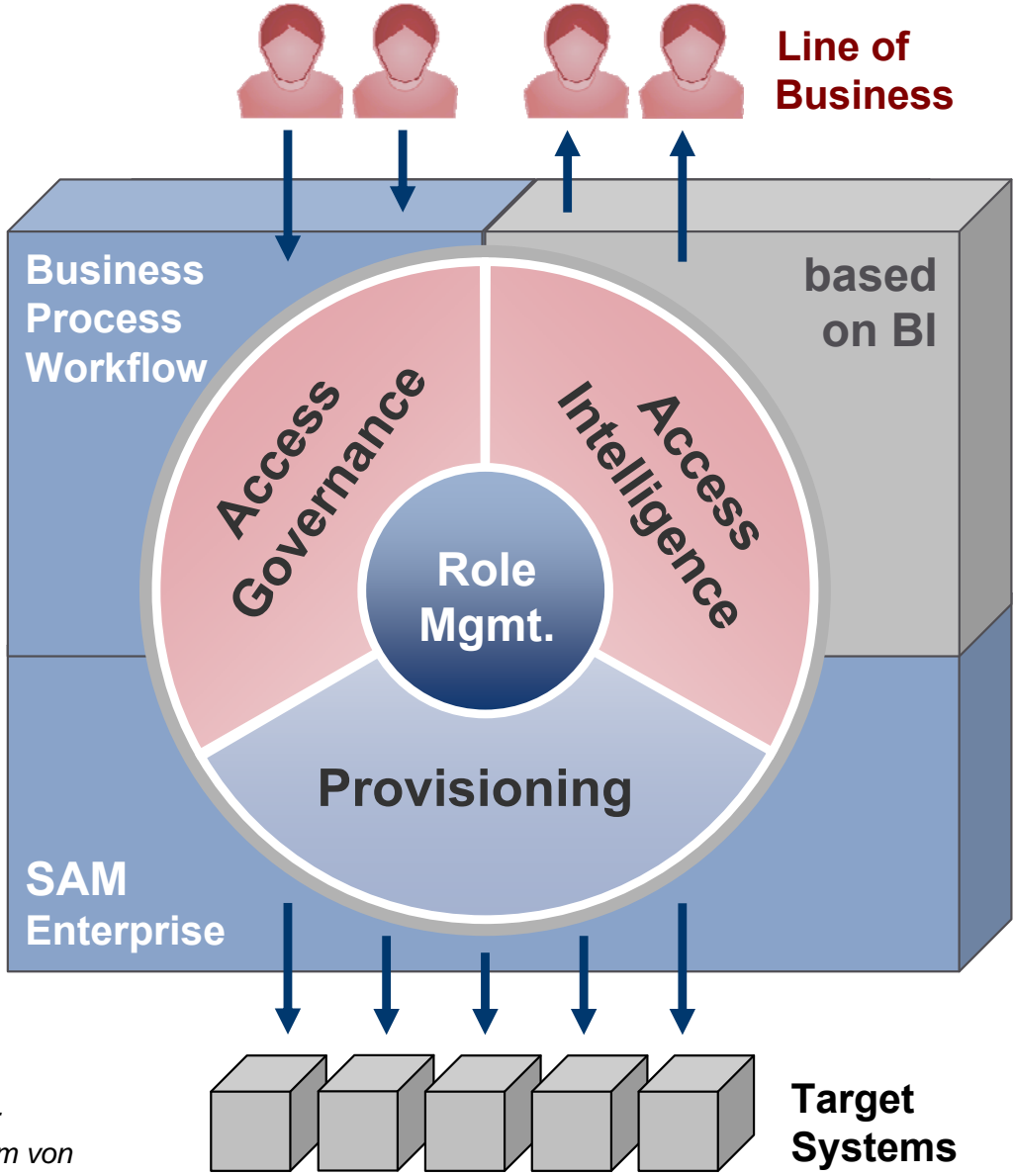


**Lieber weniger, aber dafür mit Qualität**



# Access Governance = Business-orientiertes IAM

Strategie von Beta Systems:



„IdM 2.0“

„IdM 1.0“

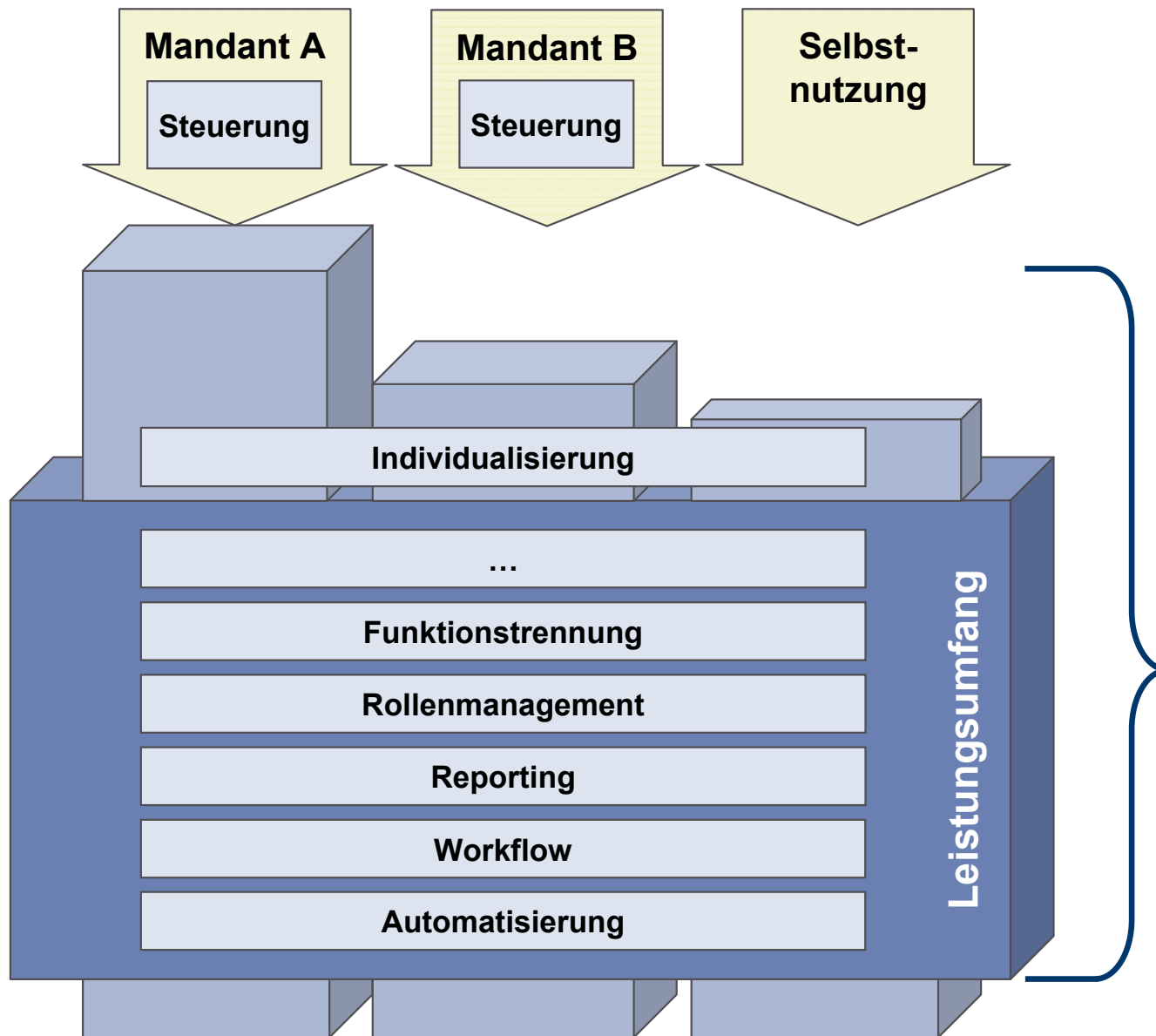
**SAM:**  
IAM-System von  
Beta Systems



# Bezug von Access Governance als Full Service

„IdM 3.0“ ?

## Das Service-Modell:



- Vorteile:**
- Verkürzung der Projektlaufzeiten
  - Plan, Build und Run aus einer Hand
  - Synergien bei Projekt und Betrieb
  - Reduzierung der Fertigungstiefe

- Full Service**
- Plattform
  - Lizenz
  - Betrieb
  - Fortschreibung

A close-up photograph of two hands shaking. The hand on the left is wearing a blue and black wristband. The hand on the right is wearing a tan bandage. The background is a plain, light-colored wall.

**Detlef Sturm**

Senior System Architect

**Christian Himmer**

Abteilungsleiter

Identity Management

**Vielen Dank**

Für Ihre Aufmerksamkeit!