



INSTITUT  
FÜR SYSTEM-  
MANAGEMENT

**be Flexible** ✦ **be Safe** ✦ **bi-Cube**

# Rollenmodellierung, Generische Prozessmodelle und Compliance

Prof. Dr. Dr. Gerd Rossa  
CEO

# Reife eines Unternehmens für eine IPM-Lösung

IPM kann kein organisatorisches Chaos verwalten!!!!

- Unternehmensstrategie und Projektpositionierung muss passen
- Architekturverständnis
- Status der Organisation
- Modellierungsverständnis
- Umsetzbares Vorgehensmodell

**Hierzu wird eine Checkliste übergeben**



## Grundsätze

Ein Rollenmodell muss neben dem direkten Berechtigungs-Management geregelt ko-existieren!

Die „sanfte“ Migration vom direkten Berechtigungs-Management zum Rollenmodell erfolgt durch eindeutige Regeln /z.B. eine rollenbasierte Berechtigung überschreibt eine direkte Systemzuweisung

Attribut- und Objekt-Referenzen ermöglichen ein übersichtliches Rollenmodell

Analytische Verfahren unterstützen die synthetische Rollenmodellierung (Cluster-Analyse bestehender Berechtigungen und Skill-Management)



# Rollenmodell und SoP

(Selbst-organisierendes Provisioning)

## Rollenmodellierung

- Organisations-, Fach- und System-Rollen
- Restriktions-Rollen (zur Einschränkung der Admins)
- Dynamische Systemrollen mit Access-Controls
- Rollenreferenzen (vereinfachte Rollenmodellierung)
- Synthetische Fach- und Systemrollen
- Security-Classification der Rollen (IKS)
- Mengenoperationen auf Rollen
- Mandanten- und Team-Rollen
- Störungsfreie Migrationsfähigkeit von direkter zu rollenbasierter Zuordnung von Berechtigungen
- Primary-Account



# Problembereiche bei SoP – Prozessen

**Bei den SoP- Prozessen sind komplexe Zusammenhänge zu beachten:**

## **Rollenkonflikte**

Zusammenfügen und Trennen von Systemberechtigungen, die aus verschiedenen Rollen dem User zugewiesen werden

Grundregel: Rollensystem überschreibt Direktzuweisung / sanfte Migration vom System- zum Rollenmodell

## **Rollenaktualisierung**

Bei Änderungen von Rollen sind diese auf die zugewiesenen Rollen „durchzudrücken“

## **Attributindizierte Rollen**

Grundlage der Automatisierung der IPM-Prozesse

## **Rollenreferenzen**

Basisrollen werden mit Spezialrollen verbunden und automatisch zugewiesen



# Problembereiche bei SoP – Prozessen

## Beachtung komplexer Zusammenhänge:

- **Gleitende Übergänge / Wechselprozesse**

Bei einer Rollenänderung (z.B. durch Organisationseinheits-Wechsel) können die Berechtigungen nicht schlagartig wechseln

- **Wiedereintritt in Konzernstrukturen**

- **Transaktionsmanagement**

Transaktionen, die durch Attributänderungen getriggert werden, müssen bestimmte Änderungen so lange blockieren, bis die Transaktion beendet ist

- **OE-Kompetenzen**

Zweite Dimension der Berechtigung: Sichten innerhalb der Unternehmensstruktur



# Rollen und Teams (Projektorganisation) (USP)

## Ziel:

- Berechtigungsvergabe an definierte temporäre Gruppen von Usern
- Zentrale Modellierung, dezentrales Provisioning

## Regeln:

- Das Team wird mit einem Beginn- und einem Ablaufdatum versehen.
- Teammitglieder werden einer Position zugeordnet (Teamleiter, Stellvertreter...)
- Der Teamleiter fordert die User für sein Team an, vergibt Berechtigungen und steuert die Laufzeit des Teams
- User erhalten die Teamrollen bei Eintritt ins Team bzw. verlieren die Rollen bei Verlassen des Teams.



## **Anforderungen an die Compliance werden vor allem durch generische Prozessmodelle erfüllt**

- Revisionierbarkeit (SOX, KONTRAG, Basel II)
- 2-stufiges Revisionsmodell
- Live Cycle eines Users
- Internes Kontrollsystem IKS
- Gesichertes Betriebskonzept
- Eigensicherheit des IPM-Systems

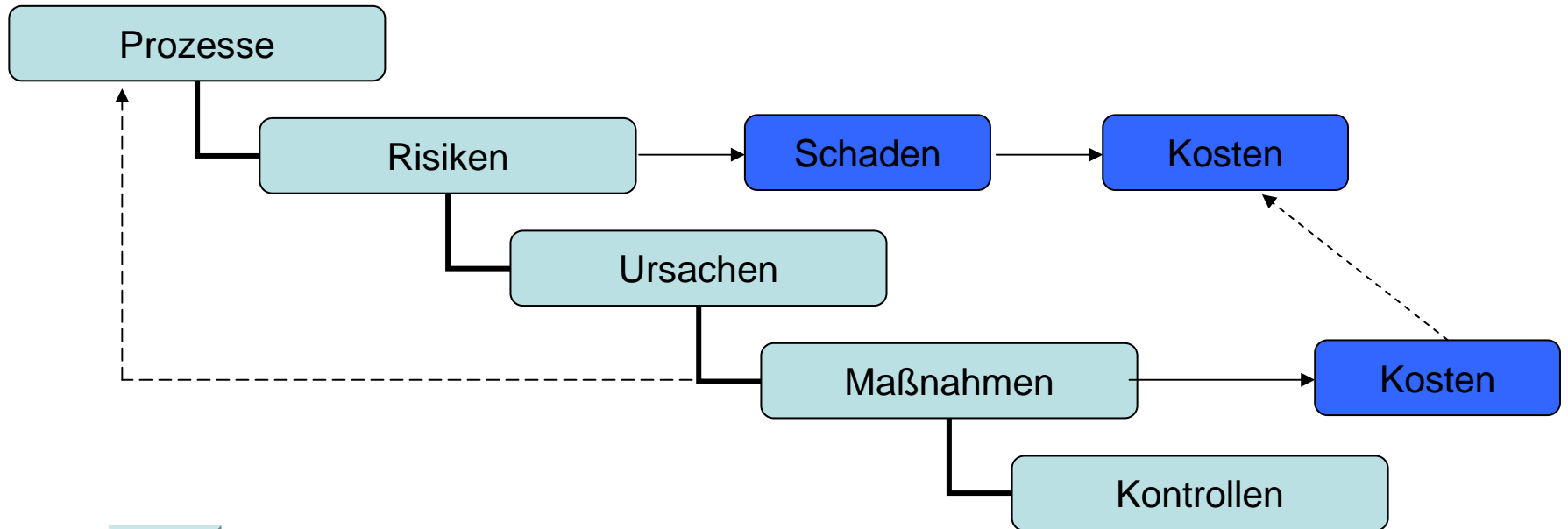


# Warum Generische IPM Prozess Modelle?

Paradigmen-Wechsel:

Nicht die Ursachen der Risiken werden primär beeinflusst

Es werden neue Prozesse mit verringerten Risiken modelliert

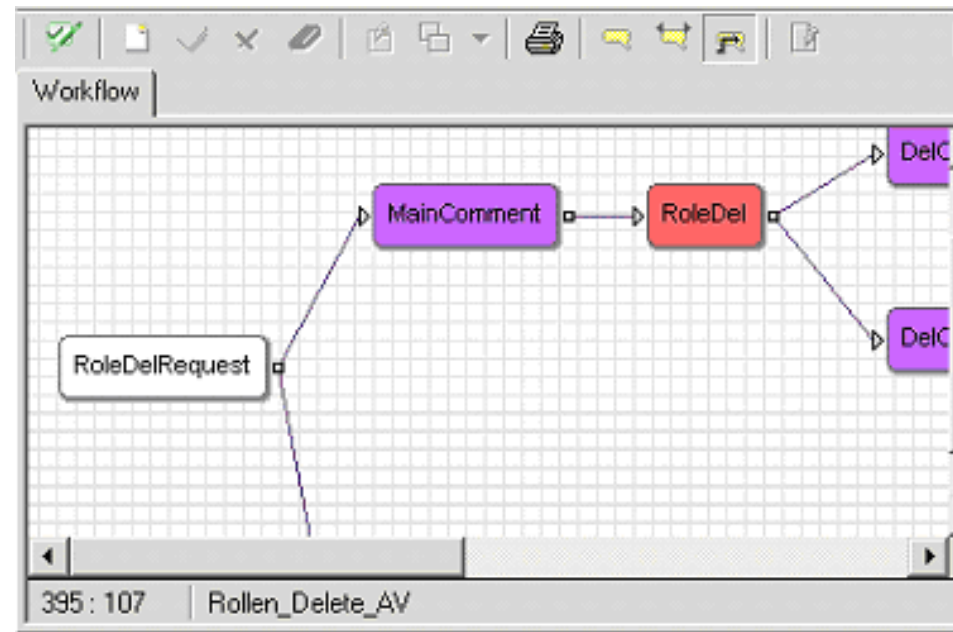


# Generische IPM Prozess Modelle

## Vordefinierte IPM Prozesse 1

Die IPM Prozesse setzen sich aus maschinellen Transaktionen und manuellen Aktionen zusammen.

Jeder automatische Prozess ist ein Beitrag zur Compliance !!!!



# Dynamik in Rollen und Teams

IPM-Systeme bergen die Gefahr der Starrheit in sich.  
Sie schränken die erforderliche Dynamik im User-  
und Berechtigungs-Management unzulässig ein!

- Temporäre interdisziplinäre Teams
- Projekte
- Stellvertreter
- Temporärer Aufgabenwechsel (Springer)
- Prozess für die Ausnahme !!!!



## Prozess-Gruppen

- Wechselprozesse des Users
- Antragverfahren
- Wiederholungsfreigaben
- Nebengelagerte Prozesse
- Serviceprozesse
- Interne Prozesse

Gegenstand der Arbeitsgruppe des NIFIS zu  
Standards von Generischen IPM Prozessen



## Wechselprozesse des Users

- Mitarbeiterereintritt
- Mitarbeiteraustritt
- Sofortiges Usersperren
- Wechselprozesse der User im Unternehmen
- Wiedereintritt in Konzernstrukturen
- User in sekundärer Organisationseinheit (OE)  
(Shadow-User)



## Antrags- und Provisioning-Verfahren 1

- Automatische regelbasierte Rollenzuteilung
- Antragsverfahren Rollen
  - Erhalt / Zuteilung einer Rolle
  - Entzug einer Rolle
- Antragsverfahren System (System mit Berechtigungen)
- Antrag für allgemeine Applikationen ohne Strukturierung der Berechtigungen
- Richtlinienabhängiges Provisioning



## Antrags- und Provisioning-Verfahren 2

- dokumentenbasierter Antrags-Prozess
- Antragsverfahren Vertretung
- Antragsverfahren Team/Projektrollen
  
- Signatur-Management in Verbindung mit PKI
- Allgemeiner Berechtigungs-Antrag



## Wiederholungsfreigaben

- Re-Validierung (regelmäßige Bestätigung der User, die nicht mit HR gesteuert werden und deren Status)
- Re-Lizensierung (regelmäßige Bestätigung einer bereits erteilten Lizenz)
- Re-Zertifizierung (regelmäßige Bestätigung eines bereits erteilten Nutzungsrechts)
- Nach-Zertifizierung (Einbeziehung der bestehenden Alt-Berechtigungen in die Zertifizierung)



## Interne Prozesse

- Antrag für neue Rollen
- Antrag für Rollen-Änderung
  - technische Attribute
  - Berechtigungsattribute
- Antrag für allg. Modellierungsänderungen



- **Serviceprozesse**

- Password  
Self-Service



- Allgemeine Supportanfrage an NBV  
(Nutzer- u. Berechtigungsverwaltung)



## Nebengelagerte Prozesse

- Antrag auf einen Arbeitsplatz bzw. Änderung der Arbeitsplatzausstattung
- Rollenbasierter Antrag auf eine Zutrittsberechtigung
- Antrag zur Abwesenheit bzw. Urlaub  
(Notwendig für Task-Manager)



# Reporting / IKS

Analyse-Ziel	Adressaten				
	IR / WP	Security	IT-Controlling	BO / Data Warehouse	sonstige
Statistik			x	x	
Leistungskennziffer/ Menge			x		SLA
Leistungskennziffer/ Transaktionszeit			x		SLA
Lizenzauslastung			x		Finanzen/ Einkauf
Aktuelle Userberechtigungen	x				
Security-lastige Einzelvorgänge	x	x			SOX
Admins / System	x	x	x		SOX
Admins/ kritische Applikationen	x	x			SOX
Freie Analyse SQL	x		x	x	
Nachvollziehbarkeit Berechtigungsdaten	x	x			
Nachvollziehbarkeit Genehmigungen	x	x		x	
Nachvollziehbarkeit Userdaten	x			x	

# IKS / Internes IPM-Kontroll-System

Das IKS basiert auf folgenden Komponenten:

- Distributives Betriebskonzept
- Security-Richtlinien für Systemkonfiguration
- Gesicherte Authentifikation für Power-User (z-B. Admins)
- **Security-Classification aller Objekte und Attribute**
- online Watchdog für auffällige Vorgänge (Regelverarbeitender Software-Agent)
- Weiterleitung und Vier-Augen-Prinzip
- Info-Eskalations-System zu besonderen Aktionen
- konfigurierter Reportgenerator



# IKS / Internes IPM-Kontroll-System

- Mit dem IKS wird eine systeminterne Überwachung der Einhaltung der Sicherheitsrichtlinien über **alle Berechtigungs-Systeme** erreicht.
- Das Security-Niveau ist abhängig von der Funktion des Systems in drei Standard-Stufen (Modellierung, Test, Produktion) einstellbar.
- Die Richtlinien können vom Kunden variiert werden. Bei Veränderungen der Richtlinien des Produktiv-Systems erlischt das vom **iSM gewährte Compliance Zertifikat**.



# IKS / Internes IPM-Kontroll-System

Kritische Systeme

Kritische Rollen

User mit hoher  
Security-Klasse

User mit kritischen  
Systemen

User mit  
kritischen Rollen

Alle kritischen  
Systemzuweisungen

Alle kritischen  
Rollenzuweisungen

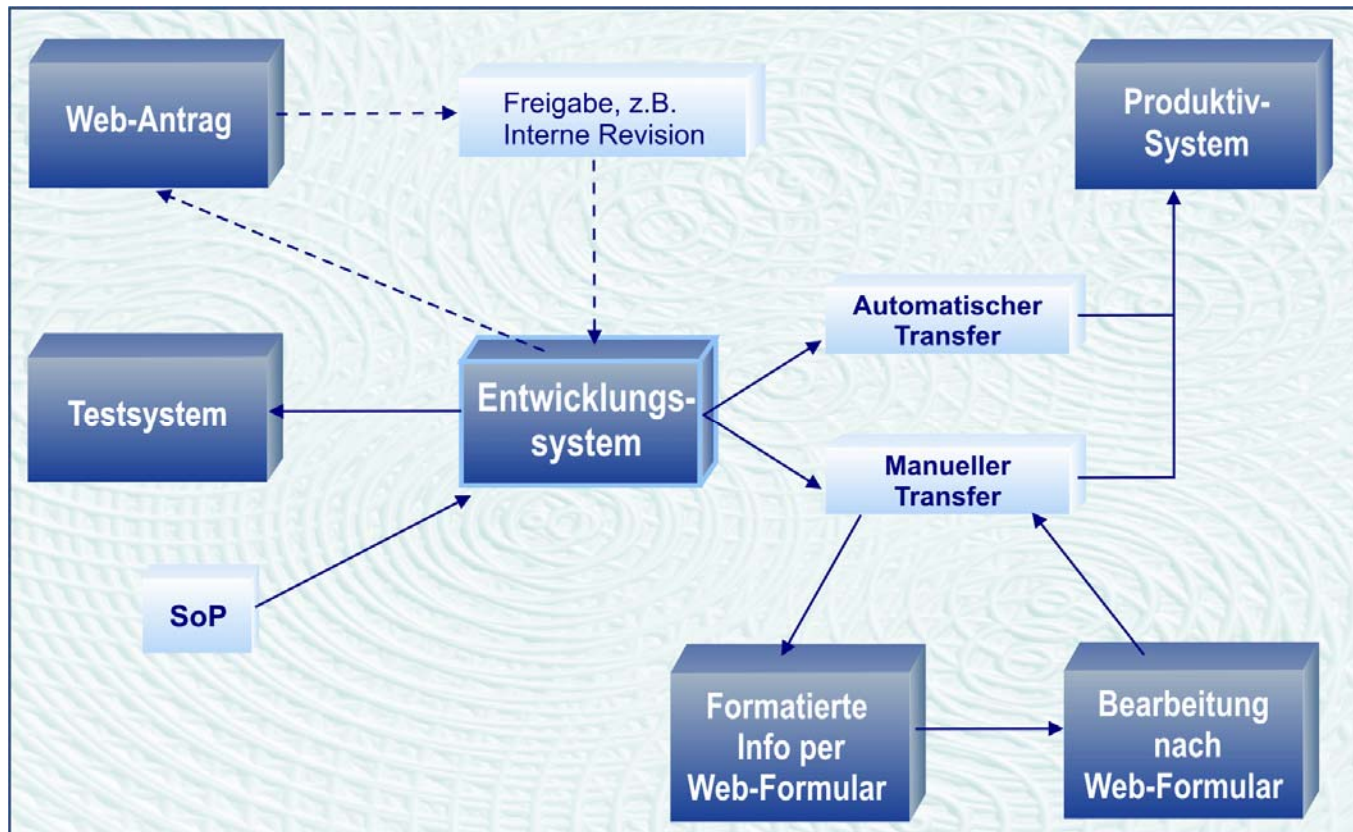
csv-Export

User	Rolle
Mathias (Secret)	Team-Leiter PZV (Secret)
Mario (Restricted)	Team-Leiter PZV (Secret)
Lothar (Restricted)	Team-Leiter PZV (Secret)
Susanne (Top Secret)	Team-Leiter PZV (Secret)
Steffen (Restricted)	Team-Leiter PZV (Secret)
Lars (Secret)	Team-Leiter PZV (Secret)



# IKS / Internes IPM-Kontroll-System

Das gesicherte IPM- Betriebskonzept trennt die Modellierung von dem Produktiv-System und fügt eine „freigebende Instanz“ ein, die bestimmte Modellierungen freigibt, bevor diese produktiv wirksam werden Kern dieser Struktur ist das Entwicklungssystem.



## IKS – Frühwarnsystem

### Security-lastige Einzelvorgänge

- Direkte Zuweisung von Systemen mit Security Classification SC > 3
- Versuch die Regeln der Security Classification zu umgehen

### Auffällige Koinzidenzen

- User mit hoher Zahl kritischer Systeme / Rollen (SC > 3)
- Admin, mit Vergabeberechtigung kritischer Objekte (System oder Rolle) und eigener Berechtigung an diesem Objekt.
- Nur kurzzeitige Berechtigungen an kritischen Objekten
- Bestimmte dynamische Prozesse (Nutzungsrate kritischer Applikationen) lassen sich mit Hilfe der SSO-Events ermitteln.

### Risikoreiche Tendenzen

- Häufige direkte Zuordnung kritischer Objekte (SC > 3)



# Differenz-Check

Zentrale IPM-Systeme bilden die Berechtigungen in den Zielsystemen ab.


In den Zielsystemen kann aber trotz organisatorischer Regelungen administriert werden, so dass es zu Differenzen kommt.

Diff-Checker decken dies auf und sollen folgende Strategien möglich machen:

- Jede Nacht wird top-down abgeglichen
- Über ein Protokoll wird differenziert abgeglichen
- Ein Wizard steuert die Abgleichlogik im Dialog



# IPM Life-Cycle eines Users

 Filter Daten anzeigen | csv-Export

Hinweis:

Nutzen Sie die Filter um die Anzeige Daten einzuschränken. Was Sie im Filter Operation eingeben können erfahren Sie, wenn Sie mit der Maus über das Infosymbol fahren. Um den Filter auszulösen klicken Sie bitte auf "GO" oder Drücken Sie die Enter-Taste.

Operation Alle von (Format Jahr: jjjj) . . bis (Format Jahr: jjjj) 23 . März . 2007  mit System-Attributänderung

Anzahl Datensätze: 19

Datum↑↓	Operation↑↓	Bearbeiter↑↓	System/Rolle/Modell↑↓	Zusatz↑↓	Daten↑↓	Daten alt↑↓
09.12.2005	Urlaubsantrag	Meier, Karin	ZUM	VAC_ID	1	20007
09.12.2005	Workflow gestartet	Schmidt, Peter	Urlaub_AV		23.12.2005;23.12.2005	
12.12.2005	Urlaubsantrag	Meier, Karin	ZUM	VAC_ID	6	20007
12.12.2005	Workflow gestartet	Schmidt, Peter	Urlaub_AV		02.01.2006;09.01.2006	
13.02.2006	Urlaubsantrag	<b>Neumann, Ralf</b>	ZUM	VAC_ID	1	20007,20002
13.02.2006	Urlaubsantrag	<b>Neumann, Ralf</b>	ZUM	VAC_ID	5	20007,20002
13.02.2006	Urlaubsantrag	<b>Neumann, Ralf</b>	ZUM	VAC_ID	1	20007,20002
13.02.2006	Workflow gestartet	Schmidt, Peter	Urlaub_AV		26.05.2006;26.05.2006	



# Erreichbarer Nutzen und Effekte

## **direkter Nutzen**

Wesentliche Reduzierung des Aufwandes in der Administration  
Verringerung des Gefährdungspotentials

## **Prozess- Nutzen**

Geordnete bzw. verbesserte Geschäftsprozesse  
Automatisierung der IPM-Prozesse erhöht die Security

## **Compliance und IKS (USP)**

durchgängige Nachvollziehbarkeit aller Aktionen und interne  
Überwachung des Systems

## **Synergetischer Nutzen**

Je mehr einzelne Komponenten im Rahmen eines Gesamtkonzeptes  
„zusammenspielen“, um so geringer ist der Aufwand zur Implementierung  
der einzelnen Komponenten

## **Nutzen neuer Funktionalität**

Die neue Lösung ermöglicht Funktionen, die vorher nicht zu realisieren  
waren



- Nachvollziehbarkeit aller Prozesse (SOX Support)
- Keine Berechtigungs-“Leichen“
- Nur aufgabenbezogene Berechtigungen
- Erhöhte Sicherheit im Access-Management
- Integration von PKI inkl. Verwaltung der Prozesse
- Integration von Sub-Directories, damit überall gleiche Berechtigungs-Regeln
- Gutes Rating im Risk-Management (KONTRAG, SOX u. Basel II)
- Erhöhte Benutzersicherheit (keine mehrfachen Passworte usw.)





Besuchen Sie  
das iSM im Internet:

[www. Secu-Sys .de](http://www.Secu-Sys.de)

[www. \*bi\*-Cube .de](http://www.bi-Cube.de)