



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

Generische Prozess-Modelle und Compliance

Prof. Dr. Dr. Gerd Rossa
CEO

Anforderungen an die Compliance werden vor allem durch generische Prozess-Modelle erfüllt

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

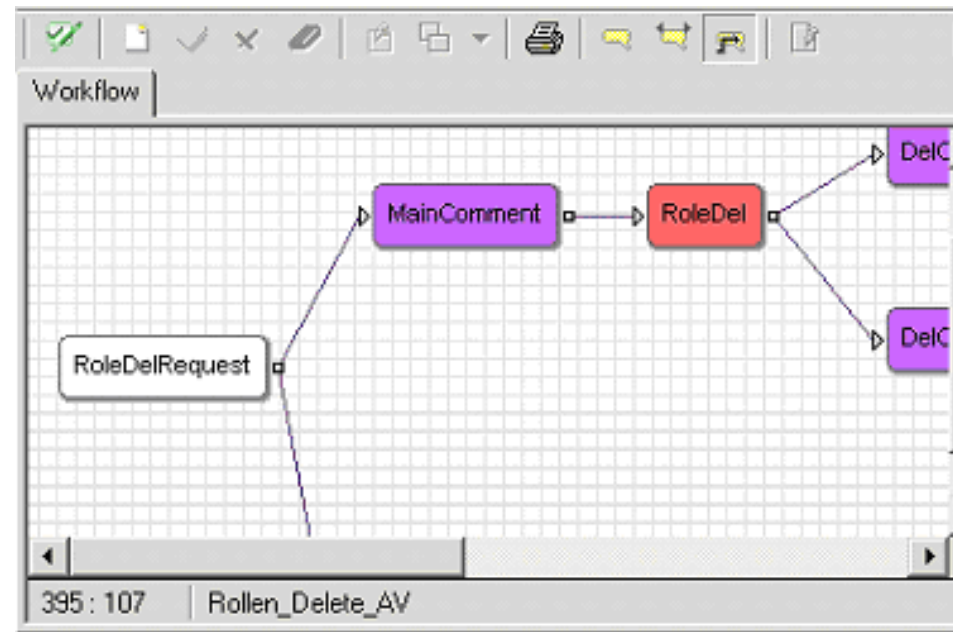


Generische IPM* Prozess-Modelle

Vordefinierte IPM-Prozesse 1

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

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

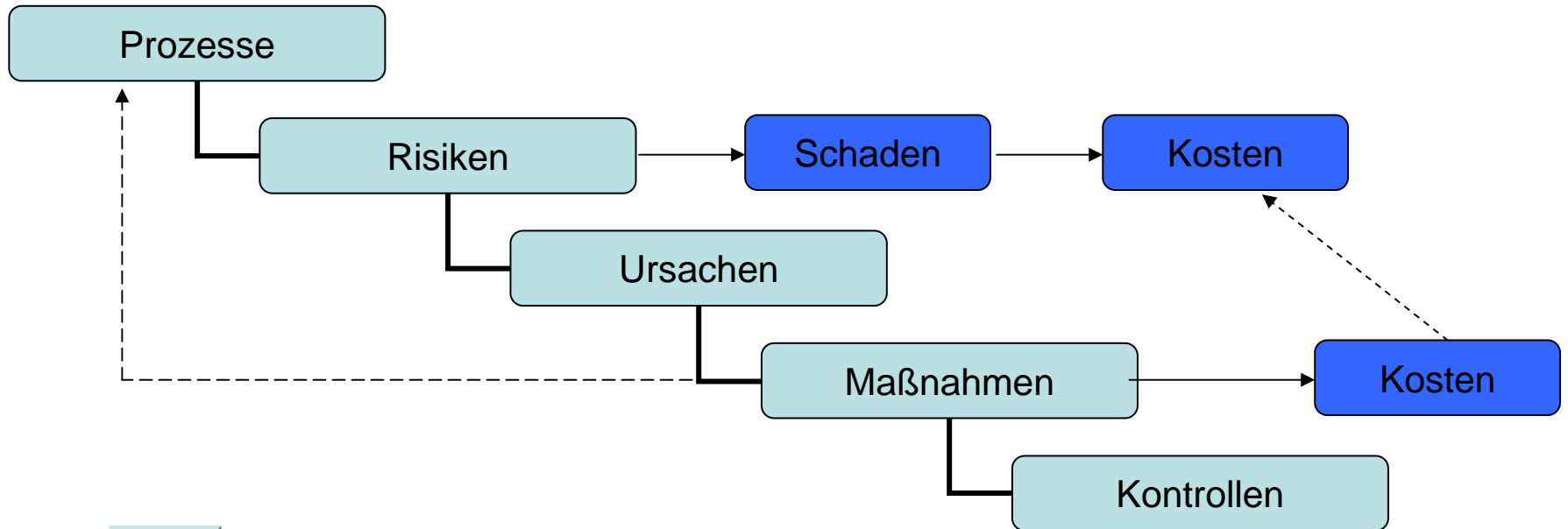


Warum Generische IPM Prozess-Modelle?

Paradigmen-Wechsel:

Nicht die Ursachen der Risiken werden primär beeinflusst

Es werden neue Prozesse mit verringerten Risiken modelliert



Prozess-Gruppen

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

Gegenstand der Arbeitsgruppe der 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)



- **Antrags- und Provisioning-Verfahren**
 - Antragsverfahren Rollen
 - Automatische regelbasierte Rollenzuteilung
 - Richtlinienabhängiges Provisioning
 - Allgemeiner dokumentenbasierter Antrags-Prozess
 - Antrag für allgemeine Applikationen ohne Strukturierung der Berechtigungen
 - Signatur-Management in Verbindung mit PKI



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



Generische IPM Prozess-Modelle

- **Serviceprozesse**

- Password
Self-Service



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



- **Interne IPM-Prozesse**

- Antrag für neue Rollen
- Antrag für Rollenänderung
- Antrag für Modellierungsänderungen
- Freigaben im gesicherten Betriebskonzept
- Analytische Rollenmodellierung



Problembereiche bei SoP – Prozessen

Bei den SoP- Prozessen sind komplexe Zusammenhänge zu beachten:

- **Gleitende Übergänge / Wechselprozesse**
Bei einer Rollenänderung (z.B. durch OE-Wechsel) können die Berechtigungen nicht schlagartig wechseln (Vor- und Nachlaufzeiten u.a. konfigurierbare Regeln)
- **Wiedereintritt in Konzernstrukturen**
- **Transaktionsmanagement**
Transaktionen, die durch Attributänderungen getriggert werden, müssen bestimmte Änderungen so lange blockieren, bis die Transaktion beendet ist



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)



Reporting / IKS

Adressaten	IR / WP	<u>Security</u>	<u>IT-Controlling</u>	<u>BO / Data Warehouse</u>	sonstige
Analyse-Ziel					
Statistik			x	x	
<u>Leistung-KZ / Menge</u>			x		SLA
<u>Leistung-KZ / Transaktionszeit</u>					SLA
Lizenzauslastung			x		Finanzen
Aktuelle Userberechtigungen					
<u>Security-lastige Einzelvorgänge</u>	x	x			SOX
<u>Admins / System</u>	x	x	x		SOX
<u>Admins/ kritische Applikationen</u>	x	x			SOX
Freie Analyse	x	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 SW-Agent)
- Weiterleitung und Vier-Augen-Prinzip
- Info-Eskalations-System zu besonderen Aktionen
- konfigurierter Reportgenerator



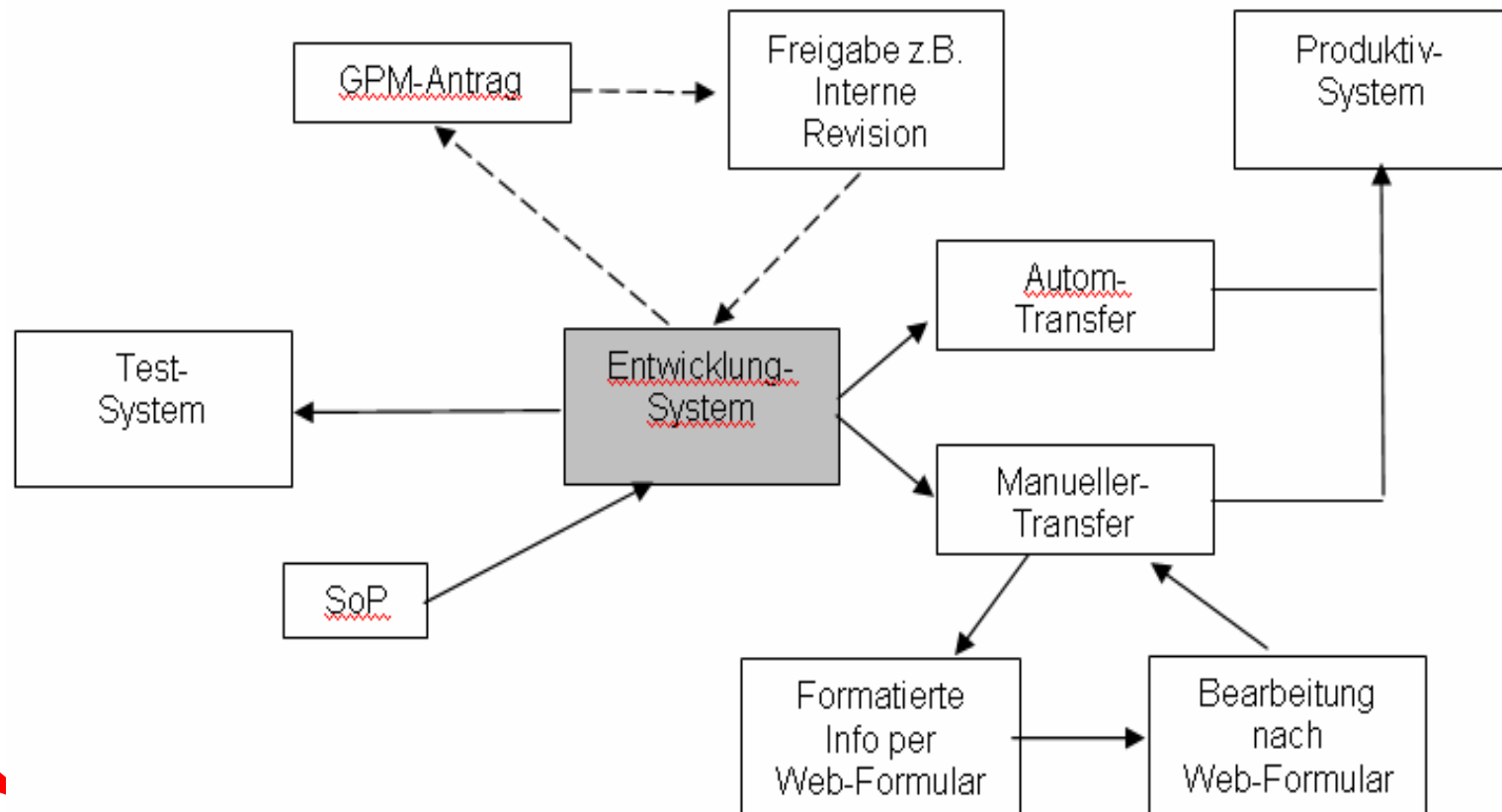
IKS / Internes IPM Kontroll System

- 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

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)





Besuchen Sie
das iSM im Internet:

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

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