

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



Compliance im Umfeld von Identity- und Provisioning- Management

Prof. Dr. Dr. Gerd Rossa
CEO

Architektur - Anforderungen

Anforderungen an die Compliance

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



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

Kritische Systeme

Kritische Rollen

User mit hoher
Security-Klasse

User mit kritischen
Systemen

User mit
kritischen Rollen

Alle kritischen
Systemzuweisungen

Alle kritischen
Rollenzuweisungen

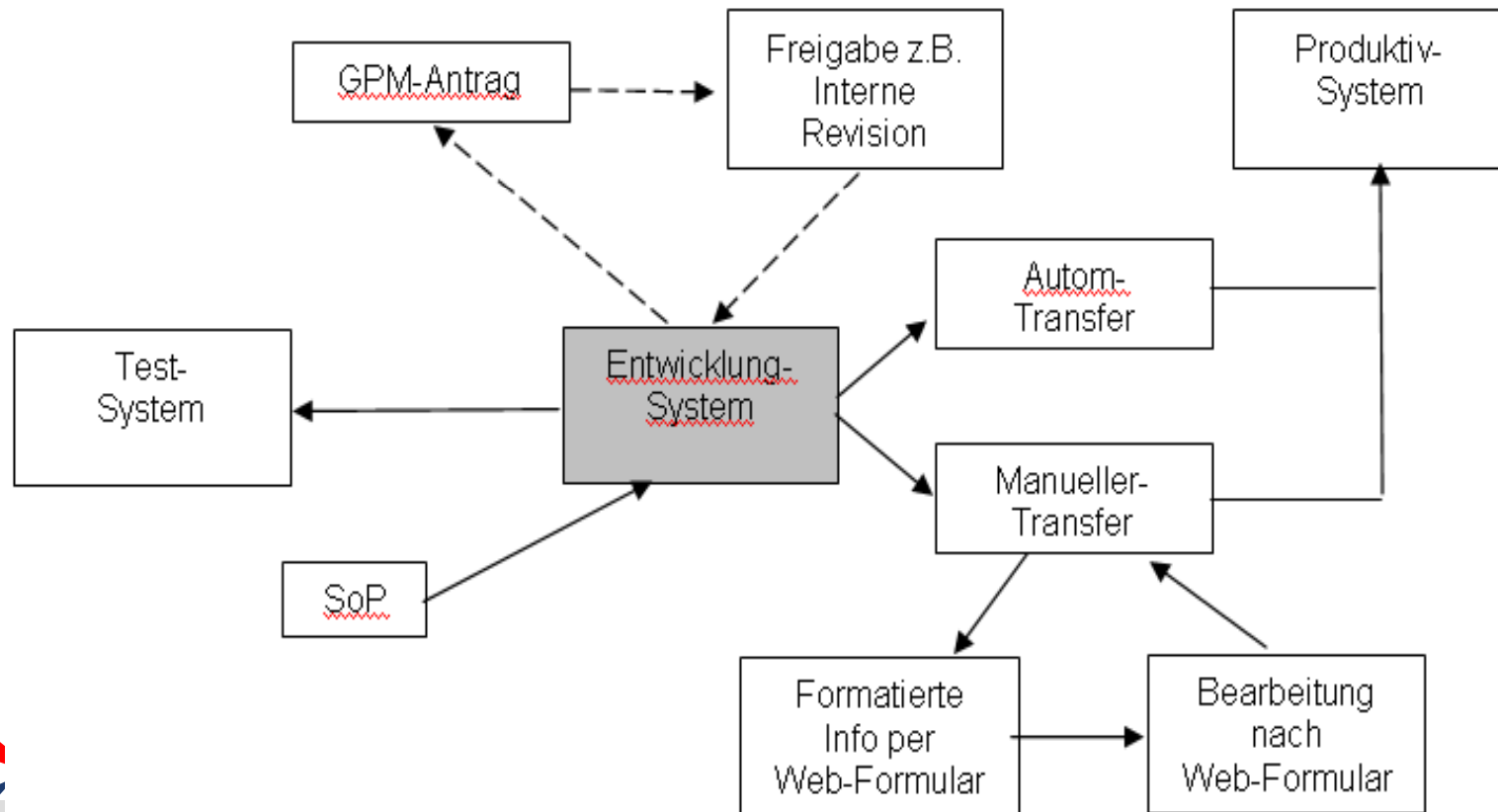
csv-Export

User	Rolle
Ohlerich, Mathias (Secret)	Team-Leiter PZV (Secret)
Göring, Mario (Restricted)	Team-Leiter PZV (Secret)
Hahn, Lothar (Restricted)	Team-Leiter PZV (Secret)
Dahmen, Susanne (Top Secret)	Team-Leiter PZV (Secret)
Wegner, Steffen (Restricted)	Team-Leiter PZV (Secret)
Hansen, Lars (Secret)	Team-Leiter PZV (Secret)



IKS / Internes IPM-Kontroll-System

Das sog. 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 / Internes IPM-Kontroll-System

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-Cicle eines Users

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:
 von (Format Jahr: jiji):
 bis (Format Jahr: jiji):

 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	2007
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	2007
12.12.2005	Workflow gestartet	Schmidt, Peter	Urlaub_AV		02.01.2006;09.01.2006	
13.02.2006	Urlaubsantrag	Görz, Holger	ZUM	VAC_ID	1	2007,2002
13.02.2006	Urlaubsantrag	Görz, Holger	ZUM	VAC_ID	5	2007,2002
13.02.2006	Urlaubsantrag	Görz, Holger	ZUM	VAC_ID	1	2007,2002
13.02.2006	Workflow gestartet	Schmidt, Peter	Urlaub_AV		26.05.2006;26.05.2006	





Besuchen Sie
das iSM im Internet:

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

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