



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

Role modeling, generic process models and compliance

Prof. Dr. Dr. Gerd Rossa
CEO

Maturity of a company for an IPM solution

IPM cannot administrate an organizational chaos!!!

- Enterprise strategy and project positioning have to go together
- Architecture comprehension
- Status of an organization
- Comprehension of modeling
- realizable modeling of procedures

For this purpose a checklist is provided!



Role model and SoP (Self-organizing Provisioning)

Principles

A role model has to exist regularly next to the direct permission management

The „soft“ migration from the direct permission management to the role model is realized by definite rules/ e.g. a role based permission overwrites a direct system allocation

Attribute and object references enable a clearly arranged role model

Analytic procedures support the synthesized role modeling (cluster analysis of existing permissions and skill management)



Role model and SoP

(Self-organizing Provisioning)

Role modeling

- Organizational roles, technical roles and system roles
- Restriction roles (for restriction of admins)
- Dynamic system roles with access controls
- Role references (simplified role modeling)
- synthesized technical and system roles
- Security classification of roles (internal control and monitoring system = ICS)
- Set operations on roles
- Client and team roles
- Failure-free migration ability from direct to role-based assignment of permissions
- Primary account



Problem areas of SoP processes

For the SoP Processes the following complex correlations have to be considered:

Role conflicts

Assembly and separating of system permissions, which are assigned to the user from different roles

Basic rule: Role system overwrites direct assignments / soft migration from system model to role model

Role updates

In case of changes of roles these have to be „extruded“ for the already assigned roles

Attribute indicated roles

Basic for the automation of IPM processes

Role references

Basic roles are connected with special roles and assigned automatically



Problem areas of SoP processes

Consideration of complex correlations:

- **Floating transitions / change processes**
In case of role changing (e.g. because of changing the organizational unit) the permissions cannot change abruptly
- **Re-entrance in corporate group structures**
- **Transaction management**
Transactions, which are triggered because of attribute changes, have to block certain changes as long as the transaction has finished.
- **OU-Competences**
Second dimension of the permission: views within the company structures



Roles and teams (project organization) (USP)

Intention:

- Assignment of permissions to defined temporary groups of users
- Centralized modeling, decentralized provisioning

Rules:

- The team is provided with a date of beginning and date of expiration.
- Team members are allocated to a position (team leader, deputy...).
- The team leader requires the users for his team, assigns permissions and controls the duration for the teams. Users receive the team role by entering the team and/or they lose the roles by leaving the team.



Compliance requirements

Requirements to the compliance are met by generic process models (GPM)

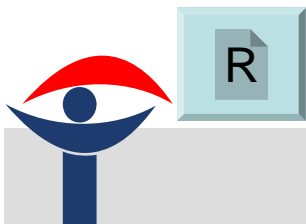
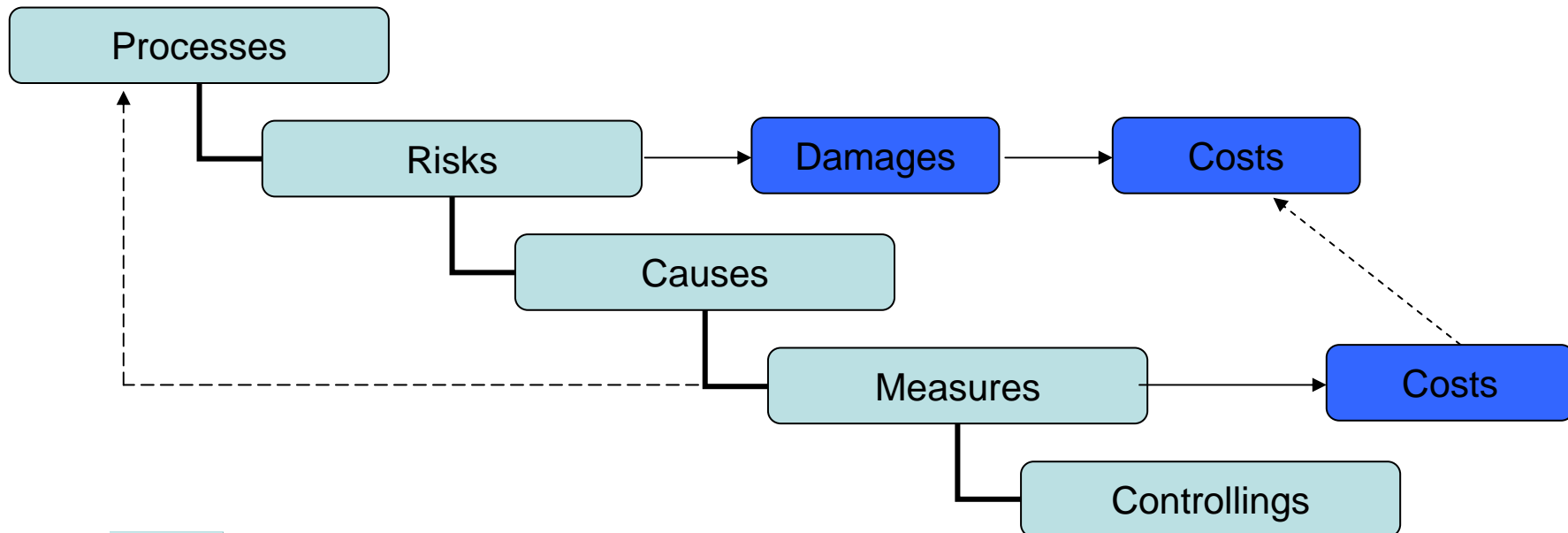
- Traceability (SOX, KONTRAG, Basel II)
- 2-step revision model
- Live cycle of a user
- Internal control and monitoring system (ICS)
- Secured operational concept
- intrinsic safety of the IPM system



Why generic IPM process models?

Change of paradigm:

Not the causes of risks are influenced primarily. There are modeled new processes with reduced risk.

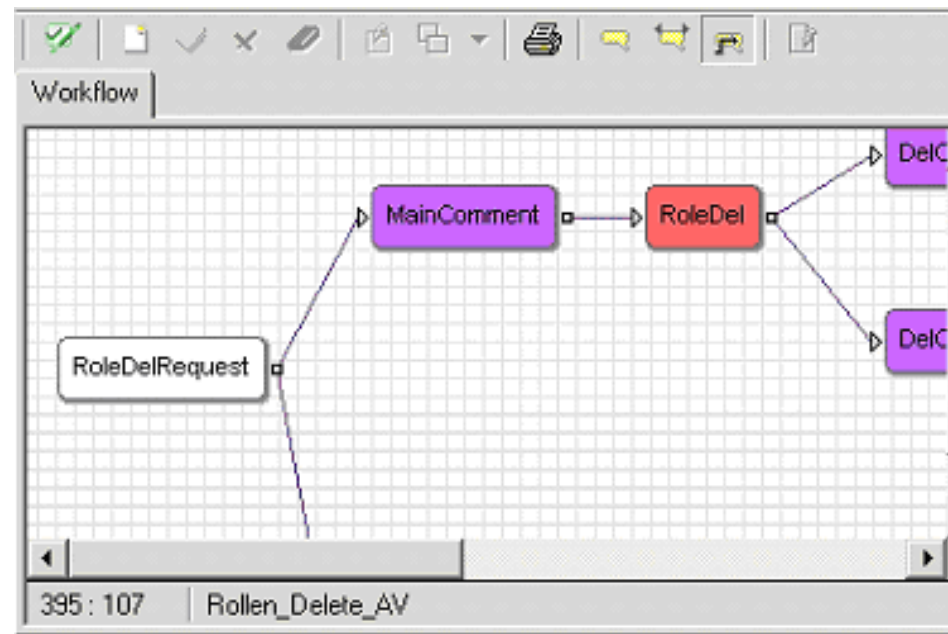


Generic IPM process models

Predefined IPM processes 1

The IPM processes are composed of automatic transactions and manual actions.

Every automatic process is a compliance contribution!!!!



Dynamics within roles and teams

IPM systems hold the danger of rigidity

They restrict the necessary dynamic of the user and permission management unduly!

- Temporarily interdisciplinary teams
- Projects
- Deputies
- Temporary change of tasks (stand-by-man)
- Process for exceptions!!!



Generic IPM process models

Process-Groups

- Changing processes of users
- Request procedure
- Release of repetitions
- Beside processes
- Service processes
- Internal processes

Item of the working group of NIFIS for standards of generic IPM processes



Generic IPM process models

Changing processes of the user

- New employee
- Leaving employee
- Immediate user locking
- Changing processes of users in the company
- Re-entry in corporate group structures
- User in secondary organizational units (OU) (shadow user)



Generic IPM process models

Request and provisioning procedure 1

- Automated rule based assignment of roles
- Request procedure roles
 - Receipt / assignment of a role
 - Removal of a role
- Request procedure system (system with permissions)
- Request for general applications without structures within permissions
- Provisioning dependent on guidelines



Generic IPM process models

Request and provisioning procedure 2

- Request process based on documents
- Request procedure deputy
- Request procedure team/project roles

- Signature management in conjunction with PKI
- General request of permission



Generic IPM process models

Releases of repetition

- Re-validation (regular confirmation of users, which are not controlled by HR and their status)
- Re-licensing (regular confirmation of an already granted license)
- Re-certification (regular confirmation of an already assigned right of use)
- after-certification (involvement of the existing old-permissions into the certification)



Generic IPM process models

Internal Processes

- Request for new roles
- Request for role changes
 - technical attributes
 - permission attributes
- Request for general changes of modeling



Generic IPM process models

- **Service processes**

- Password self-service



- General support request for AUP
(administration of users and permissions)



Generic IPM process models

Beside processes

- Request for working station and/or changing the working equipment
- Role based request for entrance permissions
- Request for absence or holiday (necessary for the Task Manager)



Reporting / IKS

Target of Analysis	Recipients				
	IR / WP	Security	ICT-controlling	BO / data warehouse	Others
Statistic			x	x	
Performance index / amount			x		SLA
Performance index / transaction time			x		SLA
License utilization			x		Finances/ purchase
Current user permissions	x				
Security dominant events	x	x			SOX
Admins / system	x	x	x		SOX
Admins/ critical applications	x	x			SOX
Free analysis SQL	x		x	x	
Traceability of permission data	x	x			
Traceability of authorizations	x	x		x	
Traceability of user data	x			x	

ICS / Internal IPM control and monitoring system

The ICS is based on the following components:

- Distributive operating concept
- Security guidelines for system configuration
- Secured authentication for power user (e.g. admin)
- **Security classification for all objects and attributes**
- online Watchdog for suspicious events (rule processing software agent)
- Forwarding and „four-eyes-principle“
- Info-escalation-system for special actions
- Configured report generator



ICS / Internal IPM control and monitoring system

- The ICS enables an internal monitoring of the adherence of security guidelines **for all permission systems.**
- The security level dependent on the function of the system can be set by three default steps (modeling, test, production)
- The guidelines can be varied by the customer. If there are any changes of guidelines in the productive system the **compliance certification granted by iSM** will expire.



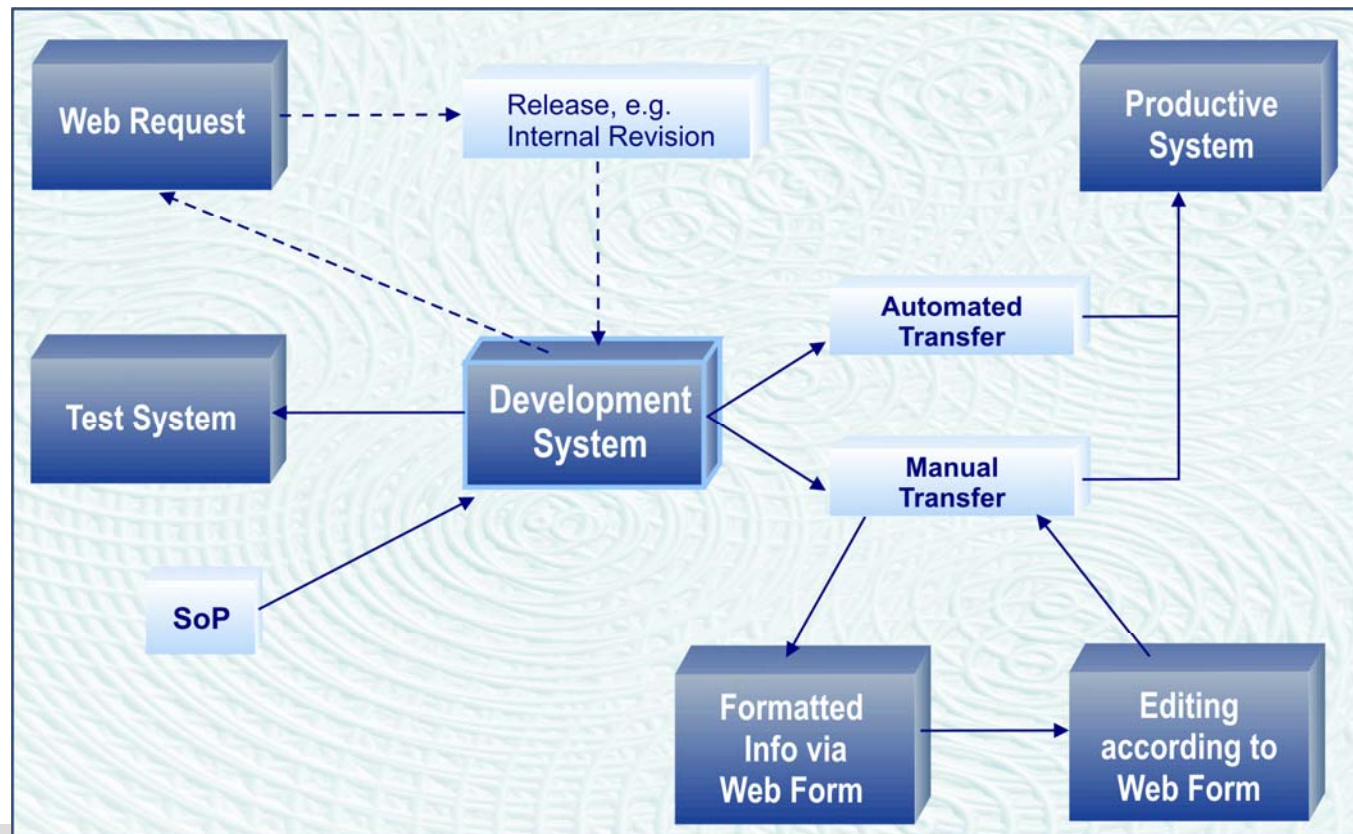
ICS / Internal IPM control and monitoring system

Critical systems	<div data-bbox="909 435 1234 512" style="border: 1px solid black; padding: 2px; display: inline-block;">csv-Export</div> <table border="1"><thead><tr><th>User</th><th>Role</th></tr></thead><tbody><tr><td>Muster, Max (Secret)</td><td>Teamleader (Secret)</td></tr><tr><td>Lauda, Olaf (Restricted)</td><td>Teamleader (Secret)</td></tr><tr><td>Pause, Anna (Restricted)</td><td>Teamleader (Secret)</td></tr><tr><td>Onario, Marc (Secret)</td><td>Teamleader (Secret)</td></tr><tr><td>Loba, Susan (Secret)</td><td>Teamleader (Secret)</td></tr><tr><td>Glunta, Lars (Top Secret)</td><td>Teamleader (Secret)</td></tr><tr><td>Erona, Katrin (Secret)</td><td>Teamleader (Secret)</td></tr><tr><td>Antoga, Holm (Top Secret)</td><td>Teamleader (Secret)</td></tr><tr><td>Lund, Marketa (Secret)</td><td>Teamleader (Secret)</td></tr><tr><td>Alboga, Jaroslav (Secret)</td><td>Teamleader (Secret)</td></tr></tbody></table>	User	Role	Muster, Max (Secret)	Teamleader (Secret)	Lauda, Olaf (Restricted)	Teamleader (Secret)	Pause, Anna (Restricted)	Teamleader (Secret)	Onario, Marc (Secret)	Teamleader (Secret)	Loba, Susan (Secret)	Teamleader (Secret)	Glunta, Lars (Top Secret)	Teamleader (Secret)	Erona, Katrin (Secret)	Teamleader (Secret)	Antoga, Holm (Top Secret)	Teamleader (Secret)	Lund, Marketa (Secret)	Teamleader (Secret)	Alboga, Jaroslav (Secret)	Teamleader (Secret)
User		Role																					
Muster, Max (Secret)		Teamleader (Secret)																					
Lauda, Olaf (Restricted)		Teamleader (Secret)																					
Pause, Anna (Restricted)		Teamleader (Secret)																					
Onario, Marc (Secret)		Teamleader (Secret)																					
Loba, Susan (Secret)		Teamleader (Secret)																					
Glunta, Lars (Top Secret)		Teamleader (Secret)																					
Erona, Katrin (Secret)		Teamleader (Secret)																					
Antoga, Holm (Top Secret)		Teamleader (Secret)																					
Lund, Marketa (Secret)	Teamleader (Secret)																						
Alboga, Jaroslav (Secret)	Teamleader (Secret)																						
Critical roles																							
User with a high security class																							
User with critical systems																							
User with critical roles																							
All critical system assignments																							
Critical role assignments																							



ICS / Internal IPM control and monitoring system

The secured IPM operating concept separates the modeling from the productive system. It adds a “releasing instance“, which releases certain modelings before these can work in the productive environment. The core of this structure is the development system.



ICS / Internal IPM control and monitoring system

ICS – early warning system

Security-dominant events

- Direct assignment of systems with security classification $SC > 3$
- Try to avoid the rules of security classifications

Conspicuous coincidences

- Users having a high number of critical systems/ roles ($SC > 3$)
- Admins, having permission of assignment of critical objects (system or role) and own permission for this object.
- Only short-term permissions for critical objects
- Certain dynamic processes (rate of use for critical applications) can be detected by means of SSO events.

Risky tendencies

- Frequently direct allocation of critical objects ($SC > 3$)



Difference Check

Centralized IPM systems reproduce the permissions in the target systems.

There can be also administration within the target systems in spite of organizational rules, so that there can appear some differences.

„Diff-Checker“ detecting such differences should enable the following

- Every night there will be a top-down synchronization
- Via protocol the synchronization is done differentially
- Wizard controls the logic of synchronization in the dialog



IPM Life-Cicle of a user


selected point of menu: **LifeCycle (as User)**

1. User search

2. User select

3. **LifeCycle (as User)**

User: Max Thunder (Verwid: 17008, Organisational Unit: Administration)

 Filter |

Hint:

Please use the filter to show only a part of the filter. For further information please move the cursor over the information symbol in the upper left corner of the filter. To start the filter please use e go-button or use ENTER on your keyboard.

operation from (format year: yyyy) with system attribute changes

Number of data sets: 51

date↑↓	operation↑↓	editor↑↓	system/role/model↑↓	addition↑↓	data↑↓	data old↑↓
04/04/2007	vacation application	Helma, Udo	bi-Cube	VAC_ID	1	8461,20002,12345678
04/04/2007	vacation application	Helma, Udo	bi-Cube	VAC_ID	1	8461,20002,12345678
04/04/2007	vacation application	Helma, Udo	Database	read	2	8461,20002,12345678
04/04/2007	workflow started	Thunder, Max	vacation_Request		30.04.2007;30.04.2007	
04/04/2007	workflow started	Thunder, Max	vacation_Request		18.05.2007;18.05.2007	
04/04/2007	workflow started	Thunder, Max	vacation_Request		10.05.2007;11.05.2007	
04/05/2006	vacation application	Helma, Udo	bi-Cube	VAC_ID	1	8461,20002,12345678
04/05/2006	workflow started	Thunder, Max	vacation_Request		26.05.2006;26.05.2006	
04/11/2005	role new	Lorau, Alwin	S_OA1	SATZ_ID	1965	
04/11/2005	role new	Lorau, Alwin	P_OA2	SATZ_ID	1966	



Achievable benefits and effects

Direct benefit

Essential reduction of expenditure of administration
Reduction of potential for danger

Process benefit

Ordered and/or improved business processes
Automation of IPM processes increases security

Compliance und IKS (USP)

Consequent traceability of all actions and internal monitoring of the system

Synergetic benefit

The more the individual components collude in the scope of a master plan the lower the expenditure for implementing these individual components will be

Benefit of new function

The new solution enables functions, which were not able to be realized before.



- Traceability of all processes (SOX Support)
- No orphaned accounts
- Only permissions concerned to jobs
- Increased security within access management
- Integration of PKI incl. administration of processes
- Integration of sub-directories, consequently the same permission rules everywhere
- Good rating in risk management (KonTraG, SOX & Basel II)
- Increased security of use (no multiple passwords ...)



Procedure model for introducing IPM

Definition of targets and product evaluation

Proof of concept or pilot

Realization

A s-step concept concerning the realization ensures short benefit and space for the solution of open organizational and conceptual questions.

During phase 1 the core system with definite and indisputable function is realized.

During phase 2 the complex processes are realized.



Procedure model for introducing IPM

1. Phase (exemplary – duration 4 months)

Productive

- Installation of the core system with direct administration of users in the IPM, if the interface to HR (e.g. SAP) is not yet built.
- Synchronization of users in the AD
- Direct assignment of permissions first of all for the core systems of the enterprise
- Definition of some basic roles incl. their possibility of web request
- Use of the first process models (new employee, leaving employee, general request)
- Introduction SSO / authentication by biometrics at Windows workstations

Conceptual

- Formulation of a technical role concept
- Solution of divers organizational problems



Procedure model for introducing IPM

2. Phase (exemplary – duration 10 months)

Productive

- Synchronization with organizational processes
- Further functions in the AD
- Transfer of further systems to the provisioning
- Further roles and processes
- Introduction of internal cost accounting
- Introduction license management

Use of centrally available data and concepts for several systems e.g. development





Visit our Website!

www.secu-sys.com

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