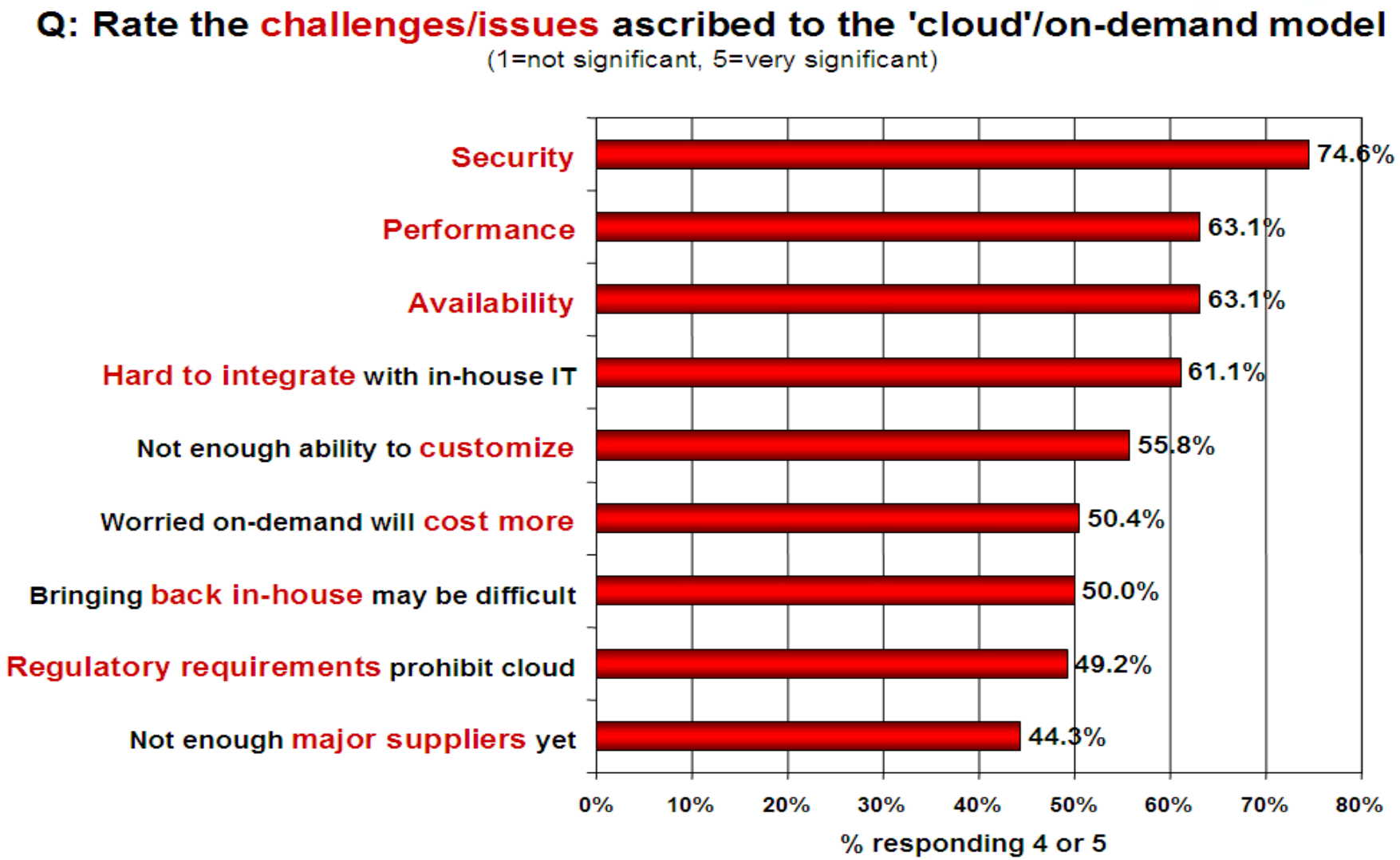
Security and Compliance in Clouds

Jan Jürjens, Kristian Beckers

Fraunhofer Institute for Software and Systems Engineering ISST (Dortmund, Germany)

http://jan.jurjens.de

Security is the Major Show-Stopper



Source: IDC Enterprise Panel, August 2008 n=244

GRC in Clouds

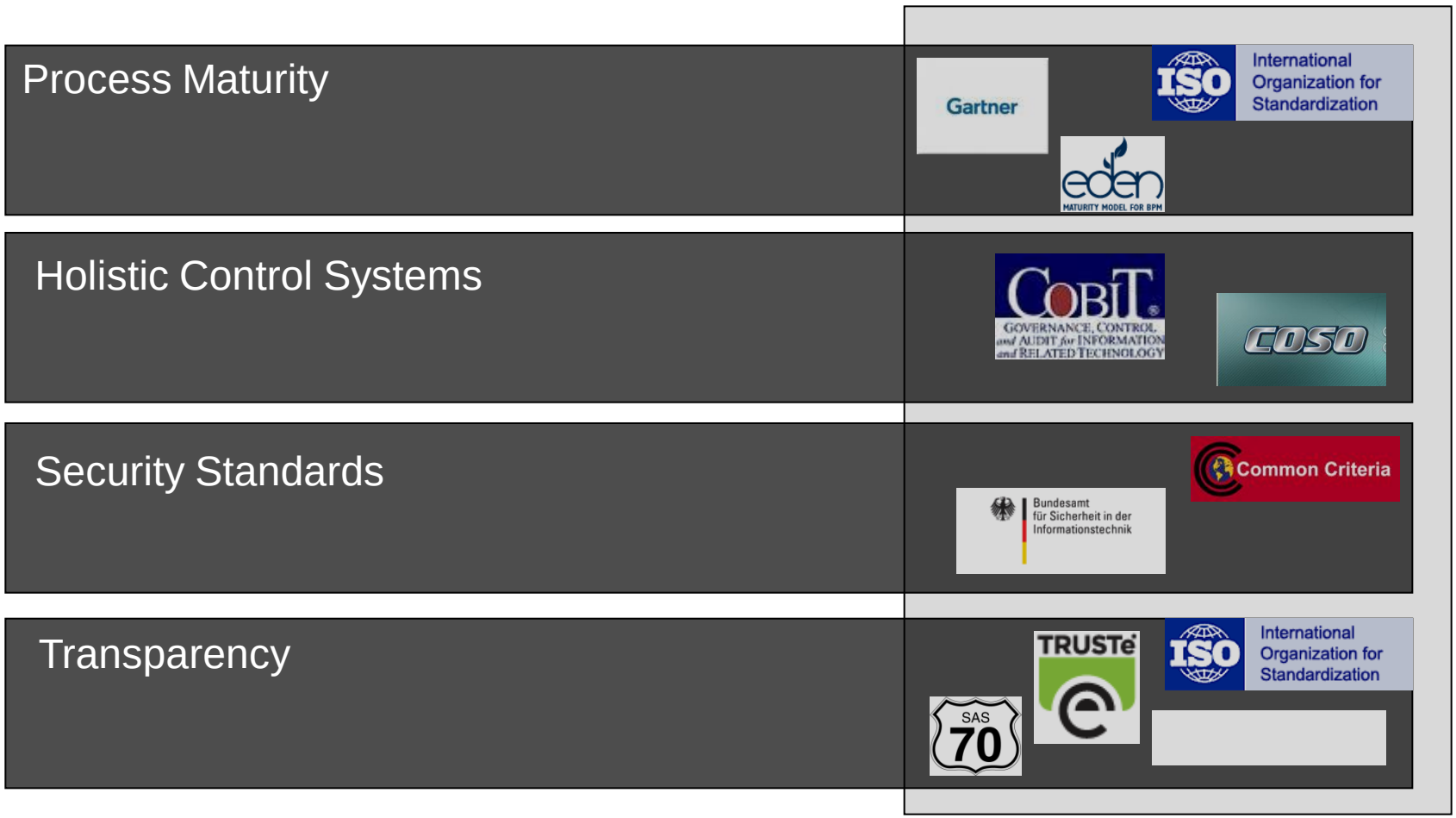
Governance	Risk	Compliance
■ Policy design ■ Classification schema for data and processes ■ Trust chain in a cloud	■ Risk strategy ■ Business Impact Analysis ■ Threat and Vulnerability Analysis ■ Risk Analysis Remediation	■ Policy enforcement ■ Legal compliance (SOX, SOLVENCY II) ■ Control implementation

The Cloud offers dynamic ressource allocation
→ For GRC in clouds we require the same dynamic

Compliance Scenarios

- **Customer -> Cloud:**
  - Security Compliance:
    - Check the security processes of the cloud for compliance with SLA
  - Legal Compliance:
    - Check the business process for SOX, MaRisk compliance
- **Cloud -> Cloud:**
  - Contract Compliance:
    - Check the interaction of two business partners in the cloud
- **Cloud -> Customer:**
  - Security Compliance:
    - Inspect the processes for cloud behavior violation

Related Standards



Architectures for Auditable Business Process Execution (APEX)

- Tool supported method for implementing business processes to IT infrastructure under consideration of compliance policy requirements (like Basel II, Solvency II, ...).
- Analysis is performed on the basis of text documents, models or other data sources
- Governance, Risk and Compliance (GRC) and measures especially for Cloud Computing for SMEs and large-scale enterprises.

Motivation

- Implementation of compliance regulations is essential:
  - Implementation of EU-Guidelines Basel II, Solvency II till 2012
  - Implementation of MaRisk from BaFin
  - US-market actors require SOX
- Today: time-consuming and expensive manual labour
- Specialists are employed for standard tasks and there is often no time for analysis of special cases e.g. risk of fraud by stuff (spectacular example: Societe Generale 2008: 5 Mrd. Euro loss).
- APEX approach reduces the manual effort and provides time for GRC experts to focus on specific issues

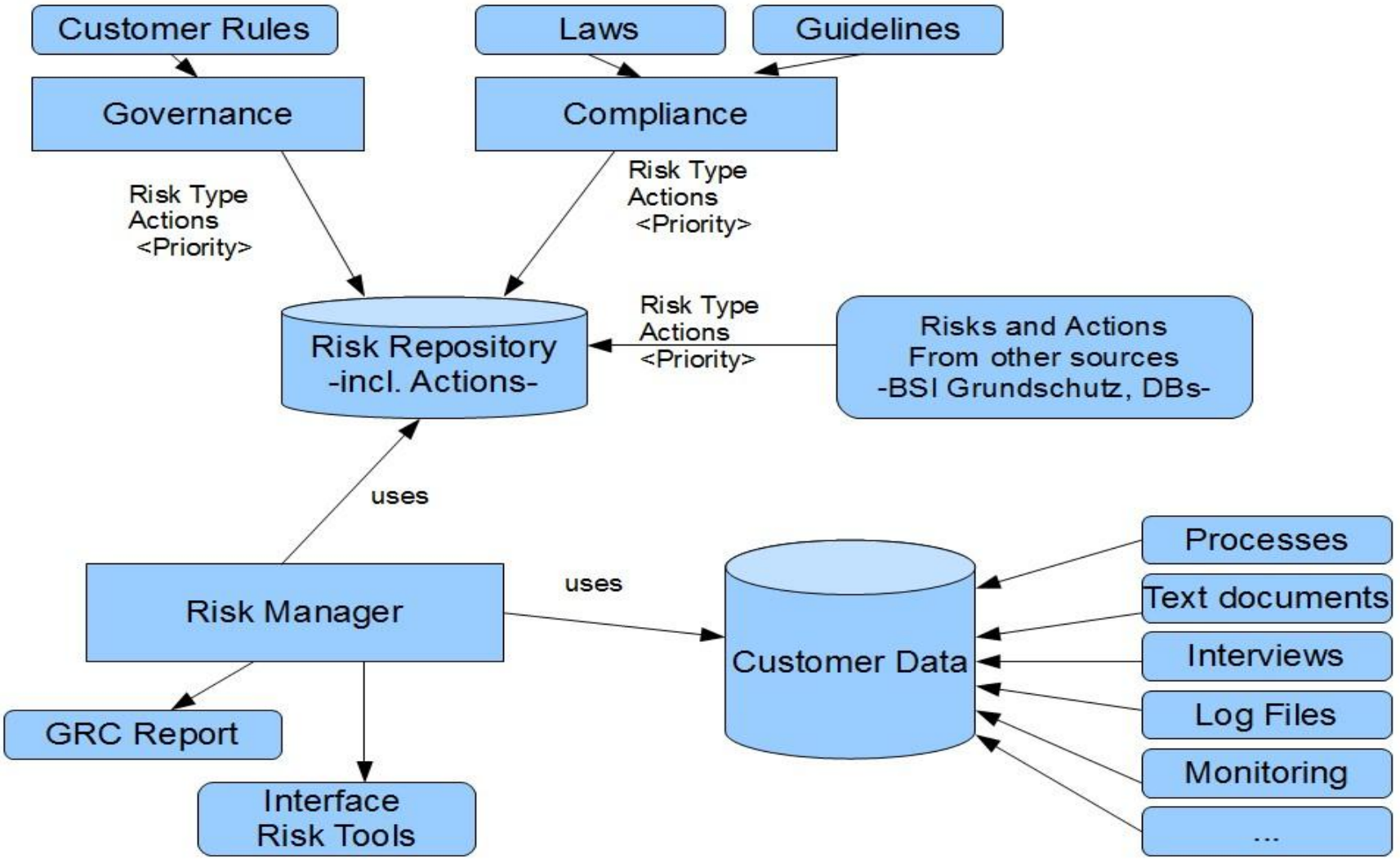
Definition Security and Compliance

- Governance, Risk und Compliance (GRC)
  - Governance: internal company guidelines
  - Compliance: external guidelines, e.g. SOX
  - Risk: risk management under consideration of all guidelines
- Security
  - Abstract security objectives, e.g. CIA applied to a company
- A company can be compliant, but not secure.

The Idea behind the APEX Approach

- Automation of standard GRC tasks
  - RoI reduction through manual work reduction
  - Experts focus on special cases
- Development of GRC information bases for companies
  - Data sources: Interviews, texts, process mining, and processes
- Risk management concept evaluation
  - Partially automated by APEX framework
- Support by measures for GRC monitoring
  - Implementation of monitoring tools e.g. in web portals
- Data can be also used in BPM sector

The APEX Framework



Log-File Analysis: Identification of Patterns

File: \\saperp\sapmnt\trans\log\ALOG0928.ERP

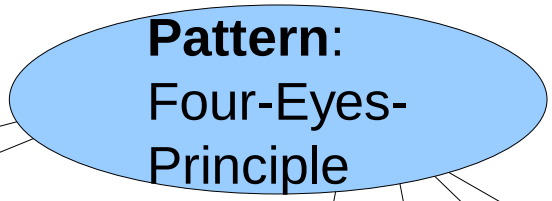
Four-Eyes-Principle

Request	SID	Cl.	S	RC	Time Stamp	Owner	User
SAPKGPPD14	ERP	ALL	H	0000	07.07.09 11:47:37	SAPUSER	SAP_BASIS
SAPKGPPD15	ERP	ALL	H	0000	07.07.09 11:47:44	SAPUSER	SAP_BASIS
SAPKGPRD12	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	…USER	SAP_BASIS
SAPKGPRD13	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	…USER	SAP_BASIS
SAPKGPRD14	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	…USER	SAP_BASIS
SAPKGPRD15	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	…USER	SAP_BASIS
SAPKGPGD12	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	…USER	SAP_BASIS
SAPKGPGD13	ERP	ALL	H	0000	07.07.09 11:47:56	SAPUSER	SAP_BASIS
SAPKGPGD14	ERP	ALL	H	0000	07.07.09 11:47:57	SAPUSER	SAP_BASIS
SAPKITLQI6	ERP	ALL	H	0004	07.07.09 11:48:17	STPIUSER	SAP_BASIS
SAPK-60012	ERP	ALL	A	0008	07.07.09 13:16:27	SAPUSER	SAP_BASIS
SAPK-60012	ERP	ALL	A	0008	07.07.09 13:16:27	ERECRUITUSER	SAP_BASIS
SAPK-60012	ERP	ALL	A	0008	07.07.09 13:16:27	SAPUSER	SAP_BASIS
SAPK-60012	ERP	ALL	A	0008	07.07.09 13:16:27	SAPUSER	SAP_BASIS
SAPK-60012	ERP	ALL	A	0008	07.07.09 13:16:27	SAPUSER	SAP_BASIS
SAPK-60012	ERP	ALL	A	0008	07.07.09 13:16:27	SAPUSER	SAP_BASIS
SAPK-60012	ERP	ALL	A	0008	07.07.09 13:16:27	SAPUSER	SAP_BASIS
SAPK-60012	ERP	ALL	A	0008	07.07.09 13:16:27	SAPUSER	SAP_BASIS
SAPK-60012	ERP	ALL	A	0008	07.07.09 13:16:27	SAPUSER	SAP_BASIS
SAPK-60012	ERP	ALL	A	0008	07.07.09 13:16:27	SAPUSER	SAP_BASIS
SAPK-60012	ERP	ALL	A	0008	07.07.09 13:16:27	SAPUSER	SAP_BASIS
SAPK-60013	ERP	ALL	A	0008	07.07.09 13:16:27	SAPUSER	SAP_BASIS
SAPK-60013	ERP	ALL	A	0008	07.07.09 13:16:27	ERECRUITUSER	SAP_BASIS
SAPK-60013	ERP	ALL	A	0008	07.07.09 13:16:27	SAPUSER	SAP_BASIS
SAPK-60013	ERP	ALL	A	0008	07.07.09 13:16:27	SAPUSER	SAP_BASIS
SAPK-60013	ERP	ALL	A	0008	07.07.09 13:16:27	SAPUSER	SAP_BASIS
SAPK-60013	ERP	ALL	A	0008	07.07.09 13:16:27	SAPUSER	SAP_BASIS
SAPK-60013	ERP	ALL	A	0008	07.07.09 13:16:27	SAPUSER	SAP_BASIS
SAPK-60013	ERP	ALL	A	0008	07.07.09 13:16:27	SAPUSER	SAP_BASIS
SAPK-60013	ERP	ALL	A	0008	07.07.09 13:16:27	SAPUSER	SAP_BASIS
SAPK-60013	ERP	ALL	A	0008	07.07.09 13:16:27	SAPUSER	SAP_BASIS
SAPK-60013	ERP	ALL	A	0008	07.07.09 13:16:27	SAPUSER	SAP_BASIS
SAPK-60013	ERP	ALL	A	0008	07.07.09 13:16:27	SAPUSER	SAP_BASIS
SAPK-60014	ERP	ALL	A	0008	07.07.09 13:16:27	SAPUSER	SAP_BASIS
SAPK-60014	ERP	ALL	A	0008	07.07.09 13:16:27	ERECRUITUSER	SAP_BASIS
SAPK-60014	ERP	ALL	A	0008	07.07.09 13:16:27	SAPUSER	SAP_BASIS
SAPK-60014	ERP	ALL	A	0008	07.07.09 13:16:27	SAPUSER	SAP_BASIS
SAPK-60014	ERP	ALL	A	0008	07.07.09 13:16:27	SAPUSER	SAP_BASIS
SAPK-60014	ERP	ALL	A	0008	07.07.09 13:16:27	SAPUSER	SAP_BASIS

- Identification of the Four-Eyes-Principle with the help of the following information:
- Request Ids are conform
- Owners are different
- Job was finished at the same point in time

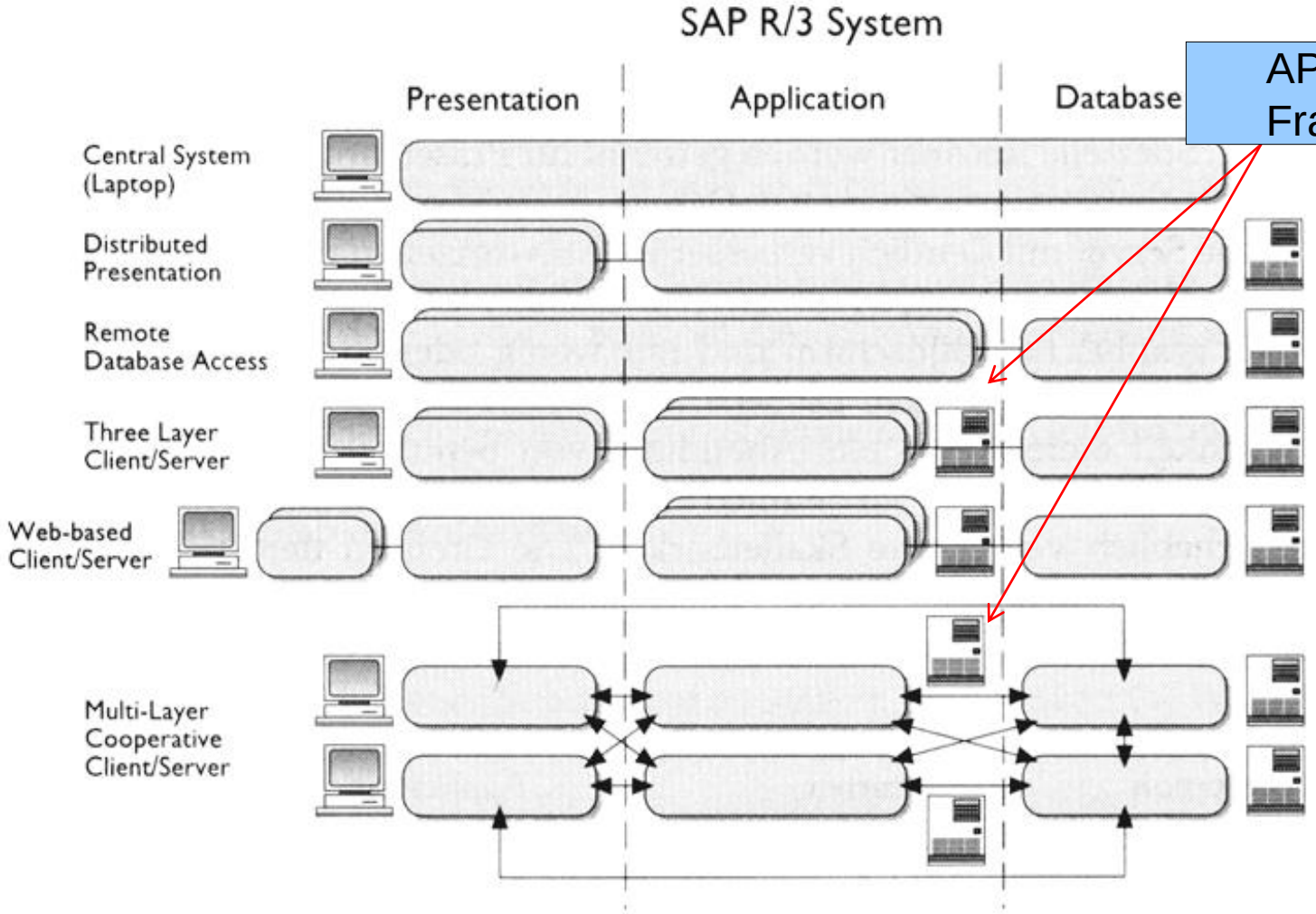
Log-File Analysis: Identification of pattern with chronology

- Chronology of the four-eyes principle is considered
- First an employee has to create a contract
- Afterwards another one has to check the contract
- The action has to have a consistent processID



ProcessID	Activity ID	Consultant	Time Stampe	Description
1	A	John	9-3-10:15.01	Create Contract
2	A	Mike	9-3-10:15.12	Print Document
1	B	Mike	9-3-10:16.07	Check Contract
2	C	Carol	9-3-10:18:25	Send Document

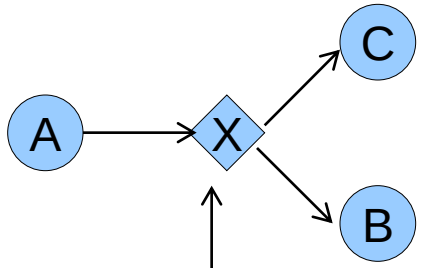
Log-File Analysis



Business Process Mining

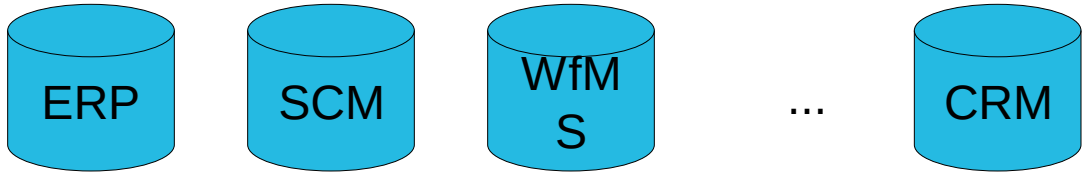
Analysis based on IT-systems

Analysis of processes derived with reverse engineering

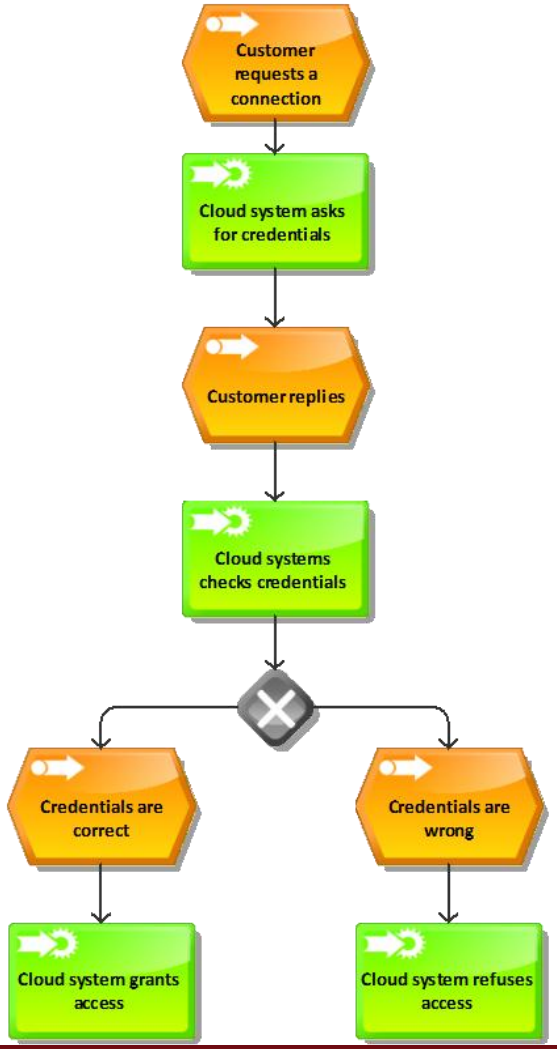


Process ID	Activity ID	Consultant	Time Stampe
1	A	John	9-3-10:15.01
2	A	Mike	9-3-10:15.12
3	B	Mike	9-3-10:16.07
4	C	Carol	9-3-10:18.25

Event dates



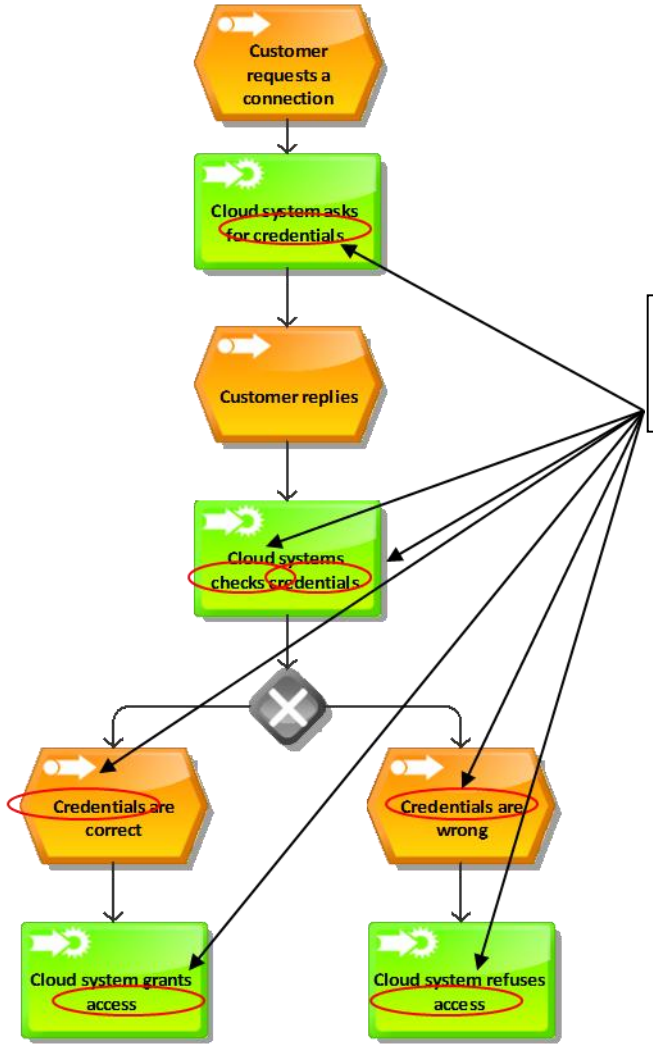
Business Process Analysis
Analysis based on models



- Automated compliance-analysis
- Two approaches:

1. Test-based analysis of the activity identifier for the automated risk identification
2. Structural analysis of the process model for compliance-violation-pattern

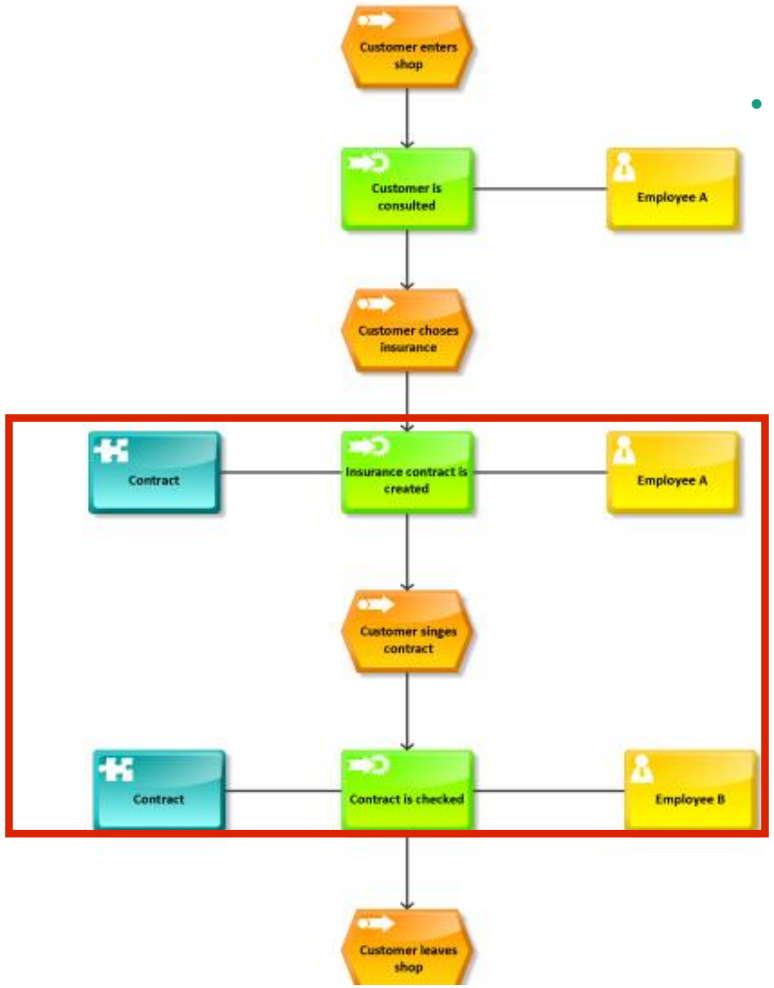
Textbased Automated Riskanalysis



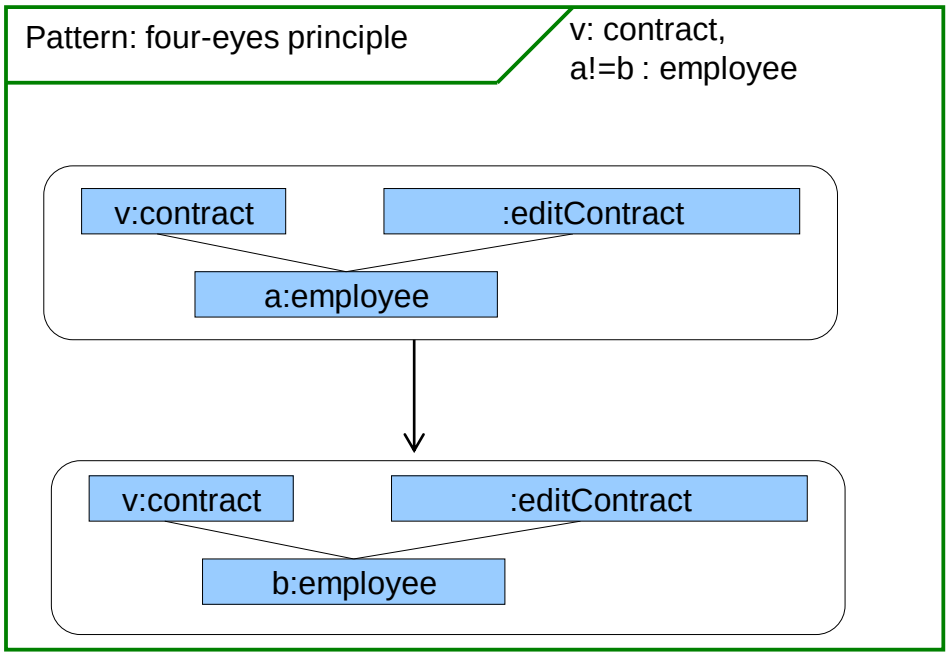
Compliance-relevant keywords:
Credentials, Login, Check

- Advantage:
  - Detailed risk analysis possible
- Disadvantage:
  - modelling required

Structural Analysis on the Model Layer



- Structural analysis of a business process against compliance pattern
- Approach:
  - Search with abstract syntax for a contract v
  - Search for the Four-Eyes-Principle for this linked v



Conclusion

Clouds ?

Make sure you are secure !

(… and compliant)

Contact: http://jan.jurjens.de