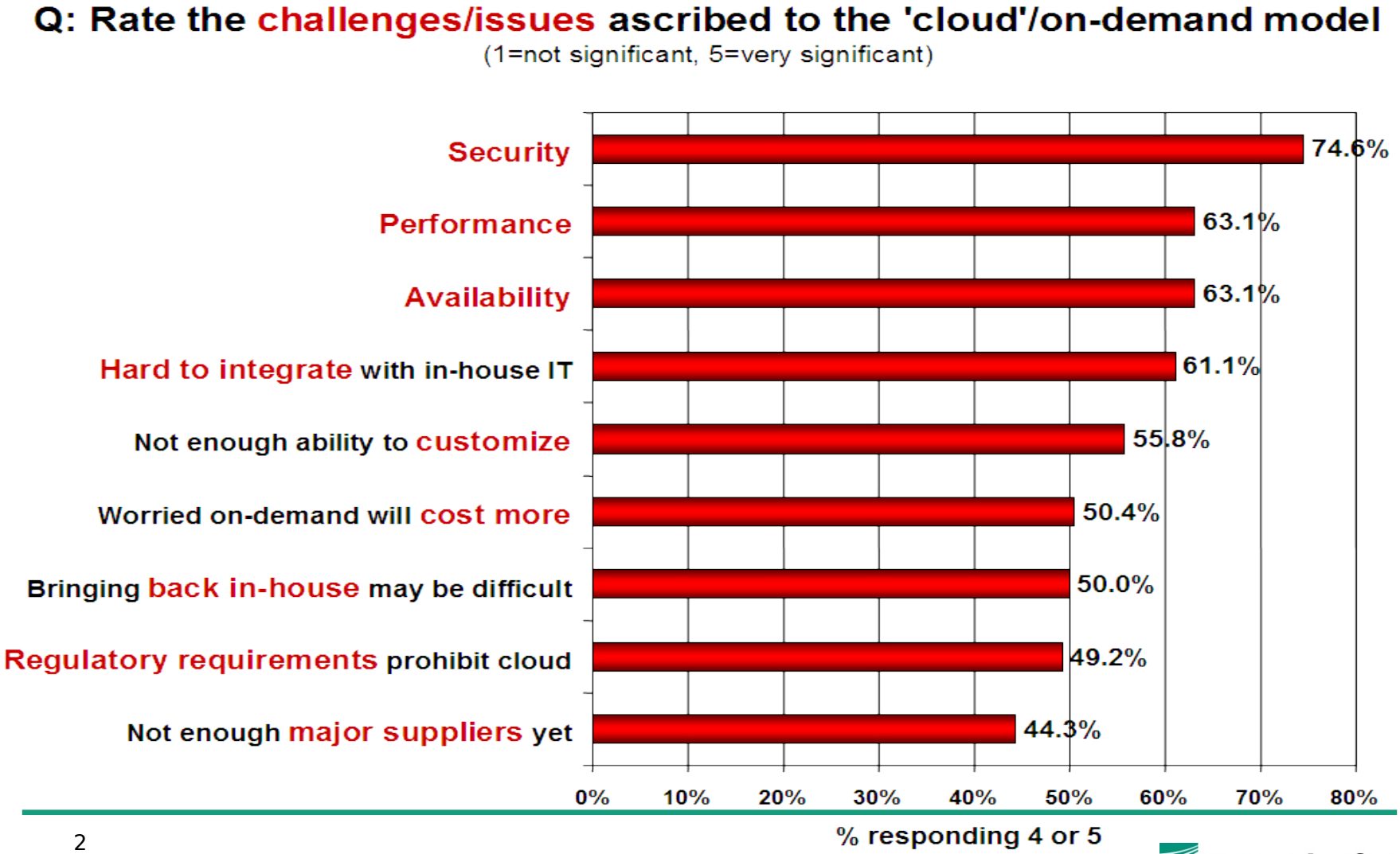
Outsourcing, SaaS & Clouds: Aber sicher ! (… und compliant)

Prof. Dr. Jan Jürjens

Fraunhofer Institut für Software- und Systemtechnologie ISST, Dortmund
http://jan.jurjens.de

Fraunhofer ISST

Security is the Major Issue



Source: IDC Enterprise Panel, August 2008 n=244

Fraunhofer ISST

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

Fraunhofer ISST

A simple cloud check list

- Is the security of the vendor documented?
  - How are security levels maintained?
- Is it possible to withdraw from the cloud with little effort?
- What Guarantees / Service Level Agreements (SLA) exist?
  - Can they be tailored to the customers need?
  - Which penalties are in the standardized SLAs?
  - How can the vendor enforce an SLA?
- What kind of cloud monitoring capabilities exist?
- Where is the physical location of the cloud?
  - Which laws apply there?
  - Can I enforce the usage of German law (“Rechtswahl”)?
  - Are German privacy laws enforced?

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

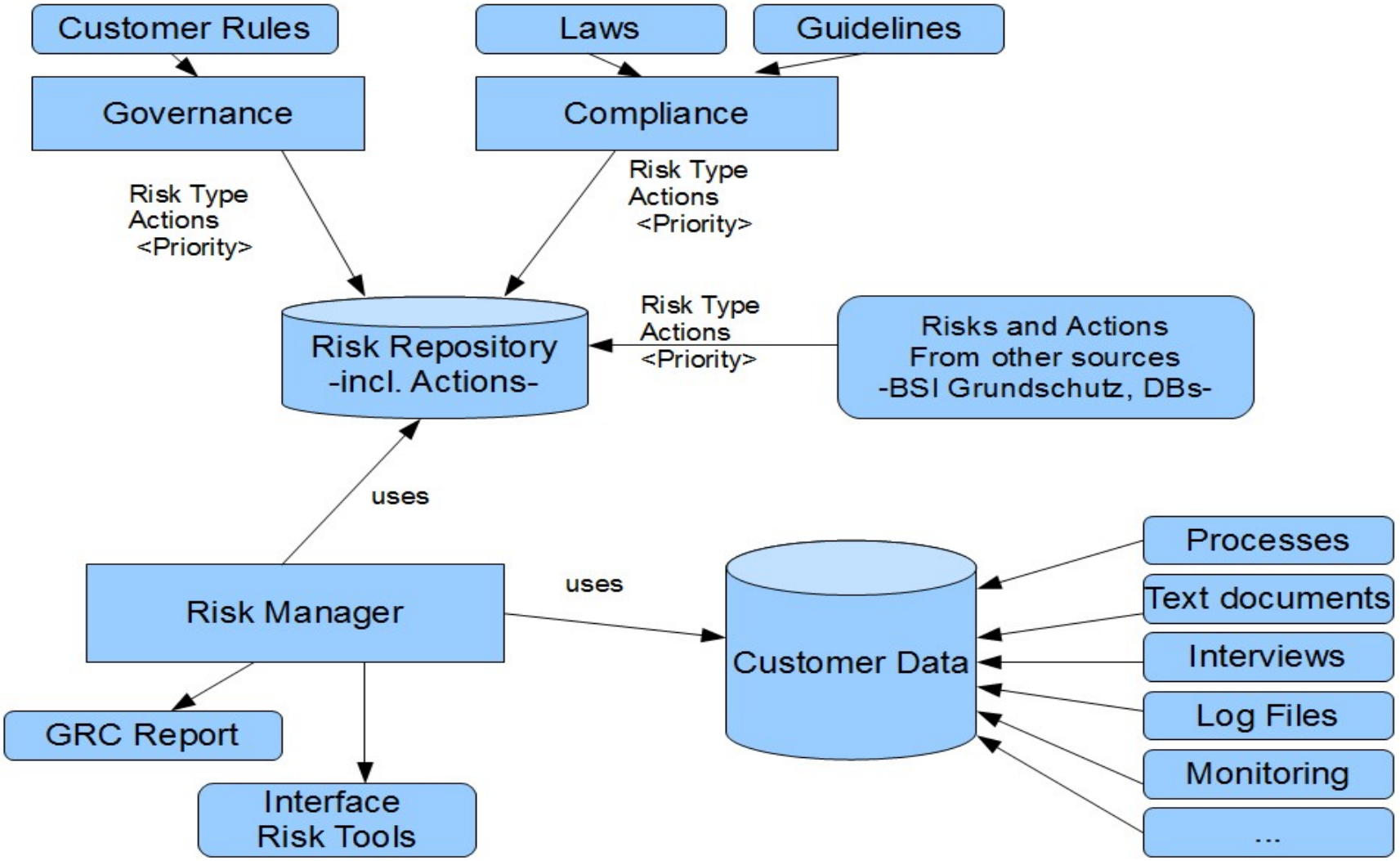
Definition Security and Compliance

- 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

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

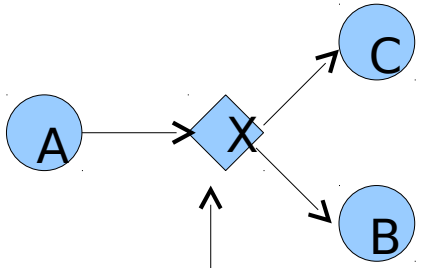
Four-Eyes-Principle

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						USER	SAP_BASIS
SAPKGPRD13						USER	SAP_BASIS
SAPKGPRD14						USER	SAP_BASIS
SAPKGPRD15						USER	SAP_BASIS
SAPKGPGD12						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

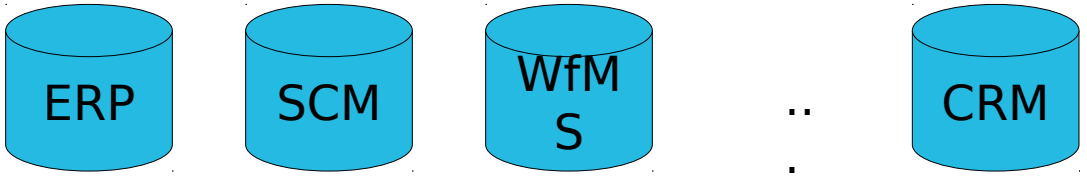
Business Process Mining

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

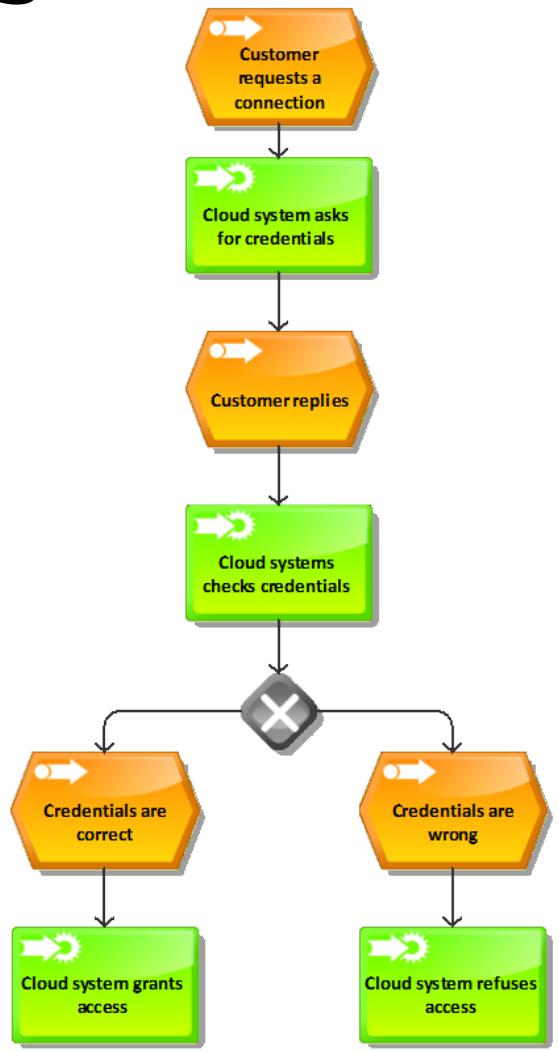


Fraunhofer ISST

Business Process Analysis

- 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



Conclusion

Clouds ?

Make sure you are secure !

(… and compliant)

Contact: http://jan.jurjens.de