Security and Compliance in Clouds: Challenges and Solutions

Prof. Dr. Jan Jürjens

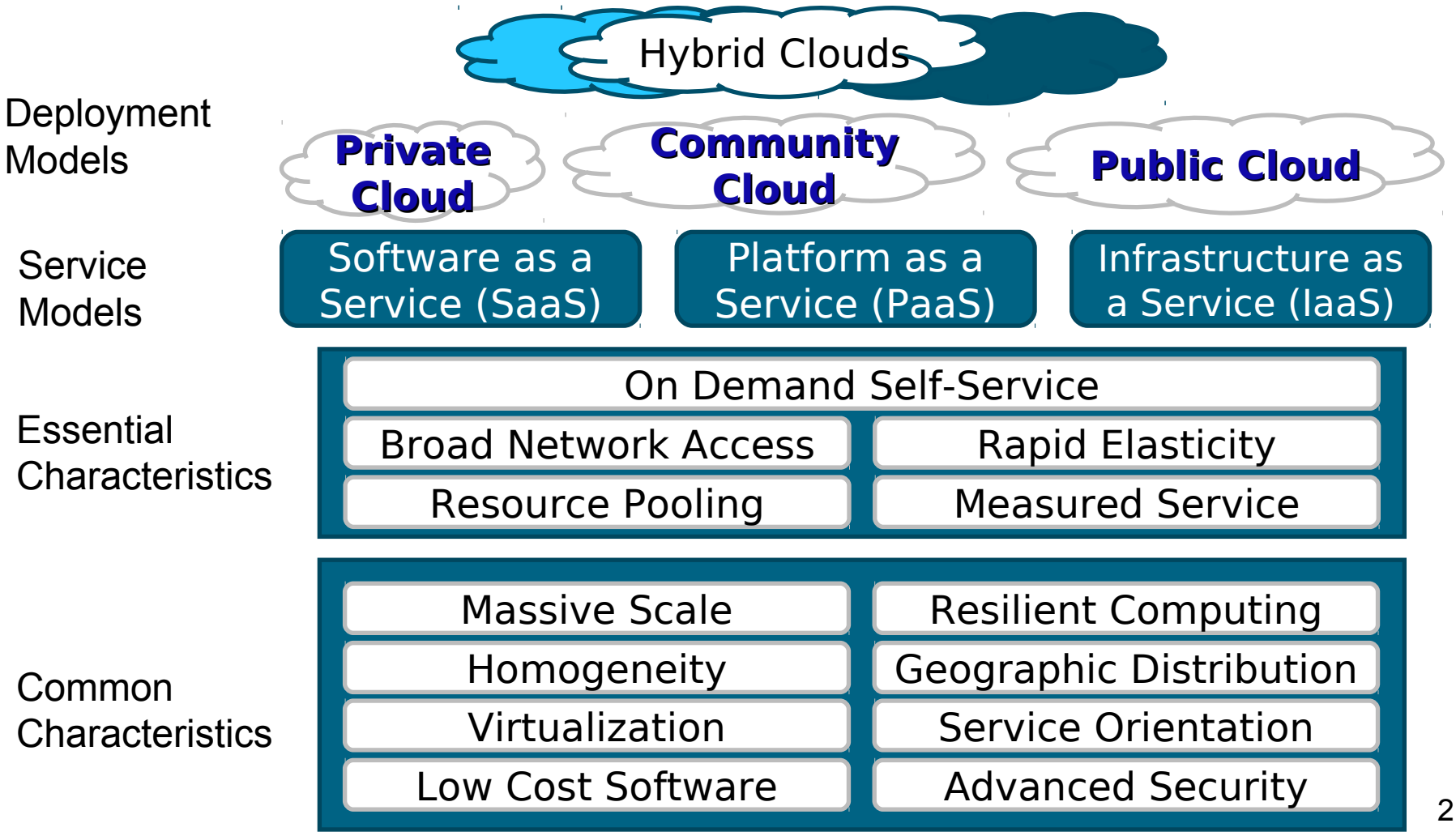
Fraunhofer Institut für Software- und Systemtechnologie ISST, Dortmund

http://jan.jurjens.de

This Talk

- What are the challenges ?
- What are the solutions ?
- What are the tools ?

The NIST Cloud Definition Framework

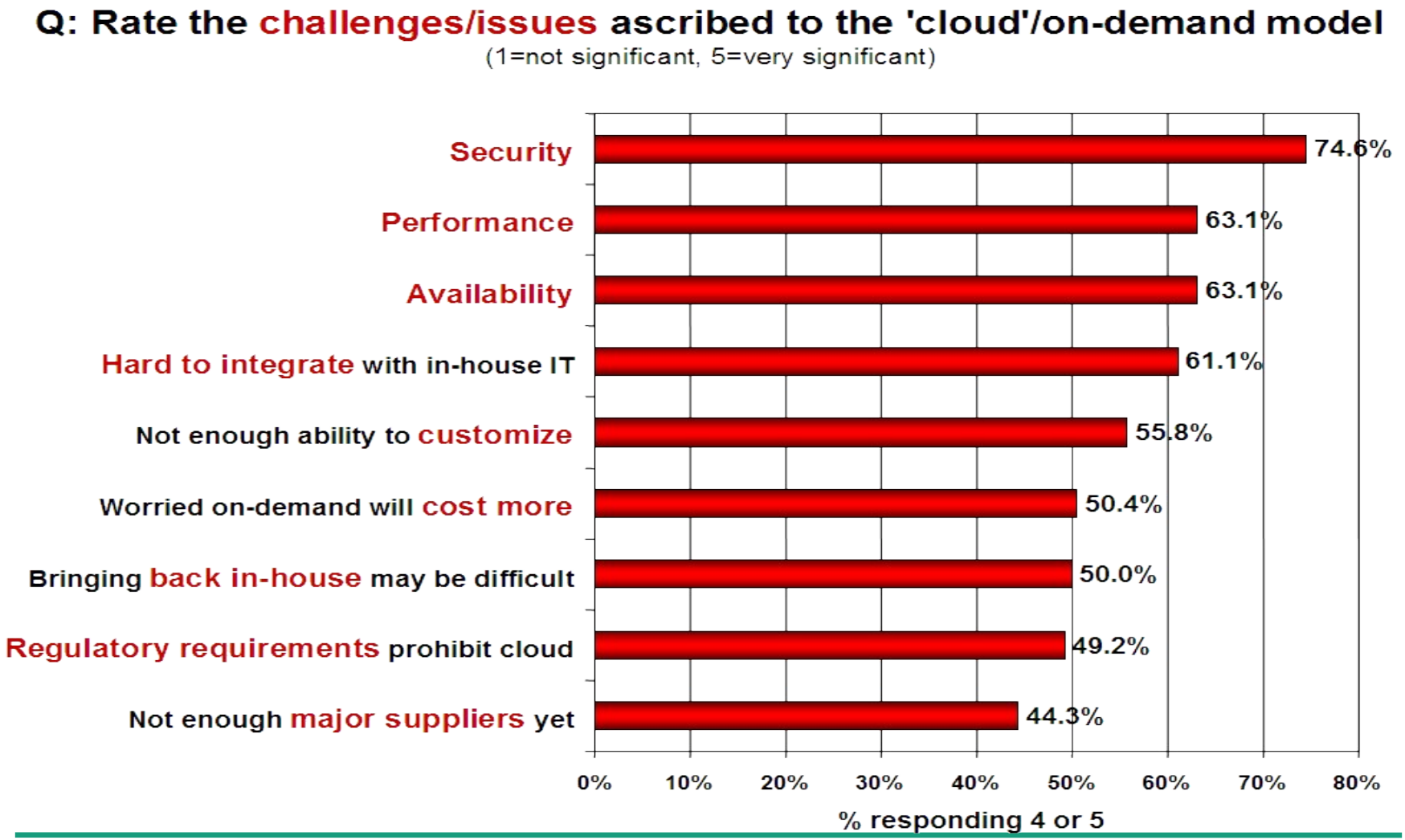


2

(Source: NIST, Effectively and Secure using the Cloud Paradigm, 2009)

Fraunhofer ISST

Security is the Major Issue



Source: IDC Enterprise Panel, August 2008 n=244

Fraunhofer ISST

Cloud Security Goals

Confidentiality	Data processing in the cloud is still unencrypted Encrypted data storage in the cloud: Shared DB Encrypted data exchange with the cloud: Secure Internet Link
Availability	Protection of the virtual space of the clouds from e.g. overwrites Redundant clouds / data storage
Integrity	Prevent unwanted and unrecognized data modification in the cloud
Authenticity	Authentication of cloud systems to users and vice versa!
Non Repudiation	Business transactions in clouds require signatures Independent checks of the signatures
Privacy	Prevent user profiling Conflicting with Non Repudiation

Cloud Computing Security Issues

- Mistakes/Attacks from employees of the provider
- Attacks from other customers
- Attacks on the availability
- Mistakes in the provisioning and the management
- Misuse of the provider platform
- Web-Service based attacks

(Source: BSI, IT-Grundschutz und Cloud Computing, 2009)

Compliance

- Compliance is the adherence to regulations (e.g. legal or governance regulations).
- The automated verification of security goals supports the build up of trust between a cloud vendor and its customers.
- Compliance checks can also verify the business processes of a cloud user for legal issues: SOX, EURO-SOX,BASEL II, SOLVENCY II
- Business process compliance is possible in two ways:
    - Compliance by design, Compliance generation
    - Compliance validation

Compliance: Importance and Challenges

- Implementation of compliance regulations is essential:
  - Implementation of EU-Guidelines Basel II (=> III), Solvency II
  - 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).
- Challenge: how to reduce the manual effort and provide time for GRC experts to focus on difficult issues ?

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

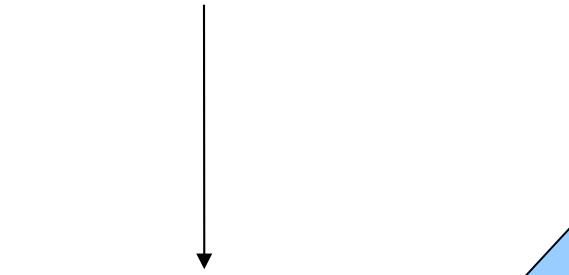
Security vs. GRC

- Governance, Risk und Compliance (GRC)
  - Governance: internal company guidelines
  - Compliance: external guidelines, e.g. SOX, EURO-SOX, BASEL II, SOLVENCY II
  - Risk: risk management under consideration of all guidelines
- Security
  - Abstract security objectives, e.g. CIA applied to a company

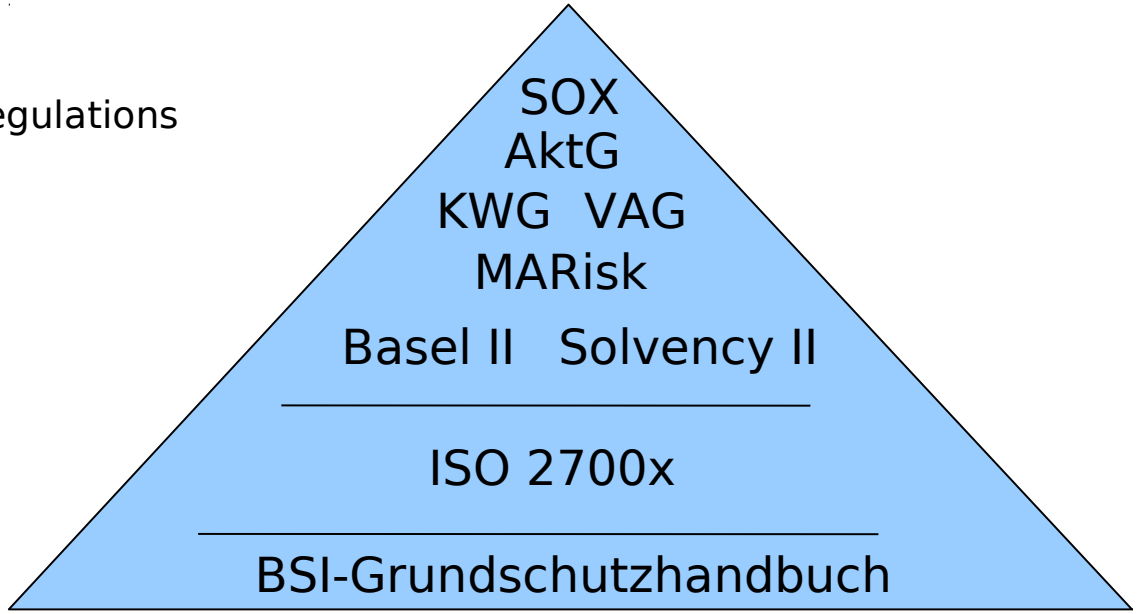
Security and compliance are closely related but different.

Security vs. Compliance: Regulations and Standards

Abstract laws and regulations



Concrete security policy rules



Fraunhofer ISST

This Talk

- What are the challenges ?
- What are the solutions ?
- What are the tools ?

Service Level Agreements (SLA)

- Precise description of the offered services and the expected limitations!
- Compare different SLAs for my needs.
  - Does a cloud vendor offer an SLA at all?
- What do the numbers mean: 99.8% per anno availability:
  - ~ 17,5 hours per year the cloud is offline!
- What are the penalties for SLA violations?
  - Can I monitor the performance of the cloud?
  - Does an early warning system exist?
- Is the cloud segregated into different security levels?
  - Do I need to separate my data before giving it to the cloud?
  - Should I avoid top secret data to enter the cloud?

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?

Some Example Considerations

- Physical security of the data center:
  - Googles Security Operations Center
  - Amazon: Two factor authentication
- Attacks on the networks level, e.g., Denial-of-Service:
  - Amazon uses Denial-of-Service Prevention, but the method is secret
  - Microsoft uses Load-Blanacer and Intrusion Prevention Systems
- Backup Solutions:
  - Goole, Amazon execute Backups on different physical locations
  - FlexiScale executes Backups, but users cannot retrieve lost data
- Amazon stores data permanent → after 5 Minutes it is in the cloud

Some Examples: Security Certificates

Vendor	TRUSTe	Safe Harbor	SAS 70 Type II	ISO/IEC 27001
Microsoft	x	x	x	x
Google	x		x	
Amazon	x	x	x	x
Salesforce	x	x	x	x
PingIdentity			x	
Postini		x	x	
CohesiveFT				
Scalr				
RightScale				
IBM	x	x	x	x
GoGrid	x		x	
FlexiScale				
Rackspace	x			
LongJump				

(Source: Fraunhofer SIT, Cloud Computing Sicherheit, 2009)

Compliance: Towards a Solution

- How to automate standard GRC tasks ?
  - RoI reduction through manual work reduction
  - Experts focus on special cases
- How to develope GRC information base for a company ?
  - Data sources: Interviews, texts, process mining, and processes
- How to organize risk management concept evaluation ?
  - Ideally (partially) tool-automated
- How to support GRC monitoring ?
  - Implementation of monitoring tools e.g. in web portals
- Ideally: reuse information for business process optimization

Related Standards

Fraunhofer ISST

This Talk

- What are the challenges ?
- What are the solutions ?
- What are the tools ?

What are the Tools ?

Which tool-support is available for:

- Analyzing one's own business process for suitability of outsourcing into a cloud (wrt. security / compliance)
- Analyzing / monitoring a cloud providers (claimed) security / compliance guarantees

Possibilities:

- Log-data analysis
- Business process mining
- Business process analysis

Log-File Analysis

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

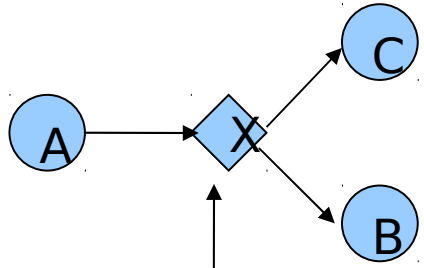
Request	SID	Cl.	S	RC	Time Stamp	Owner	User
SAPKGPPD14	ERP	ALL	H	0000	07.07.09 11:47:37	SAPUSER	SAP_BASIS
SAPKGPPD15	ERP	ALL	H	0000	07.07.09 11:47:44	SAPUSER	SAP_BASIS
SAPKGPRD12	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	…USER	SAP_BASIS
SAPKGPRD13	[illegible]	[illegible]	[illegible]	[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

Four-Eyes-Principle

- 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

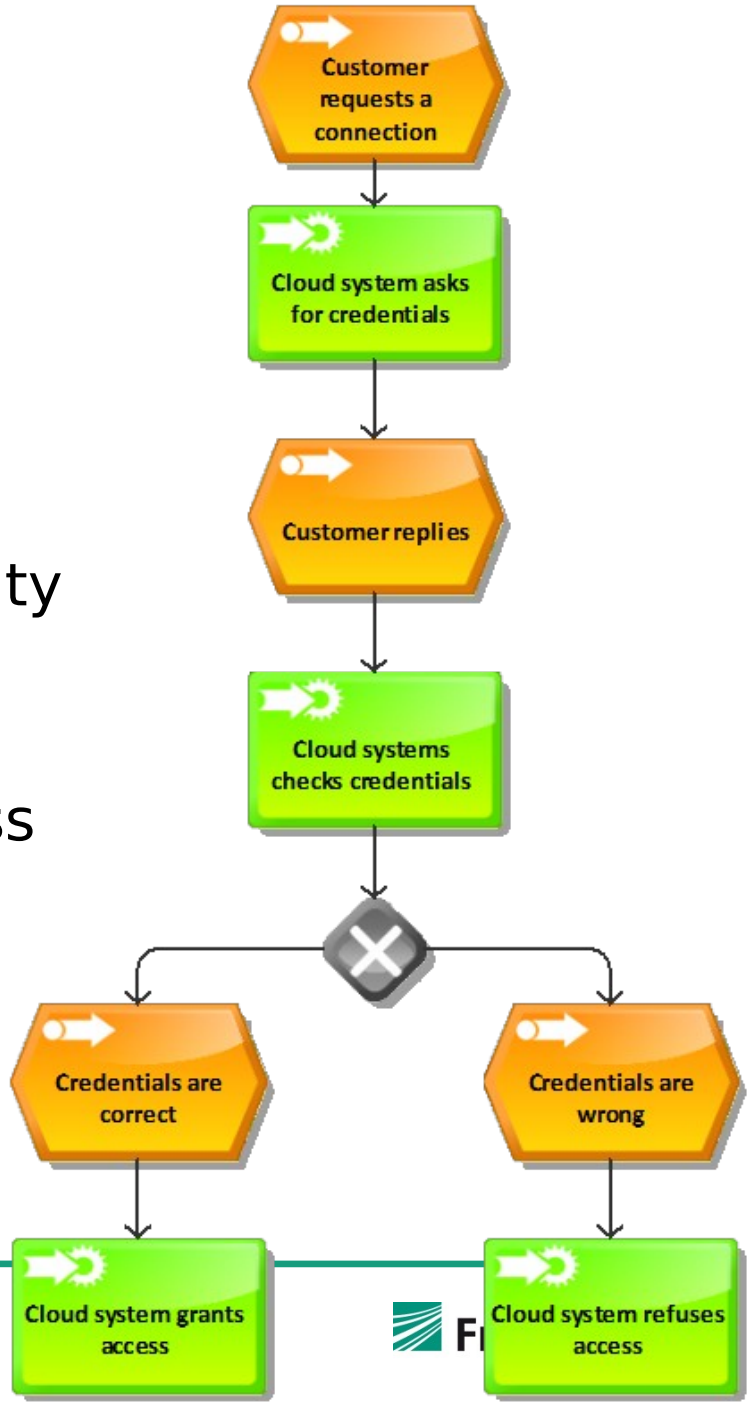
Event dates

Business Process Analysis

- Automated compliance-analysis
- Two approaches:

1. Text-based analysis of the activity identifier for the automated risk identification

2. Structural analysis of the process model for compliance-violation-pattern



SecureClouds Project (http://secureclouds.de)

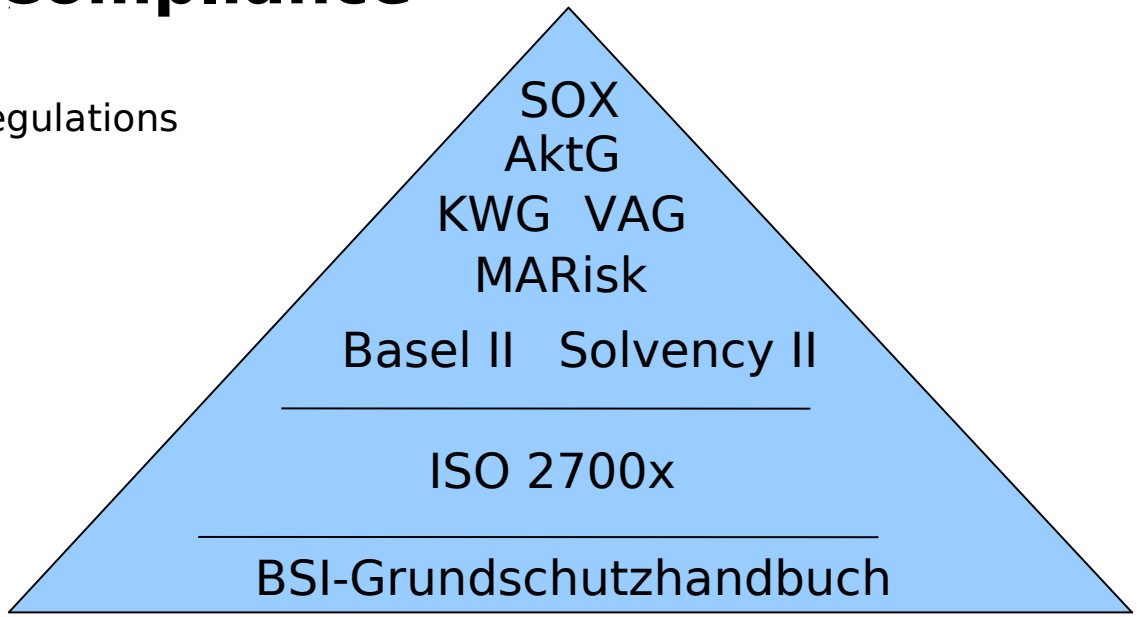
- Tool supported method for implementing business processes to IT infrastructure under consideration of compliance policy requirements (like Basel II, Solvency II, ...).
- Analysis is performed on the basis of text documents, models or other data sources
- Governance, Risk and Compliance (GRC) and measures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

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung
DLR
Projektträger im DLR

Tool-based Analysis and Enforcement for Security & Compliance

Abstract laws and regulations

Concrete security policy rules



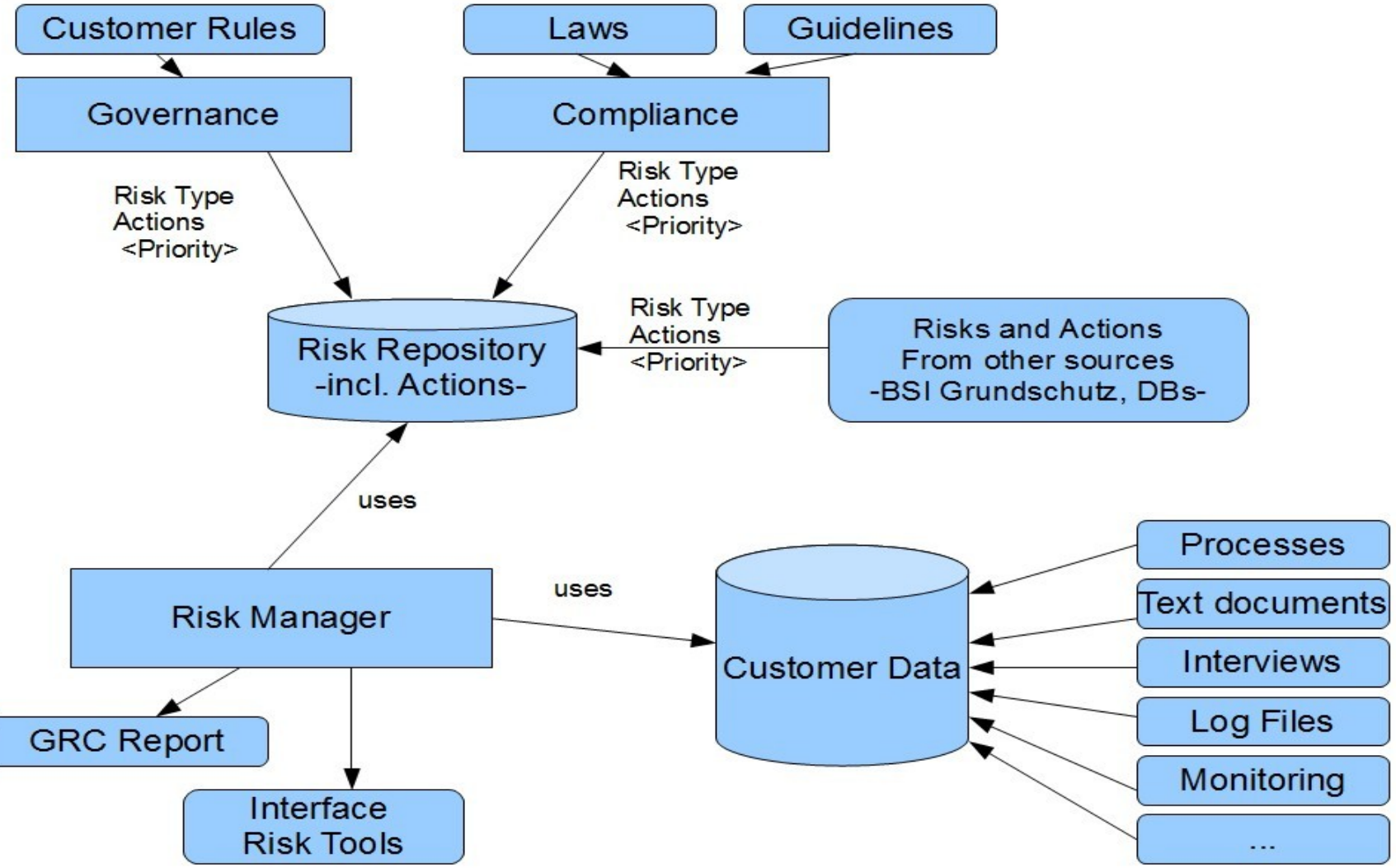
SecureClouds tools

Risk finder

Compliance pattern analyzer

Fraunhofer ISST

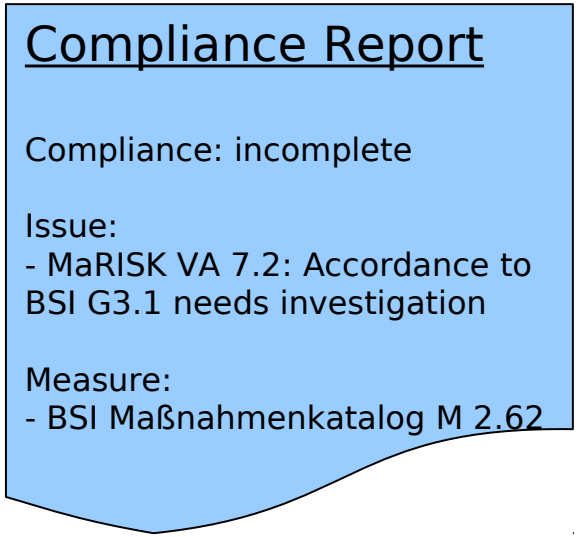
The SecureClouds Framework



Benefit

Automatically generated compliance report:

- For example: „Compliant wrt: MaRISK VA (yes / no)“
- Lists requirements that may need further investigation
- Suggests measurements to improve alignment with compliance requirements:
  - automated correction
  - manual correction



Services Offered by Fraunhofer ISST

- Preparation of compliance reports using automated tools
- Data mining of log files
  - Compliance analysis of business process execution
  - Automated process model generation
- Security & compliance analysis of business processes on the basis of process documentation
- Preparation and execution of compliance checks

NB: Possibility for public financial support as pilot customers in funded projects.

Some Client Projects

- German electronic health card architecture (Gesundheitskarte)
- Mobile architectures and policies (O2 (Germany))
- Digital file store (HypoVereinsbank)
- Common Electronic Purse Specifications
  (global standard for electronic purses, Visa International)
- Intranet information system (BMW)
- Return-on-Security Investment analysis (Munich Re)
- Digital signature architecture (Allianz)
- IT security risk assessment (Infineon)
- Smart-card software update platform (Gemalto)
- Cloud security ceritification (TÜV-IT, Itesys, LinogistiX)
- Cloud user security assessment (adMERITia, LinogistiX)

Conclusion

- Security & compliance in cloud-based environments is a complex and diverse issue.
  - As diverse as clouds themselves (cf NIST definition)
- There are solutions (and tools) available to tackle the challenges.
  - Analyzing one's own business process for suitability of outsourcing into a cloud (wrt. security / compliance)
  - Analyzing / monitoring a cloud provider's (claimed) security / compliance guarantees

Contact: http://jan.jurjens.de
Information: http://www.isst.fraunhofer.de/geschaeftsfelder/insuranceandfinance/refpro/gruppe-apex