
Security und Compliance in Clouds

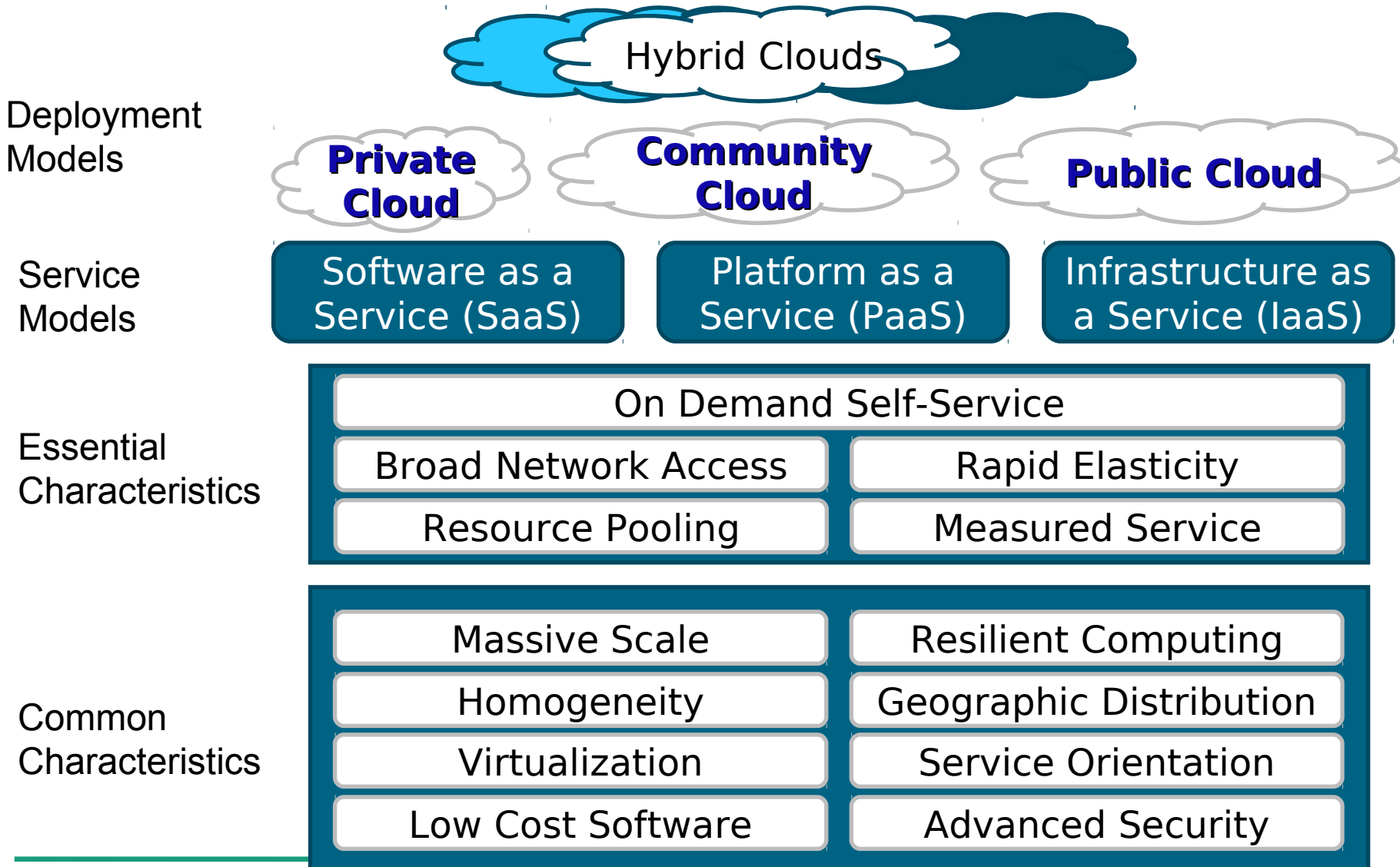
Prof. Dr. Jan Jürjens, Kristian Beckers

Fraunhofer Institut für Software- und Systemtechnologie ISST, Dortmund



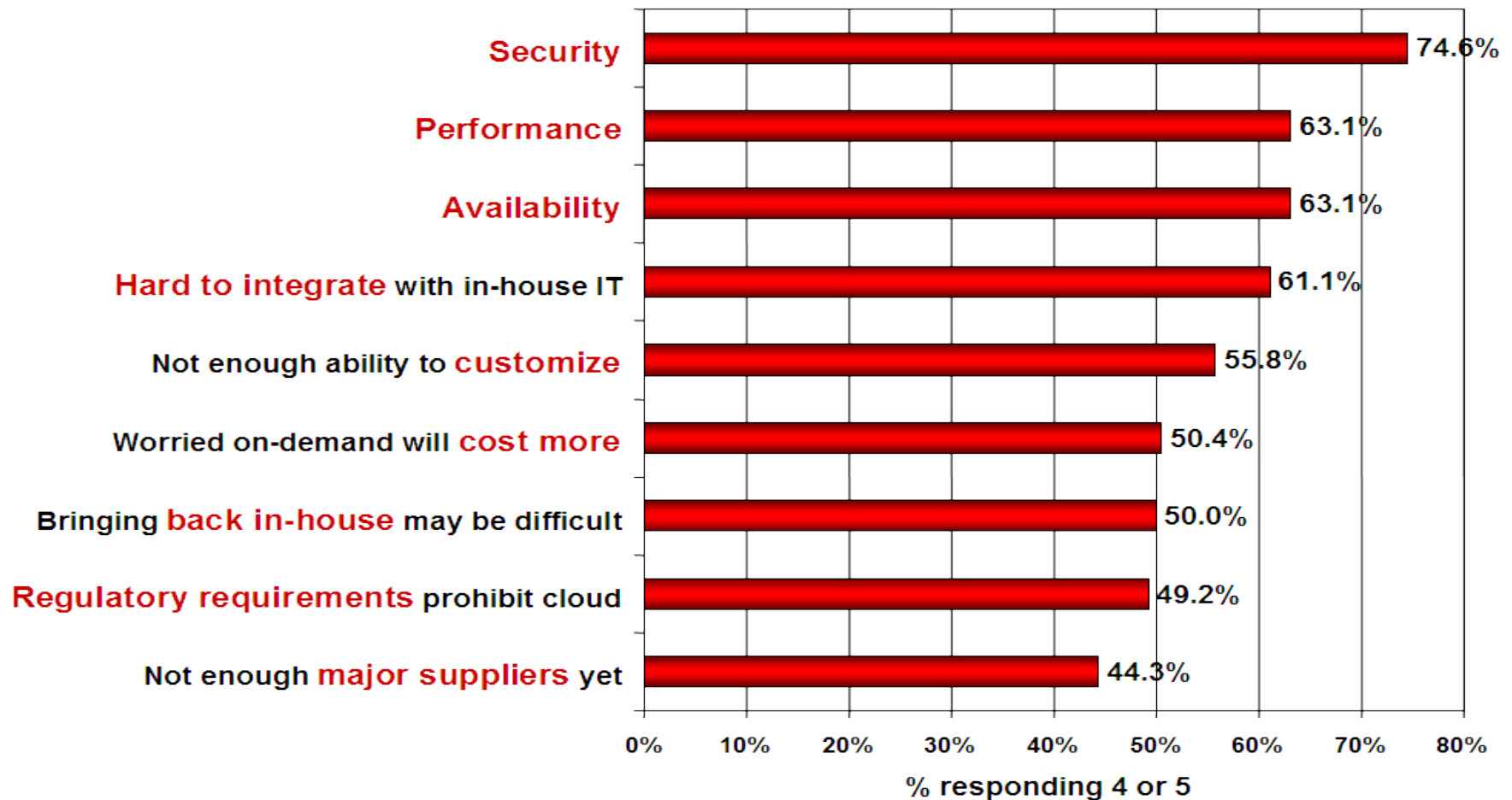
<http://jan.jurjens.de>

The NIST Cloud Definition Framework



Security is the Major Issue

Q: Rate the **challenges/issues** ascribed to the 'cloud'/on-demand model
(1=not significant, 5=very significant)



Source: IDC Enterprise Panel, August 2008 n=244

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)

Security Level Assurance (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?

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











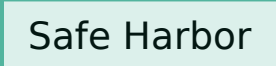
Security and compliance are closely related but different.

GRC in Clouds

Governance	Risk	Compliance
<ul style="list-style-type: none">■ Policy design■ Classification schema for data and processes■ Trust chain in a cloud	<ul style="list-style-type: none">■ Risk strategy■ Business Impact Analysis■ Threat and Vulnerability Analysis■ Risk Analysis Remediation	<ul style="list-style-type: none">■ Policy enforcement■ Legal compliance (SOX, SOLVENCY II)■ Control implementation

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

Related Standards

Process Maturity	  International Organization for Standardization  MATURITY MODEL FOR BPM
Holistic Control Systems	 GOVERNANCE, CONTROL, and AUDIT for INFORMATION and RELATED TECHNOLOGY 
Security Standards	 Bundesamt für Sicherheit in der Informationstechnik 
Transparency	 SAS 70  TRUSTe  International Organization for Standardization  Safe Harbor

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

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.

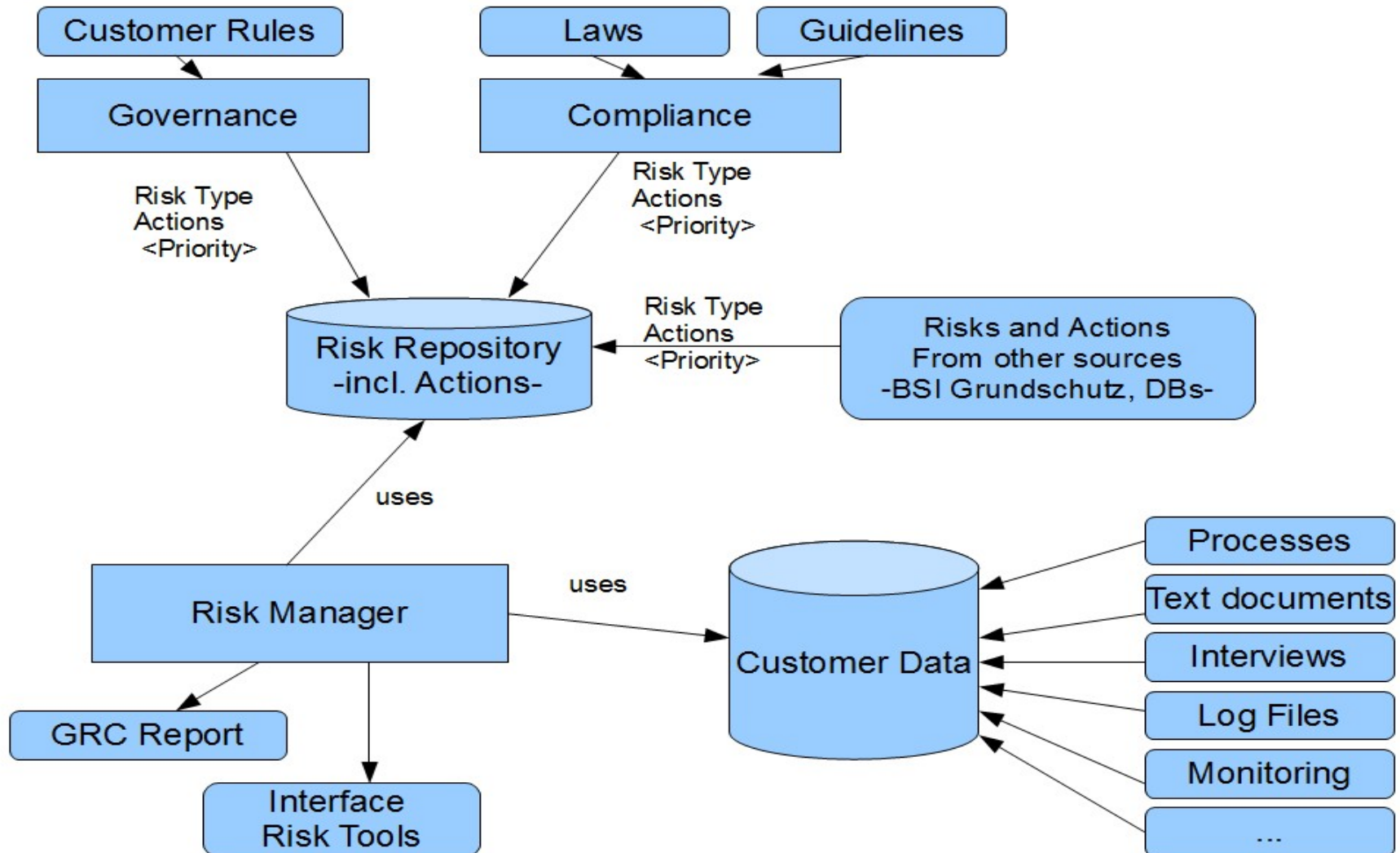
Motivation

- 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

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

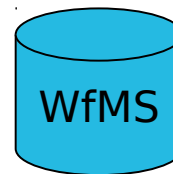
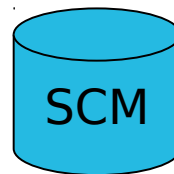
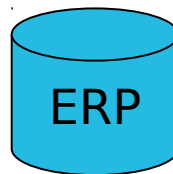
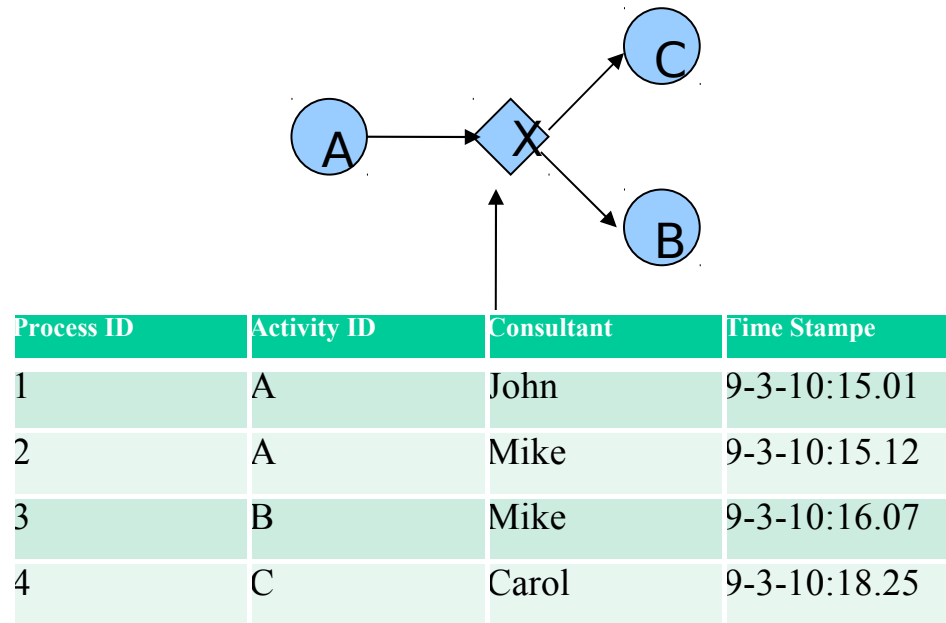
[illegible]

- 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

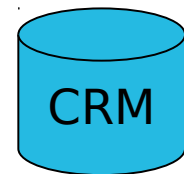
Business Process Mining

Analysis of
processes
derived with
reverse
engineering

Event
dates

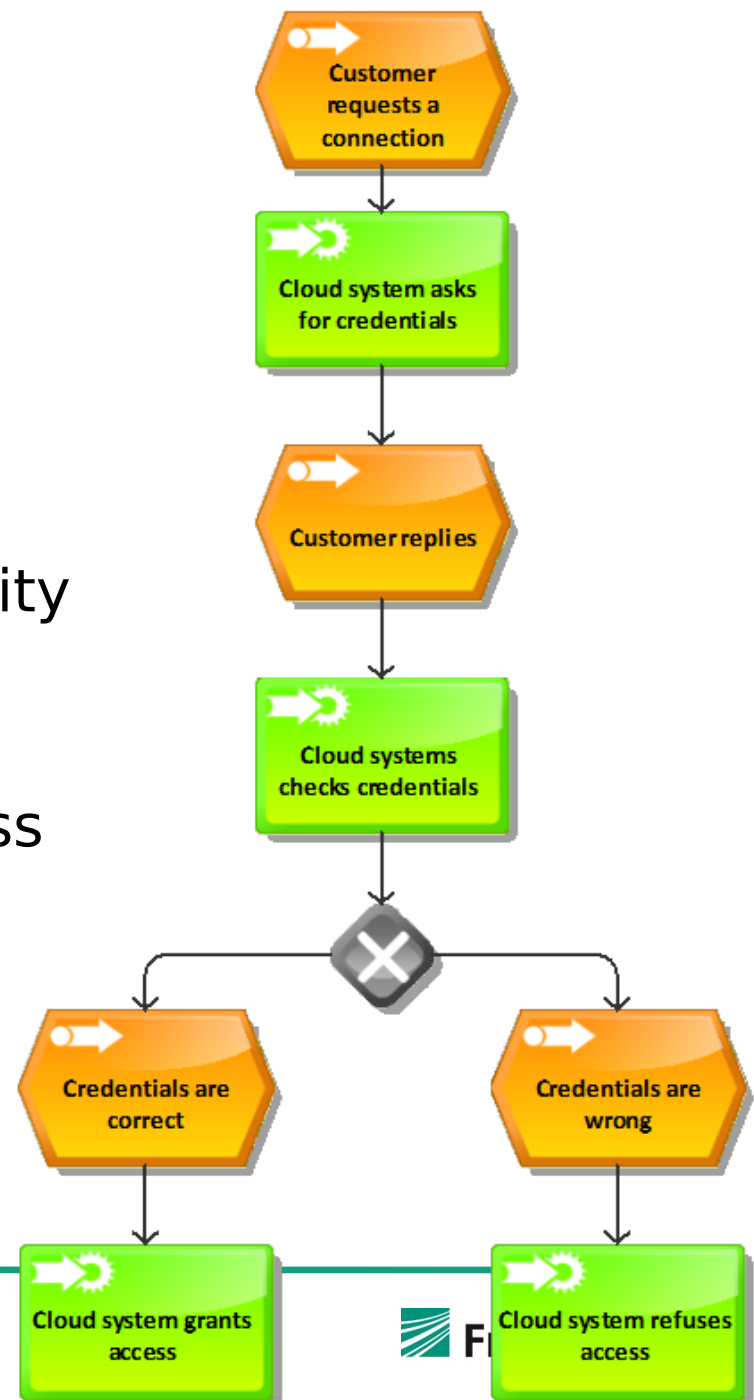


...

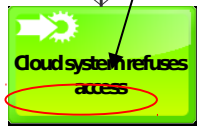
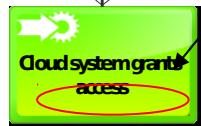
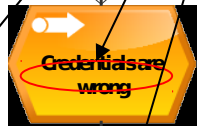
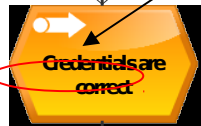
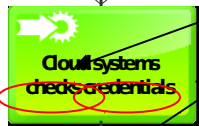
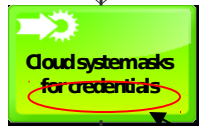


Business Process Analysis

- 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



Text-based Analysis of Process Documentation

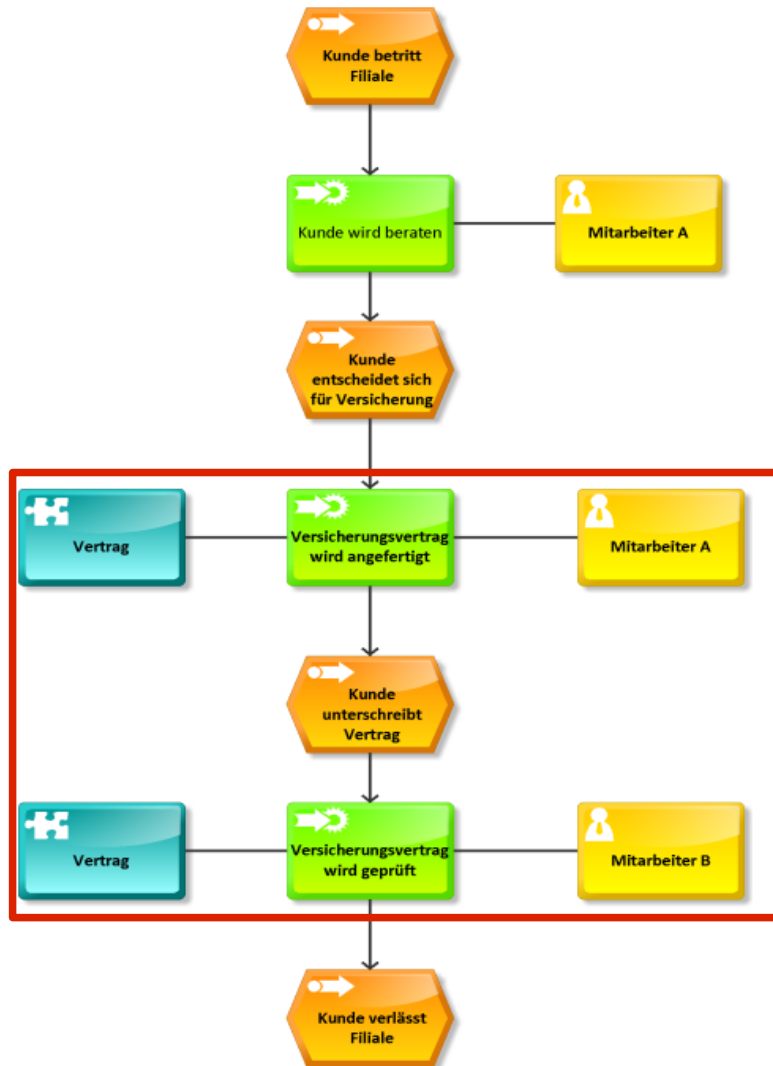


- A text-based analysis of the word in the EPC functions
- The functions of the EPC are checked for the words

Identify an compliance relevant task:
Look for words: Credentials, Login, Check, Verification that hint towards an authentication

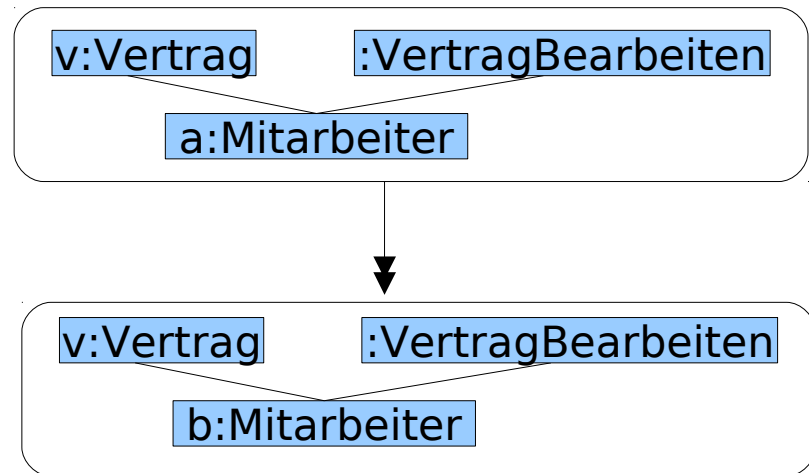
Structural Analysis of Process Model

- Structural analysis of business process models against compliance patterns
- Example: Check that separation-of-duty is implemented for significant contracts.



Pattern: Separation of duty

v:Vertrag,
a!=b : Mitarbeiter

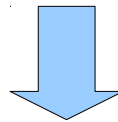
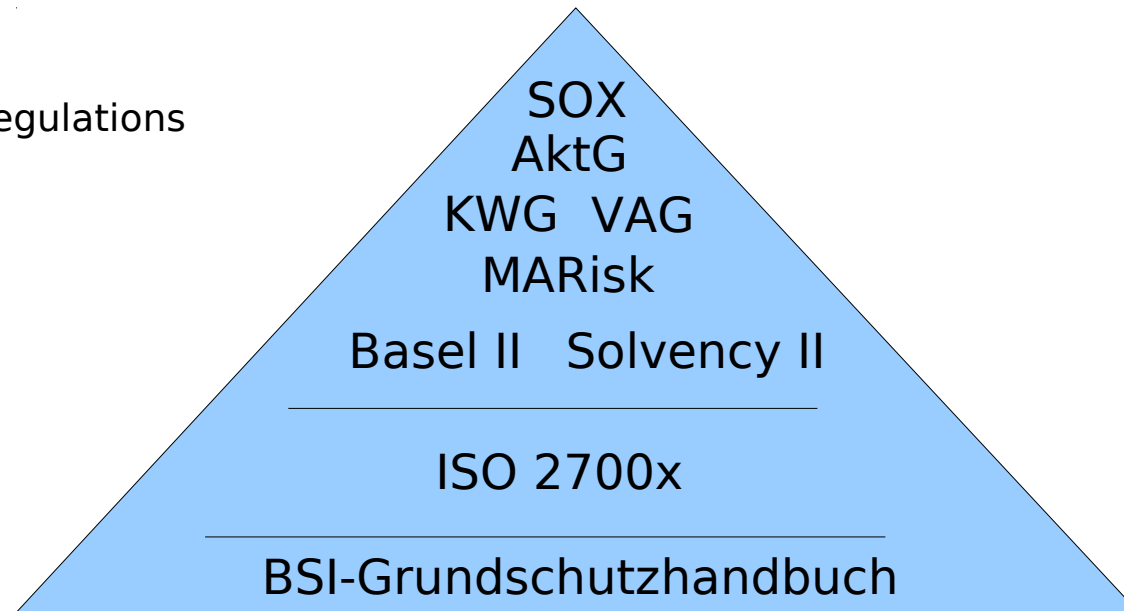


Compliance Pyramid

Abstract laws and regulations

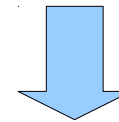


Concrete security
policy rules



APEX tools

Risk finder



Compliance
pattern
analyzer

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

Compliance Report

Compliance: incomplete

Issue:

- MaRISK VA 7.2: Accordance to BSI G3.1 needs investigation

Measure:

- BSI Maßnahmenkatalog M 2.62

Possibilities for Cooperation Projects

Offerings:

- Preparation of compliance reports using automated tools
- Data mining of log files
 - Compliance analysis of business process execution
 - Automated process model generation
- Support for business process modelling
- Support for preparation and execution of compliance checks

NB: Possibility for public financial support (e.g. BMBF)

Technical Prerequisites

Ideally:

- System and/or business process documentation
- Interface to extract log data

Note: Our approach can be easily instantiated to a given architecture (via simple architecture specific adapters).

=> No restriction on the architecture to be analyzed.

Some Projects

Pre-cloud:

- 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:

- Cloud security certification (TÜV-IT, Itesys, LinogistiX)
- Cloud user security assessment (adMERITia, LinogistiX)



Conclusion

Clouds ?

Make sure you are secure !

(... and compliant)

Contact: <http://jan.jurjens.de>