Compliance in Clouds
A cloud computing security perspective

Kristian Beckers, Martin Hirsch, Jan Jürjens

GI Workshop: Governance, Risk & Compliance on the 19th of March 2010

Fraunhofer
ISST

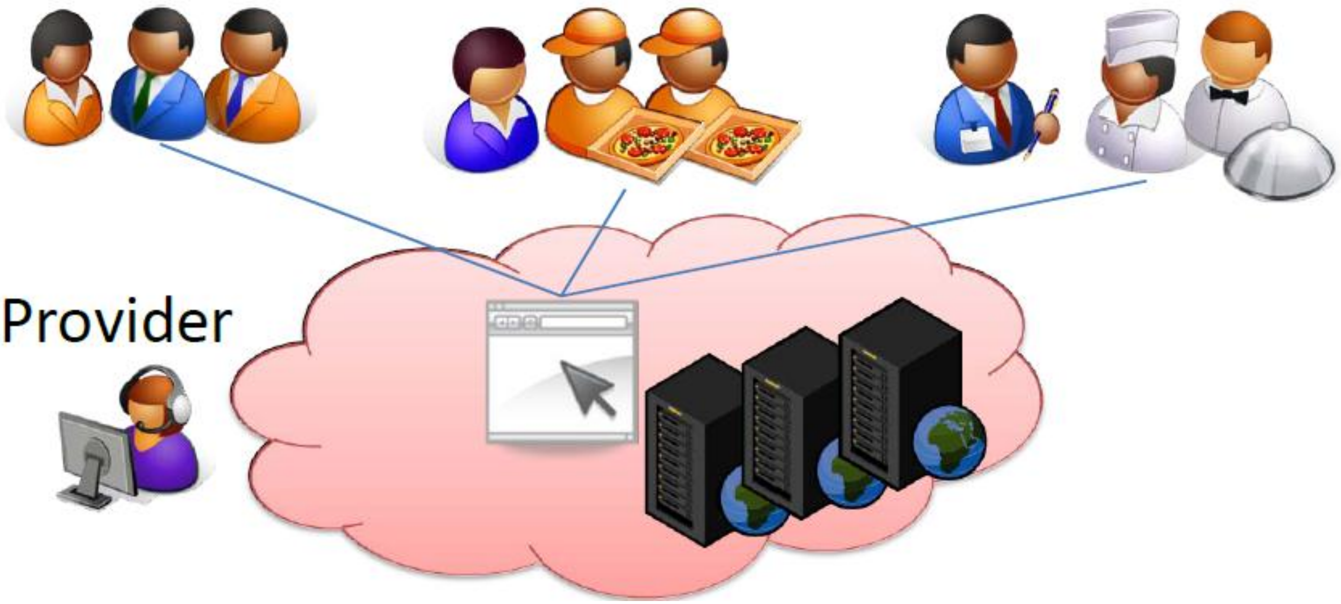
What is Cloud Computing?

- Today:

(Source: IPVS, University Stuttgart)

What is Cloud Computing?

- Services in the Cloud:



(Source: IPVS, University Stuttgart)

What is Cloud Computing?

The illusion of infinite resources available on demand

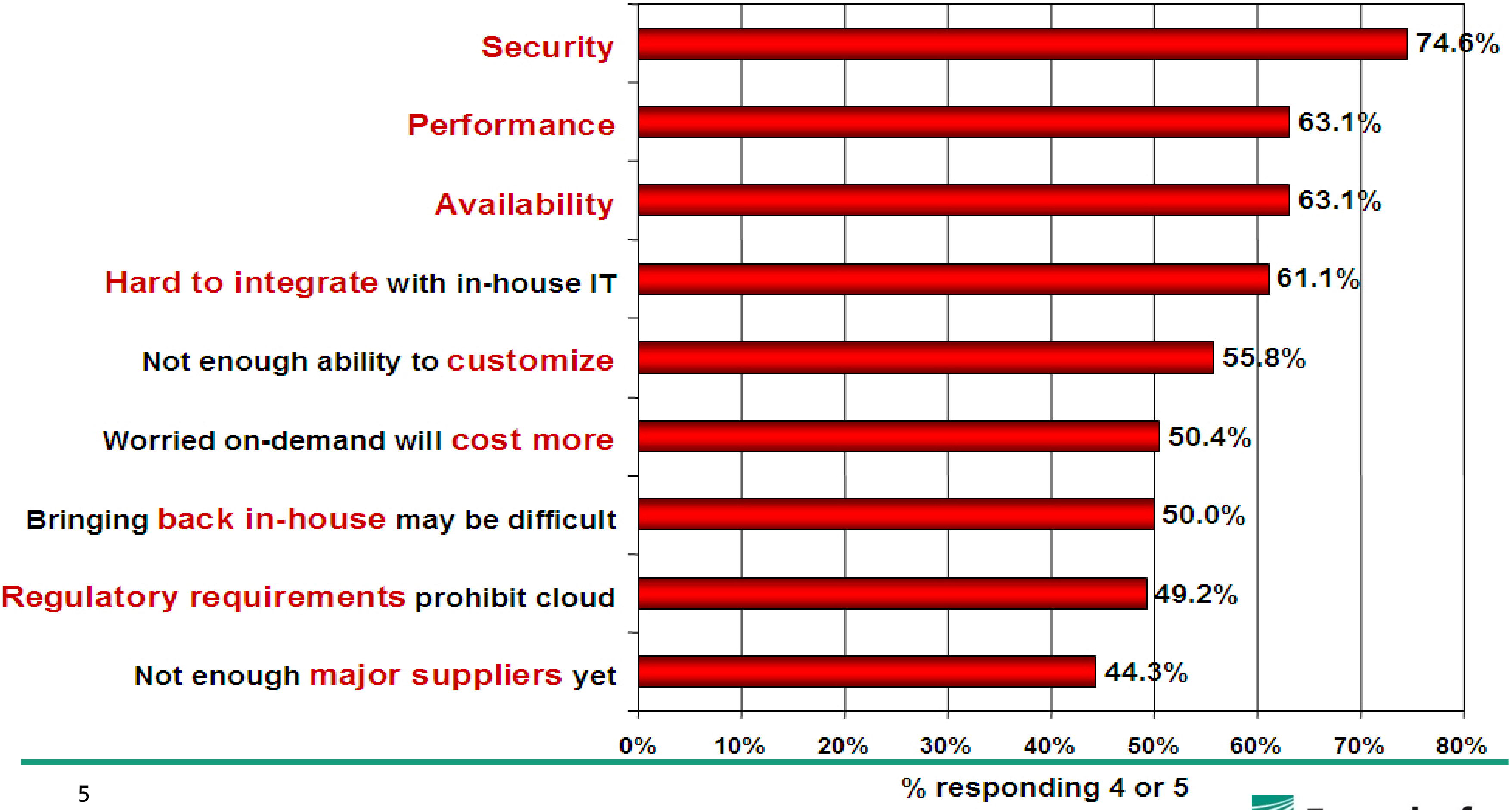
The elimination of an up-front commitment by Cloud users

The ability to pay for use of computing resources on a short-term basis as needed

(Source: Berkley, Above the Clouds, 2009)

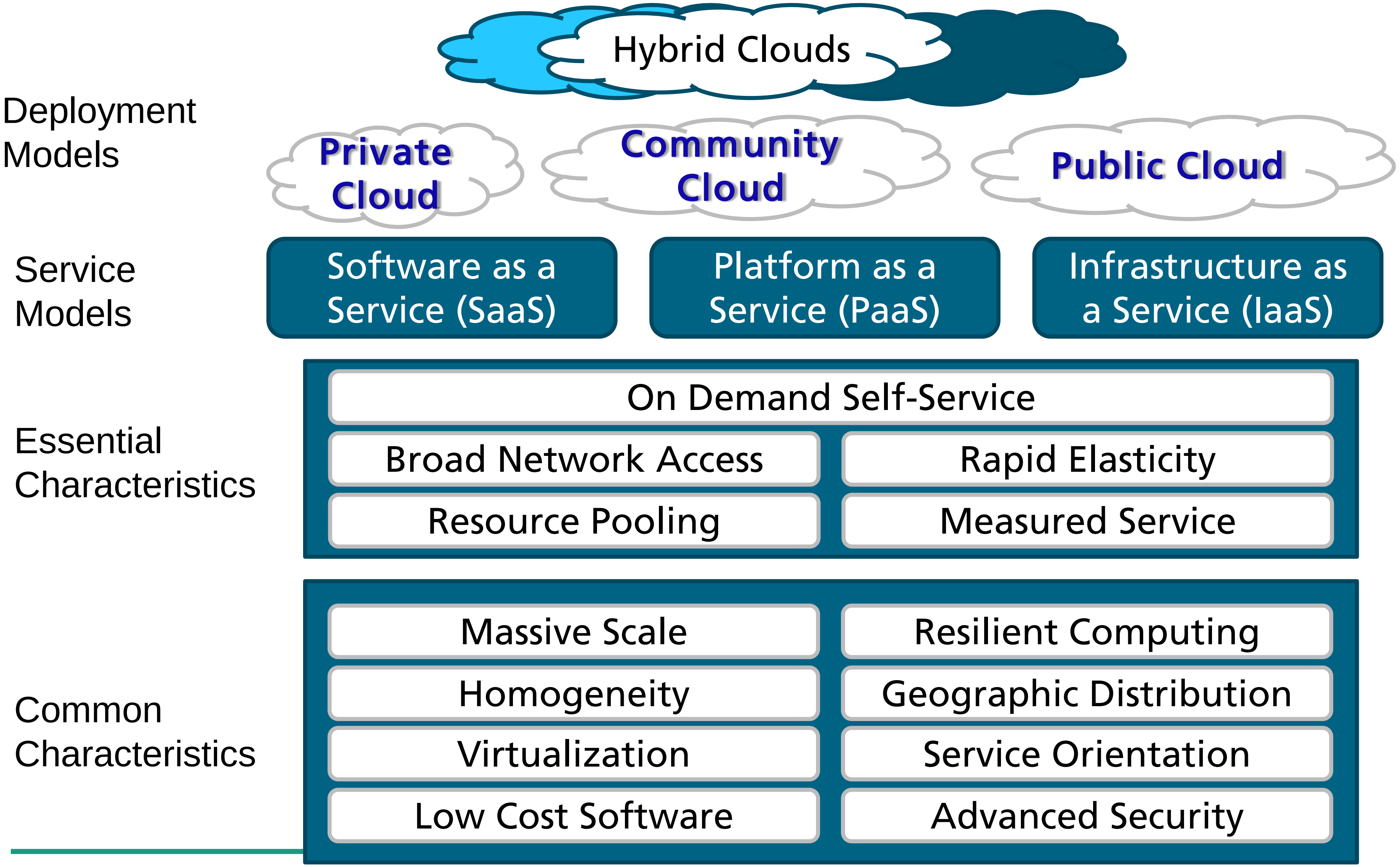
Security is the Major Issue

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

The NIST Cloud Definition Framework



Hybrid Clouds

Deployment Models

Private Cloud

Community Cloud

Public Cloud

Service Models

Software as a Service (SaaS)

Platform as a Service (PaaS)

Infrastructure as a Service (IaaS)

Essential Characteristics

On Demand Self-Service

Broad Network Access

Rapid Elasticity

Resource Pooling

Measured Service

Common Characteristics

Massive Scale

Resilient Computing

Homogeneity

Geographic Distribution

Virtualization

Service Orientation

Low Cost Software

Advanced Security

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

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 in Clouds is a Trust Issue

“IT security is about trust. You have to trust your CPU manufacturer, your hardware, operating system and software vendors -- and your ISP. Any one of these can undermine your security: crash your systems, corrupt data, allow an attacker to get access to systems. We've spent decades dealing with worms and rootkits that target software vulnerabilities. We've worried about infected chips. But in the end, we have no choice but to blindly trust the security of the IT providers we use.

Saas moves the trust boundary out one step further -- you now have to also trust your software service vendors -- but it doesn't fundamentally change anything. It's just another vendor we need to trust.”

(Source: Bruce Schneier, Schneier on Security: Cloud Computing, 2009)

Security in Clouds is a Trust Issue

A good way to generate trust for a cloud vendor is transparent security.

GRC in Clouds

Governance

- Policy design
- Classification schema for data and processes
- Trust chain in a cloud

Risk

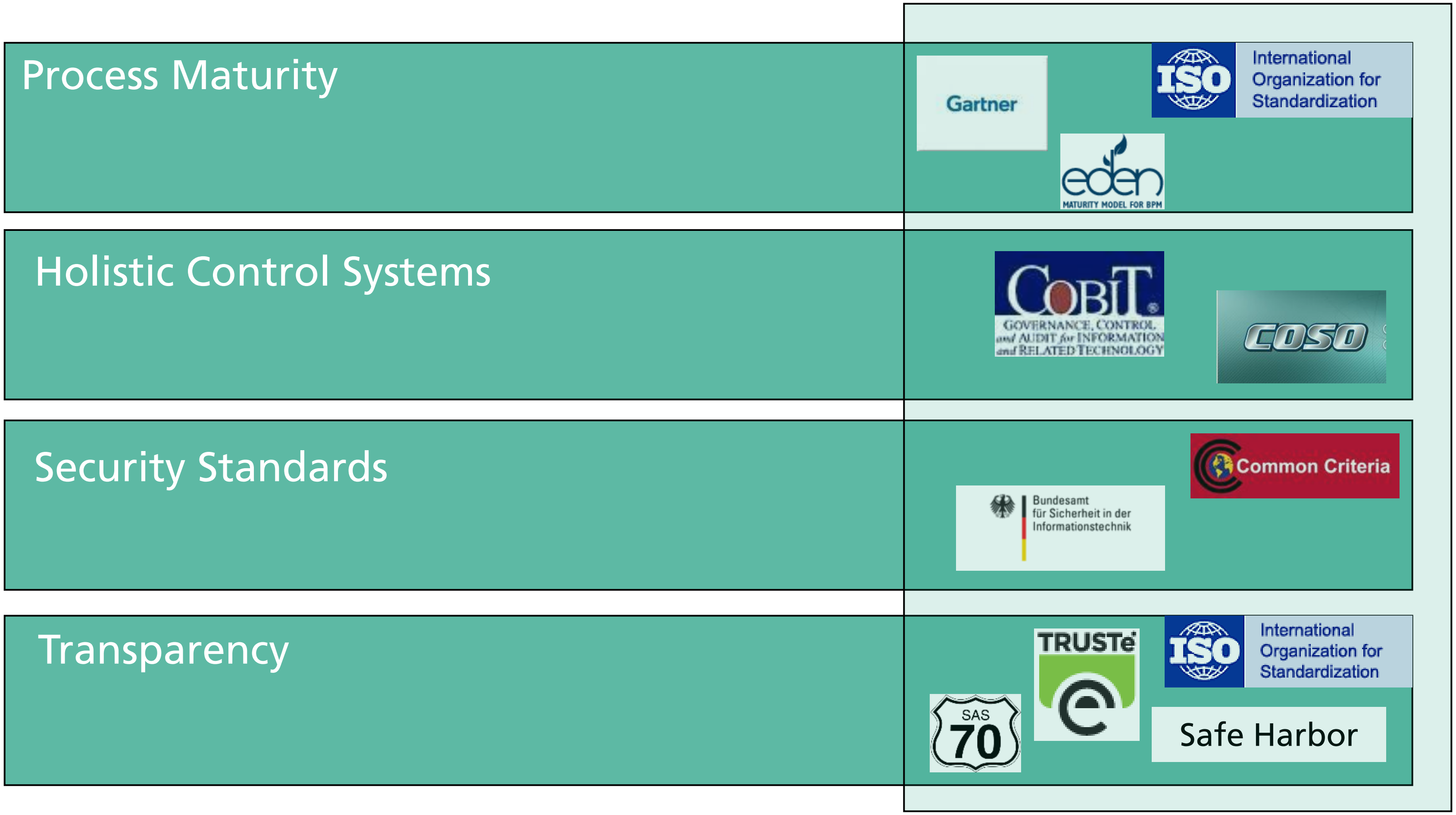
- Risk strategy
- Business Impact Analysis
- Threat and Vulnerability Analysis
- Risk Analysis Remediation

Compliance

- Policy enforcement
- Legal compliance (SOX, SOLVENCY II)
- Control implementation

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

Cloud GRC Related Standards



Process Maturity

Holistic Control Systems

Security Standards

Transparency

Gartner
ISO International Organization for Standardization
eden MATURITY MODEL FOR BPM
COBIT GOVERNANCE, CONTROL and AUDIT for INFORMATION and RELATED TECHNOLOGY
COSO
Common Criteria
Bundesamt für Sicherheit in der Informationstechnik
TRUSTe
ISO International Organization for Standardization
SAS 70
Safe Harbor

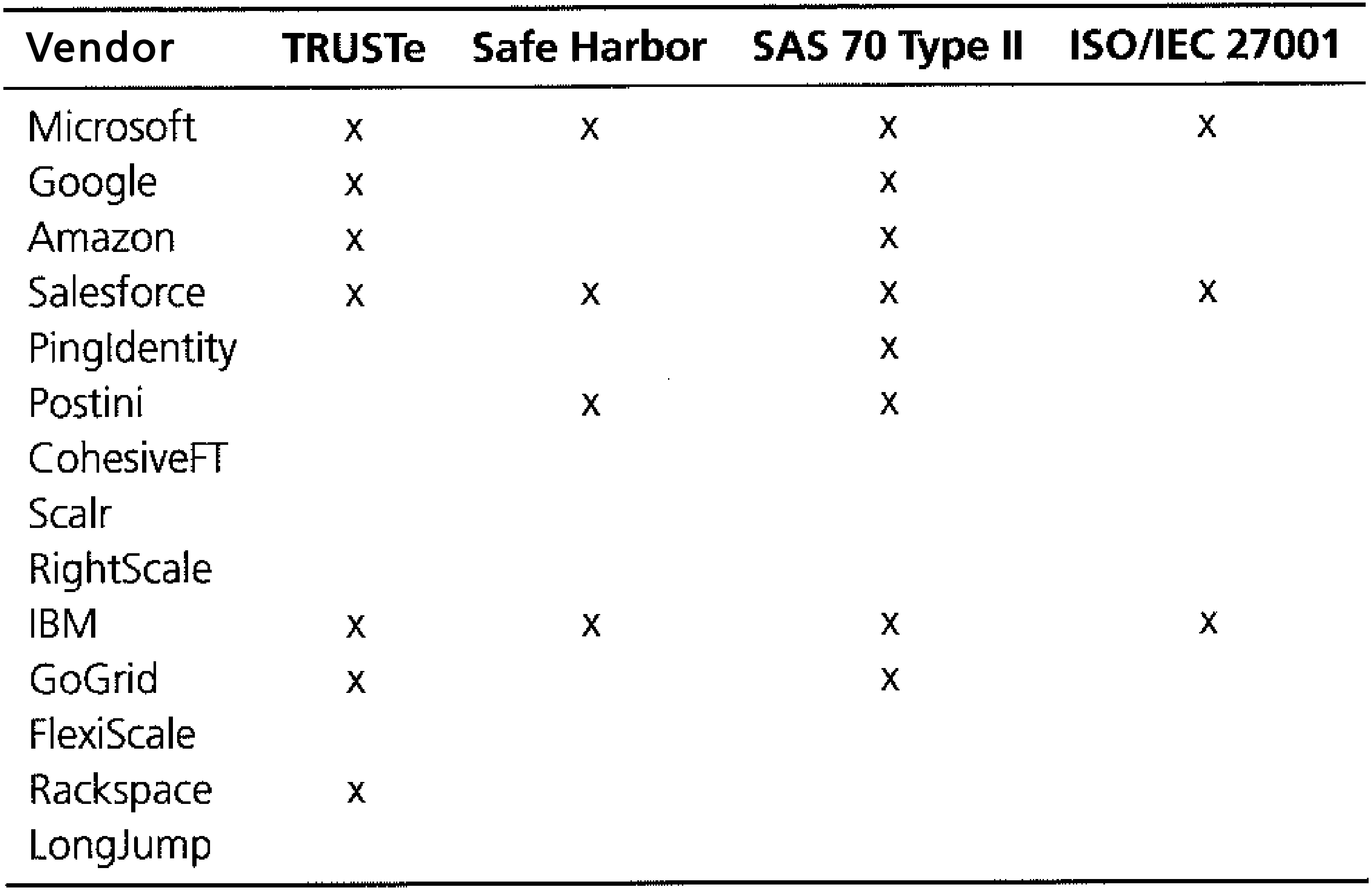
Security Level Assurance (SLA)

- 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?

Cloud Security Vendor Evaluation

- 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 in an unencrypted fashion
  - Amazon stores data permanent → after it is 5 Minutes in the cloud

Security certificats of the cloud vendors



Vendor	TRUSTe	Safe Harbor	SAS 70 Type II	ISO/IEC 27001
Microsoft	x	x	x	x
Google	x		x	
Amazon	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)

Security as a Service

- Google Message Security
    - 12$ per anno - per user
- Identitiy Management von PingIdentity
    - 1€ per user - per application - per month
- VPN-Cubed for EC2 von CohesiveFT
    - Connection of 2 Servers are for free
    - Connection of 4 Servers are 0.05$ per hour

Compliance

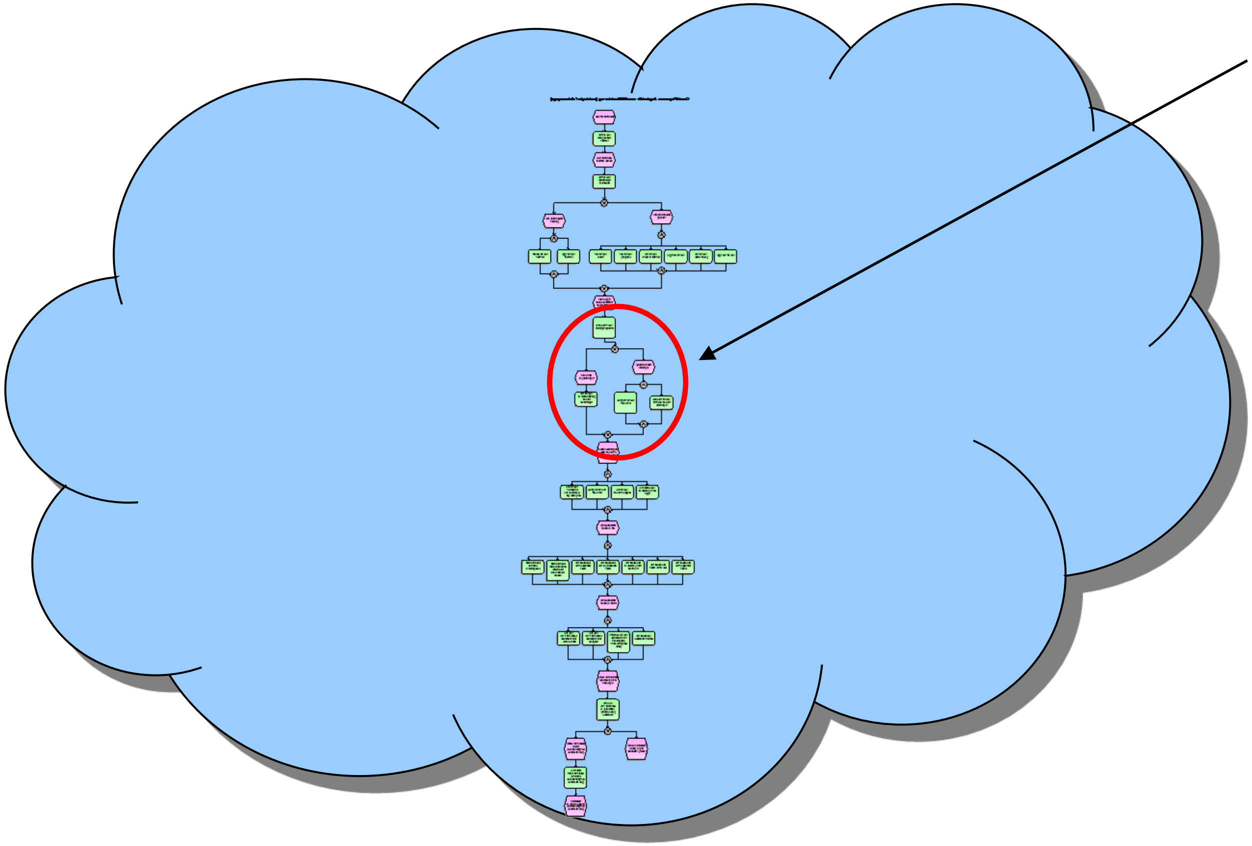
- Compliance is the adherence of regulations. These can be legal regulations, governance regulations or regulations of any other kind. In the context of this work we use compliance as the goal to adhere to laws and security goals.
- The automated verification of security goals supports the build up of 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 Scenarios

- Customer → Cloud:
  - Security Compliance:
    - Check the security processes of the cloud to 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

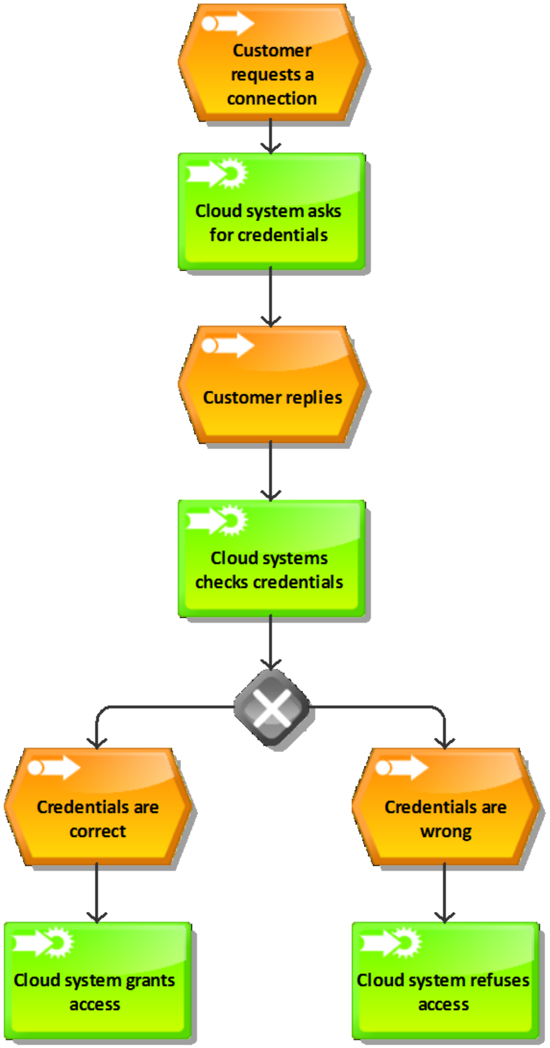
Trust is good, Compliance is better

- Business Process Analysis of the clouds IT security properties.



Compliance Risk

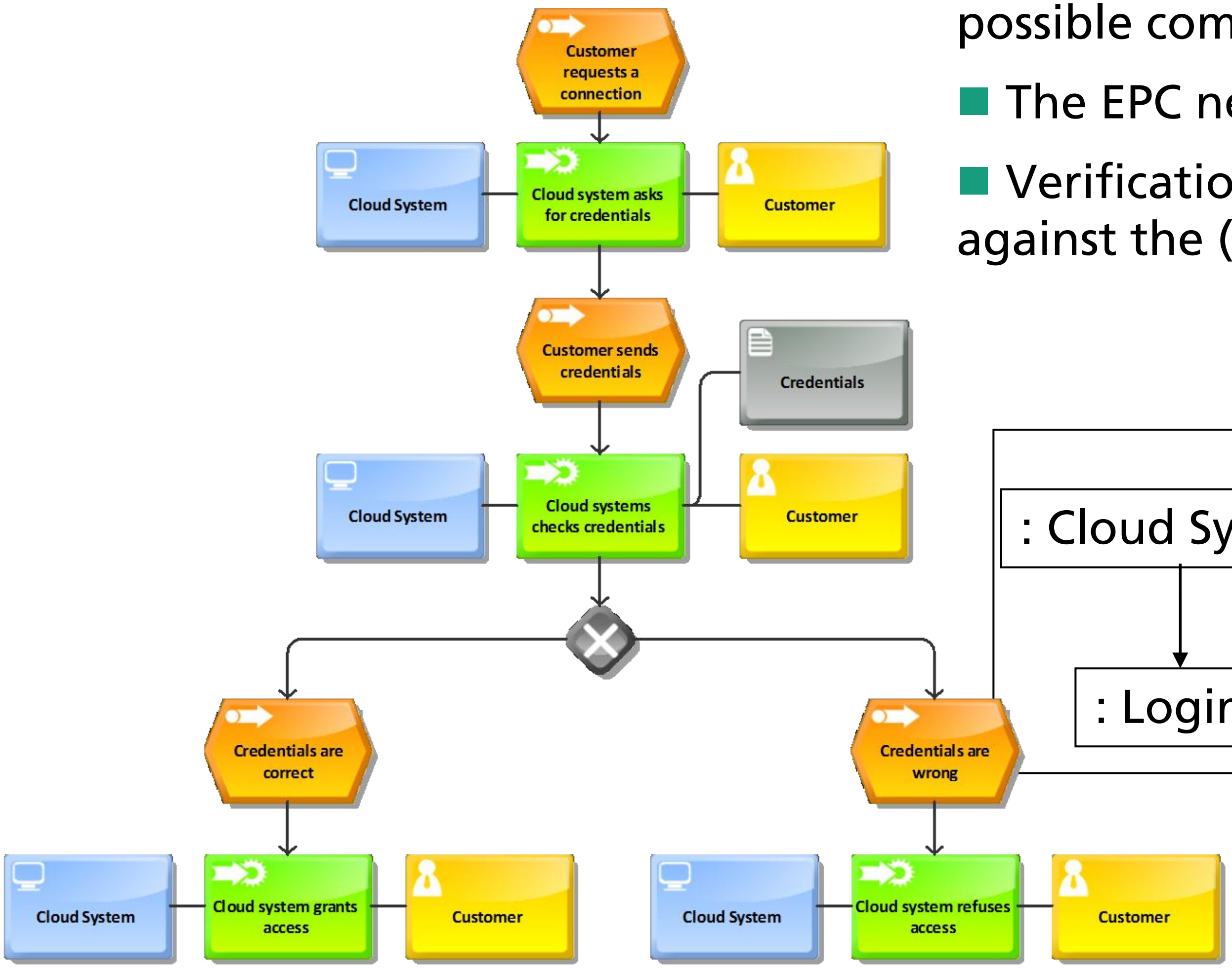
Example Cloud Authentication

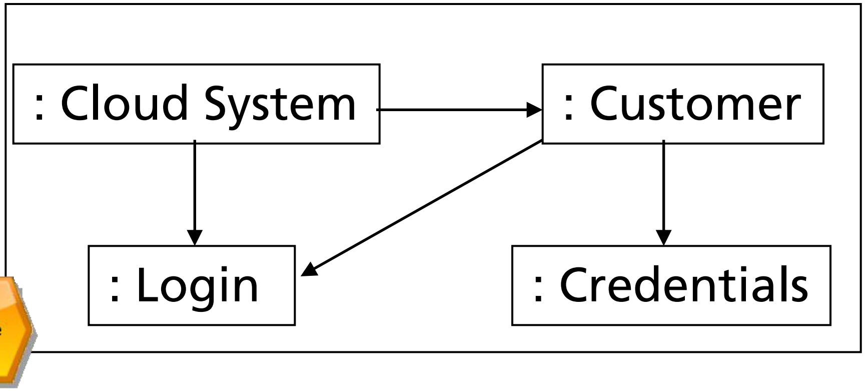

Customer requests a connection
Cloud system asks for credentials
Customer replies
Cloud systems checks credentials
Credentials are correct
Credentials are wrong
Cloud system grants access
Cloud system refuses access

- We aim towards an automated compliance analysis
- The analysis will work in two phases:
  1. A structure analysis of the EPC for a possible compliance violation pattern
  2. Second a text-based analysis of the word in the EPC functions

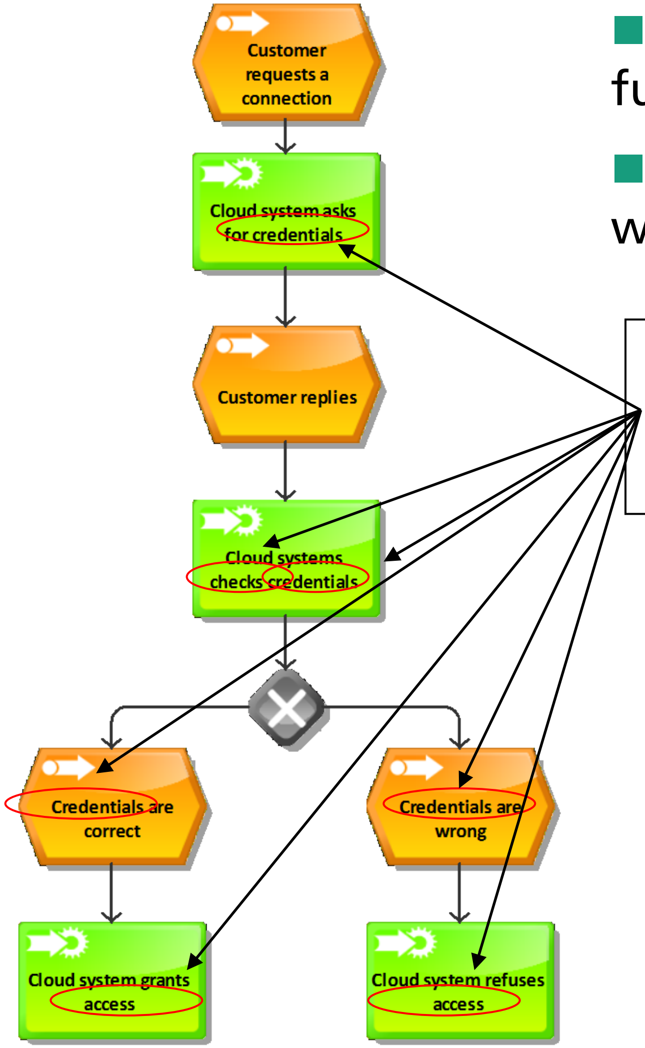
Example Cloud Authentication

- A structure analysis of the EPC for a possible compliance pattern
- The EPC needs to be augmented
- Verification against a control pattern against the (Meta-)Model of the EPC


Customer requests a connection
Cloud System
Cloud system asks for credentials
Customer
Customer sends credentials
Credentials
Cloud System
Cloud systems checks credentials
Customer
Credentials are correct
Credentials are wrong
Cloud System
Cloud system grants access
Customer
Cloud System
Cloud system refuses access
Customer



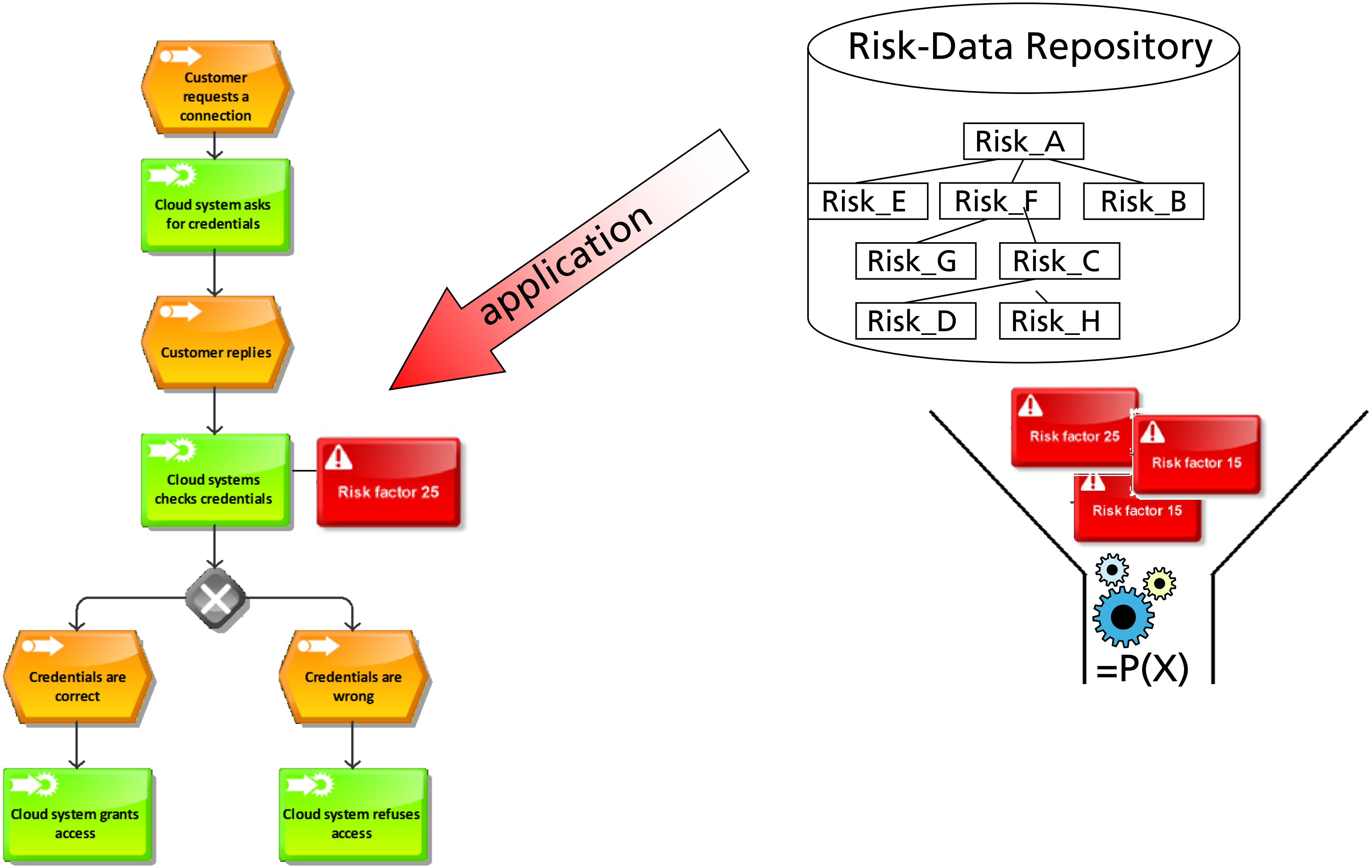
Example Cloud Authentication


Customer requests a connection
Cloud system asks for credentials
Customer replies
Cloud systems checks credentials
Credentials are correct
Credentials are wrong
Cloud system grants access
Cloud system refuses access

- 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

Automated cloud risk identification and aggregation



Customer requests a connection

Cloud system asks for credentials

Customer replies

Cloud systems checks credentials

Risk factor 25

Credentials are correct

Credentials are wrong

Cloud system grants access

Cloud system refuses access

application

Risk-Data Repository

Risk_A

Risk_E

Risk_F

Risk_B

Risk_G

Risk_C

Risk_D

Risk_H

Risk factor 25

Risk factor 15

Risk factor 15

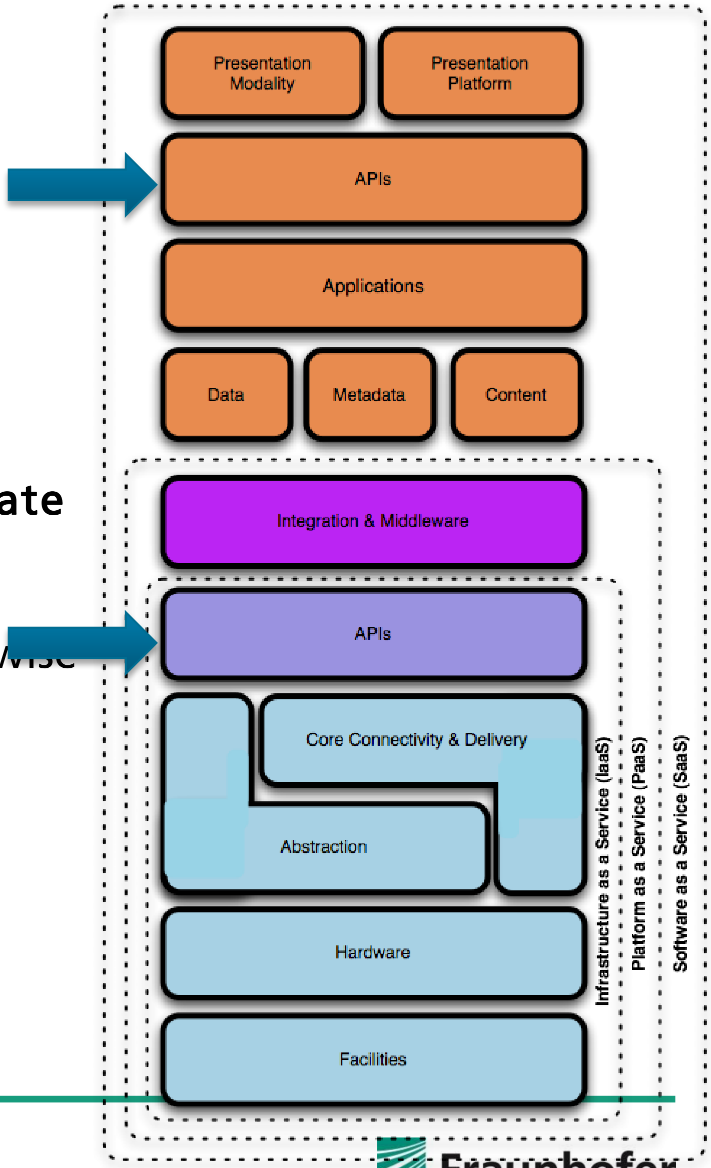
=P(X)

CloudAudit (A6) Overview

A6 is the geeky byline for the working group of CloudAudit and stands for:
Automated Audit, Assertion, Assessment, and Assurance API

The goal of CloudAudit is to provide a **common interface** that allows Cloud providers to **automate the Audit, Assertion, Assessment, and Assurance** of their environments and allow authorized consumers of their services to do likewise **via an open, extensible and secure API**.

(Source: Cloud Audit A6 Group)



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?

Last Slide

"Trust is a concept as old as humanity, and the solutions are the same as they have always been. Be careful who you trust, be careful what you trust them with, and be careful how much you trust them. Outsourcing is the future of computing. Eventually we'll get this right, but you don't want to be a casualty along the way."

(Source: Bruce Schneier, Schneier on Security: Cloud Computing, 2009)

Where can I learn more?

- The Fraunhofer-Attract-Group >>APEX<<: http://www.isst.fraunhofer.de/geschaeftsfelder/insuranceandfinance/refpro/gruppe-apex/
- The Cloud Security Alliance, homepage,http://www.cloudsecurityalliance.org/, 2009
- Cloud Computing Sicherheit - Schutzziele.Taxonomie.Marktübersicht, Fraunhofer Institute for Secure Information Technology SIT,2009
- Above the Clouds: A Berkeley View of Cloud Computing, technical report, UCB/EECS-2009-28, EECS Department University of California, Berkeley ,2009.
- IT-Grundschutz und Cloud Computing, SECMGT Workshop , BSI, 2009
- Cloud Security, TüV Informationstechnik GmbH, 2009
- Effectively and Securely Using the Cloud Computing Paradigm, NIST, 2009
- Cloud Audit A6, http://www.cloudaudit.org/page3/page3.html, 2010
- yo delmars blog, http://yogrc.typepad.com/yo_delmars_grc_and_beyond/2009/11/the-grcenabled-cloud-governance-risk-and-compliance-may-be-simpler-faster-cheaper-more-trusted-event.html, 2010