Security and Compliance in Clouds

Pattern-Based Compliance and Security Requirements Engineering

Martin Hirsch, Jan Jürjens, Jan-Christoph Küster

Fraunhofer Institut für Software- und Systemtechnologie ISST, Dortmund

iqnite 2011, Düsseldorf

24. May 2011

Contact: *jan-christoph.kuester@isst.fraunhofer.de*

Fraunhofer ISST

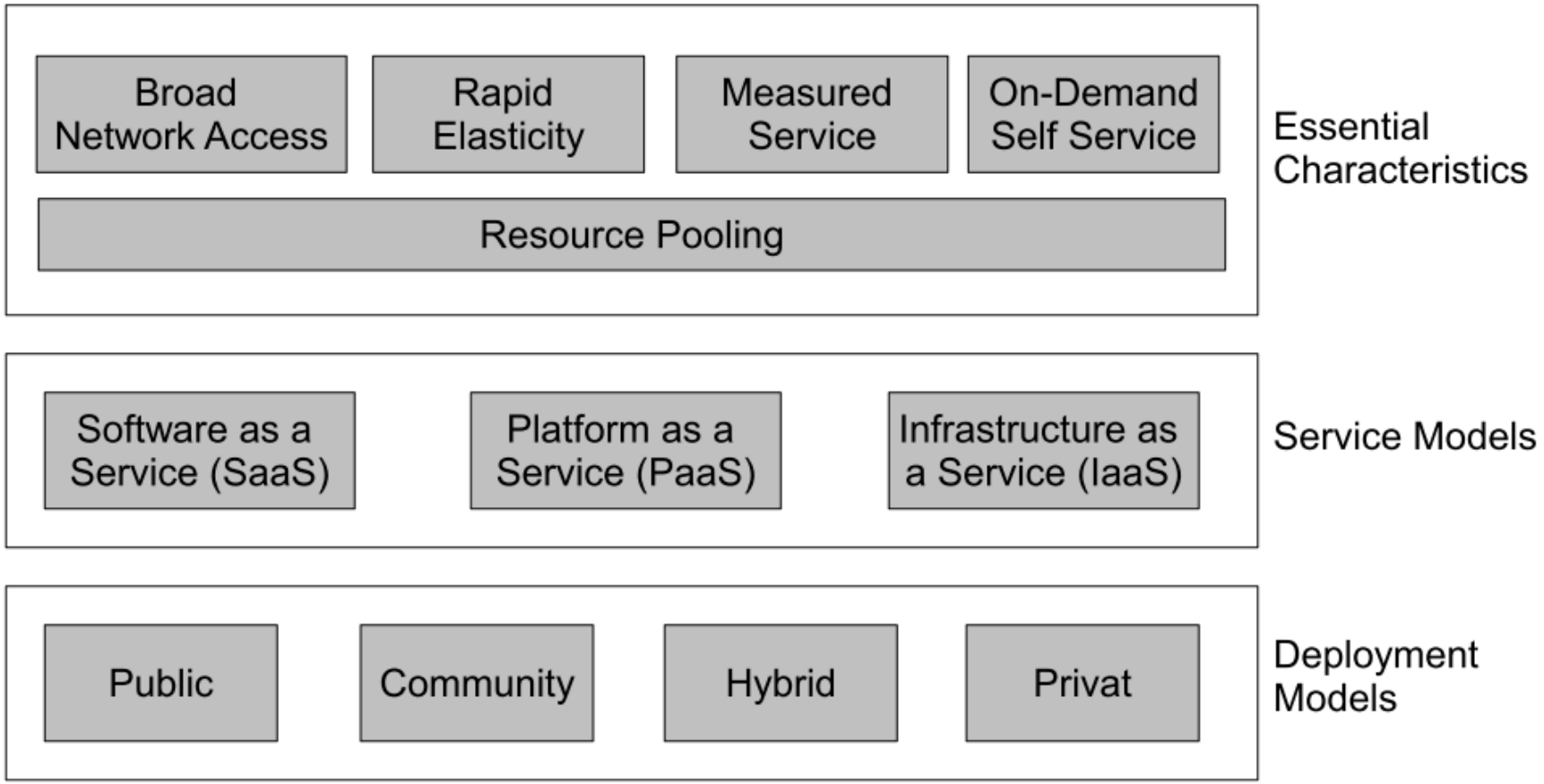
Architectures for Auditable Business Process Execution (APEX)

- Tool supported methods for security and compliance checks on business processes
  - Modeling time: Syntax checks of models
  - Runtime: Conformance checks with log data
- Analysis based on different types of models
  - BPMN2.0, UMLsec or system log data
- Attract-Program at Fraunhofer ISST
- Focus on insurance domain

Agenda

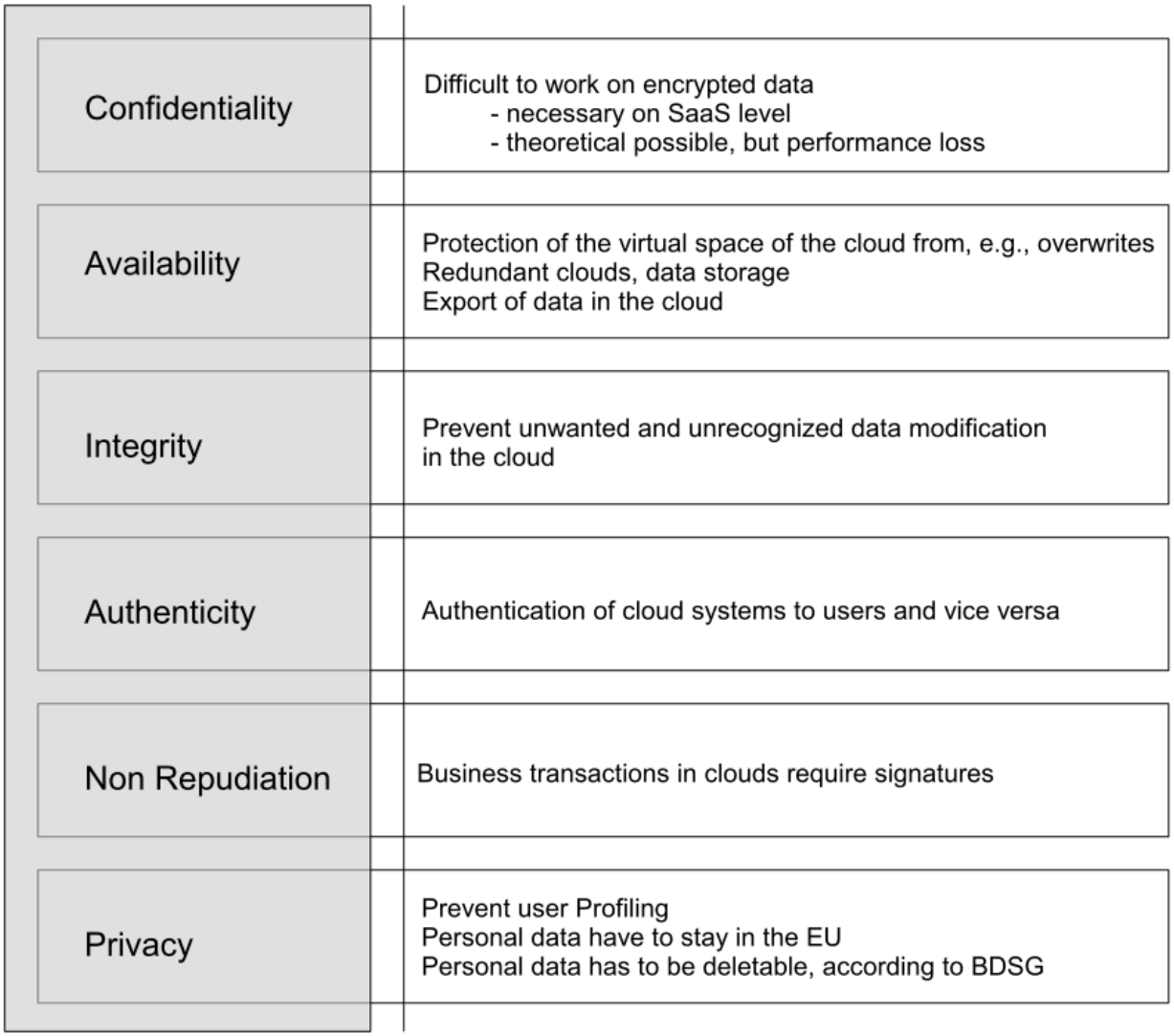
- NIST Cloud Definition Framework
- Cloud Security and Compliance Goals
  - Challenges and Conflicts
- Pattern-Based Compliance and Security Engineering
  - Cloud System Analysis Pattern
  - Example: Cloud Online Banking Scenario
  - Supporting the Information Security Standard ISO 2700x
- Vision and Future Work

The NIST Cloud Definition Framework



P. Mell and T. Grance, “The NIST definition of cloud computing,”
Working Paper of the National Institute of Standards and Technology (NIST), 2009

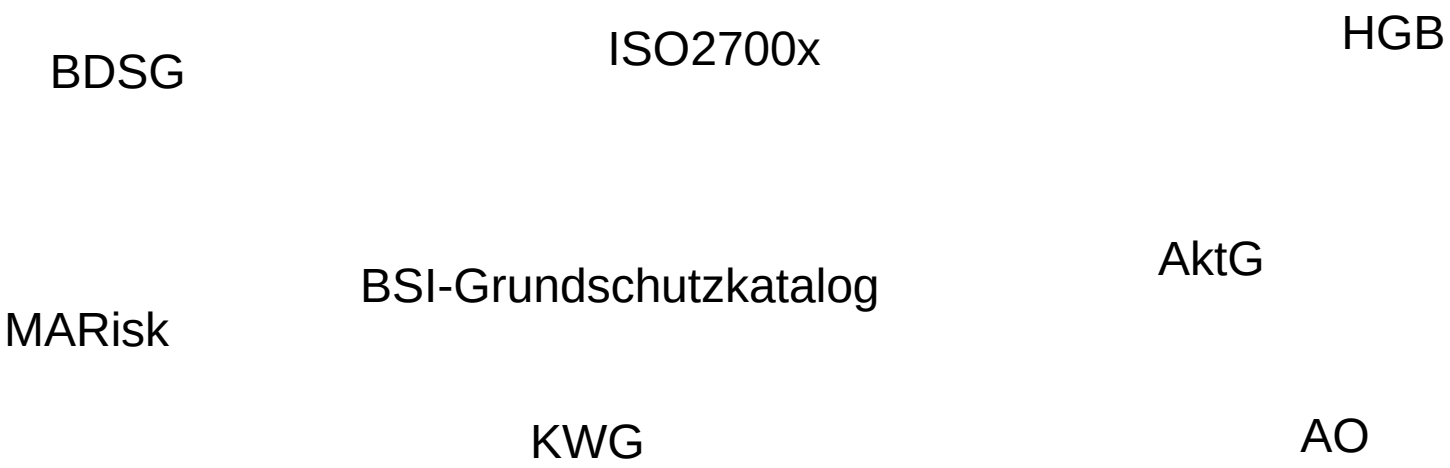
Cloud Security Goals



Regulatory compliance

- Compliance management is a “broad term covering all activities and methods to ensure that a company follows all policies required by an external or internal regulation”

  E. K. Marwane and S. Stein, “Policy-based semantic compliance checking for business process management”, 2008.



- Even for a small outsourcing task, a huge number of laws might become relevant

Regulatory compliance

- Compliance management is a “broad term covering all activities and methods to ensure that a company follows all policies required by an external or internal regulation”

E. K. Marwane and S. Stein, “Policy-based semantic compliance checking for business process management”, 2008.

- §91, 93 AktG
- Responsibility of management to implement early warning risk management
- Not mentioned explicitely, but also for IT

BDSG

AktG

BSI-Grundschutzhandbuch

MARisk

KWG

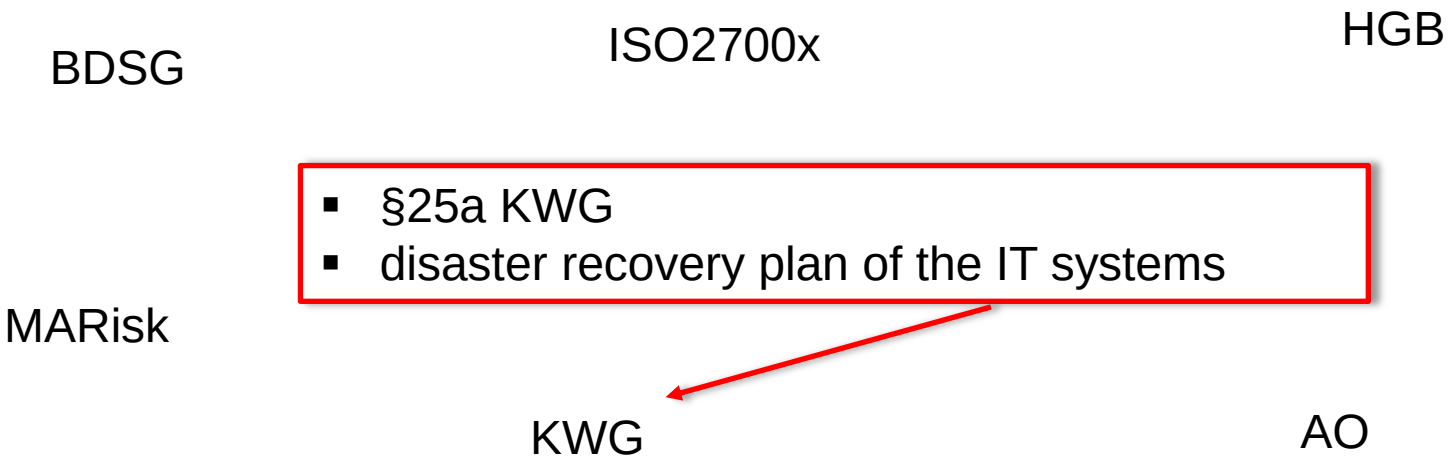
AO

- Even for a small outsourcing task, a huge number of laws might become relevant

Regulatory compliance

- Compliance management is a “broad term covering all activities and methods to ensure that a company follows all policies required by an external or internal regulation”

  E. K. Marwane and S. Stein, “Policy-based semantic compliance checking for business process management”, 2008.

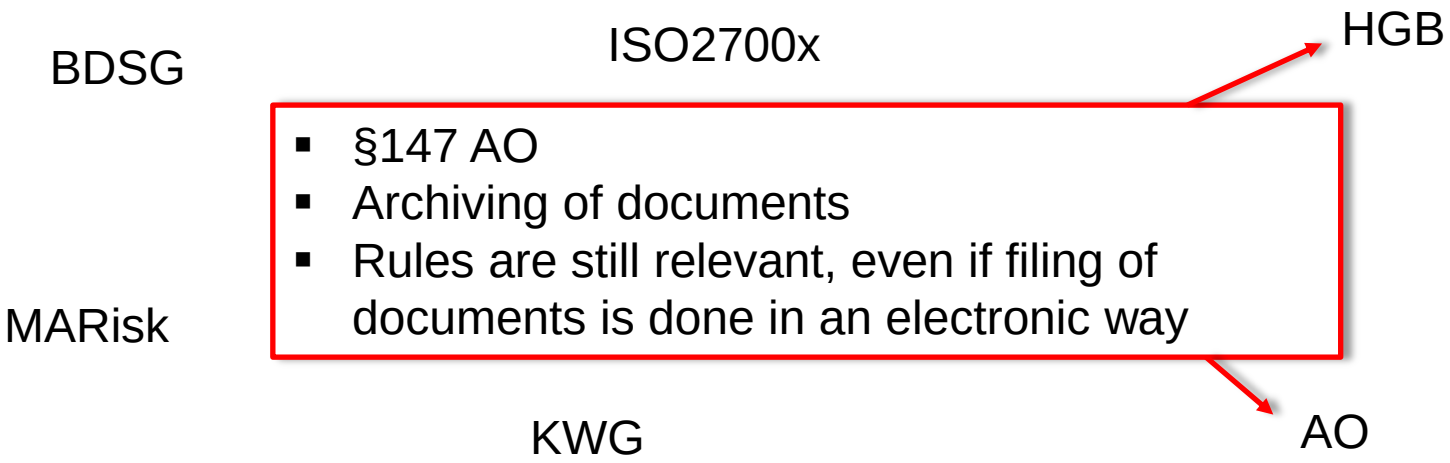


- Even for a small outsourcing task, a huge number of laws might become relevant

Regulatory compliance

- Compliance management is a “broad term covering all activities and methods to ensure that a company follows all policies required by an external or internal regulation”

  E. K. Marwane and S. Stein, “Policy-based semantic compliance checking for business process management”, 2008.

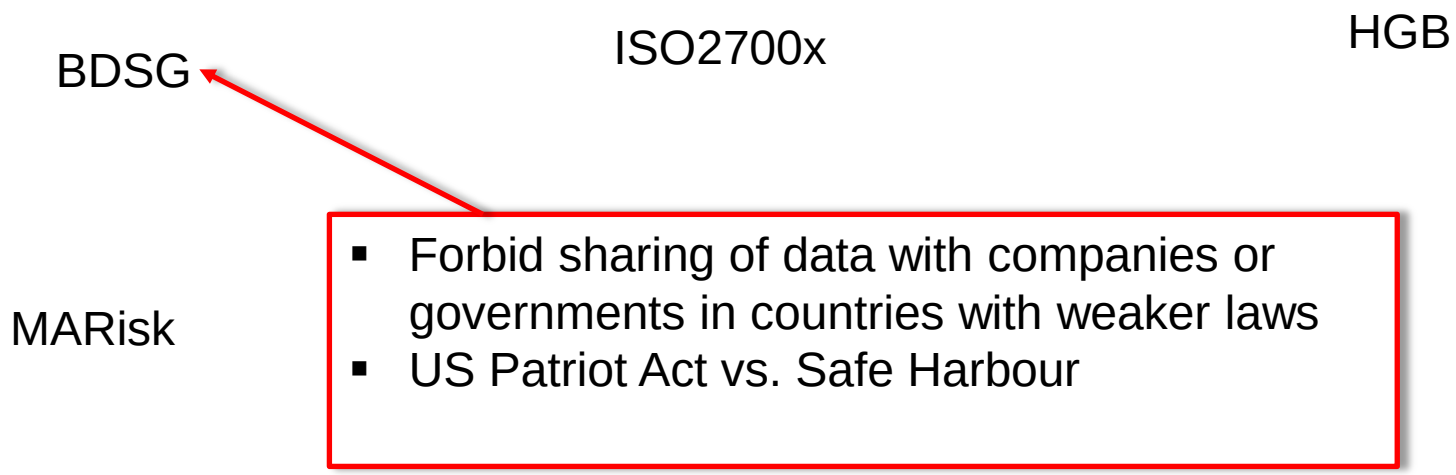


- Even for a small outsourcing task, a huge number of laws might become relevant

Regulatory compliance

- Compliance management is a “broad term covering all activities and methods to ensure that a company follows all policies required by an external or internal regulation”

  E. K. Marwane and S. Stein, “Policy-based semantic compliance checking for business process management”, 2008.



- Even for a small outsourcing task, a huge number of laws might become relevant

Motivation

Cloud Computing is a specific case of outsourcing:

- Short term outsourcing decisions are possible
- Multiple customers on one outsourcing platform
- The scope of IT outsourcing increases

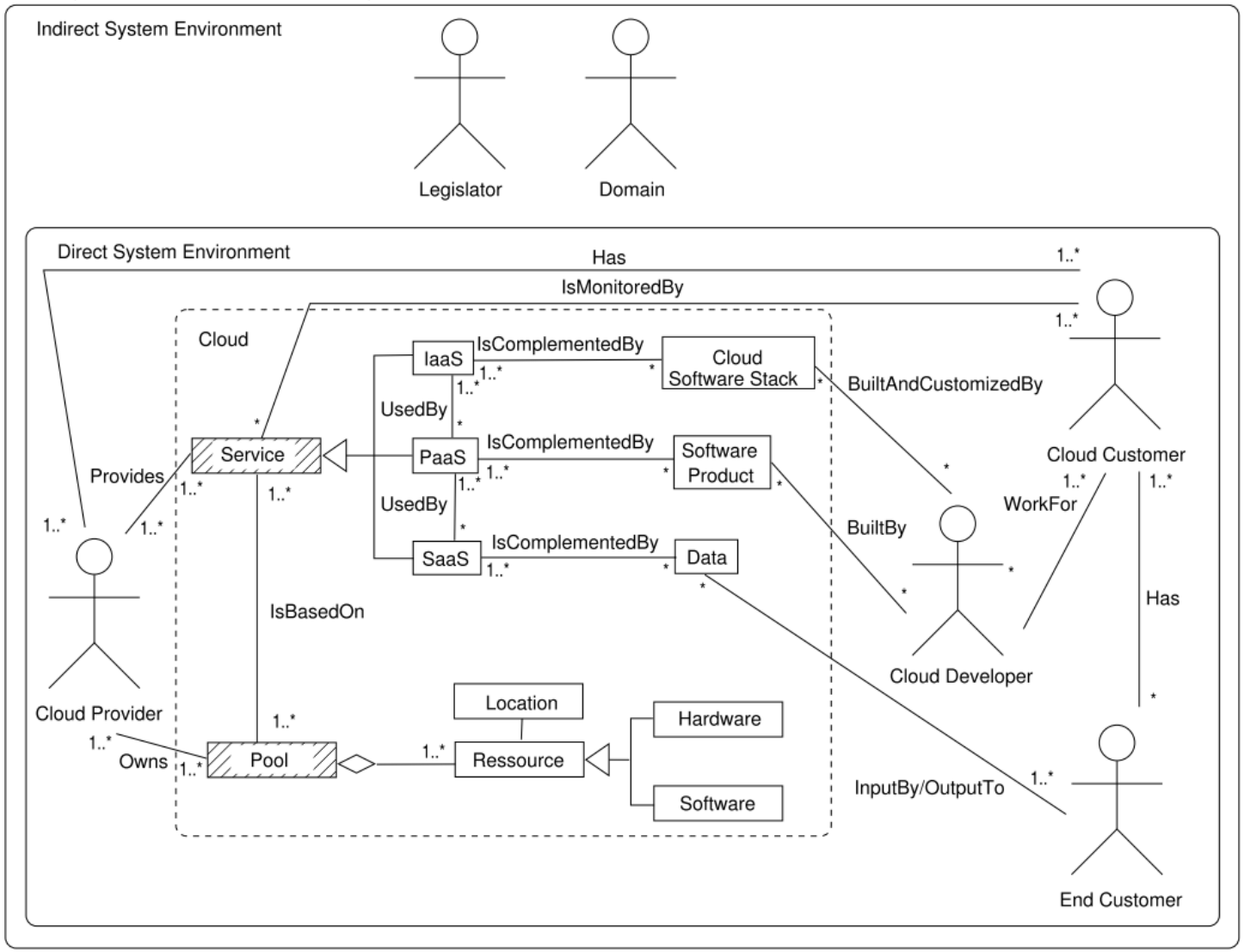
Security and Compliance:

- Identifying relevant security requirements, laws and regulations for an international cloud scenario is a challenge:
  - Complex environment with many stakeholders
  - Location independence

Patterns:

- Pattern-based approaches ease and provide a structured way of elicitation of security or compliance requirements
- Offer re-usability and tool-support

Cloud System Analysis Pattern



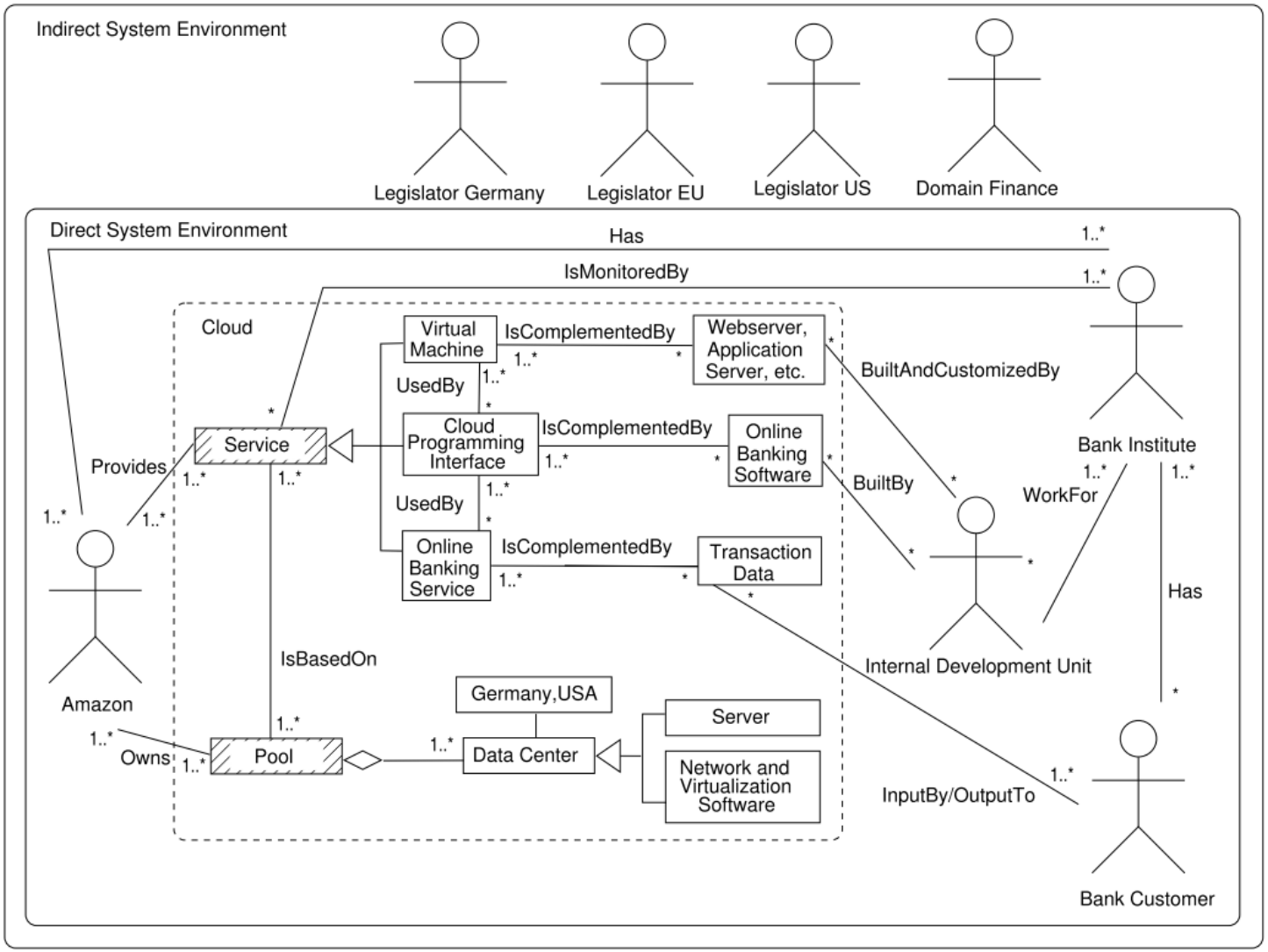
Beckers, Faßbender, Küster, Schmidt, „A Pattern-Based Method for Identifying and Analysing Laws in the Field of Cloud Computing Compliance“, ARES 2011, to appear.

Example: Cloud Online Banking Scenario

A *German* bank plans to offer online banking services, that includes:

- Offering service access to customers in *Germany* via web interface
- Integrate significant scalability in terms of customers using the online banking services
- Customer data, e.g., account information, amount and transaction histories are stored in the cloud
- Task a subsidiary with the required software development
- Outsource the affected IT processes to a cloud provider in the *USA*

Instantiated Cloud System Analysis Pattern

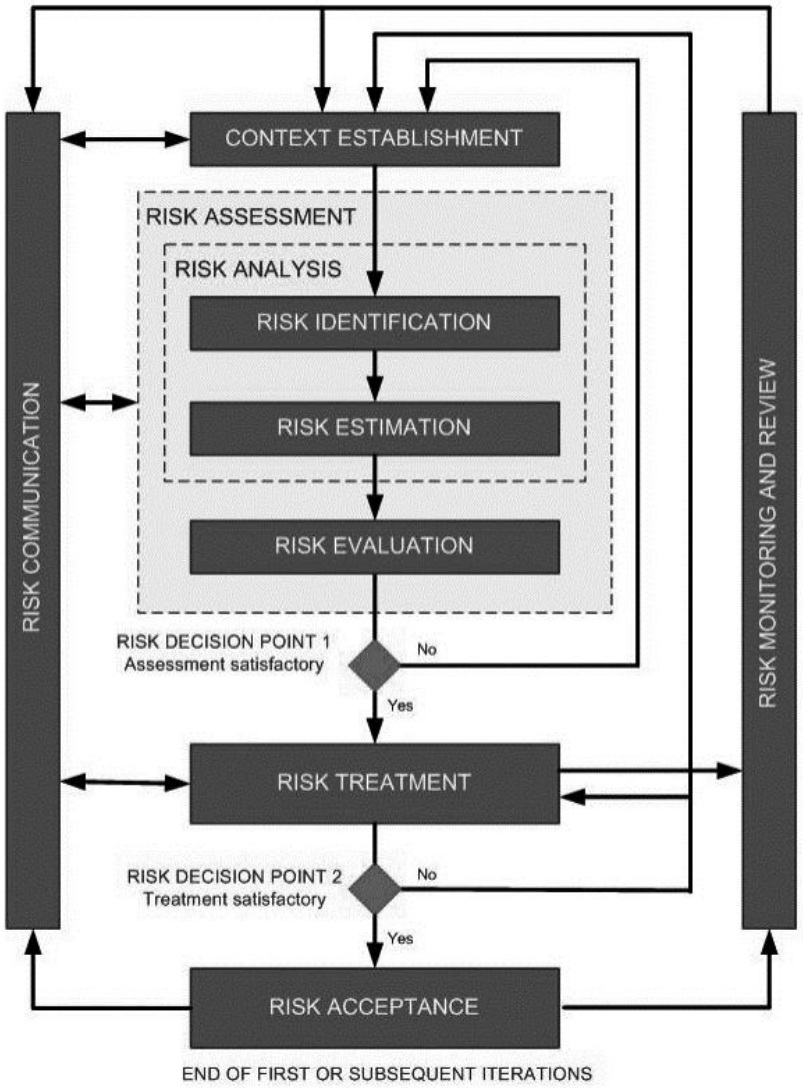


Fraunhofer ISST

Direct Stakeholder Template

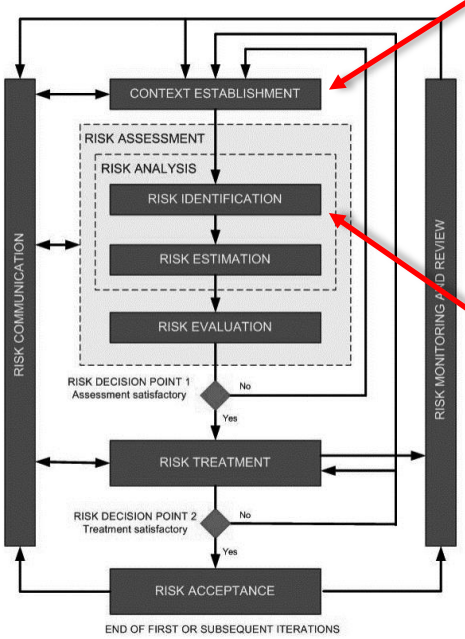
		Instance
Name	The identifier of the stakeholder	Bank Customer
Description	Describe the stakeholder informally	The *Bank Customer* uses the online banking service of the *Bank Institute*
Relations to the cloud	Inputs/outputs relation between the stakeholder and the cloud, e.g., kind of data or software	*Input:* Financial transaction data, personal related data *Output:* Transaction history
Motivation	Stakeholder's motivation for using the cloud → e.g., consider relations to the cloud	The *Bank Customer* wants cheap and secure financial transactions via the bank's cloud computing offer
Relations to other direct stakeholders	The kind of dependency between the stakeholders, e.g., *served by, controlled by contract, influenced by customer-demand*	*Served by:* Bank Institute as SaaS-Provider *Influenced by customer-demand:* Security, Availability, Performance, Cost
Assets	Assets relevant for this stakeholder → e.g., consider relations to the cloud	Financial transaction data, personal related data
Compliance and Privacy	Identify relevant laws/regulations for the cloud scenario	BDSG

ISO 27005 - Information Security Risk Management

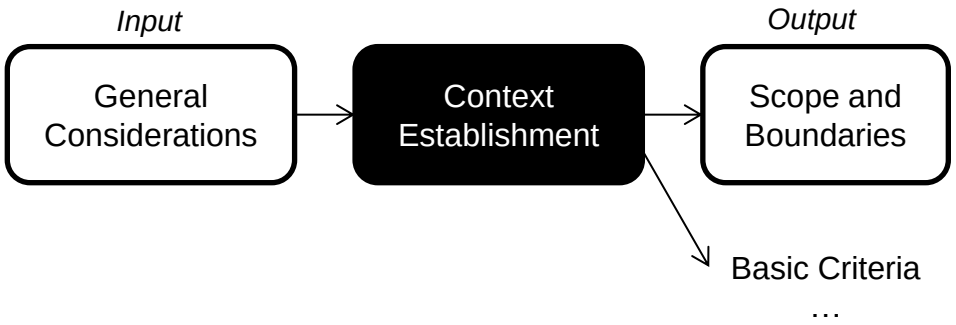


ISO/IEC, “Information technology - security techniques - information security risk management,” ISO/IEC 27005, 2008

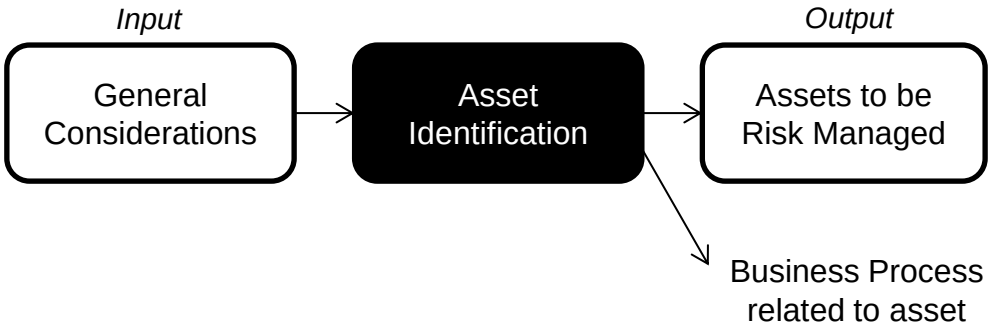
Context Establishment and Asset Identification in ISO 27005



Context Establishment (ISO 27005, Clause 7)



Asset Identification (ISO 27005, Clause 8.2.1.2)

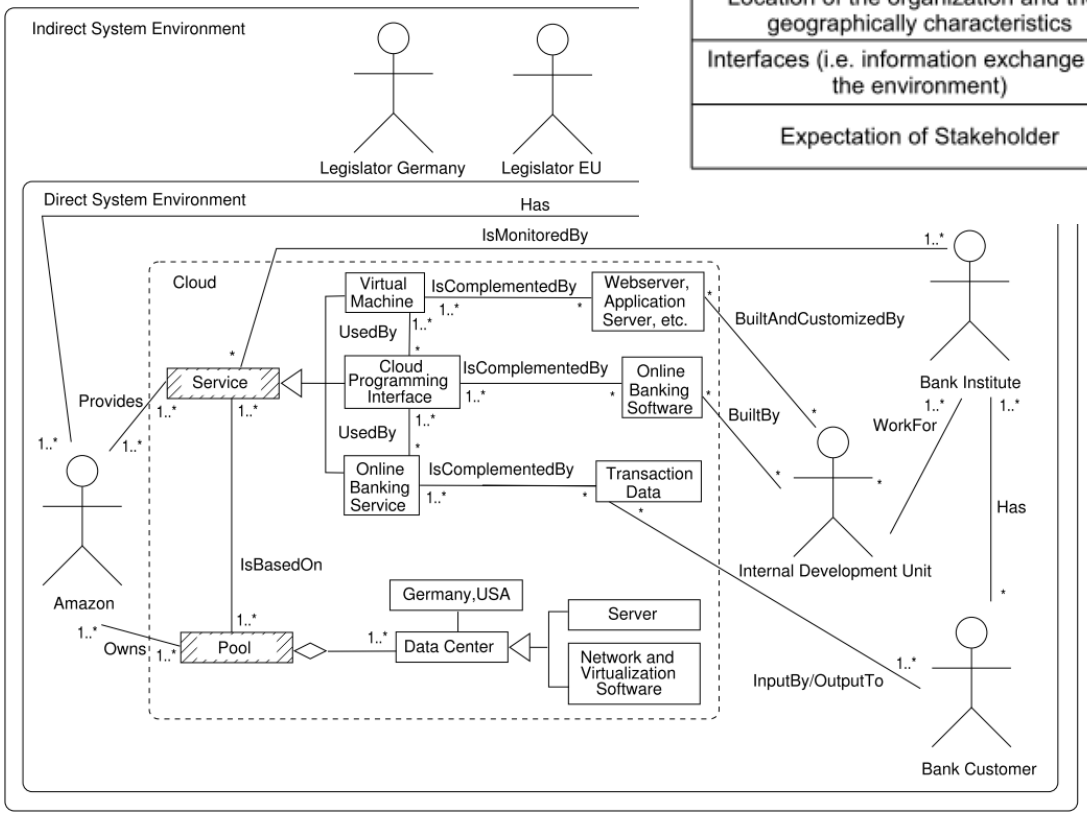


Fraunhofer ISST

Instantiated Cloud System Analysis Pattern

Context Establishment

	Cloud Analysis Pattern
The organization's strategic business objectives, strategies and policies	Motivation in stakeholder template
Location of the organization and their geographically characteristics	Location information in the cloud analysis pattern
Interfaces (i.e. information exchange with the environment)	Relations in the cloud analysis pattern
Expectation of Stakeholder	Collecting security requirements

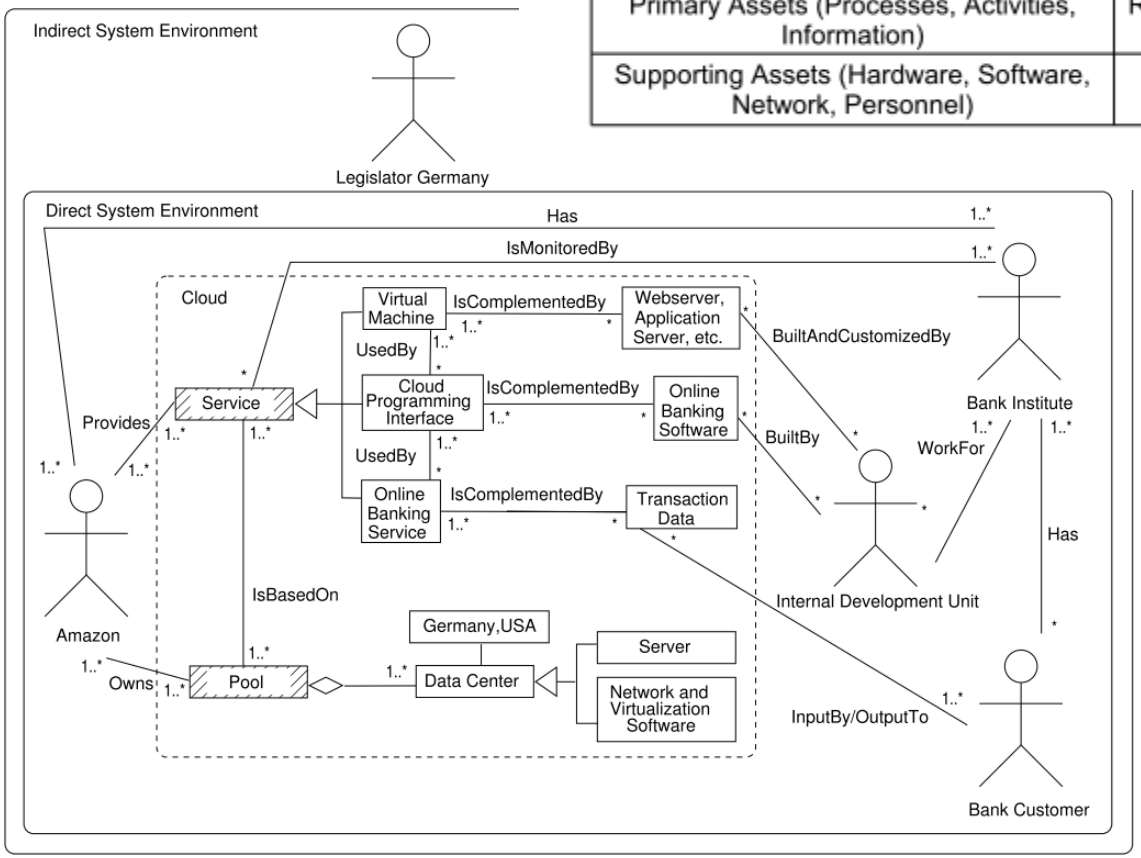


Fraunhofer ISST

Pattern-based Support for Context Establishment and Asset Identification in ISO 27005

Asset Identification

	Cloud Analysis Pattern
Primary Assets (Processes, Activities, Information)	Relations between direct stakeholder and the cloud
Supporting Assets (Hardware, Software, Network, Personnel)	Instantiated boxes of the cloud



- Asset owner
- Types of information:
  - Vital
  - Personal
  - Strategic
  - High-cost

Fraunhofer ISST

Conclusion and Future Work

Conclusion:

- Conflicts of Cloud Security Goals
- Identifying of Security and Compliance Requirements challenging
- Pattern-based analysis of cloud scenarios
- Support of ISO 2700x standard

Future Work:

- Requirements engineering method for cloud security and compliance
- Tool-Support, e.g., recommender-system