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

ignite 2011, Düsseldorf
24. May 2011
Contact: jan-christoph.kuester@isst.fraunhofer.de
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

Essential Characteristics

- Broad Network Access
- Rapid Elasticity
- Measured Service
- On-Demand Self Service

Resource Pooling

Service Models

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

Deployment Models

- Public
- Community
- Hybrid
- Privat

# Cloud Security Goals

<table>
<thead>
<tr>
<th></th>
<th>Details</th>
</tr>
</thead>
</table>
| **Confidentiality** | Difficult to work on encrypted data  
- necessary on SaaS level  
- theoretical possible, but performance loss |
| **Availability** | Protection of the virtual space of the cloud from, e.g., overwrites  
Redundant clouds, data storage  
Export of data in the cloud |
| **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 |
| **Privacy** | Prevent user Profiling  
Personal data have to stay in the EU  
Personal data has to be deletable, according to BDSG |
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”
  

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

BDSG   ISO2700x   HGB

BSI-Grundschutzkatalog   AktG

MARisk   KWG   AO
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”


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

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”


- BDSG
- ISO2700x
- HGB
- MARisk
- §25a KWG
- disaster recovery plan of the IT systems
- KWG
- AO

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


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

- §147 AO
- Archiving of documents
- Rules are still relevant, even if filing of documents is done in an electronic way
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”


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

  ▪ Forbid sharing of data with companies or governments in countries with weaker laws
  ▪ US Patriot Act vs. Safe Harbour
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
Example: Cloud Online Banking Scenario

A *Germany* 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

<table>
<thead>
<tr>
<th>Name</th>
<th>The identifier of the stakeholder</th>
<th>Instance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Describe the stakeholder informally</td>
<td>Bank Customer uses the online banking service of the Bank Institute</td>
</tr>
<tr>
<td>Relations to the cloud</td>
<td>Inputs/outputs relation between the stakeholder and the cloud, e.g., kind of data or software</td>
<td>Input: Financial transaction data, personal related data</td>
</tr>
<tr>
<td>Motivation</td>
<td>Stakeholder's motivation for using the cloud → e.g., consider relations to the cloud</td>
<td>Output: Transaction history</td>
</tr>
<tr>
<td>Relations to other direct stakeholders</td>
<td>The kind of dependency between the stakeholders, e.g., served by, controlled by contract, influenced by customer-demand</td>
<td>The Bank Customer wants cheap and secure financial transactions via the bank’s cloud computing offer</td>
</tr>
<tr>
<td>Assets</td>
<td>Assets relevant for this stakeholder → e.g., consider relations to the cloud</td>
<td>Served by: Bank Institute as SaaS-Provider</td>
</tr>
<tr>
<td>Compliance and Privacy</td>
<td>Identify relevant laws/regulations for the cloud scenario</td>
<td>Influenced by customer-demand: Security, Availability, Performance, Cost</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Financial transaction data, personal related data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BDSG</td>
</tr>
</tbody>
</table>
ISO 27005 - Information Security Risk Management
Context Establishment and Asset Identification in ISO 27005

Context Establishment (ISO 27005, Clause 7)

Input
General Considerations

Context Establishment

Output
Scope and Boundaries

Basic Criteria...

Asset Identification (ISO 27005, Clause 8.2.1.2)

Input
General Considerations

Asset Identification

Output
Assets to be Risk Managed

Business Process related to asset
Instantiated Cloud System Analysis Pattern

Context Establishment

<table>
<thead>
<tr>
<th>Indirect System Environment</th>
<th>Cloud Analysis Pattern</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legislation Germany</td>
<td>The organization's strategic business objectives, strategies and policies</td>
</tr>
<tr>
<td>Legislation EU</td>
<td>Location of the organization and their geographically characteristics</td>
</tr>
<tr>
<td>Direct System Environment</td>
<td>Interfaces (i.e. information exchange with the environment)</td>
</tr>
<tr>
<td>Has</td>
<td>Expectation of Stakeholder</td>
</tr>
</tbody>
</table>

Diagram:

- Cloud
- Service
- Provides
- IsMonitoredBy
- IsComplementedBy
- Virtual Machine
- UsedBy
- Webserver, Application Server, etc.
- Cloud Programming Interface
- Online Banking Service
- Transaction Data
- Bank Institute
- WorkFor
- BuiltAndCustomizedBy
- BuiltBy
- Internal Development Unit
- Has
- Germany, USA
- Cloud
- Data Center
- Network and Virtualization Software
- InputBy/OutputTo
- Bank Customer
Pattern-based Support for Context Establishment and Asset Identification in ISO 27005

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