Outsourcing, SaaS & Clouds: Aber sicher! (... und compliant)

Prof. Dr. Jan Jürjens

Fraunhofer Institut für Software- und Systemtechnologie ISST, Dortmund
http://jan.jurjens.de
Security is the Major Issue

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

- **Security**: 74.6%
- **Performance**: 63.1%
- **Availability**: 63.1%
- **Hard to integrate with in-house IT**: 61.1%
- **Not enough ability to customize**: 55.8%
- **Worried on-demand will cost more**: 50.4%
- **Bringing back in-house may be difficult**: 50.0%
- **Regulatory requirements prohibit cloud**: 49.2%
- **Not enough major suppliers yet**: 44.3%

(Source: DDS Enterprise Panel, August 2008  n=244)
# GRC in Clouds

<table>
<thead>
<tr>
<th>Governance</th>
<th>Risk</th>
<th>Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Policy design</td>
<td>- Risk strategy</td>
<td>- Policy enforcement</td>
</tr>
<tr>
<td>- Classification schema for data and processes</td>
<td>- Business Impact Analysis</td>
<td>- Legal compliance (SOX, SOLVENCY II)</td>
</tr>
<tr>
<td>- Trust chain in a cloud</td>
<td>- Threat and Vulnerability Analysis</td>
<td>- Control implementation</td>
</tr>
</tbody>
</table>

The Cloud offers dynamic resource 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
Related Standards

- Process Maturity
  - Gartner
  - eden
  - ISO

- Holistic Control Systems
  - COBIT
  - COSO

- Security Standards
  - Bundesamt für Sicherheit in der Informationstechnik
  - Common Criteria

- Transparency
  - TRUSTe
  - SAS 70
  - ISO
  - Safe Harbor
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?
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
Definition Security and Compliance

- Governance, Risk und Compliance (GRC)
  - Governance: internal company guidelines
  - Compliance: external guidelines, e.g. SOX
  - Risk: risk management under consideration of all guidelines

- Security
  - Abstract security objectives, e.g. CIA applied to a company

A company can be compliant, but not secure.
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

Customer Rules

Governance

Risk Type Actions <Priority>

Laws

Compliance

Risk Type Actions <Priority>

Guidelines

Risk Repository -incl. Actions-

Risks and Actions From other sources -BSI Grundschutz, DBs-

Risk Manager

uses

GRC Report

Interface Risk Tools

uses

Customer Data

Processes

Text documents

Interviews

Log Files

Monitoring

...
Log-File Analysis

- 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

<table>
<thead>
<tr>
<th>Process ID</th>
<th>Activity ID</th>
<th>Consultant</th>
<th>Time Stampe</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>A</td>
<td>John</td>
<td>9-3-10:15.01</td>
</tr>
<tr>
<td>2</td>
<td>A</td>
<td>Mike</td>
<td>9-3-10:15.12</td>
</tr>
<tr>
<td>3</td>
<td>B</td>
<td>Mike</td>
<td>9-3-10:16.07</td>
</tr>
<tr>
<td>4</td>
<td>C</td>
<td>Carol</td>
<td>9-3-10:18.25</td>
</tr>
</tbody>
</table>
Business Process Analysis

- Automated compliance-analysis
- Two approaches:
  1. Test-based analysis of the activity identifier for the automated risk identification
  2. Structural analysis of the process model for compliance-violation-pattern
Conclusion

Clouds?

Make sure you are secure!

(... and compliant)

Contact: http://jan.jurjens.de