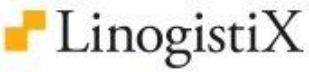
SECURING PROCESSES FOR OUTSOURCING INTO THE CLOUD

Sven Wenzel[1], Christian Wessel[1], Thorsten Humberg[2], Jan Jürjens[1,2]

[1] technische universität dortmund

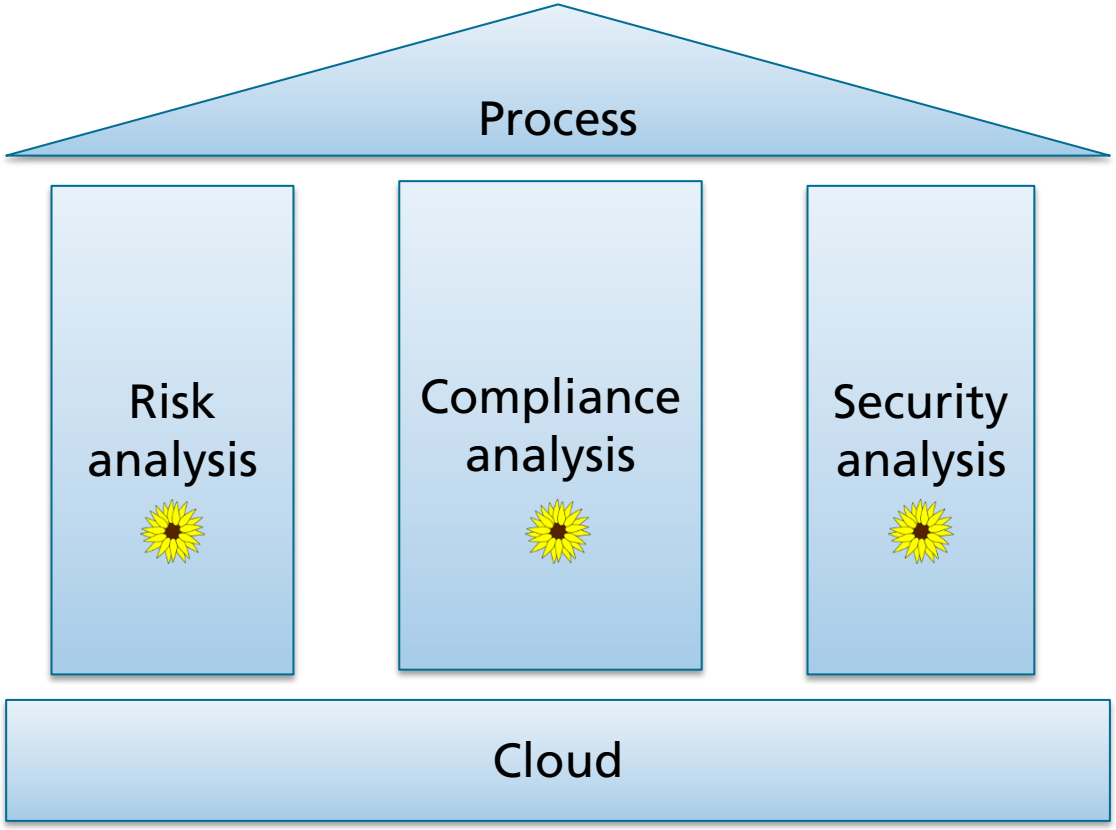
[2] Fraunhofer ISST



SPONSORED BY THE

CloudSecGov, 19.4.2012

Overview

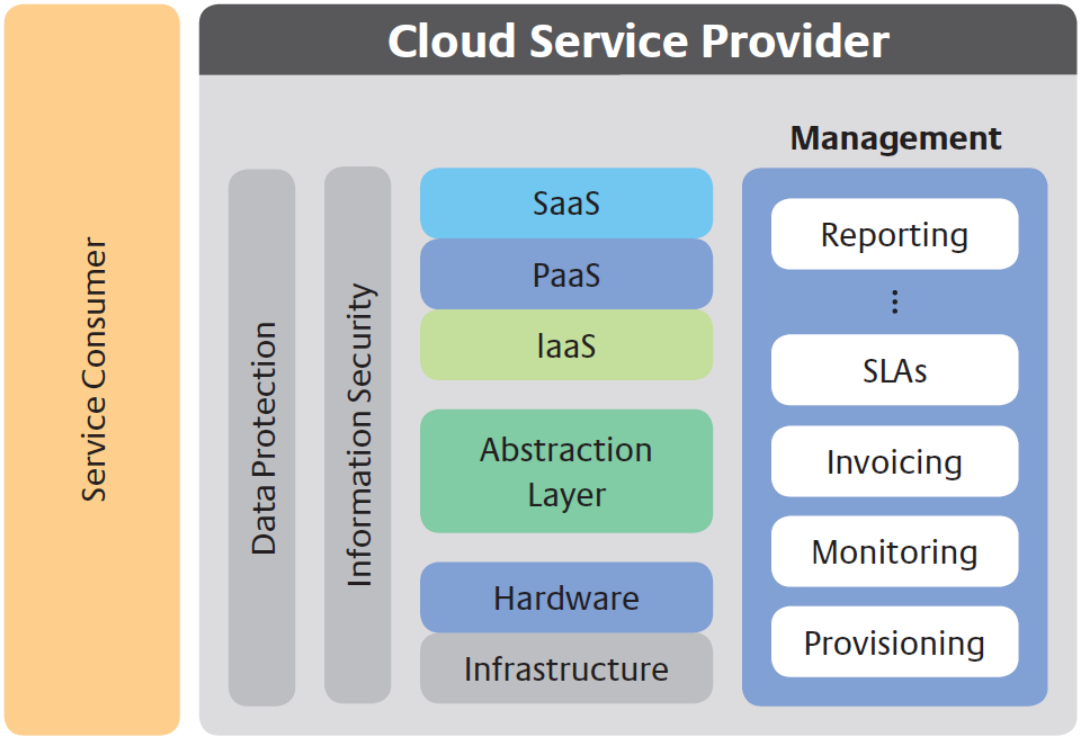


Toolsupport:

Fraunhofer ISST

Cloud Computing

- Most common definition: „The NIST Definition of Cloud Computing" by Peter Mell, Tim Grance



[BSI: Security Recommendations for Cloud Computing Providers]

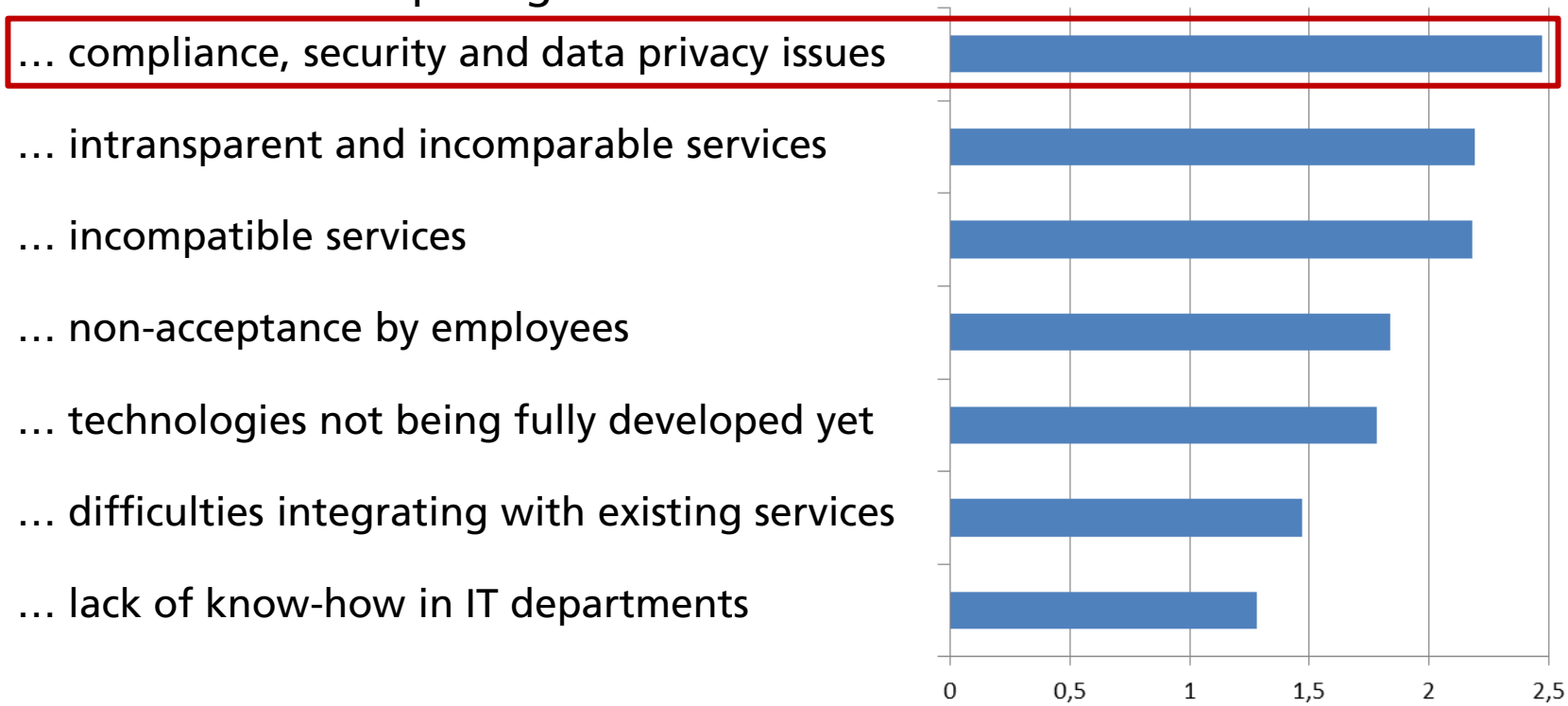
Fraunhofer ISST

Clouds for Small and Medium-sized Enterprises (SMEs)

- Most significant advantages of cloud computing
  - Flexibility: Less inhouse IT-infrastructure needed
  - Pay-per-use: Overhead costs can be avoided
  - Less effort for infrastructure maintenance
- Advantages are especially valid for SMEs
- But: Cloud computing is hardly used by SMEs!

Concerns regarding Cloud Computing

„I consider Cloud Computing as critical due to …“

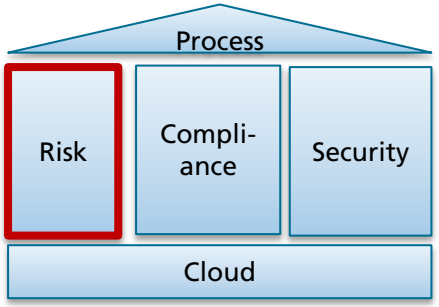


[Source: CW market study 2010]

- Security
  - Confidentiality
  - Availability
- Compliance
  - Legal regulations have to be met

Fraunhofer ISST

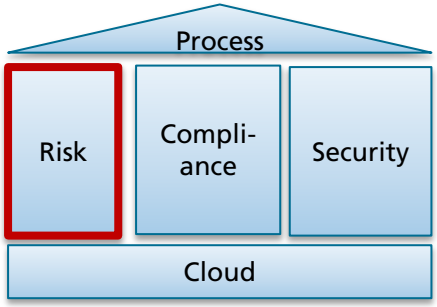
1: Risk analysis



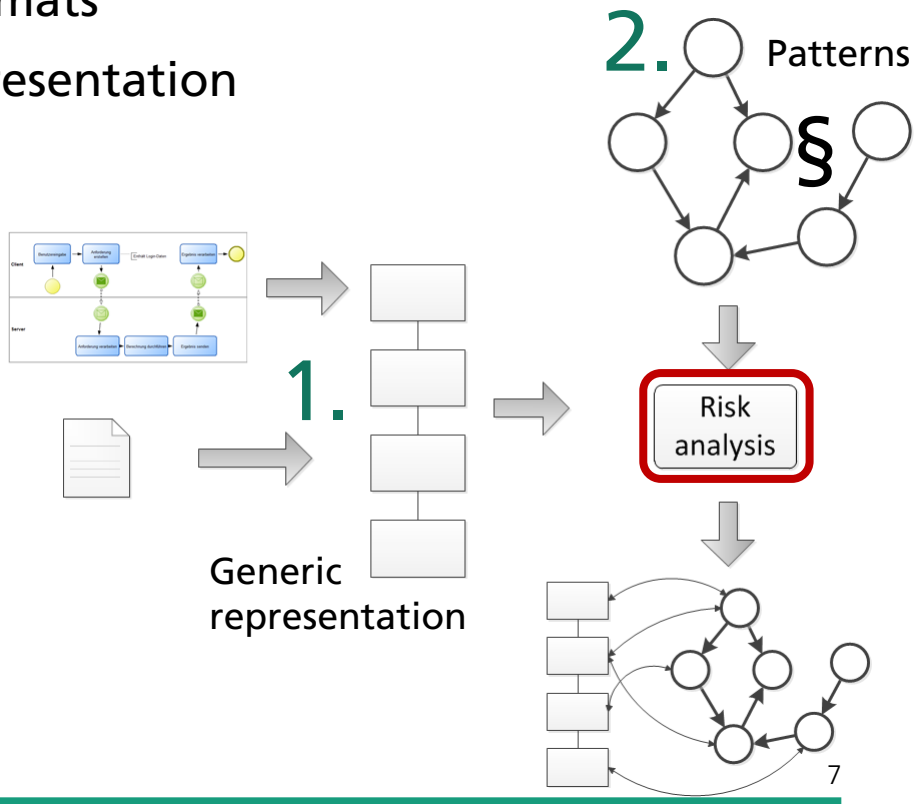
- First checkup before migrating processes
- Business processes are assessed for „risky“ elements
  - No consideration of probabilities of occurrence
- Identification of risks is a matching on security or compliance standards
  - E.g. BSI basic protection catalogues, ISO norms
- Various forms of input
  - Process models: UML, BPMN
  - Semi-formal: Spreadsheets

Fraunhofer ISST

Risk analysis: Methodology

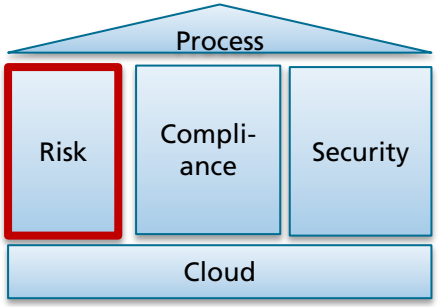


- Input
  1. Process descriptions in various formats
     - Converted into a simplified representation
  2. Security and Compliance patterns
- Risk analysis searches for relations
- Output
  - Matching between components and relevant patterns

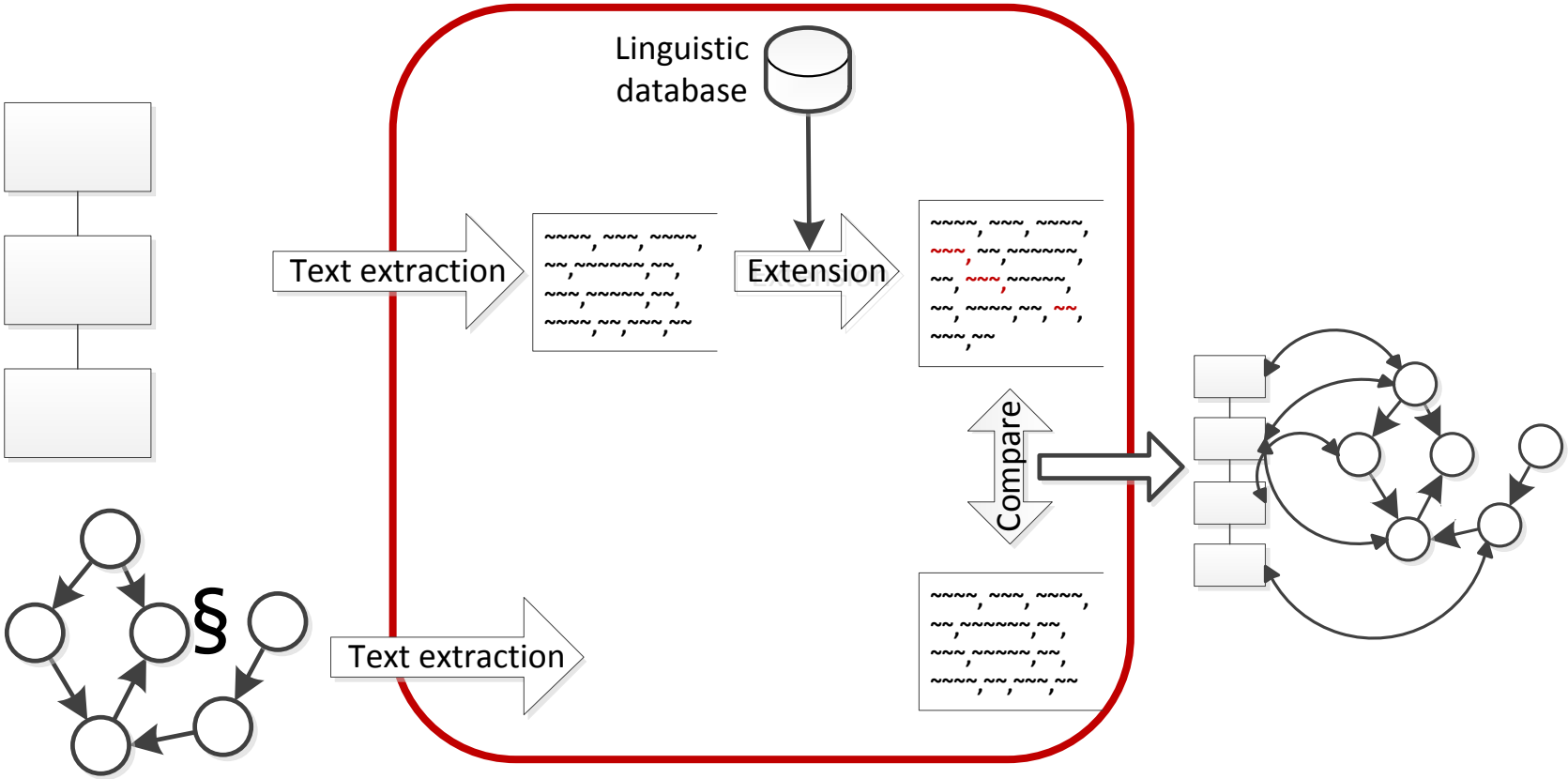


Fraunhofer ISST

Risk analysis: Determine matchings

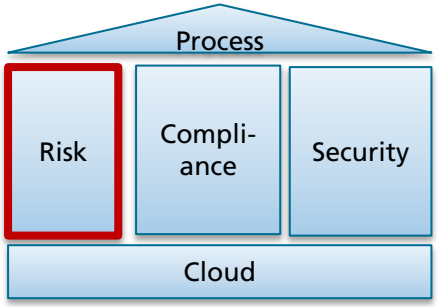


Simple method: Text-based matchings



Fraunhofer
ISST

Risk analysis: Results



- For each activity, relevant patterns are identified
  - With a coarse rating of relevance

Activity label

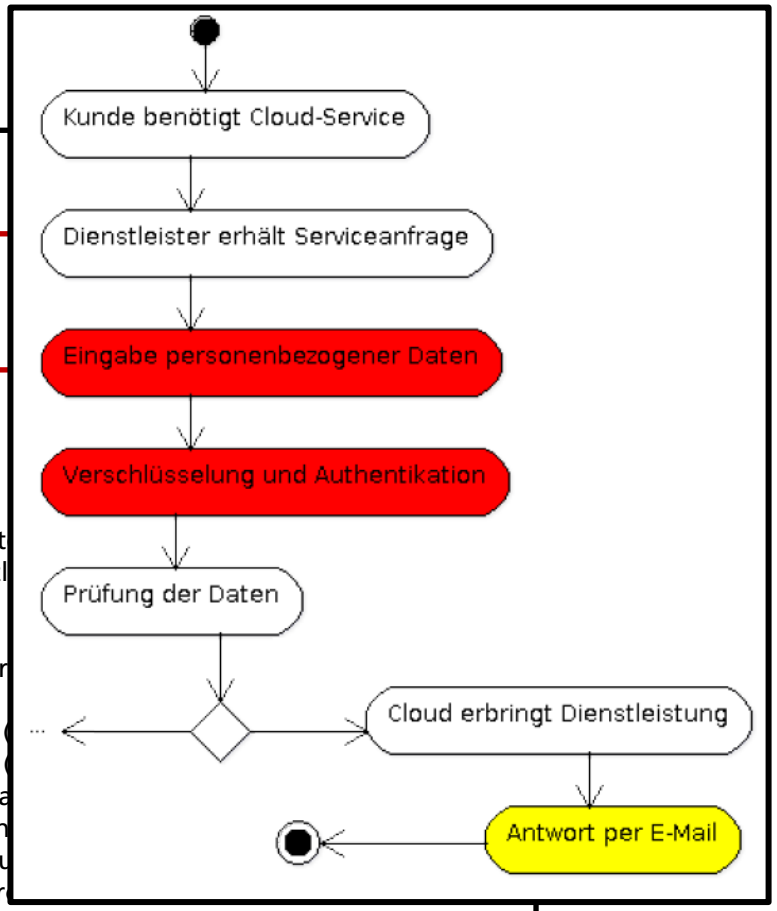
Matching expressions (rated)

Identified patterns

[Kunde benötigt Cloud-Service]
Relevante Worte: [Information(200.0), Meldung(200.0), Nachricht(200.0)]
Relevante Pattern:
BSIGrundschutz_B_5.10 : Internet ... mation Server (200.0)
BSIGrundschutz_G_4.32 : Nichtz ... nt (200.0)
BSIGrundschut_G_5.27 : Nichta ... richt (200.0)
BSIGrundschutz_M_2.158 : Meld ... m-Infektionen (200.0)
...

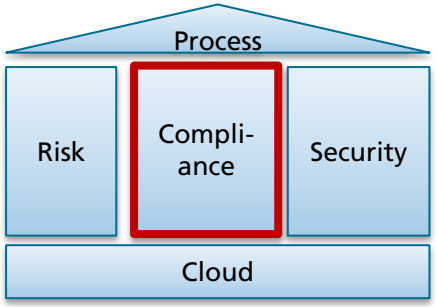
[Dienstleister erhä ... erviceanfrage]
Relevante Worte: [Di ... ister(500.0)]
Relevante Pattern
BSIGrundschutz ... iche vertragliche Regelungen mit einem ext
BSIGrundschutz ... ng von Datenträgern durch externe Dienstl

[Eingabe personenbezogener Daten]
Relevante Worte: [Daten(500.0), personenbezogener(500.0), Dateien(200.0), Unter
Relevante Pattern:
BSIGrundschutz_G_2.61 : Unberechtigte Sammlung personenbezogener Daten (
BSIGrundschutz_G_2.61 : Unberechtigte Sammlung personenbezogener Daten (
BSIGrundschutz_G_2.116 : Datenverlust beim Kopieren oder Verschieben von Da
BSIGrundschutz_G_2.15 : Vertraulichkeitsverlust schutzbedürftiger Daten im Un
BSIGrundschutz_G_2.24 : Vertraulichkeitsverlust schutzbedürftiger Daten des zu
BSIGrundschutz_G_3.1 : Vertraulichkeits- oder Integritätsverlust von Daten dur
...

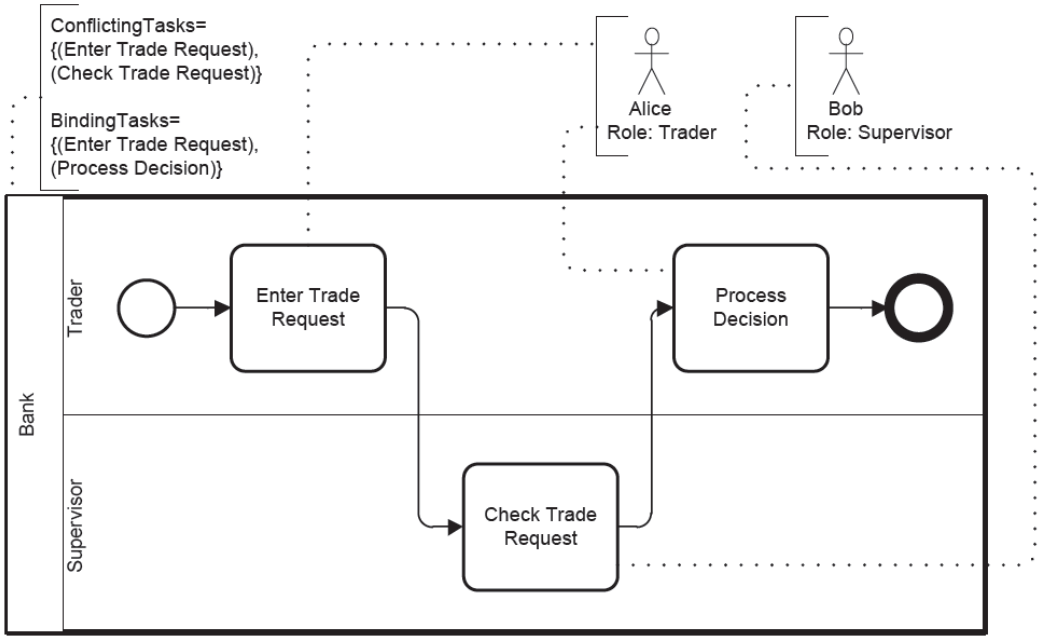


Fraunhofer ISST

2. Compliance Analysis: Modelling



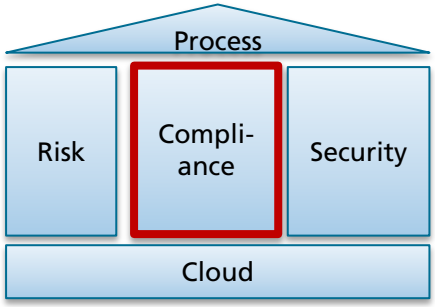
- Outsourcing processes might affect their compliance
  - E.g. server locations matter
- Models must contain the examined aspects, e.g. role assignments for Separation of Duties (SoD)



[Marcel Michel 2011]

Fraunhofer ISST

Verification of compliance properties



- Simple properties can be formulated using Object Constraint Language
  - E.g. Separation of duty

```
context TaskSet inv: self.selectedTasks
-> forAll(x,y | x <> y implies x.performer
-> forAll(z | y.performer -> includes(z) ) )
```

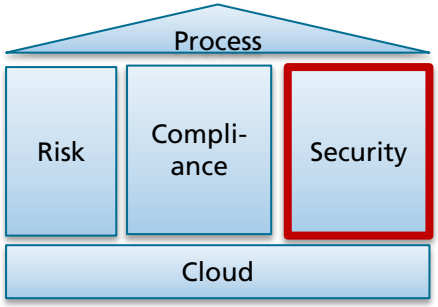
- More complex properties require more advanced techniques
  - E.g. Process fragments or temporal logic for workflow-based features

```
[](pay -> <> (pickup || reclaim))
```

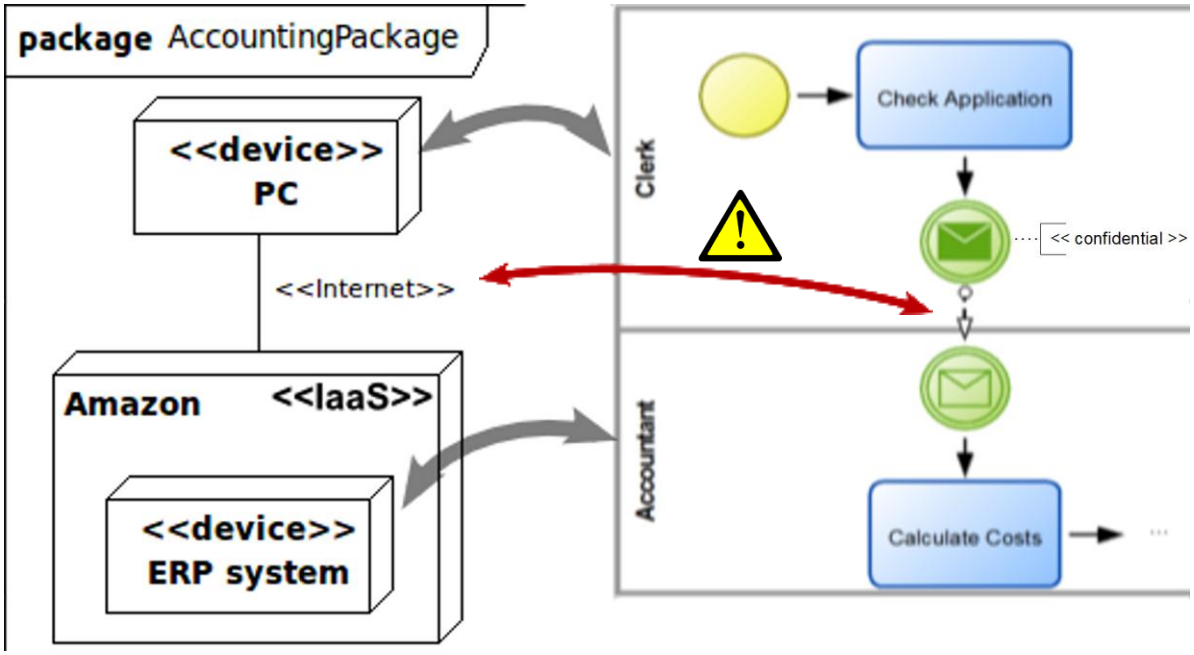
Automated verification requires detailed descriptions of both the process and the requirements.

Fraunhofer ISST

3. Security Analysis (ongoing)



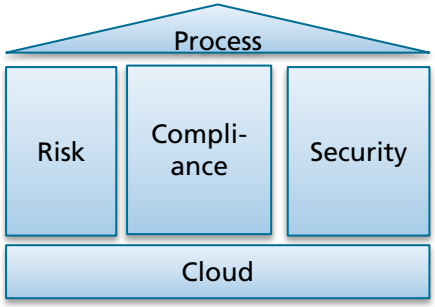
- Goal: Reveal security concerns in early design stages
- Processes and their distribution are considered



- Transfer of UMLsec annotations to business process models

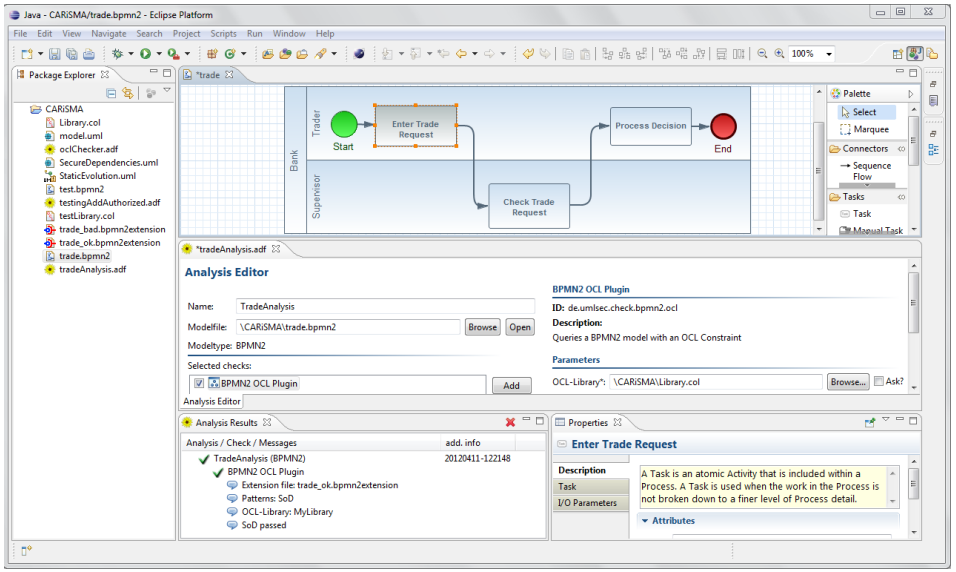
Fraunhofer ISST

Tool Support



CARiSMA

- Provides checks for the UMLsec profile
- Plugin for Eclipse
  - Integrates established modeling tools, e.g. Topcased
  - Open Source
- Ongoing:
  - Implementation of SecureClouds analysis tools



http://carisma.umlsec.de

Fraunhofer ISST

Conclusions and Outlook

- Cloud Computing for SMEs
  - Offers economic chances
  - … as well as security and compliance concerns
- The SecureClouds project supports SMEs in utilizing cloud services
  - Work is still ongoing, especially concerning security analysis and tool support

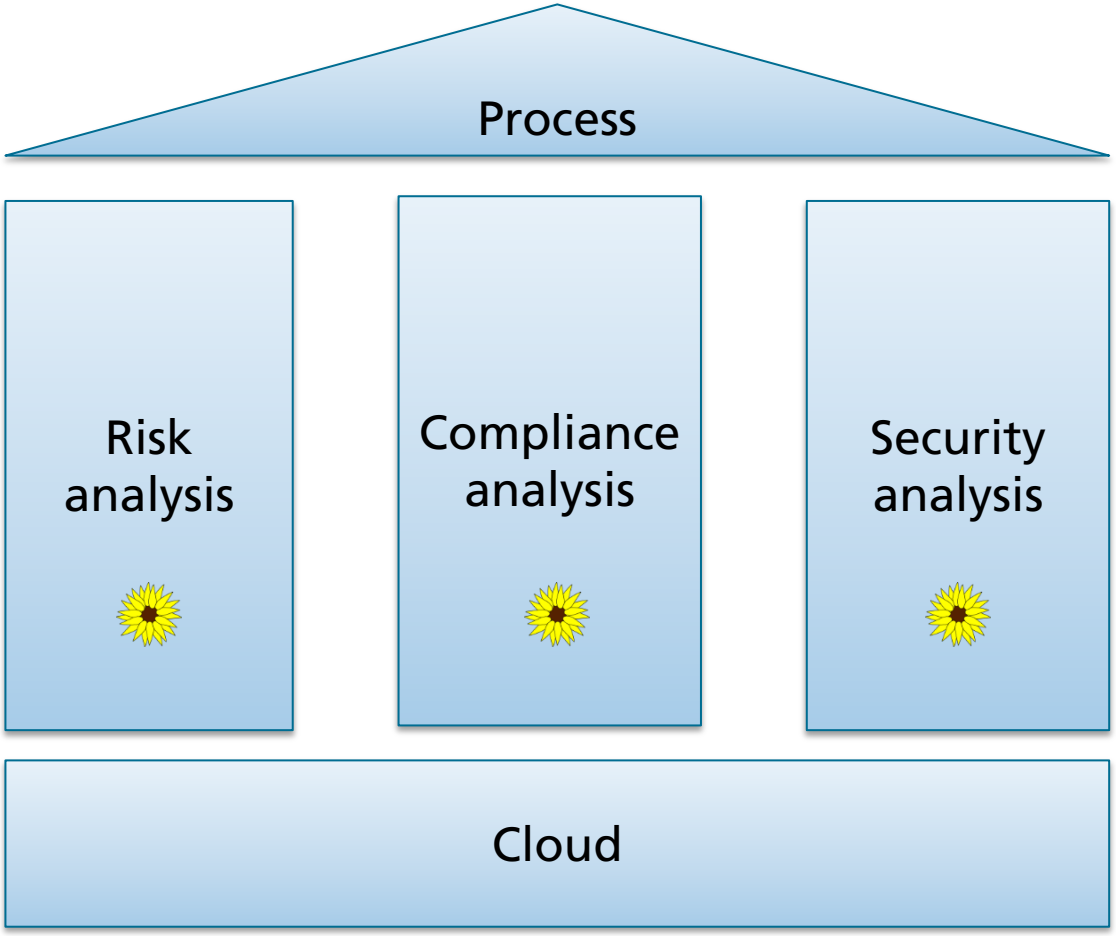
http://www.secureclouds.de

Fraunhofer ISST

Thank you

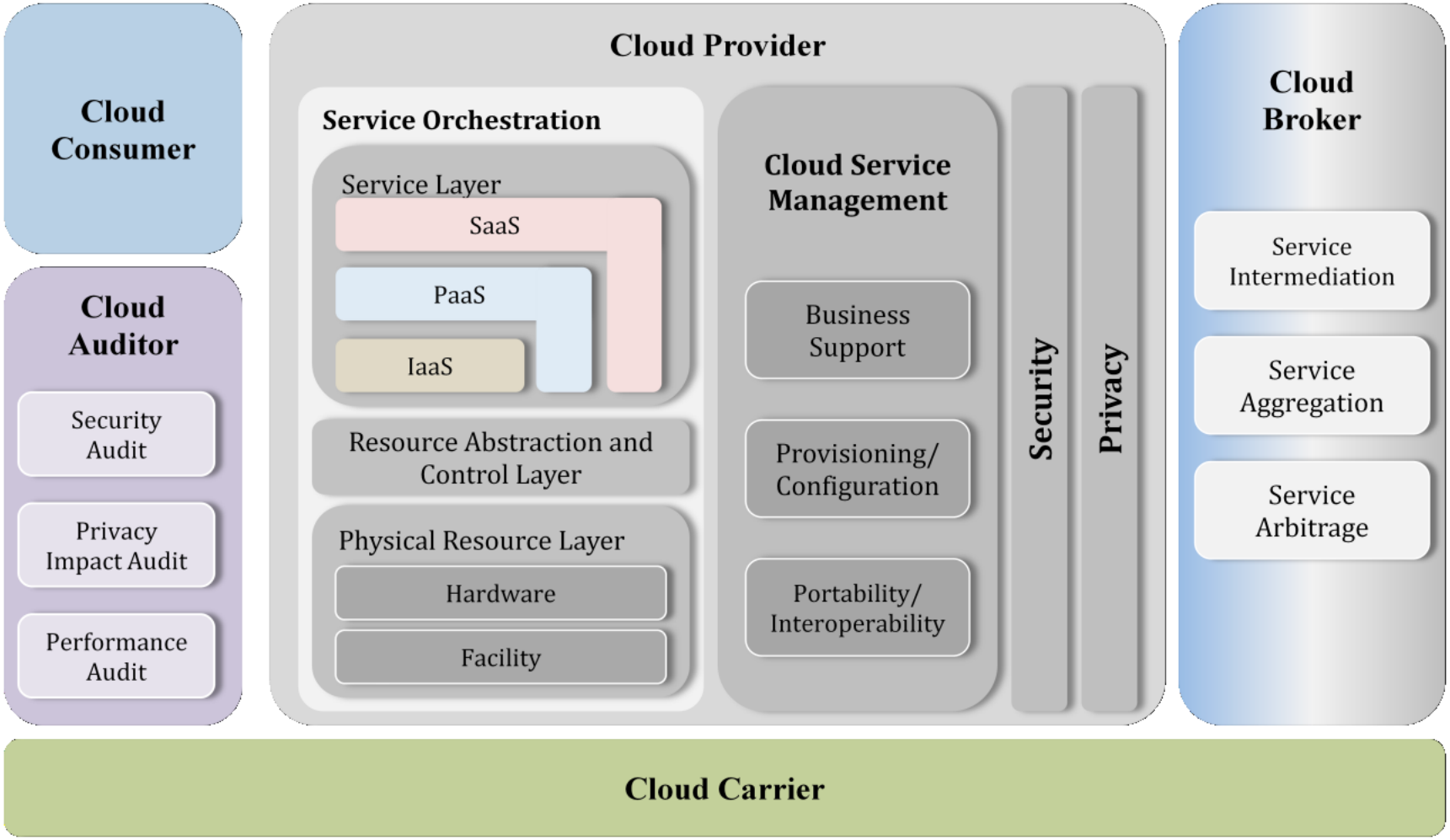
Thorsten.Humberg@isst.fraunhofer.de

Our contribution



Fraunhofer ISST

NIST Cloud reference architecture



Fraunhofer ISST