



# Security RiskFlows –

Konzepte für die organisierte Suche nach der Nadel im  
Heuhaufen

Ruth Breu, Michael Brunner  
*Universität Innsbruck*

## Quality Engineering Laura Bassi Lab Living Models for Collaborative Systems



### Industry Partners



*PoSecCo's vision is to establish and maintain a consistent, transparent, sustainable and traceable link between high-level, business-driven security and compliance requirements on one side and low-level technical configuration settings of individual services on the other side.*



## Zwei zentrale Fragen für Produkthersteller



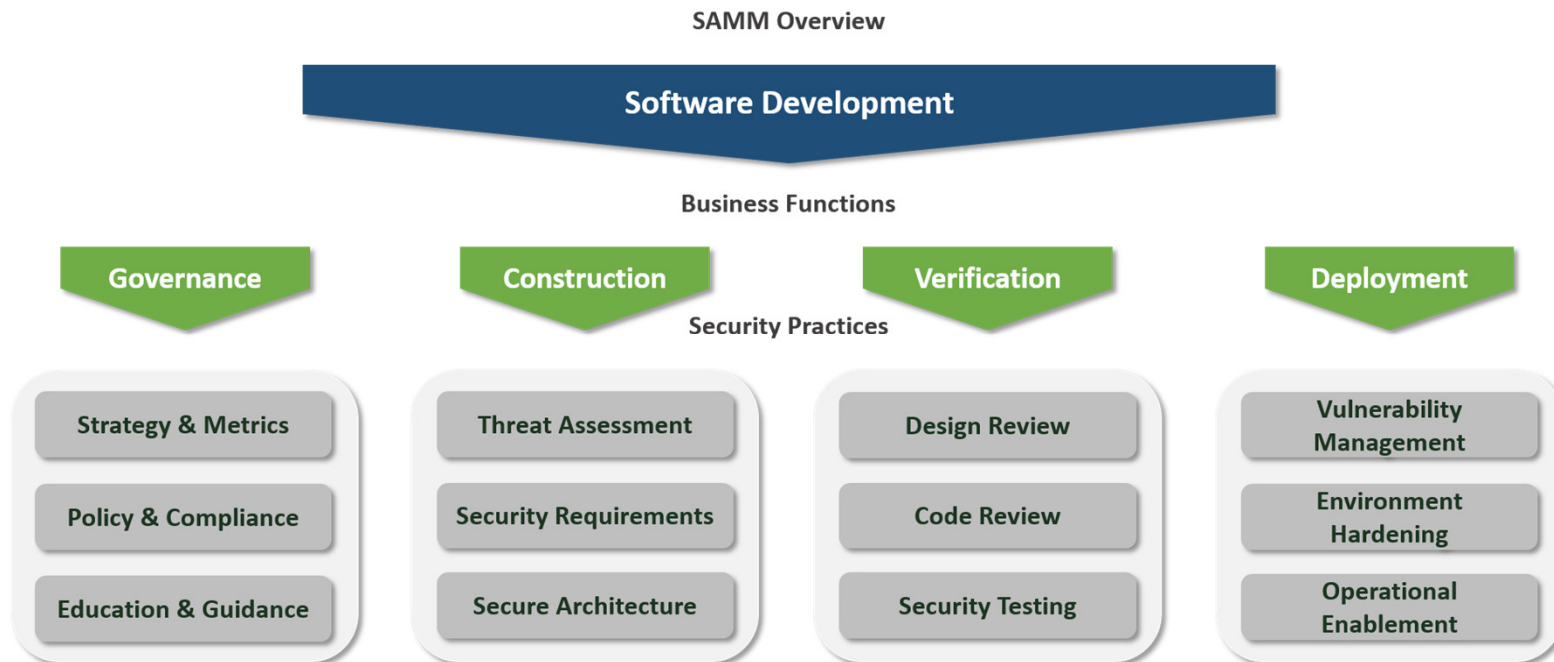
**Wieviel Security braucht das Produkt?**



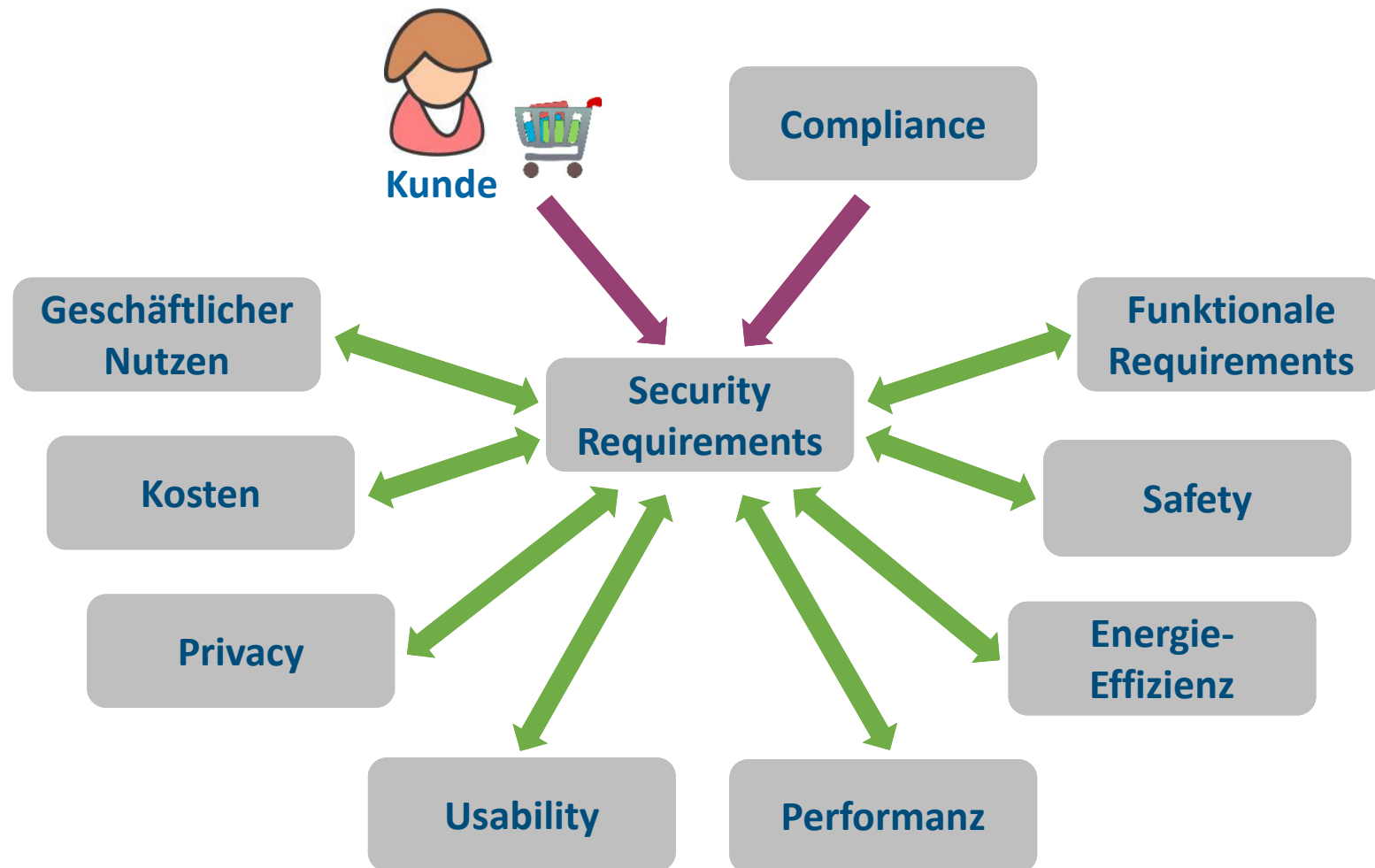
**Wie sicher ist das Produkt aktuell?**

# State of the Art: Security Lifecycle Management

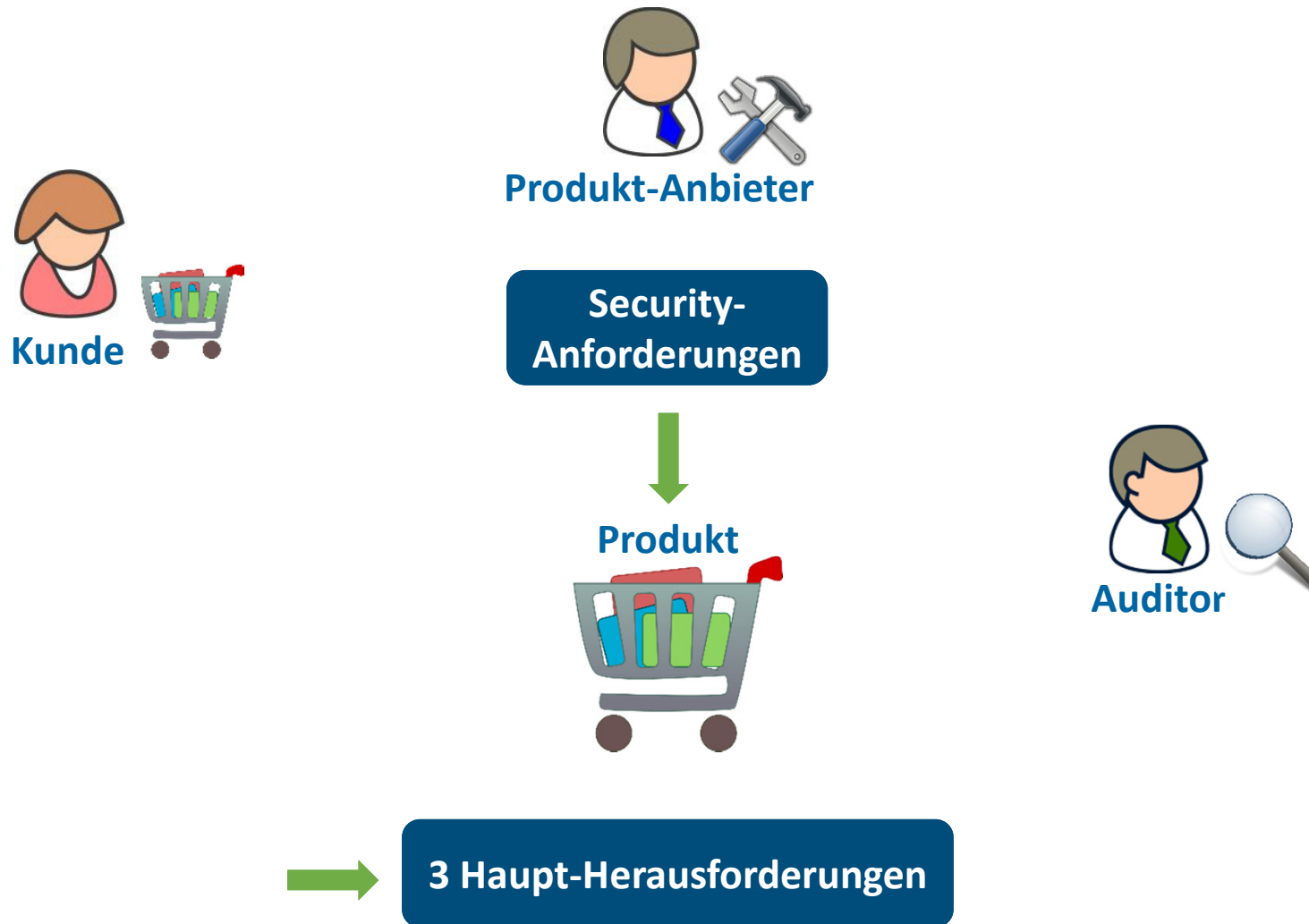
## SAMM



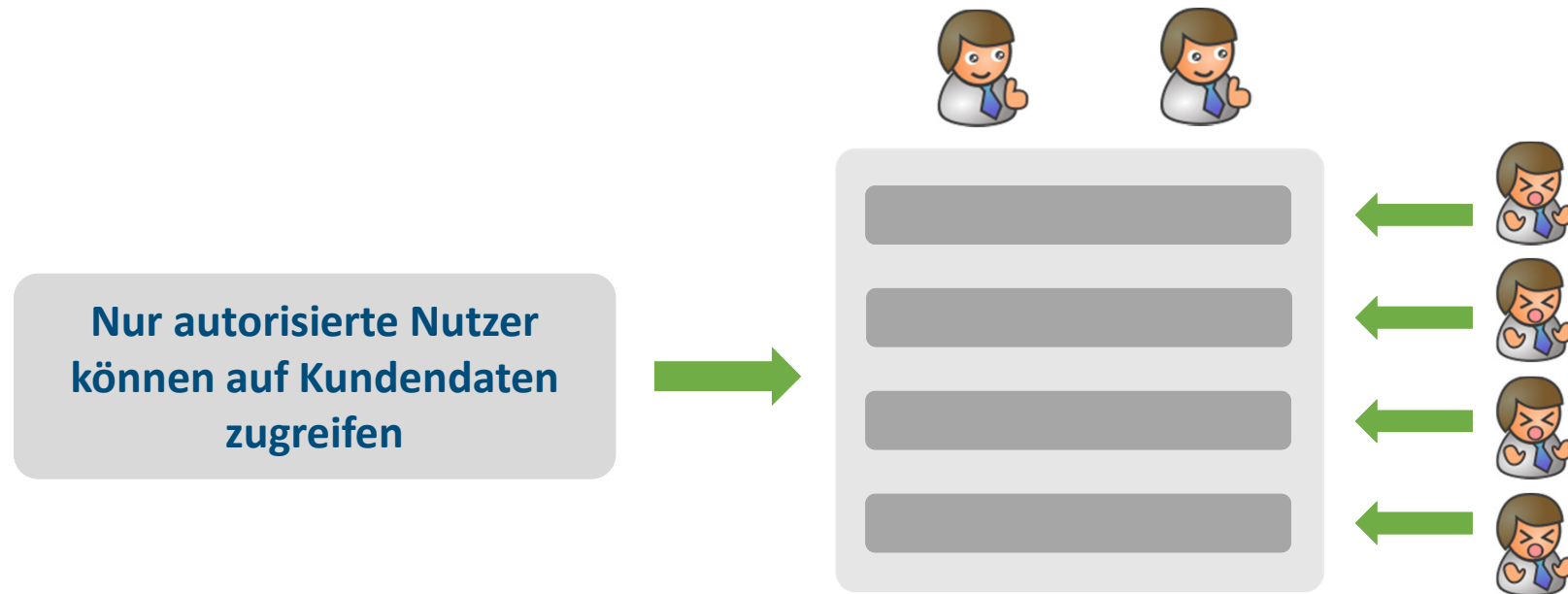
## Wie viel Security braucht das Produkt?



# Wie sicher ist das Produkt aktuell?

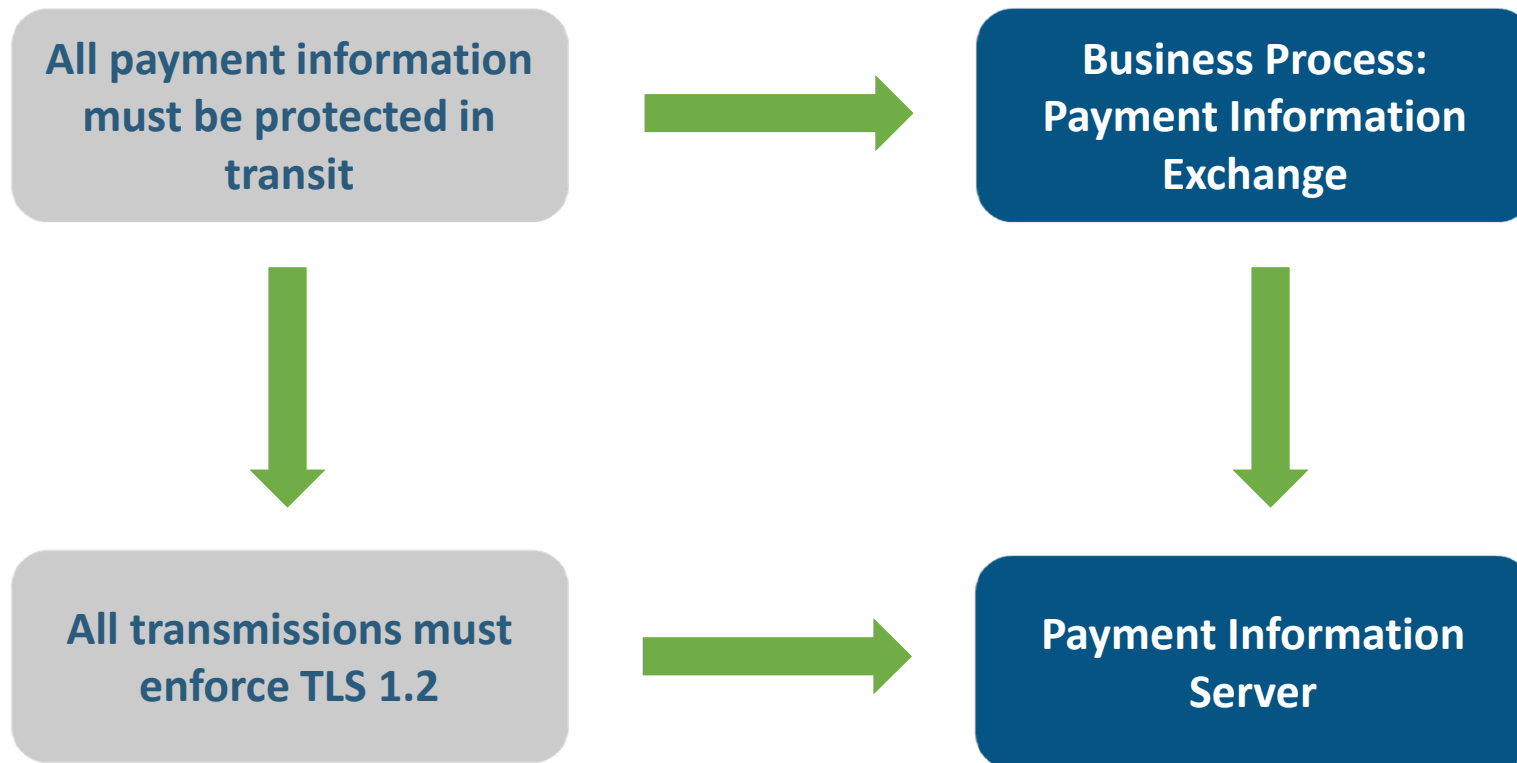


# 1. Negative Natur von Sicherheitsanforderungen

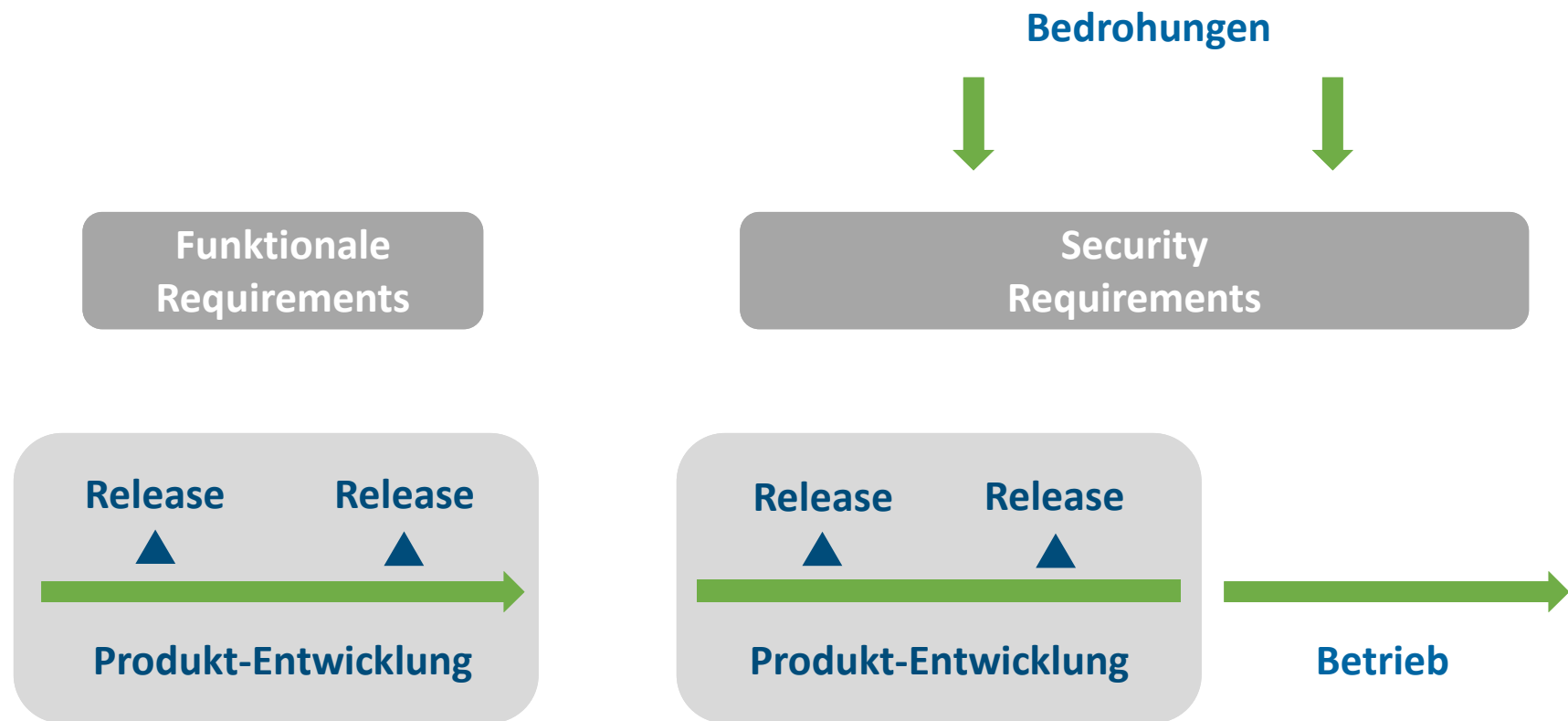




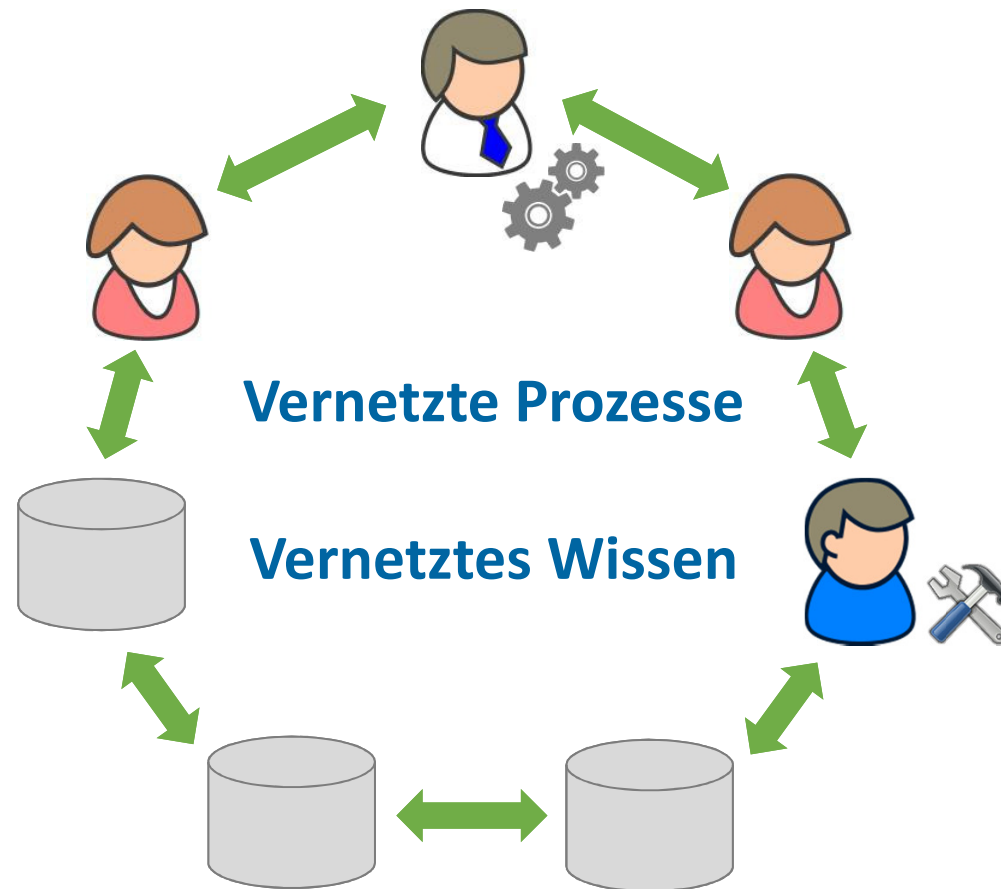
## 2. Abhängigkeit von Assets



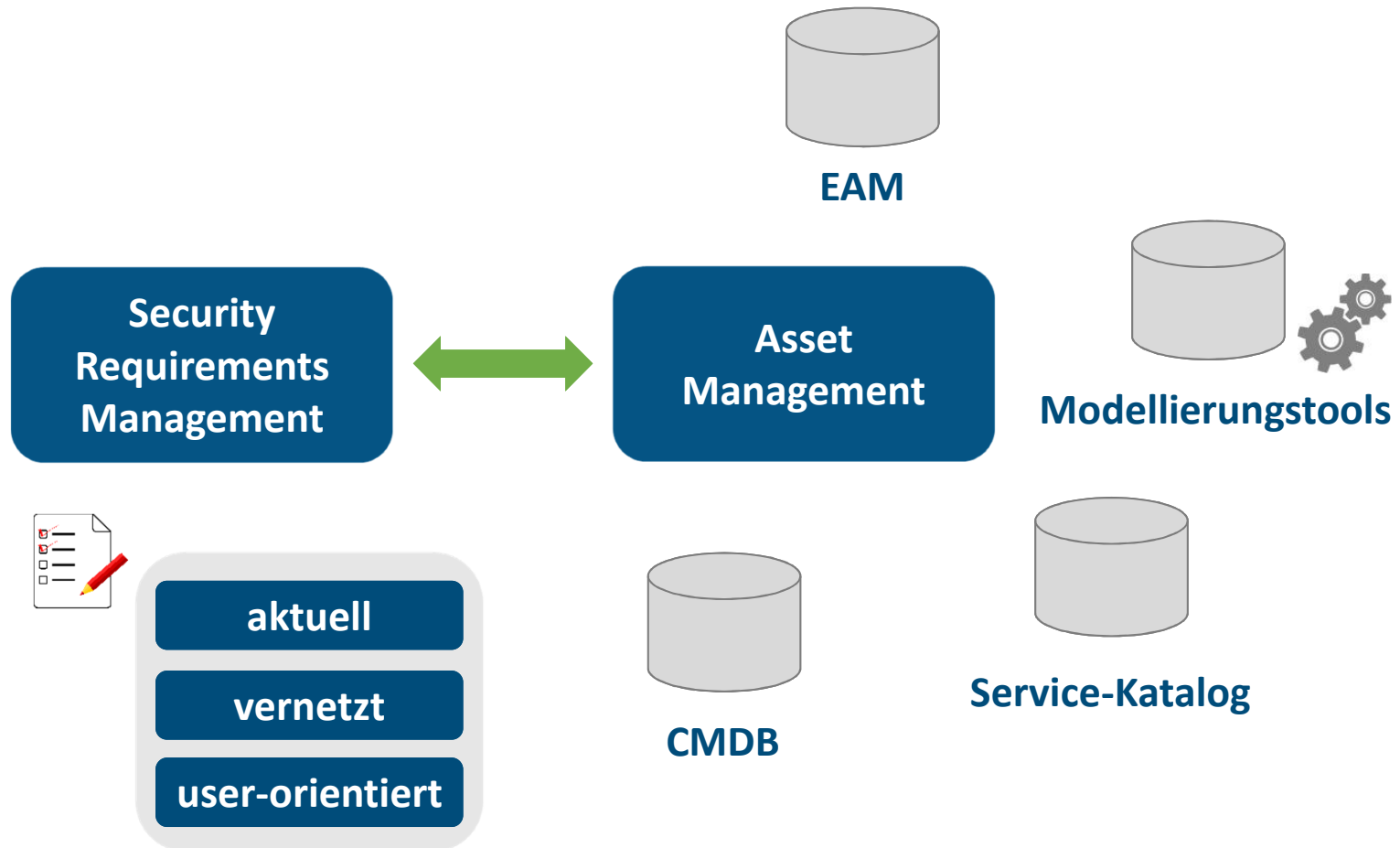
### 3. Eigener Lebenszyklus



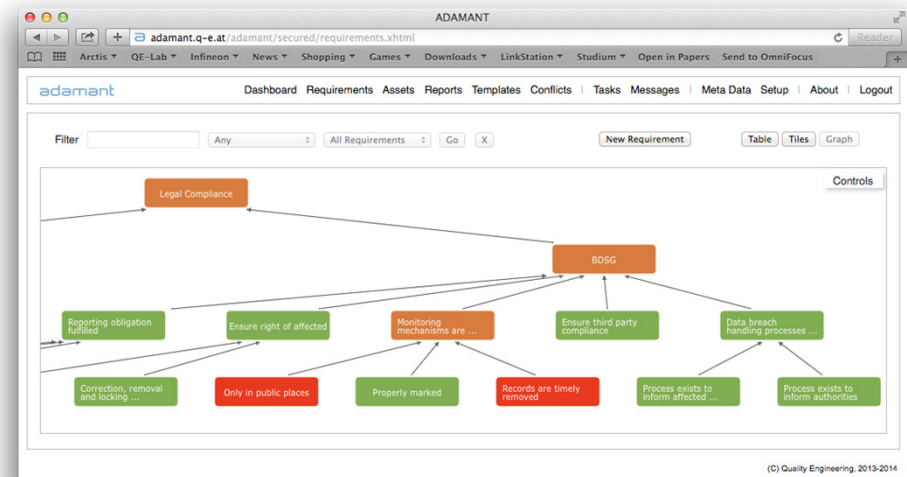
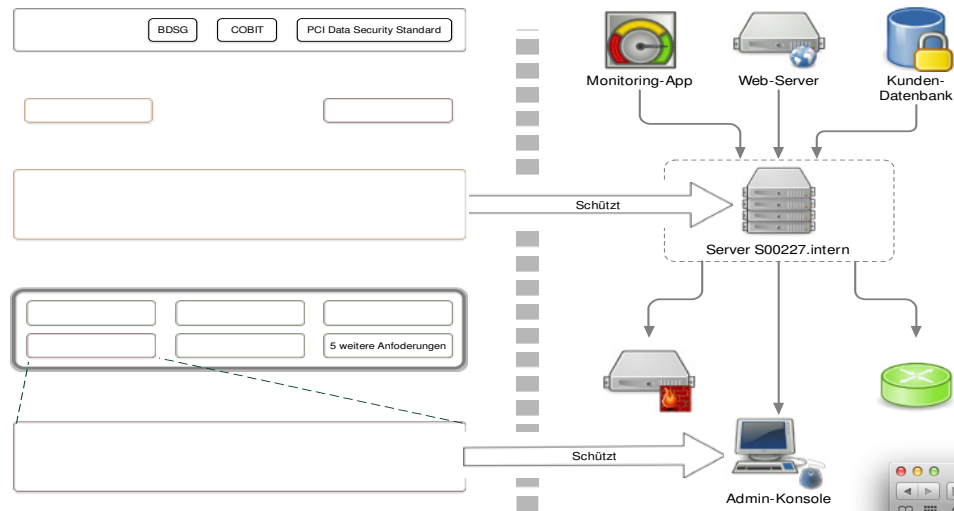
# Security als Aufgabe kooperativen Wissensmanagements



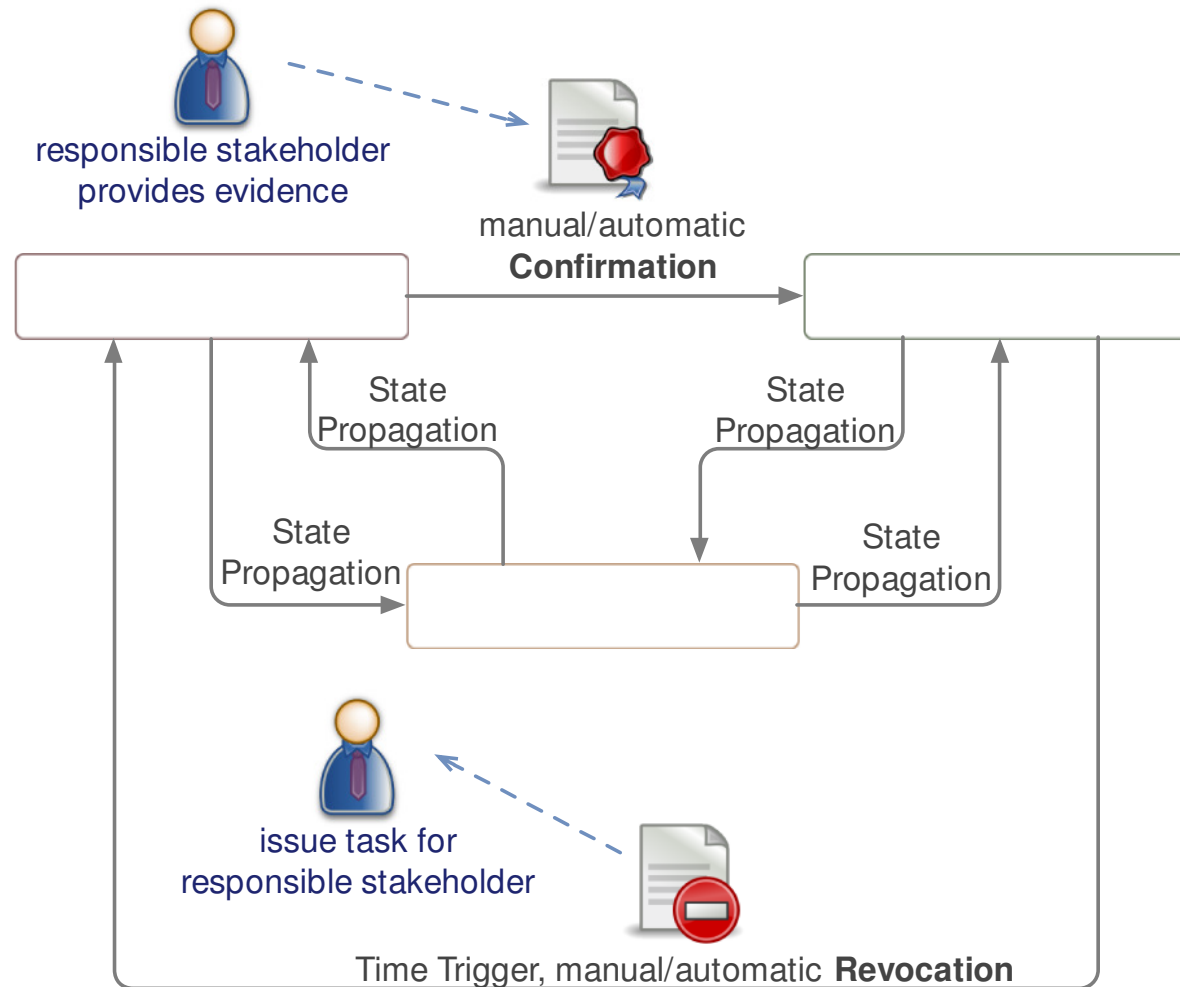
# Qualitativ hochwertiges Asset Management



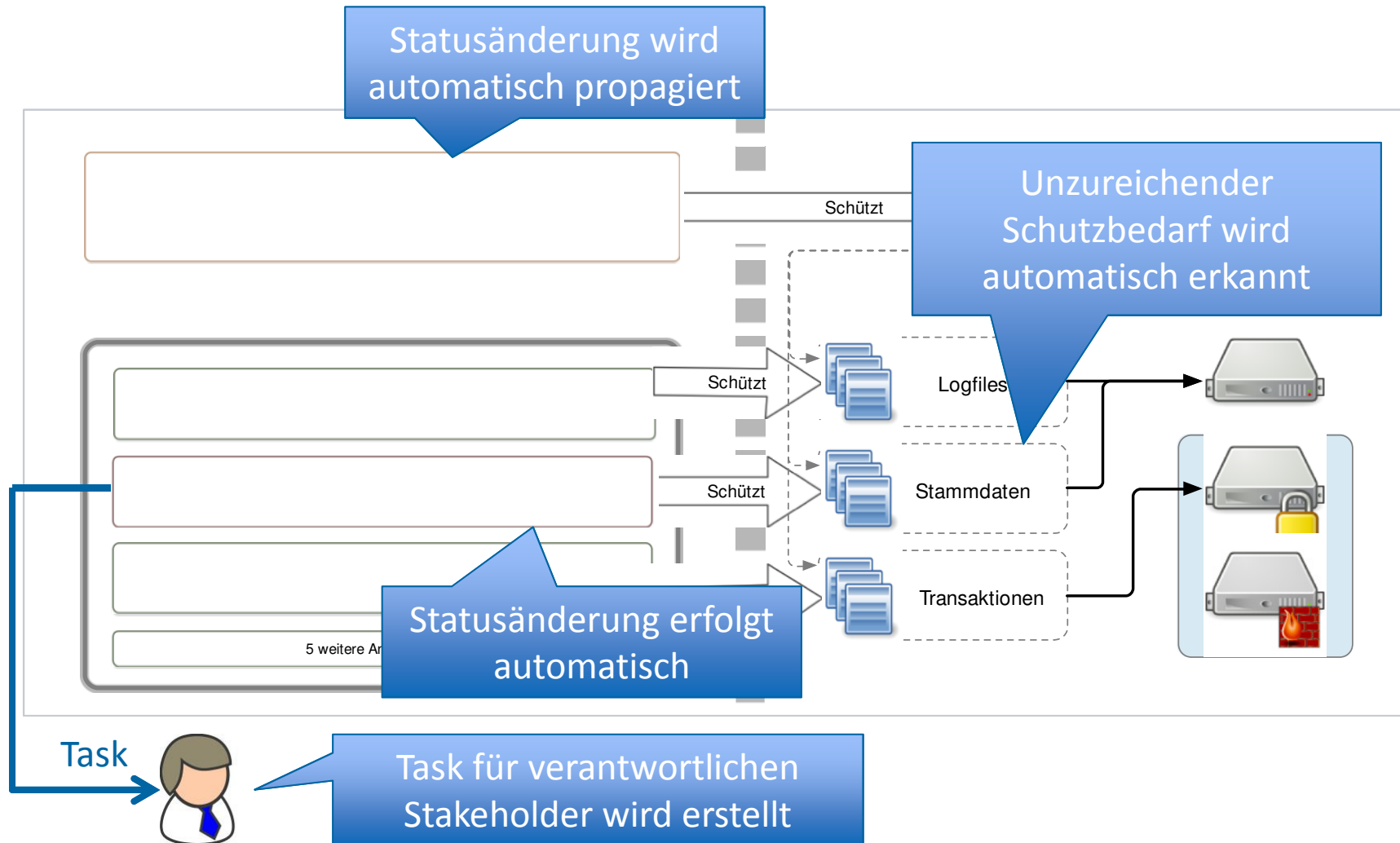
# Nachverfolbare Security Requirements



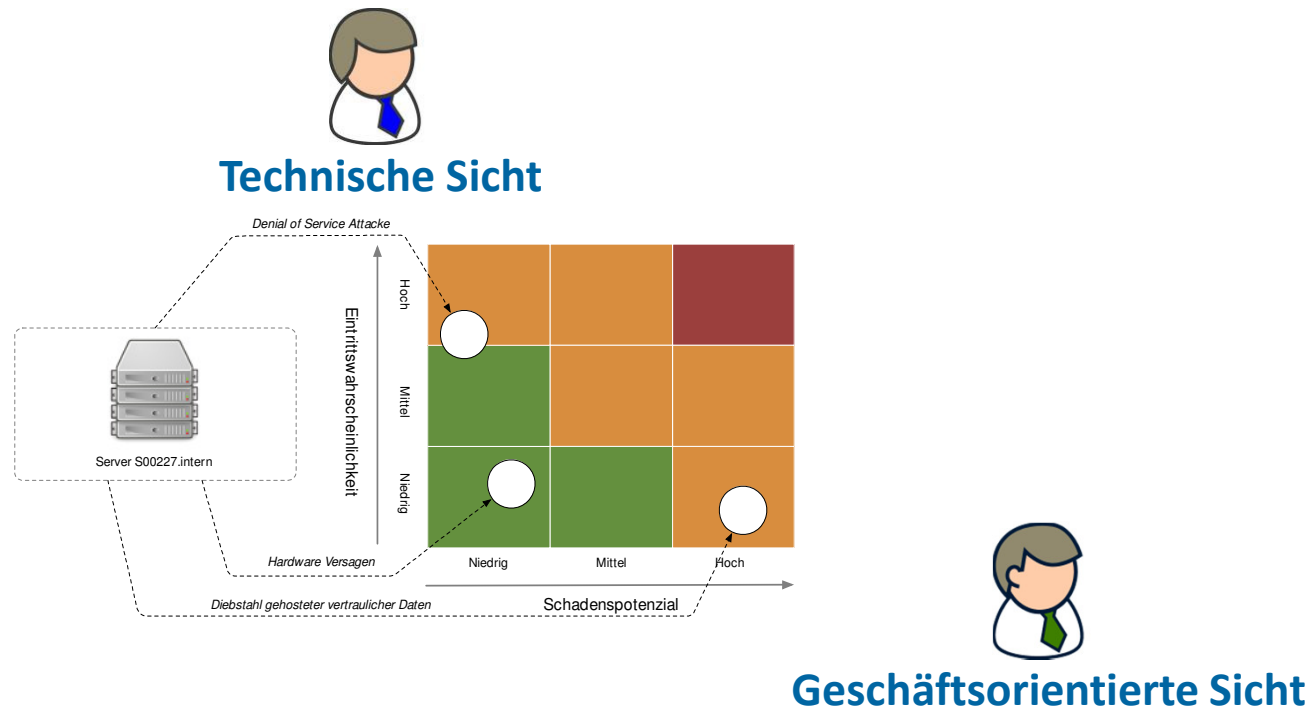
# Workflow-Unterstützung /1



## Workflow-Unterstützung /2



# Risikogetriebenes Vorgehen



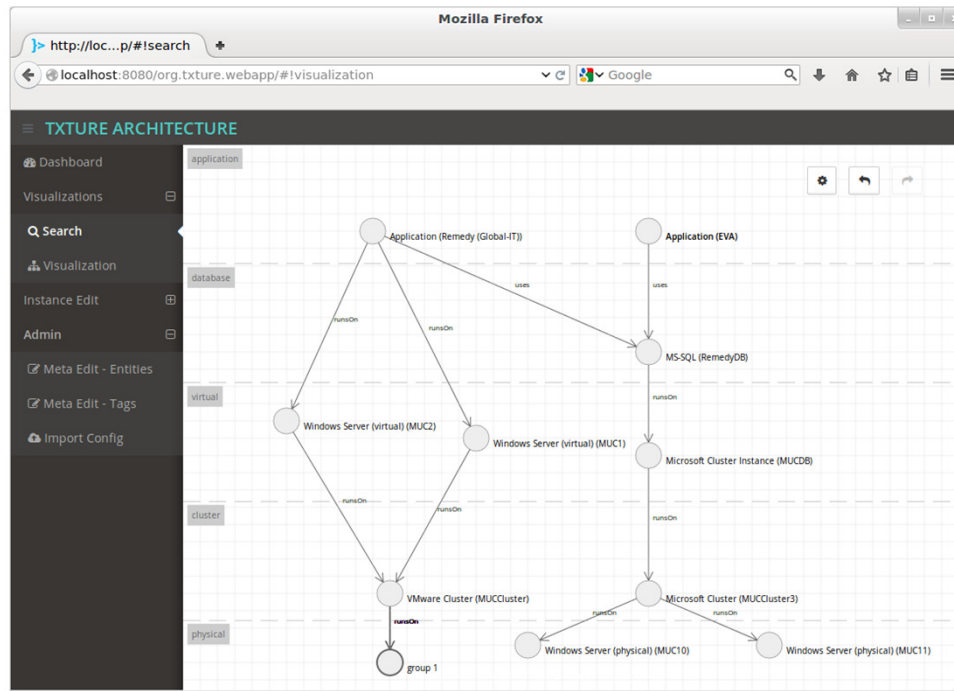
- Risikobewertungsprozess
- Risikogetriebener Prozess (z.B. Integration mit Asset-Modellierung, Testen, Task-Priorisierung)



# Automation

- **Prozess-Unterstützung**
- **Risiko-Metriken**
- **Überwachung von Security Requirements**
- **Generieren von Requirements/Unterstützung von Standards und Guidelines**
- **Generieren von Assets**
- **Überwachen von Qualitätsregeln**

# Datenvisualisierung



Self-service

Dynamisch

User-zentriert

# QE LaB Methoden und Prototypen

IT Landscape Intelligence



Efficient Security and Compliance



Modellgetriebener  
Ansatz

Risikobasiertes Testen

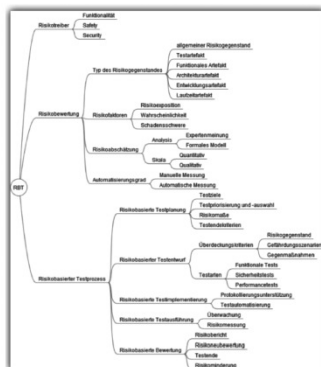


Abb. 1: Taxonomie für das risikobasierte Testen

Model-Based Security

```
1 // The domain model to use
2 model "ISM-Model"
3
4 // The name of the domain working activity
5 is-a "Family practitioner"
6
7 // Descriptions for the generated tool's user interfaces
8
9 interface "..."
10 description "..."
11
12 // Select the practitioner you regularly visit and/or trust most.
13 visualise "Family practitioner"
14 text "Practitioner" > "PRAC" > "has been selected as a trusted practitioner"
15
16
17 // Defines who can use the scenario and view the settings from a scenario instance
18 context {
19   edit Patient
20   visualise Practitioner via PRAC, Patient via THIS
21 }
22
23 // Arbitrary pre-defined variables which are constant regarding a single scenario instance
24 environment {
25   RECORDS : ListOf Record with filter( Feature( Record-Identities ) contains value( THIS ) )
26 }
27
28 // Variables which consist of user inputs, like "text" or "selections"
29 input {
30   PRAC NAME : java.lang.String as "Practitioner name"
31   PRAC : mandatory Practitioner as "Practitioner" with filter(
32     Feature( Practitioner-name ) startsWith value( PRAC NAME )
33   )
34 }
35
36 // Access control and domain settings to support this scenario
37 context {
38   permission {
39     and PRAC, RECORDS, read with condition(
40       context "read" > "date" > "/2020"
41     )
42   }
43   domain( THIS->trusts set value( PRAC ) )
44 }
45 }
```

## Links und Literatur

- Txture: [www.txture.org](http://www.txture.org)
- ADAMANT: [adamant.q-e.at](http://adamant.q-e.at)
- R. Breu, M. Brunner, C. Sillaber: Security im Produkt-Lifecycle – Lästige Pflicht oder Chance? Juni-Ausgabe Objektspektrum, 2015
- R. Breu, A. Kuntzmann-Combelles, M. Felderer: New Perspectives on Software Quality, IEEE Software, January/February 2014
- M. Felderer, I. Schieferdecker: Handreichung zur Methodenauswahl – Eine Taxonomie risikobasierter Softwaretests, Objektspektrum, Ausgabe Testing, 2014

[http://www.sigsgdatacom.de/fachzeitschriften/objektspektrum/archiv/artikelansicht.html?tx\\_mwjournals\\_pi1%5Bpointer%5D=0&tx\\_mwjournals\\_pi1%5Bmode%5D=1&tx\\_mwjournals\\_pi1%5BshowUid%5D=7737](http://www.sigsgdatacom.de/fachzeitschriften/objektspektrum/archiv/artikelansicht.html?tx_mwjournals_pi1%5Bpointer%5D=0&tx_mwjournals_pi1%5Bmode%5D=1&tx_mwjournals_pi1%5BshowUid%5D=7737)