Security RiskFlows –

Konzepte für die organisierte Suche nach der Nadel im Heuhaufen

Ruth Breu, Michael Brunner

Universität Innsbruck

http://www.qe-lab.at/

Quality Engineering Laura Bassi Lab
Living Models for Collaborative Systems

CENTRES OF EXPERTISE LAURA BASSI

Industry Partners

AV comparatives

infineon

ITH icoserve technology for healthcare
a siemens company

PORSCHE INFORMATIK GMBH

SwissLife

PoSecCo

Policy and Security Configuration Management

http://posecco.eu

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.

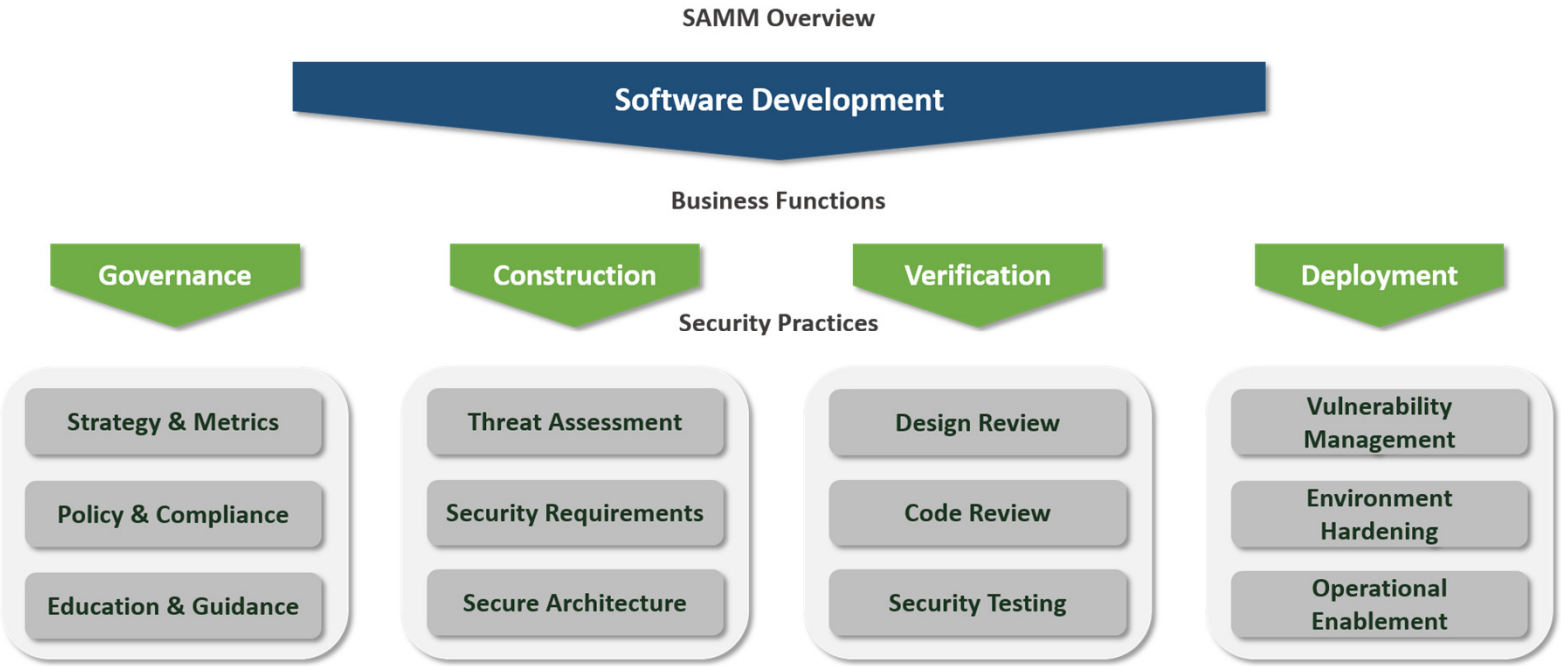
Zwei zentrale Fragen für Produkthersteller

Wieviel Security braucht das Produkt?

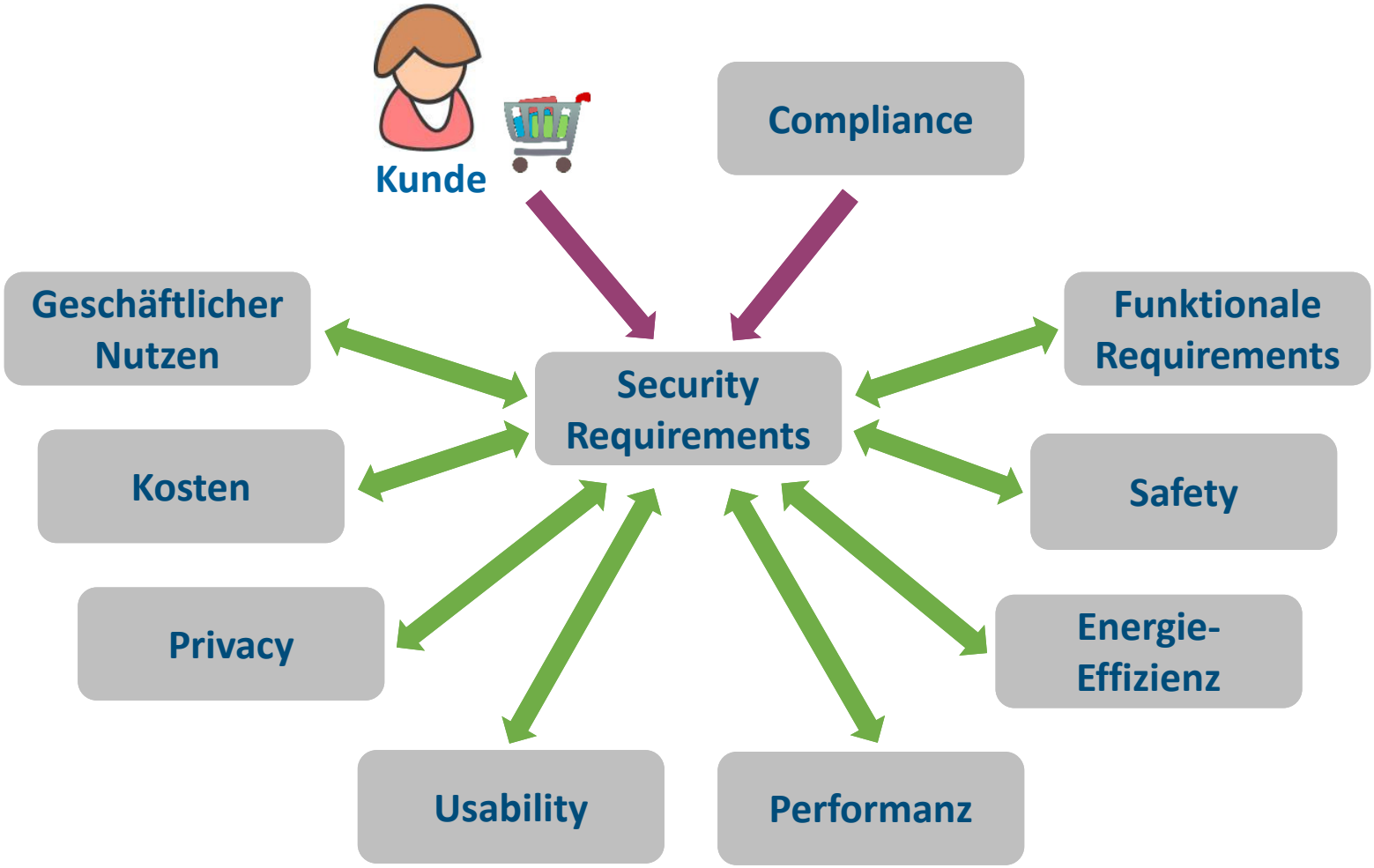
Wie sicher ist das Produkt aktuell?

State of the Art: Security Lifecycle Management

SAMM



Wie viel Security braucht das Produkt?



Wie sicher ist das Produkt aktuell?

Kunde

Produkt-Anbieter

Security-Anforderungen

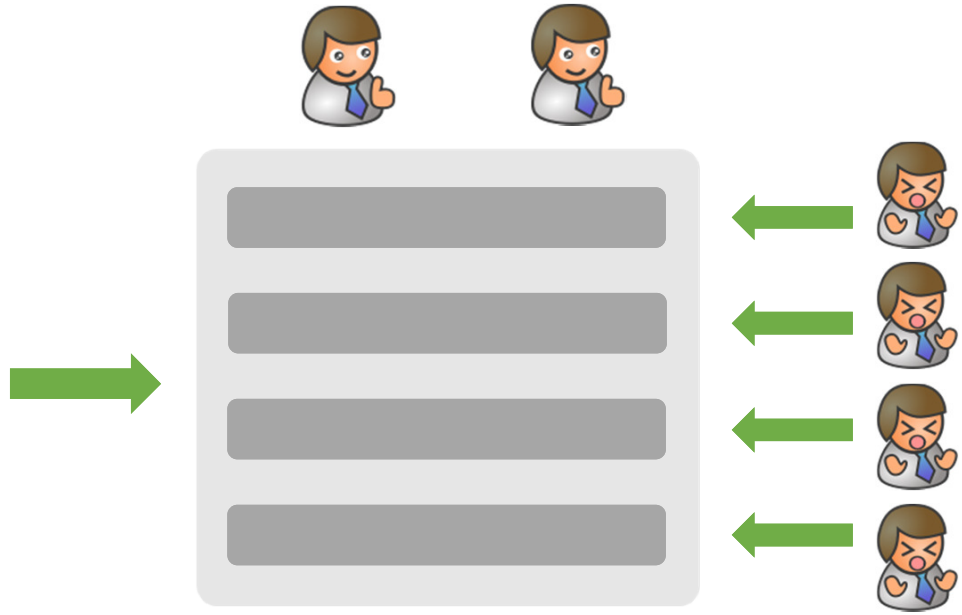
Produkt

Auditor

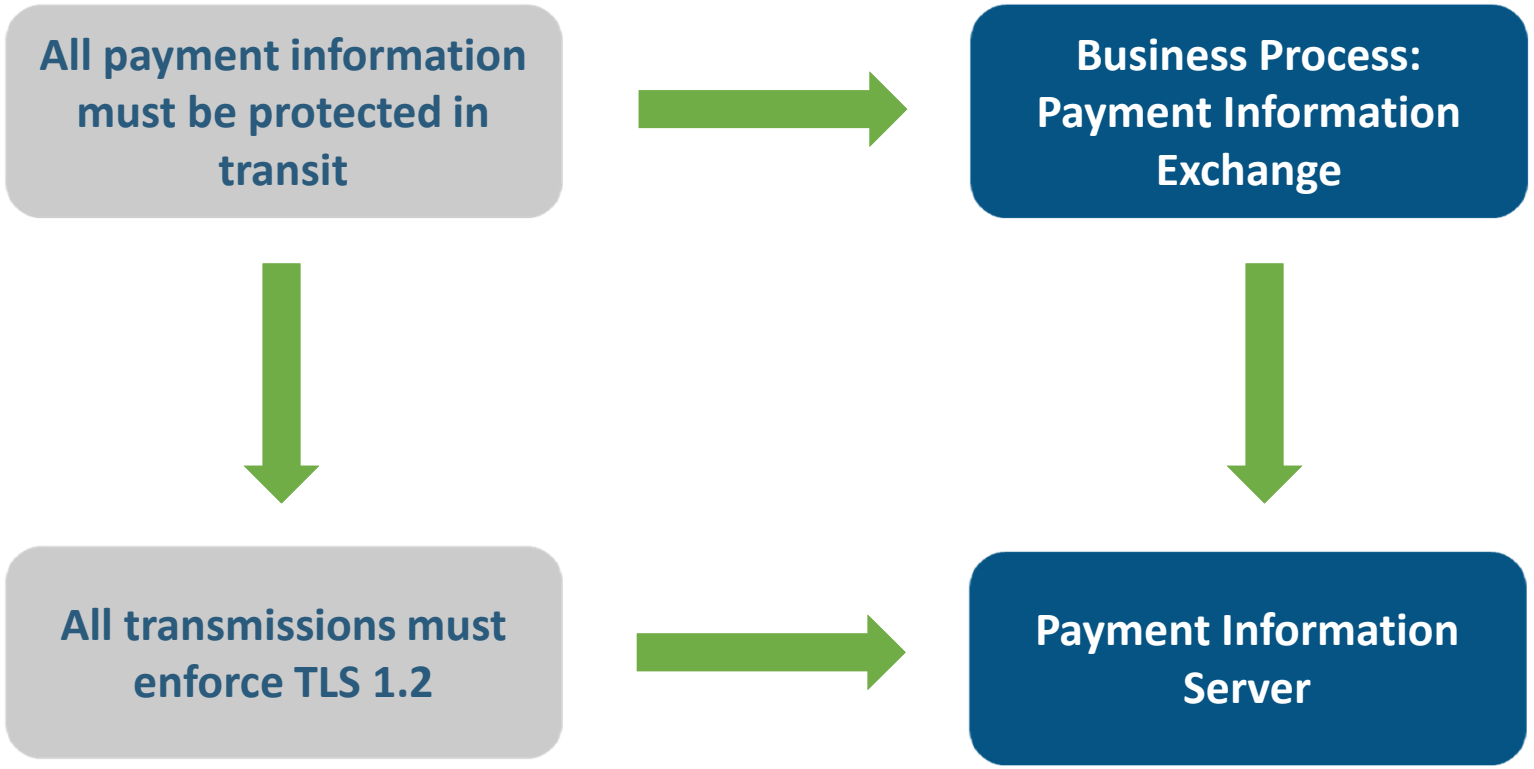
3 Haupt-Herausforderungen

1. Negative Natur von Sicherheitsanforderungen

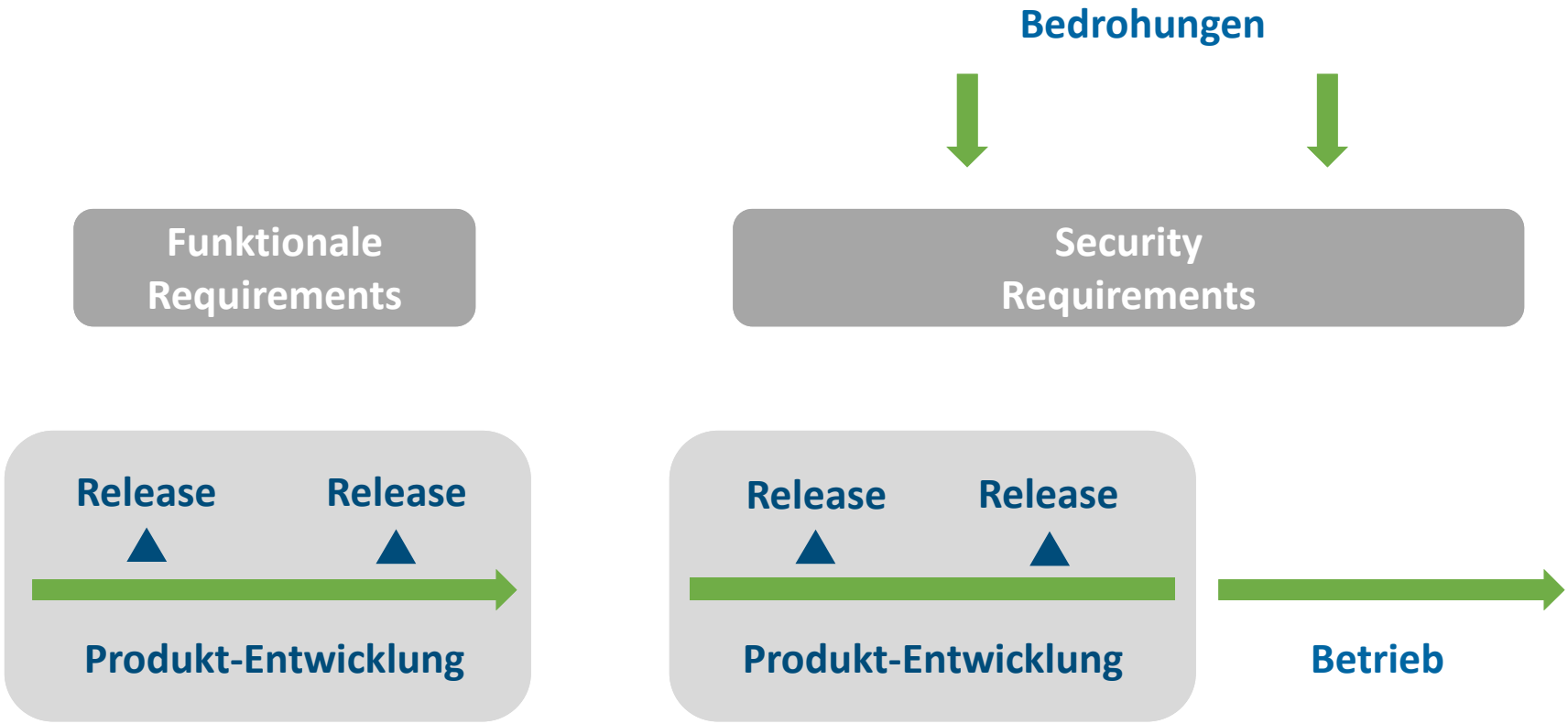
Nur autorisierte Nutzer können auf Kundendaten zugreifen



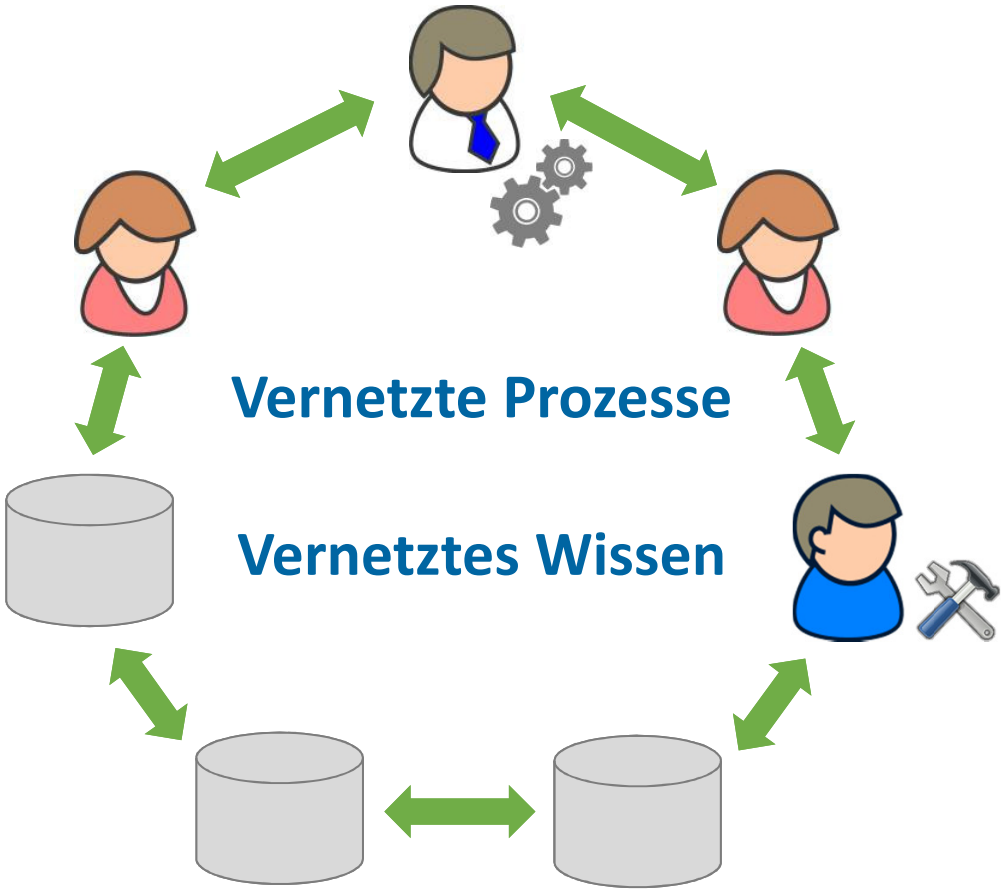
2. Abhängigkeit von Assets



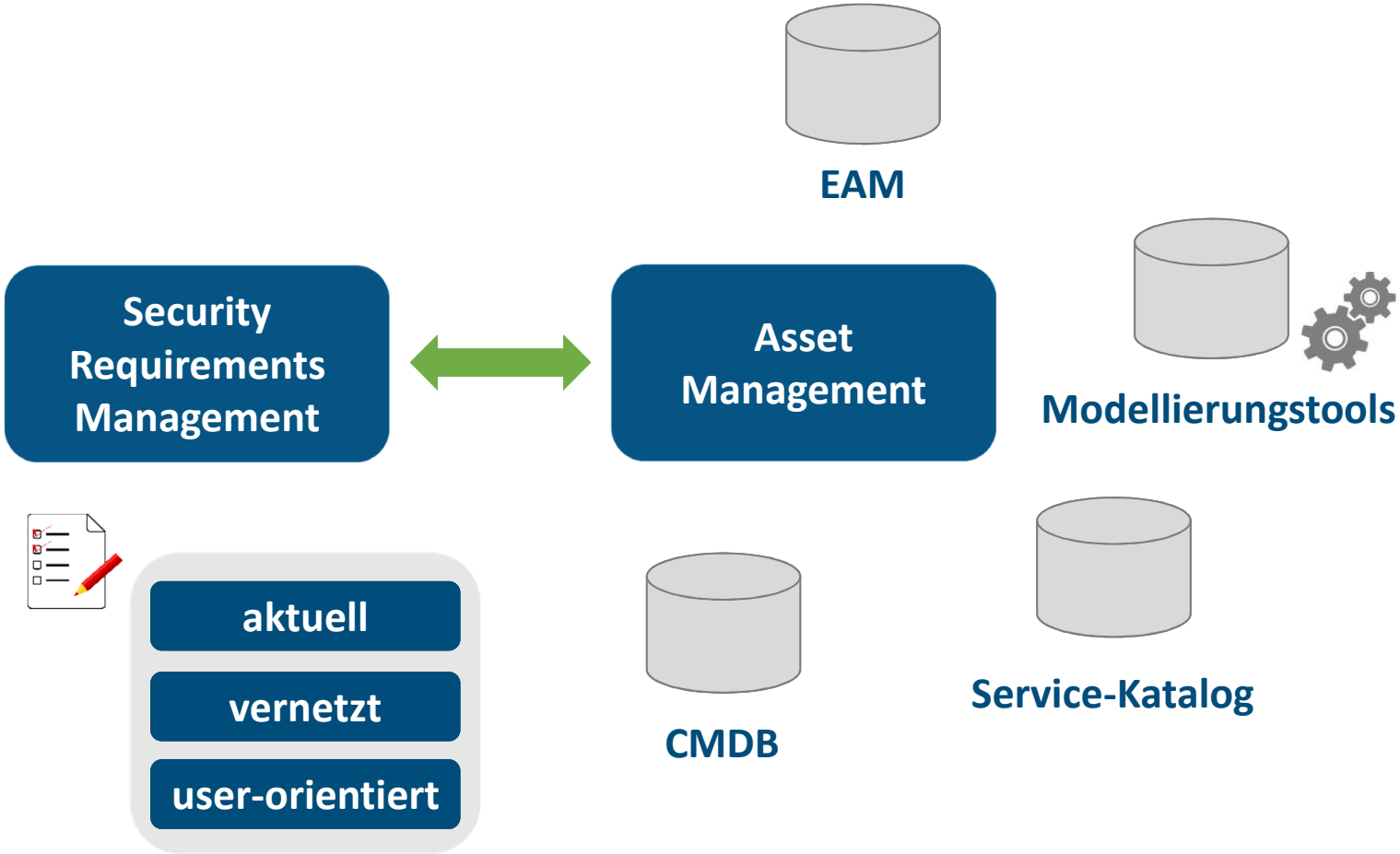
3. Eigener Lebenszyklus



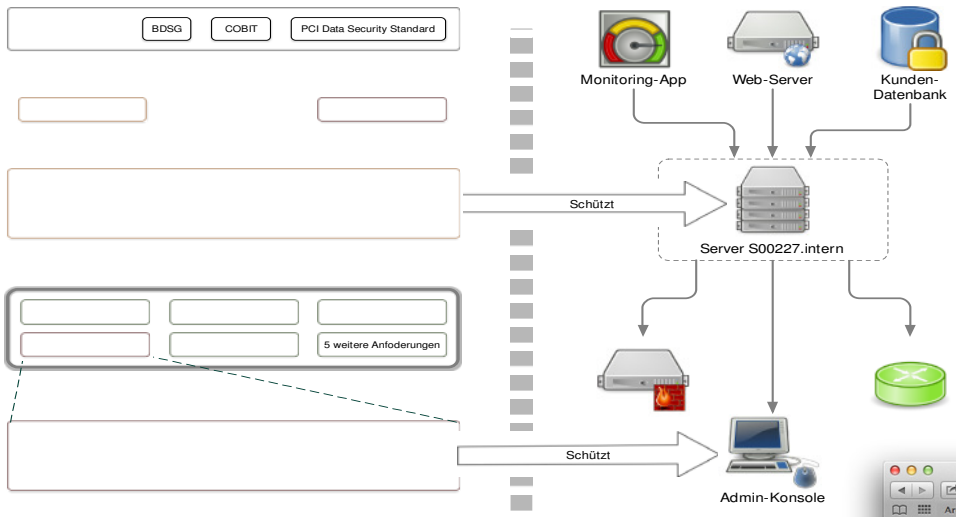
Security als Aufgabe kooperativen Wissensmanagements

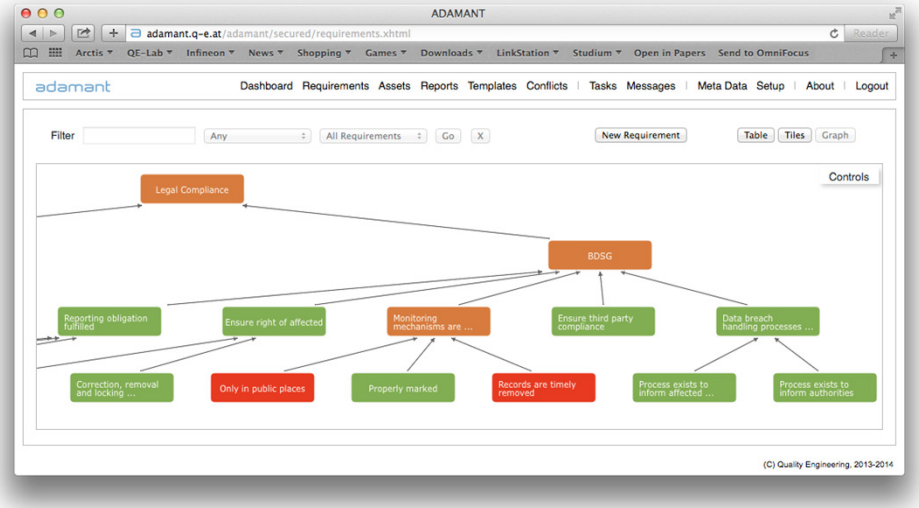


Qualitativ hochwertiges Asset Management

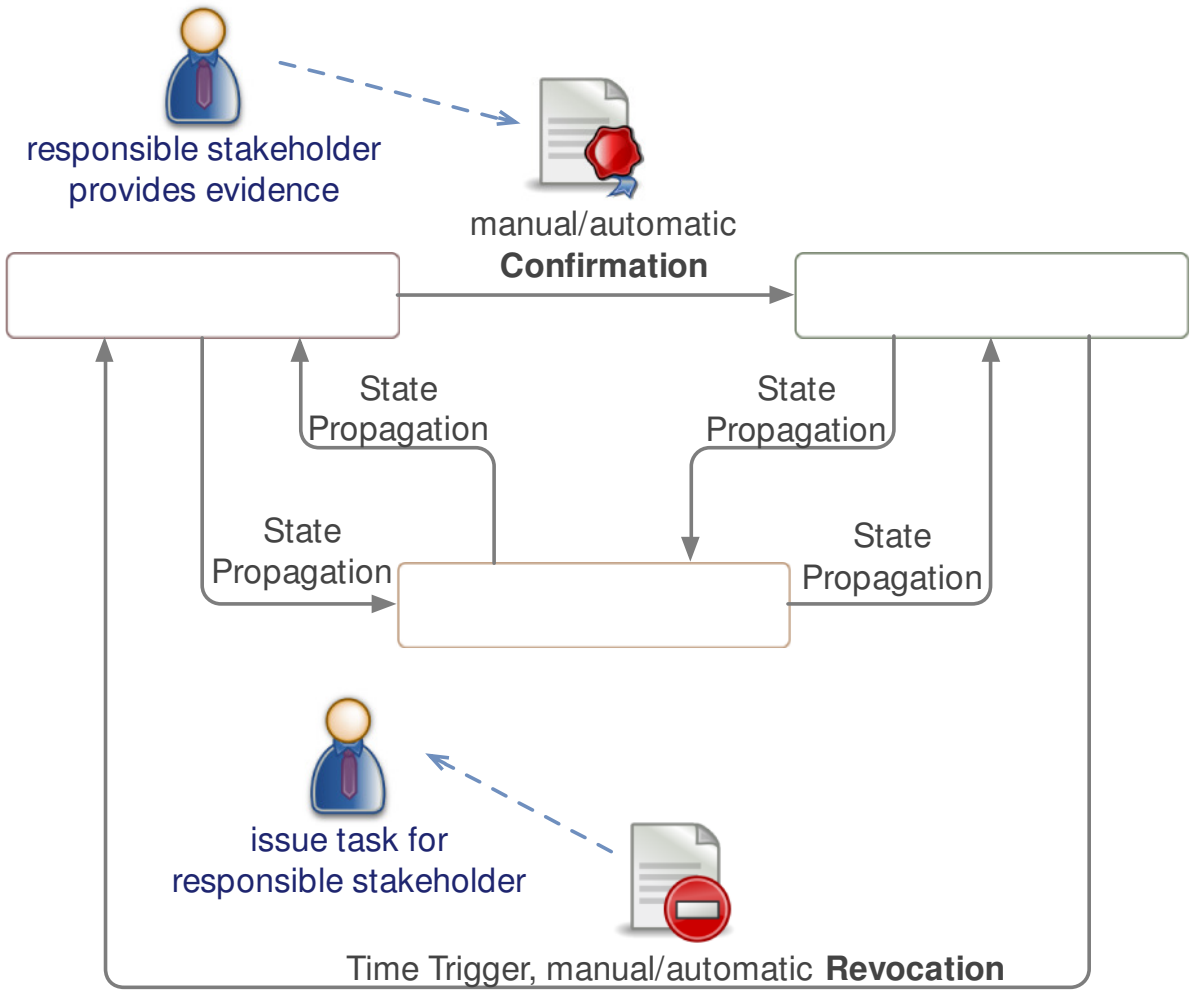


Nachverfolgbare Security Requirements

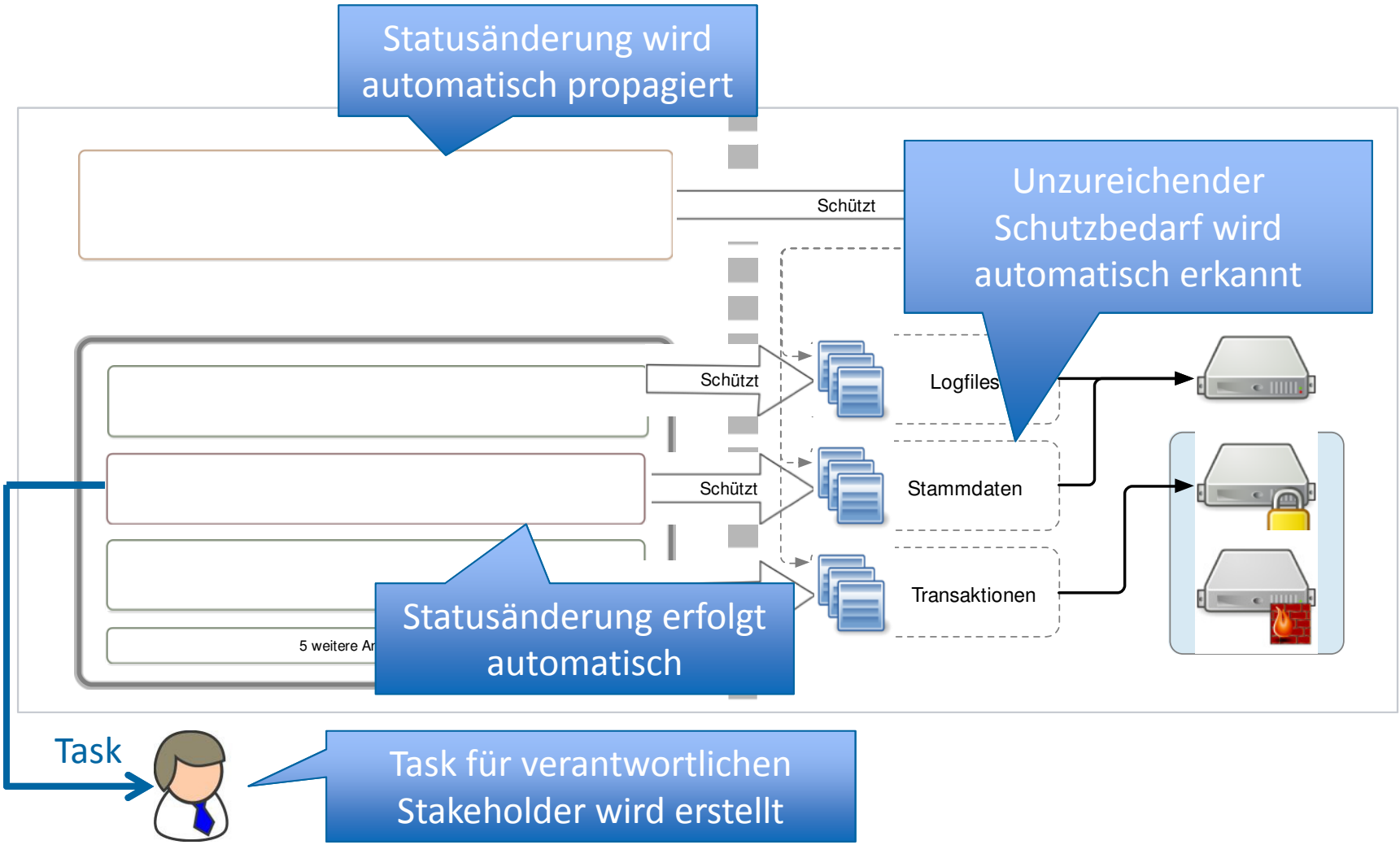




Workflow-Unterstützung /1

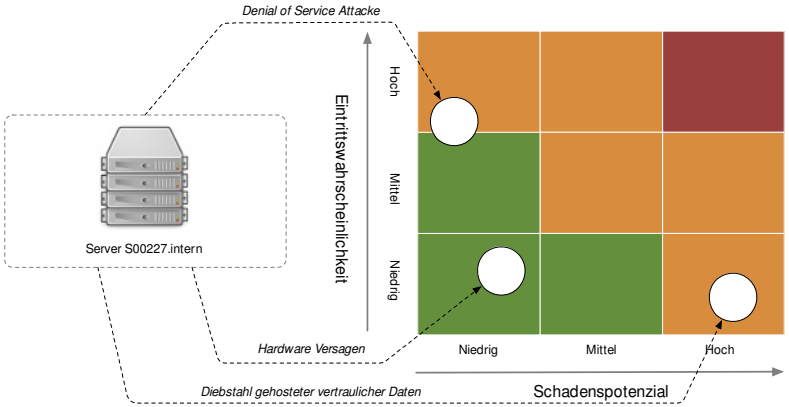


Workflow-Unterstützung /2



Risikogetriebenes Vorgehen

Technische Sicht



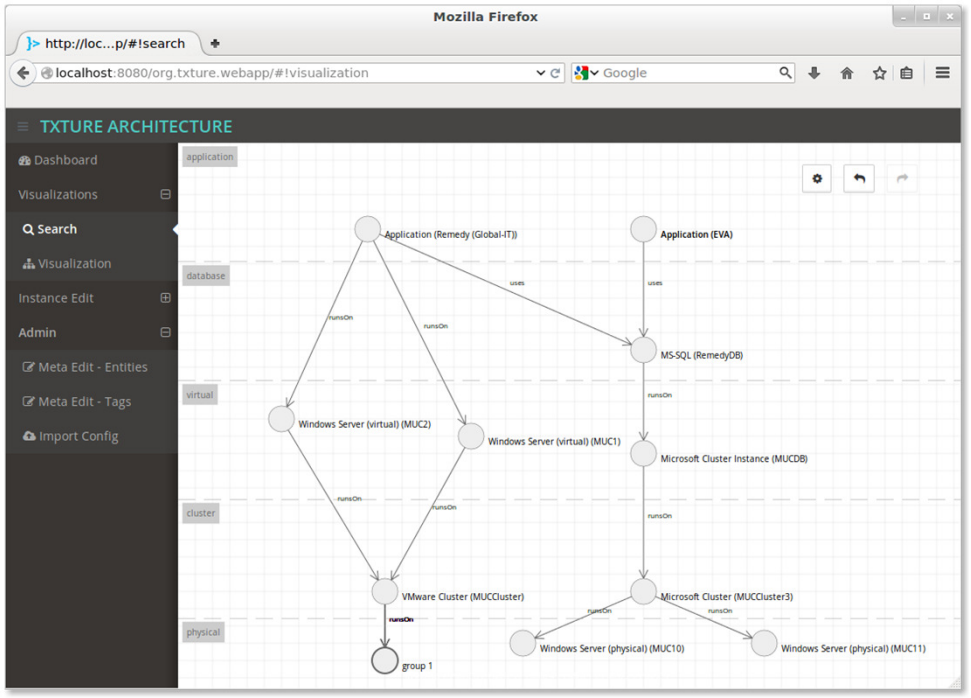
Geschäftsorientierte Sicht

- 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

txture

Efficient Security and Compliance

adamant

Modellgetriebener Ansatz

Risikobasiertes Testen

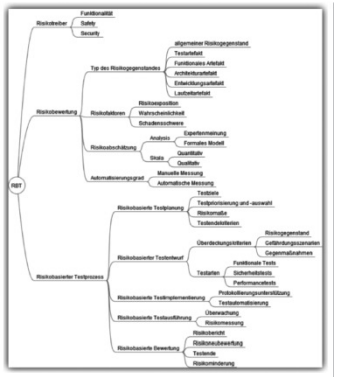
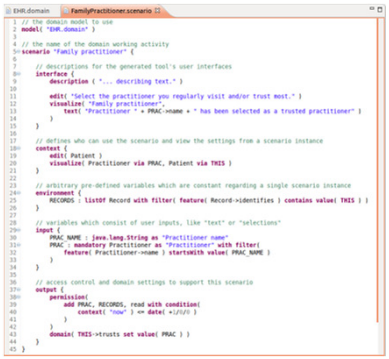


Abb. 1: Taxonomie für das risikobasierte Testen

Model-Based Security



Links und Literatur

- Txture: www.txture.org
- ADAMANT: 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.sigsdatacom.de/fachzeitschriften/objektspektrum/archiv/artikelansicht.html?tx_mwjournals_pi1%5Bpointer%5D=0&tx_mwjournals_pi1%5Bmode%5D=1&tx_mwjournals_pi1%5BshowUid%5D=7737