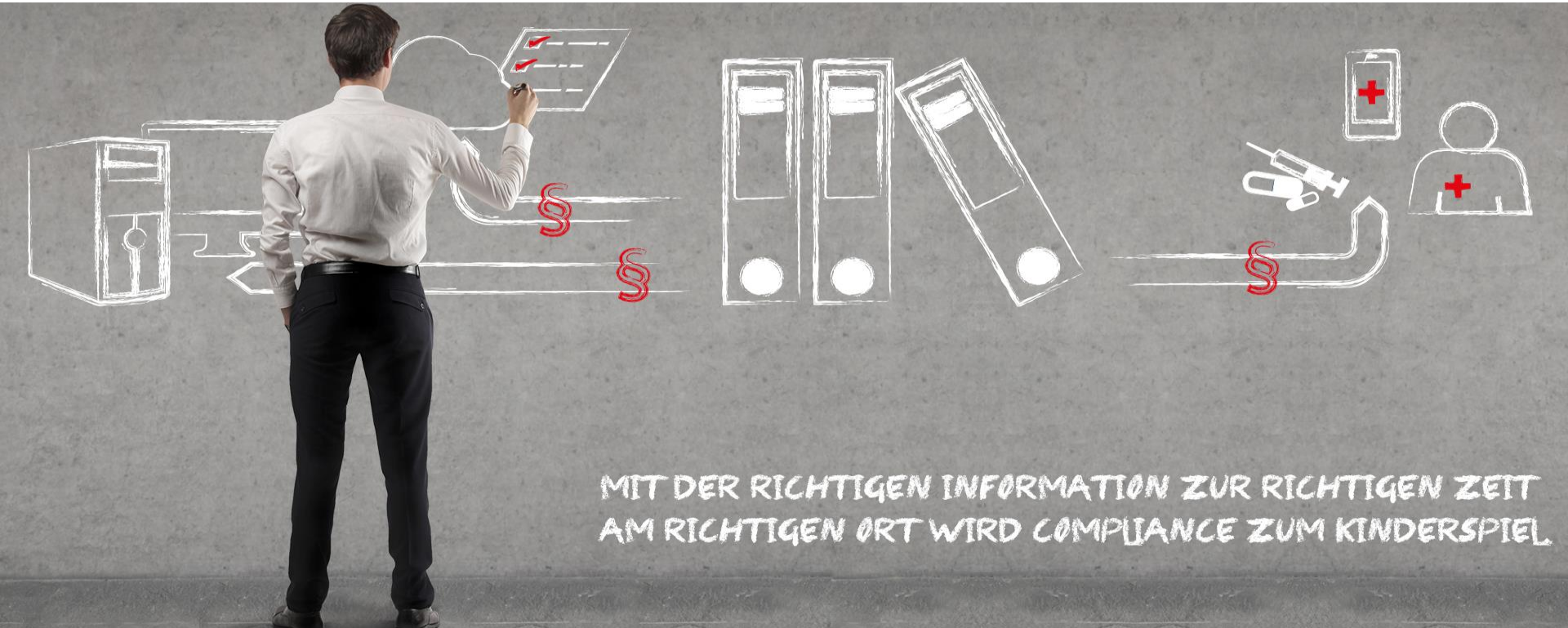
Modellbasiertes Sicherheits-Testen für Cloud-basierte Prozesse

Prof. Dr. Jan Jürjens

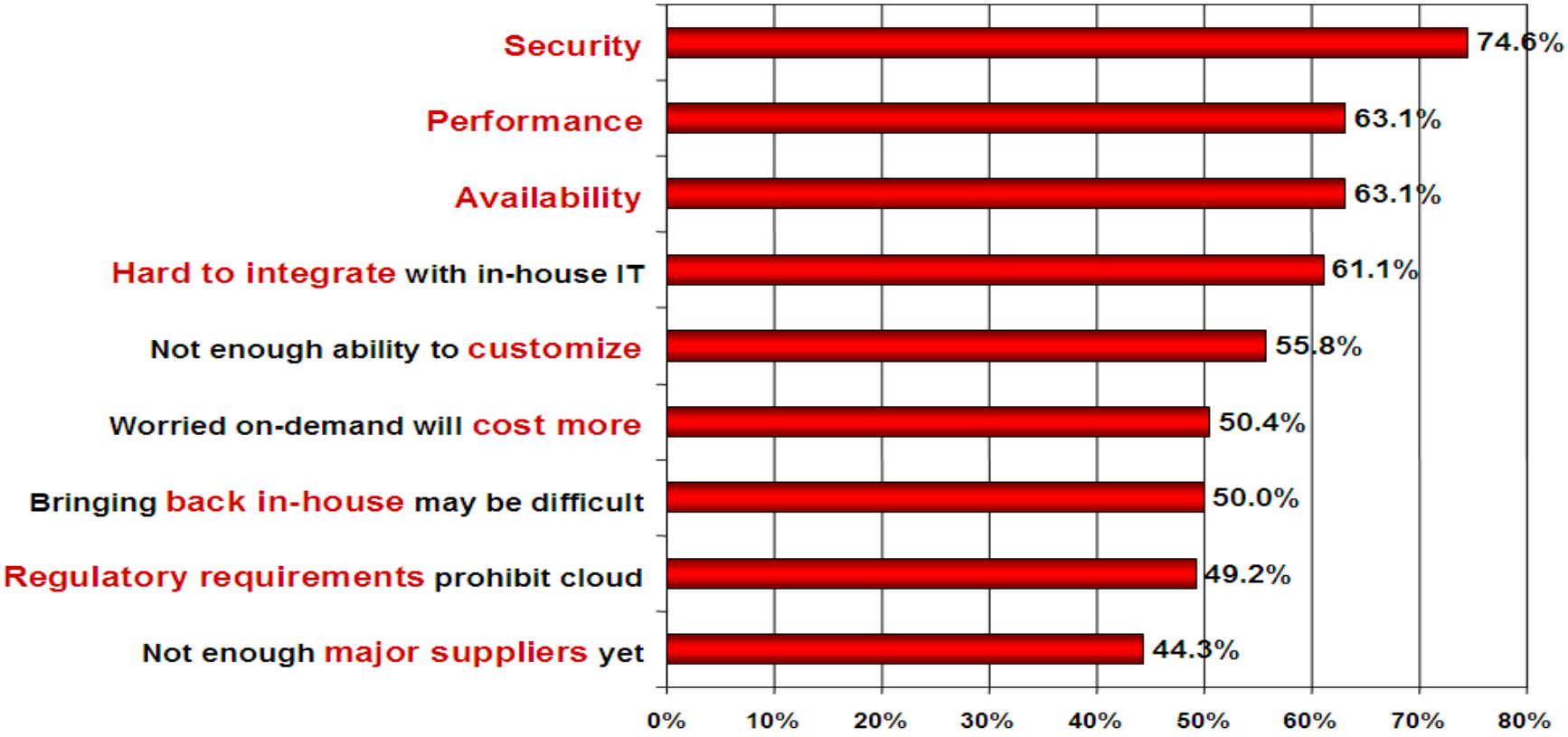
TU Dortmund

Das Forschungsprojekt ClouDAT (Förderkennzeichen 300267102) wird/wurde durch das Land NRW und Europäischen Fonds für regionale Entwicklung „Investition in unsere Zukunft“ unterstützt.



Herausforderung: Sicherheit und Compliance in der Cloud

Umfrage: **Größte Herausforderungen**
beim Einsatz von **Clouds** ?

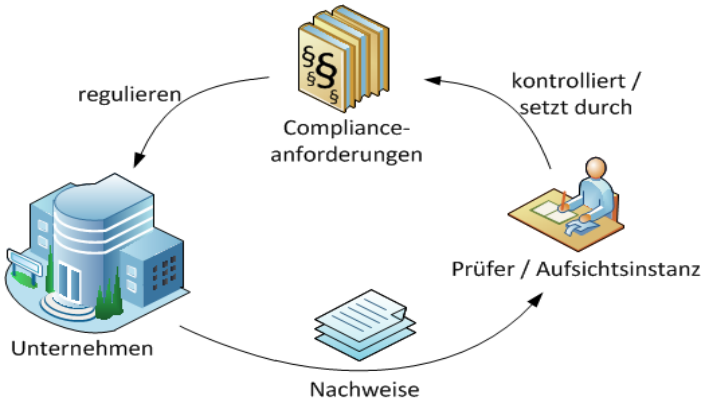


Spezifische Sicherheitsprobleme bei Cloud Computing

- Fehler / Angriffe von **Mitarbeitern** des **Providers**
- Angriffe von anderen **Kunden**
- Angriffe auf **Verfügbarkeit** (DOS)
- Fehler bei **Zuteilung** und Management von **Cloud-Ressourcen**
  - Z.B. Unzureichende Mandantentrennung
- Missbrauch der **Verwaltungsplattform**
- Angriffe unter Nutzung von **Web-Services**
- Probleme bei **Vertragsgestaltung**

(Quelle: BSI, IT-Grundschutz und Cloud Computing, 2009
und Eckpunktepapier "Sicherheitsempfehlungen für Cloud Computing Anbieter", 2011)

Herausforderung Compliance



Steigende Anzahl von **Regulierungen**

z.B. **Finanzen**: Solvency II, Basel III; **Gesundheit**: Medizinproduktegesetz (MPG); **Pharma**: Arzneimittelmarktneuordnungsgesetz (AMNOG)

Steigende Komplexität des **Compliance-Nachweises:**

- **Viele Facetten**: Anforderungen an Geschäftsprozesse (Design + Ausführung), IT-Infrastruktur (+ deren Prozesse), deren Abhängigkeiten…
- **Wechselseitige Abhängigkeiten** von Vorgaben
- **Aggregation** von Vorgaben bei komplexen IT-Systemen

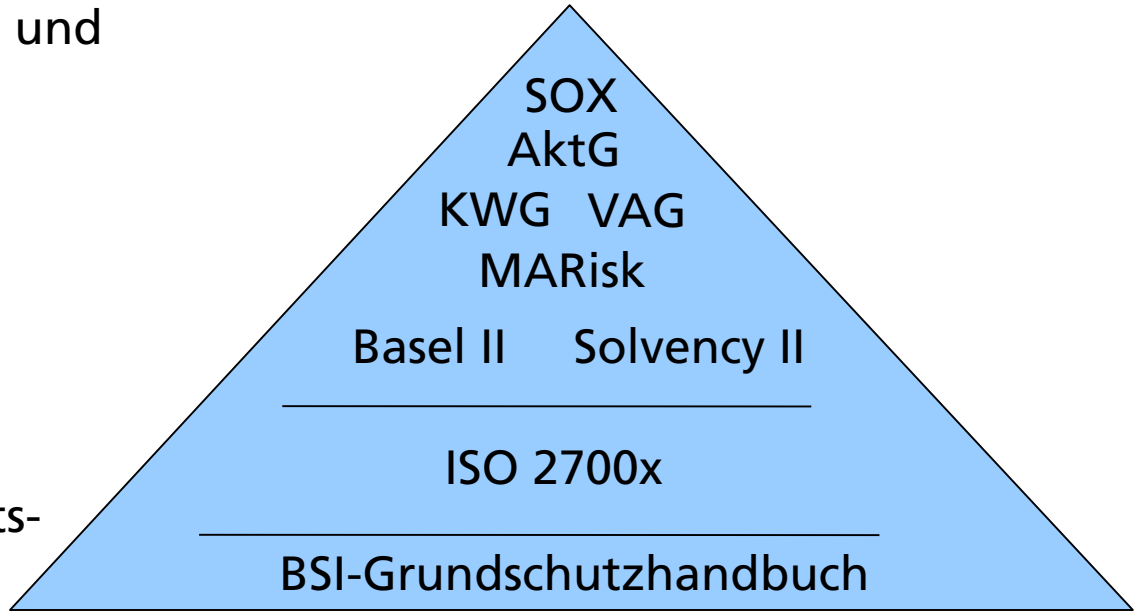
Cloud-Computing → besondere Anforderungen

Sicherheit vs. Compliance: Regularien und Standards

Abstrakte Gesetze und Regelungen

↓

Konkrete Sicherheits-Bestimmungen



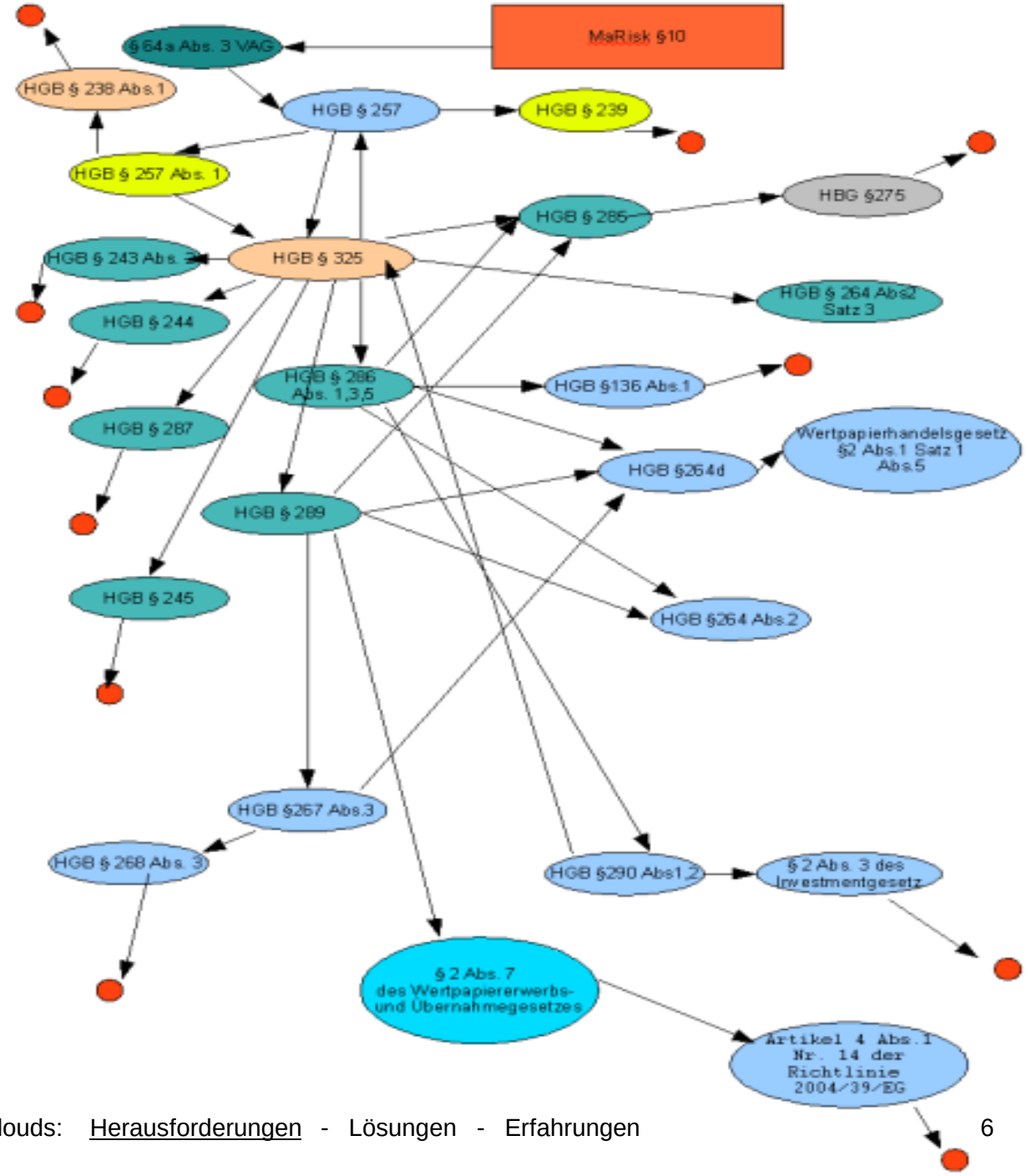
Herausforderung: Komplexität

Beispiel: MaRisk (VA)

(Mindestanforderungen an das Risikomanagement im Versicherungswesen)

Querverweise

ausgehend von §10 (Ausschnitt)



Compliance-Szenarien in der Cloud

Kunde -> Cloud:

- Sicherheits-Compliance:
  - **Sicherheitsprozesse** der Cloud auf Compliance mit SLA
- Legale Compliance:
  - Compliance vs. **Auslagerung** der Geschäftsprozesse

Cloud -> Kunde:

- Sicherheits-Compliance:
  - Überprüfung der **Kundenprozesse** auf Verstoß gegen Verhaltensbestimmungen

Wichtig: Compliance bleibt in Verantwortung des Kunden !

Notwendig: Werkzeuge für Compliance-Management

Manueller Nachweis aufwendig und kostenintensiv.

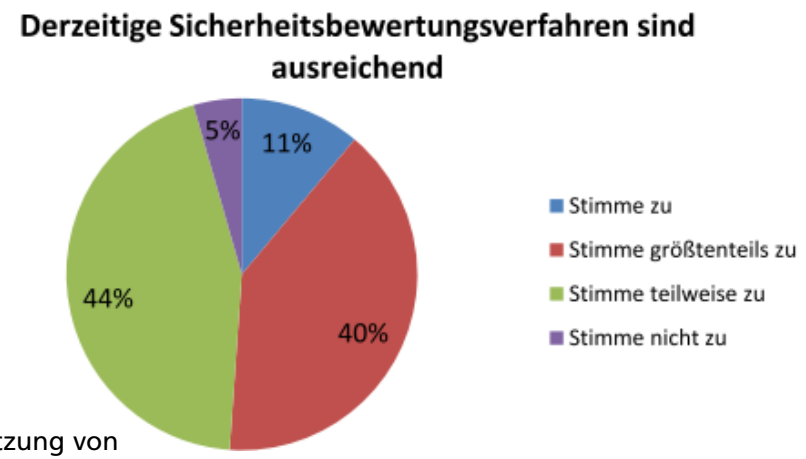
- Erforderliche Daten schwer manuell erfassbar.
- **Prüfung** einzelner Eigenschaften bereits **komplex** und umfangreich.

→ Großer Bedarf an **Compliance-Werkzeugen** (1,3 Mrd.$ [Forrester 2011])

Werkzeuge: bislang i.W. Unterstützung der manuellen Dokumentation.

Schwachpunkte:

- **Automatisierte Erfassung / Analyse** von Complianceanforderungen.
- **Überwachung** der Compliancevorgaben.
- Derzeitige **Risiko-Bewertungsmethoden** generell **nicht ausreichend**.[1]



[1] S. Taubenberger, J. Jürjens: Durchführung von IT-Risikobewertungen und die Nutzung von Sicherheitsanforderungen in der Praxis. Studie, Fraunhofer ISST 2011 und DACH security 2011

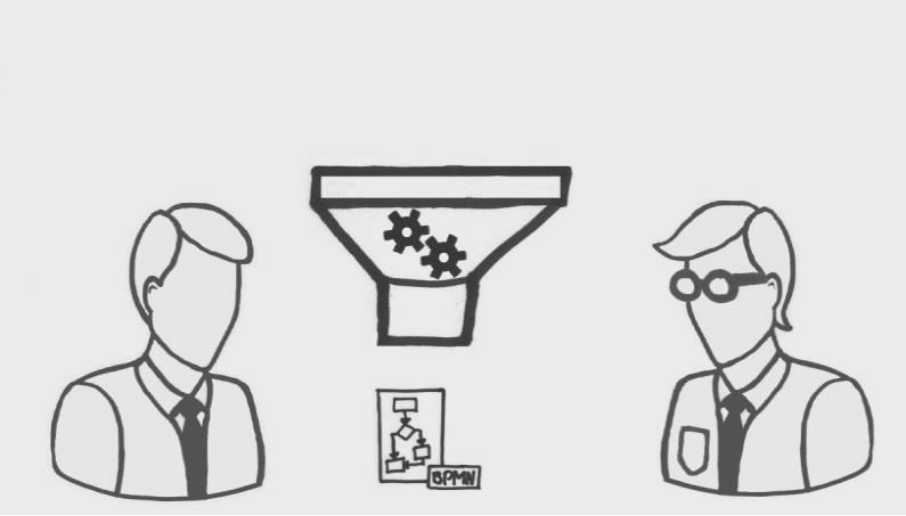
Roadmap

Herausforderungen

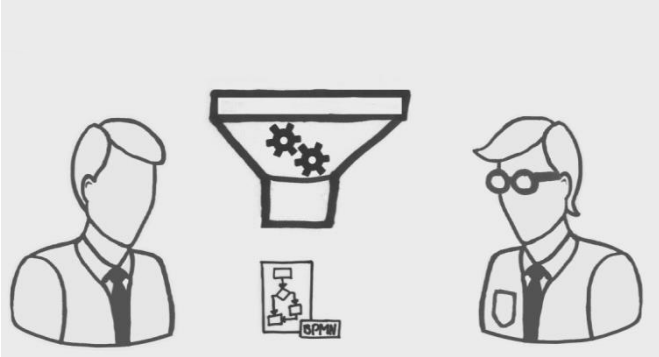
Lösungen

- Auswertungsschnitt-stellen & Automatische Validierung
- Automatiserte Datenerhebung aus Drittsystemen

Erfahrungen



Lösung: Werkzeuggestützte Compliance-Analysen



Ziele:

- Bewältigung der **Komplexität** und **Kostenersparnis** durch werkzeuggestützte Compliance-Analysen.
- Bessere **Überprüfbarkeit** der Ergebnisse.

Idee:

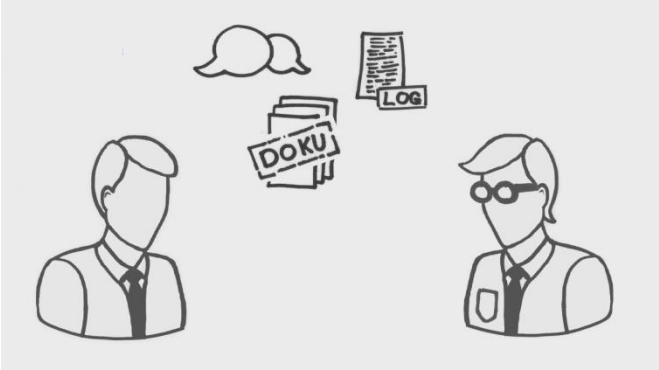
- Entwicklung Werkzeuge für: **Management und Analyse** von **Compliance-Anforderungen** mit vorhandenen Artefakten:
  - Textdokumente, Software- / Geschäftsprozessmodelle, Logdaten…

→ **„Expertensystem“ für Compliance**

Compliance-Report

Compliant: NEIN
Verstöße:
- MaRISK VA 7.2: Einhaltung von BSI G3.1 nicht erfüllt
Maßnahmen:
- BSI Maßnahmen-katalog M 2.62

Projekt CloudDAT



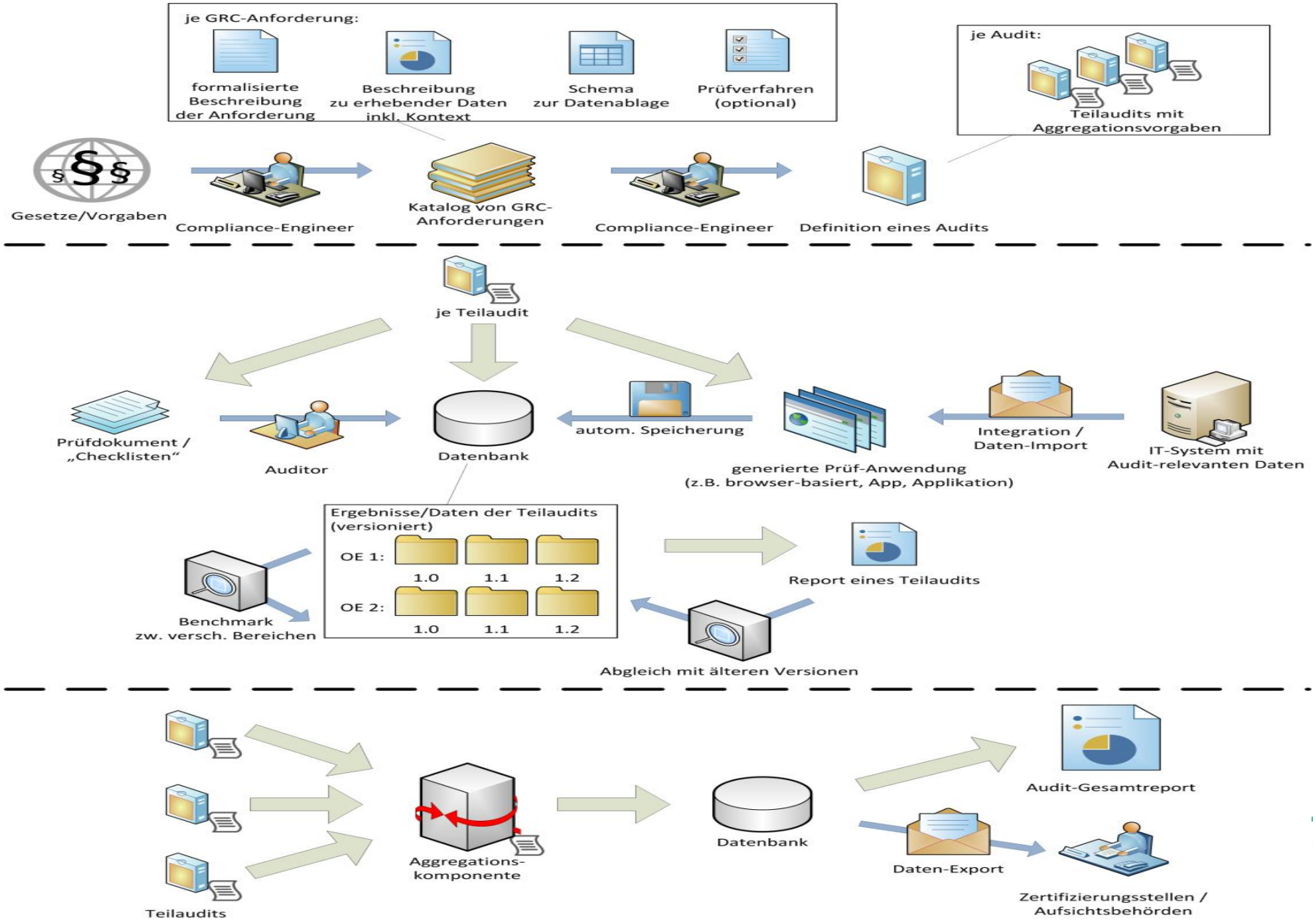
Werkzeugunterstützung für:

- Analyse der **eigenen Geschäftsprozesse** auf Eignung zur Auslagerung in eine Cloud (bzgl. Sicherheit und Compliance)
- Analyse / Überwachung der vom **Cloud-Anbieter** zugesicherten Sicherheits- und Compliance-Garantien

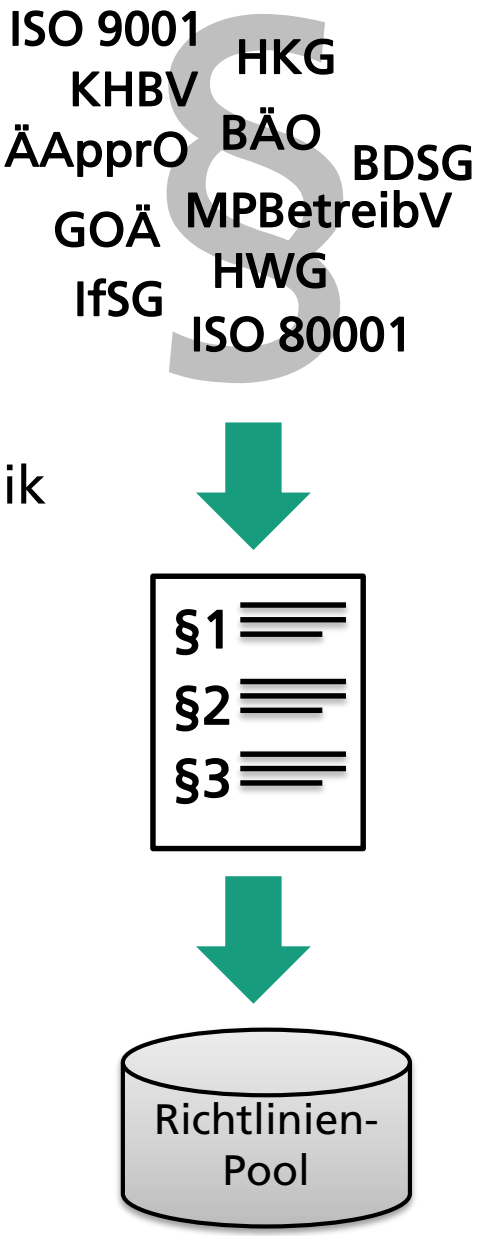
Unter Verwendung u.a.:

- **Business process mining**
  - Untersuchung von Log-Daten
- **Business process analysis**

Integrierte Compliance Management Plattform: Workflow



Sicherheitsbedarfsanalyse: Unterstützte Regelwerke



Import-Werkzeug: **Regelwerke** in **Ontologie**.

Mögliche Eingaben z.B.:

- Bundesamt für Sicherheit in der Informationstechnik
  - **IT-Grundschutz-Kataloge**
  - Standards 100-1, 100-2, 100-3, 100-4
- Bundesgesetze (www.juris.de)
  - z.B. **Bundesdatenschutzgesetz**
- Mindestanforderungen an das Risikomanagement
  - **MARisk VA** (Versicherungen)
- ISO/IEC 2700x-Reihe

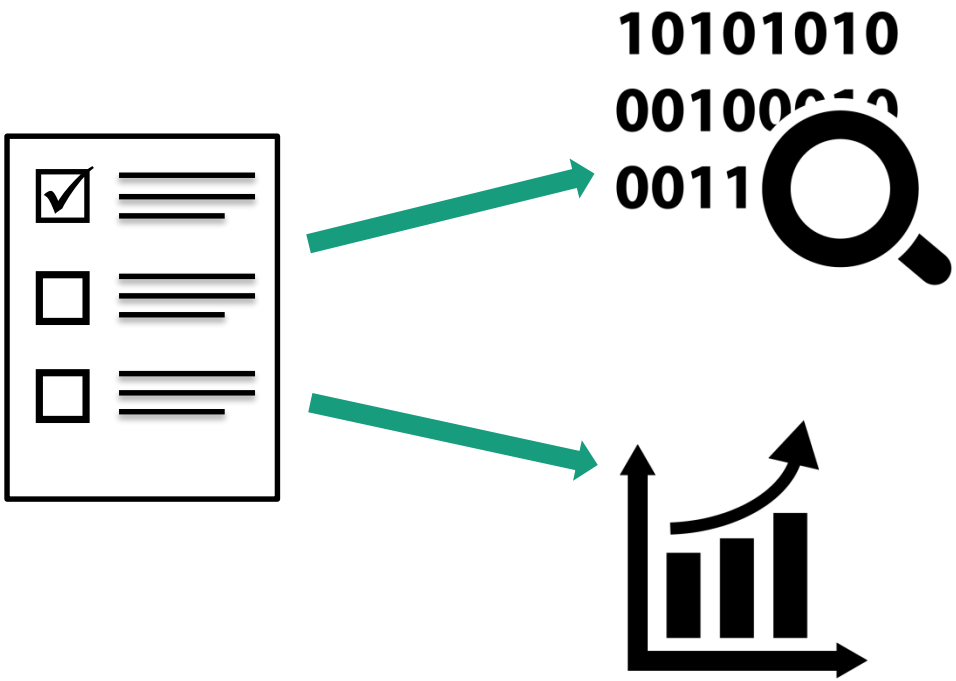
Roadmap

Herausforderungen

Lösungen

- **Auswertungsschnitt-stellen & Automatische Validierung**
  - **Architekturebene**
  - **Geschäftsprozesse**
- Automatiserte Datenerhebung aus Drittsystemen

Erfahrungen



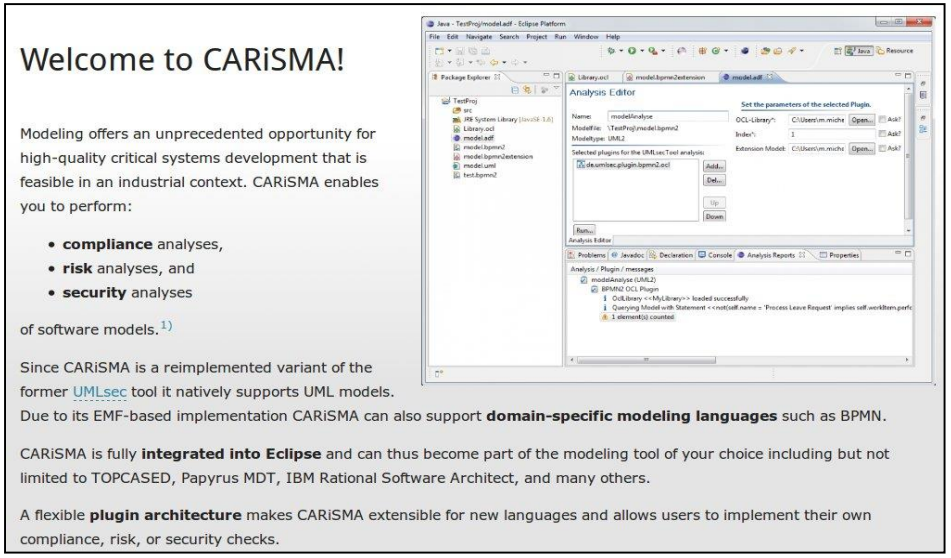
Analysewerkzeug CARiSMA

Sicherheitsanalysen auf GP-/Softwaremodellen

Eclipse Plugin-Architektur

- Integriert etablierte Modellierungs-werkzeuge, z.B. Topcased
- Open Source
- Plattformunabhängig
- Erweiterbarkeit

http://carisma.umlsec.de



Welcome to CARiSMA!

Modeling offers an unprecedented opportunity for high-quality critical systems development that is feasible in an industrial context. CARiSMA enables you to perform:

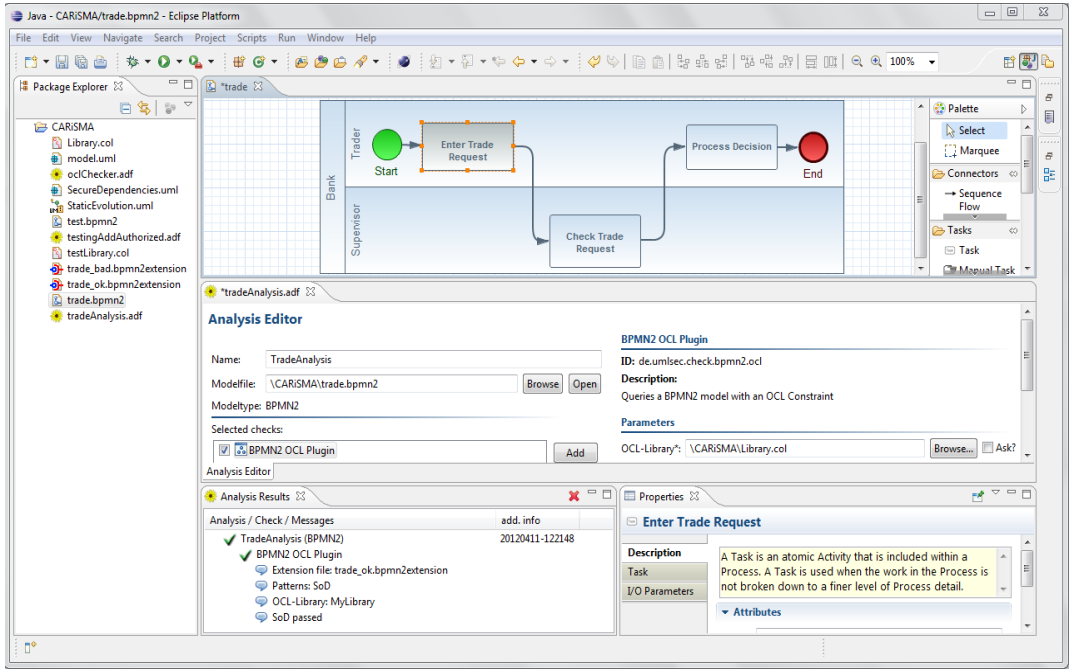
- **compliance** analyses,
- **risk** analyses, and
- **security** analyses

of software models.[1)]

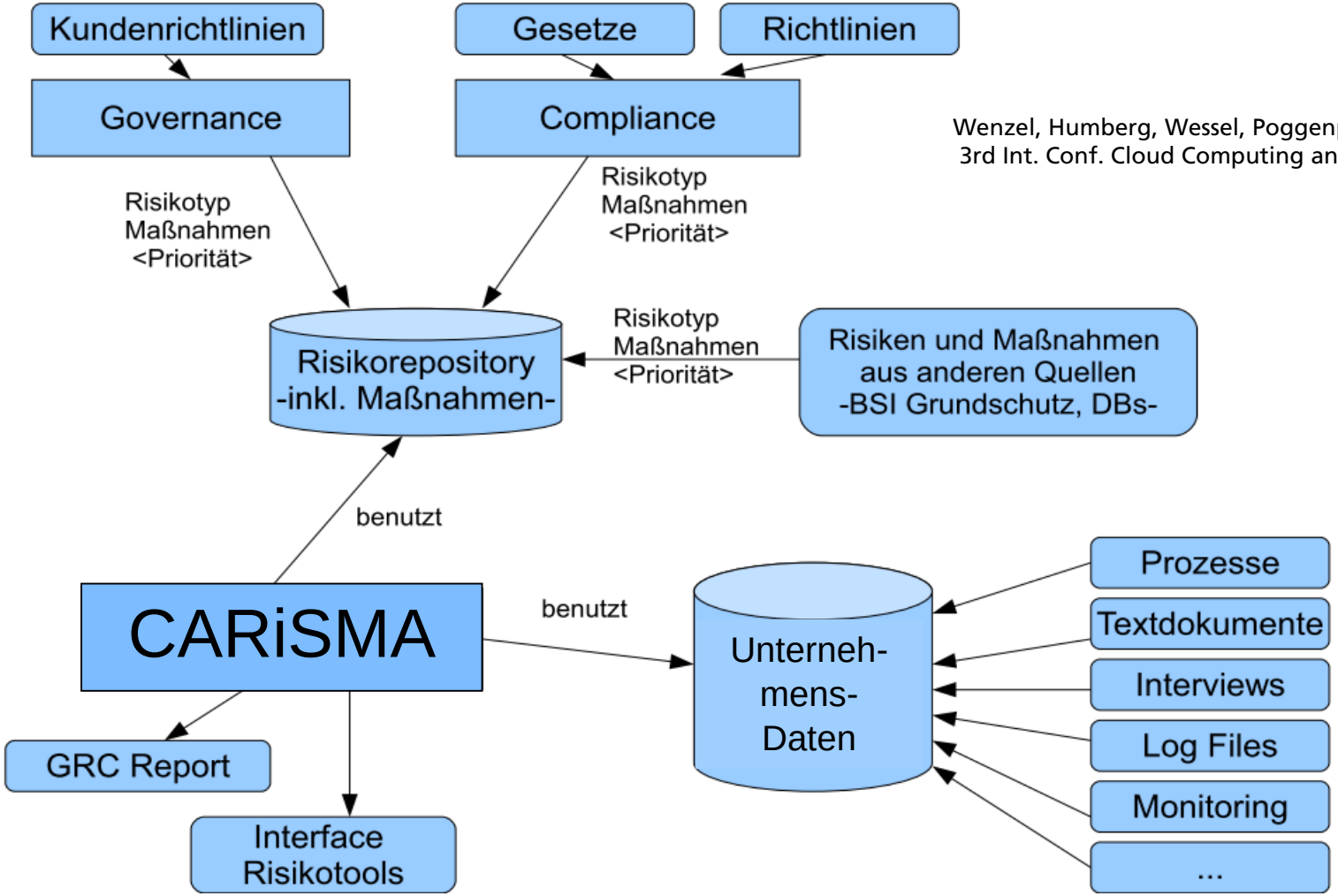
Since CARiSMA is a reimplemented variant of the former UMLsec tool it natively supports UML models. Due to its EMF-based implementation CARiSMA can also support **domain-specific modeling languages** such as BPMN.

CARiSMA is fully **integrated into Eclipse** and can thus become part of the modeling tool of your choice including but not limited to TOPCASED, Papyrus MDT, IBM Rational Software Architect, and many others.

A flexible **plugin architecture** makes CARiSMA extensible for new languages and allows users to implement their own compliance, risk, or security checks.



Compliance-Analyse-Werkzeug CARiSMA: Architektur

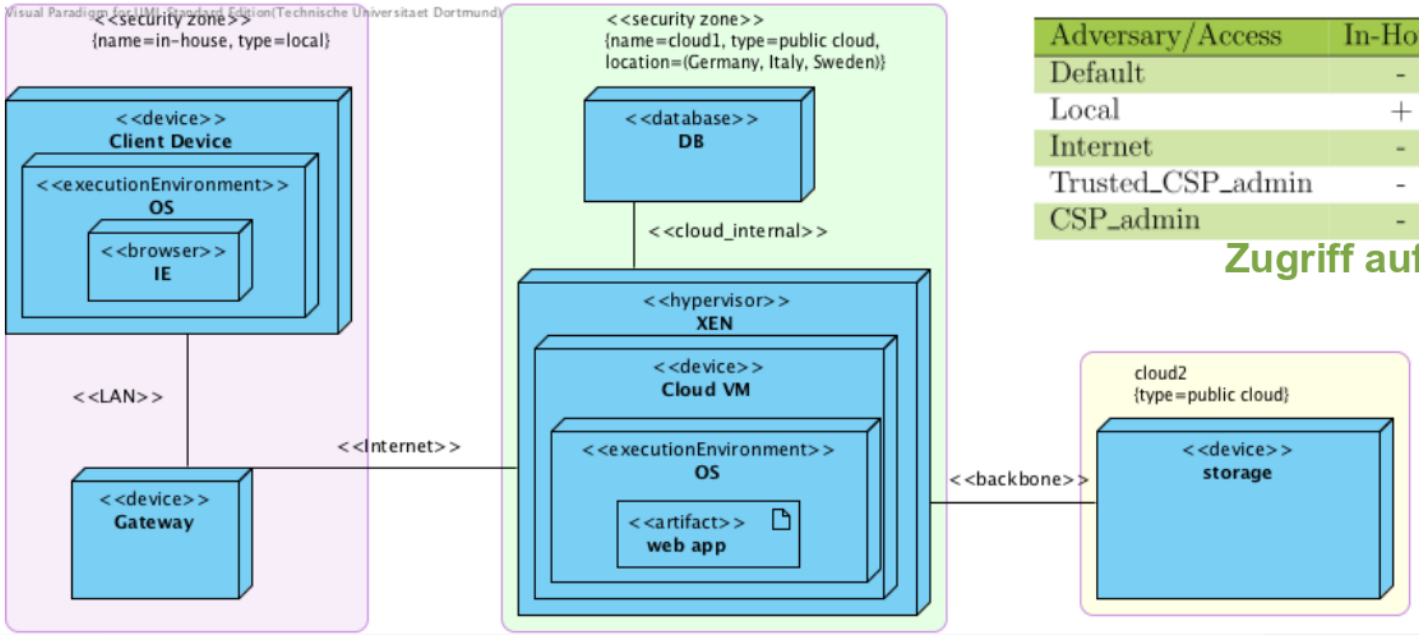


Wenzel, Humberg, Wessel, Poggenpohl, Ruhroth, Jürjens.
3rd Int. Conf. Cloud Computing and Services Science, 2013

Architekturebene:
Cloud- / Sicherheits-Modellierung mit UMLsec

Adversary/link	LAN	Internet	cloud_internal	backbone
Default	{}	{r, i, d}	{}	{}
Local	{read,insert,delete}	{}	{}	{}
Internet	{}	{r, i, d}	{}	{}
Trusted_CSP_admin	{}	{r, i, d}	{r, i, d}	{r, i, d}
CSP_admin	{}	{}	{}	{r, i, d}

Zugriff auf Links.

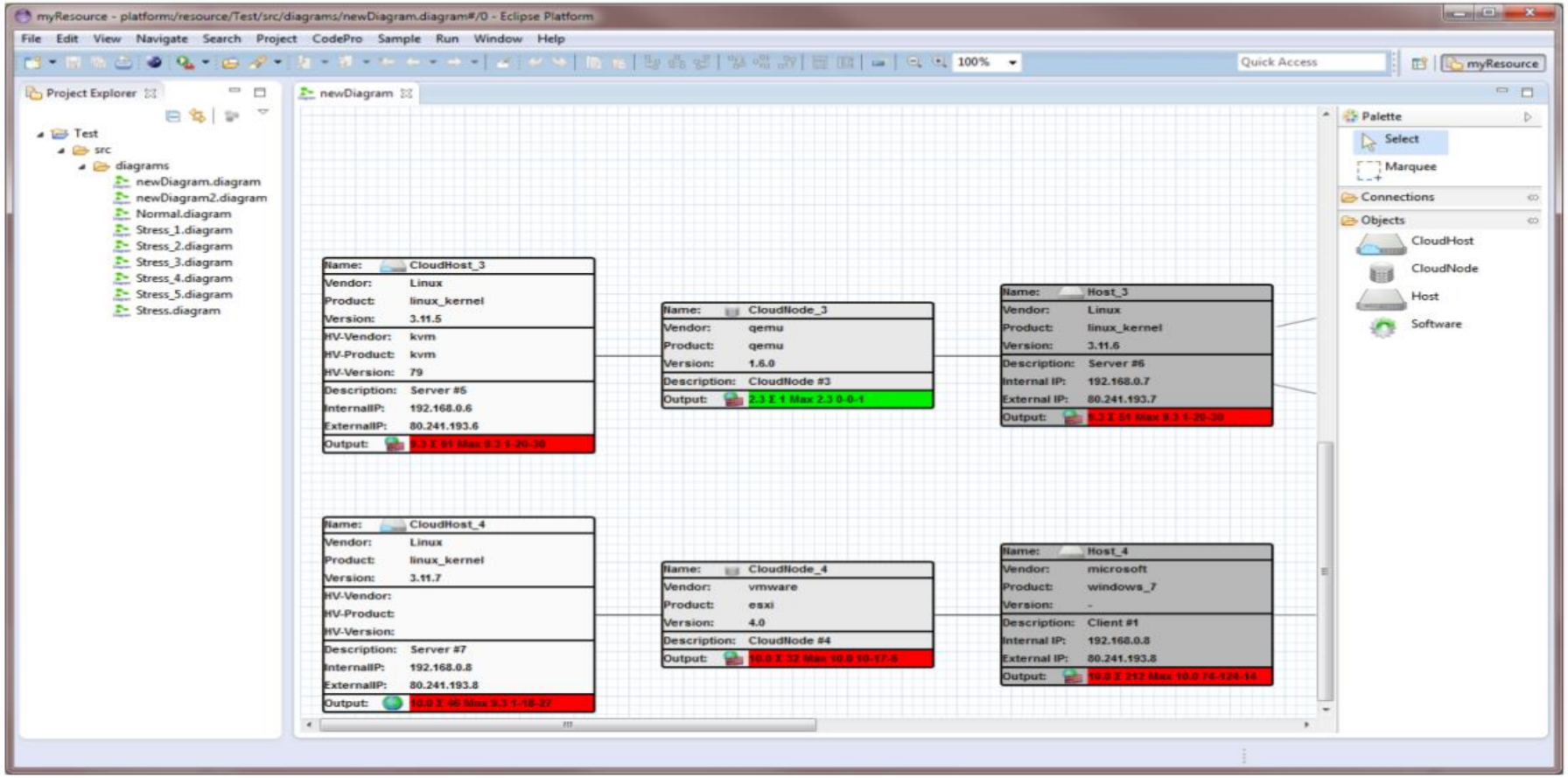


Adversary/Access	In-House	Cloud1	Cloud2
Default	-	-	-
Local	+	-	-
Internet	-	-	-
Trusted_CSP_admin	-	+	-
CSP_admin	-	-	+

Zugriff auf Knoten.

[N. Astahov 2014]

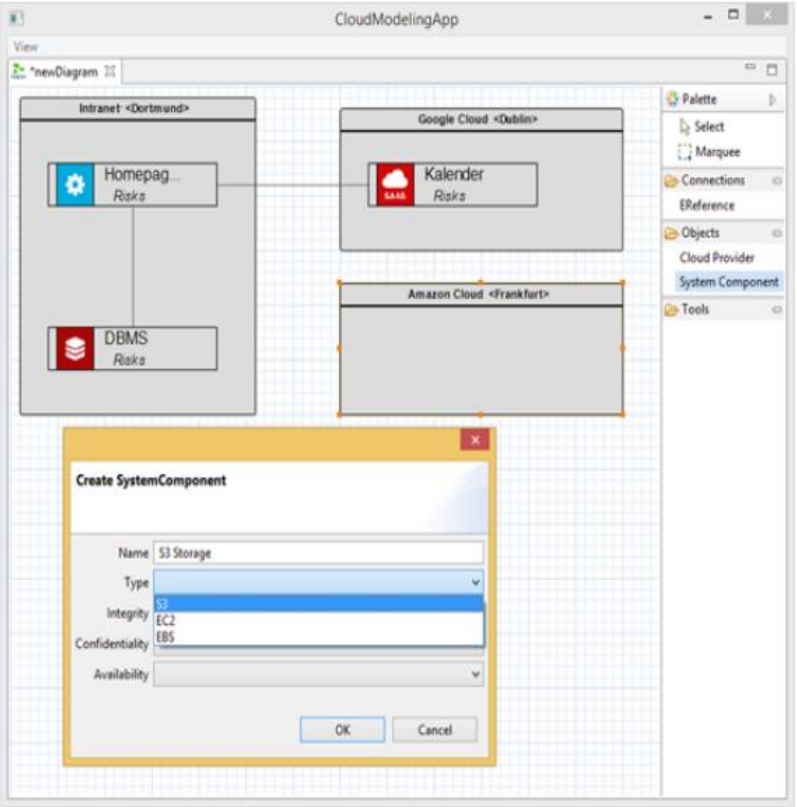
Architekturebene: Exploit-Checking für Cloud-Umgebungen

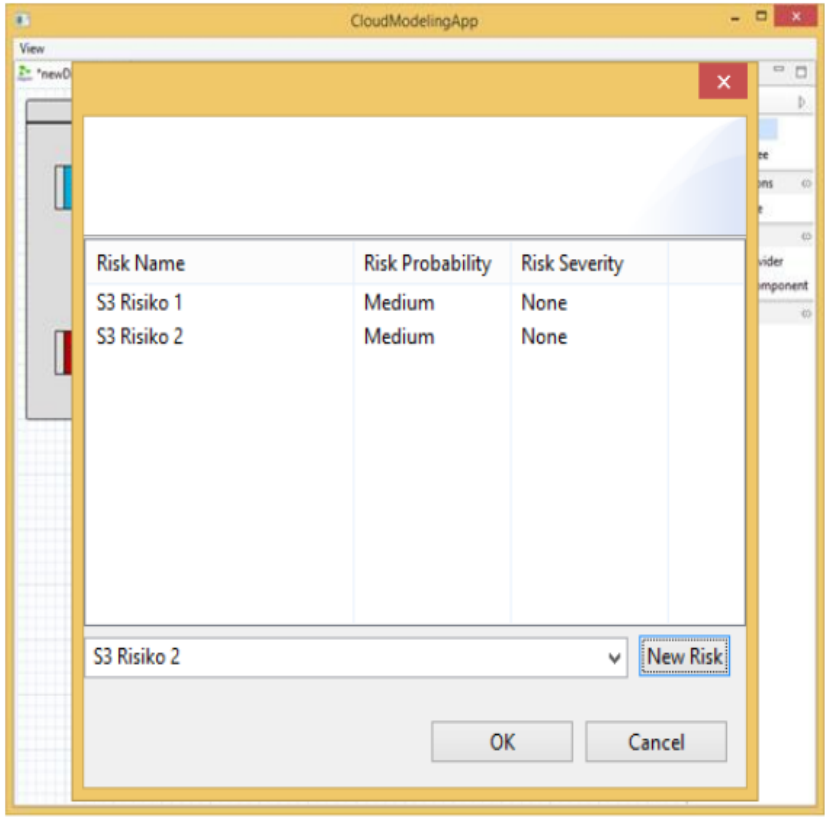


Mittels **Exploit-Datenbanken** (Common Vulnerabilities and Exposures (CVE), Common Platform Enumeration (CPE), Common Vulnerability Scoring System (CVSS v2))

[M. Nimbs 2014]

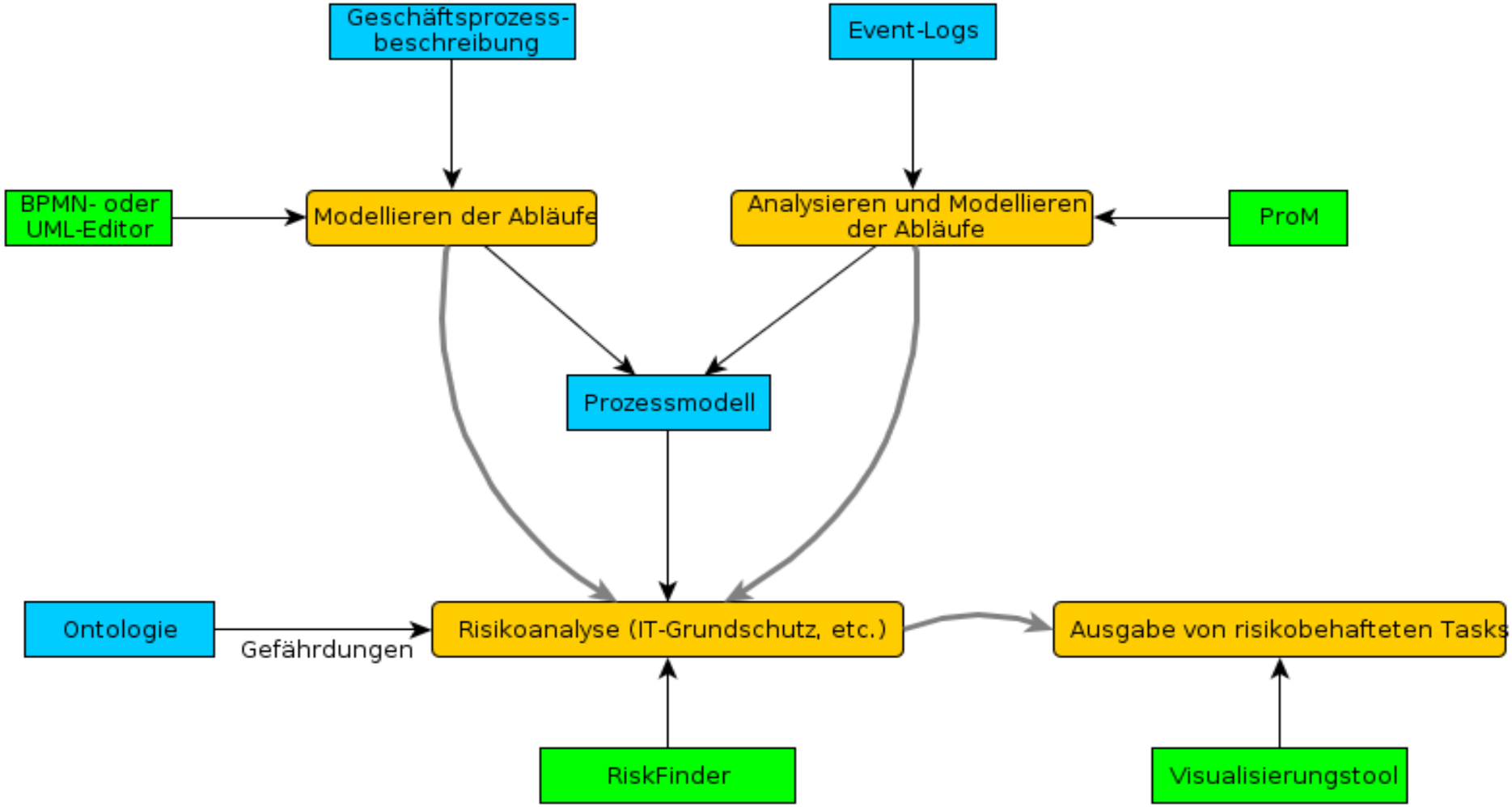
Architekturebene: Architektur-basierte Risikoanalyse





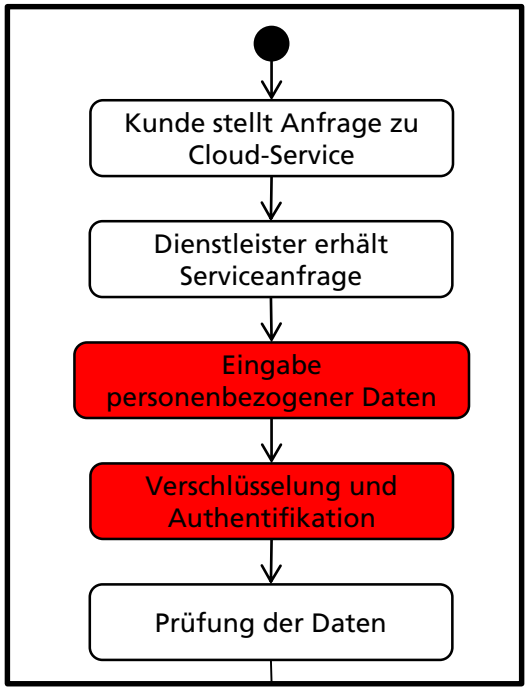
[F. Coerschulte 2014]

Analyse der Geschäftsprozesse



GP-Ebene: Textbasierte Risiko-Identifikation

Jürjens et al., Journal of Software and Systems Modeling, 2011



Gefundene Pattern

Aktivität

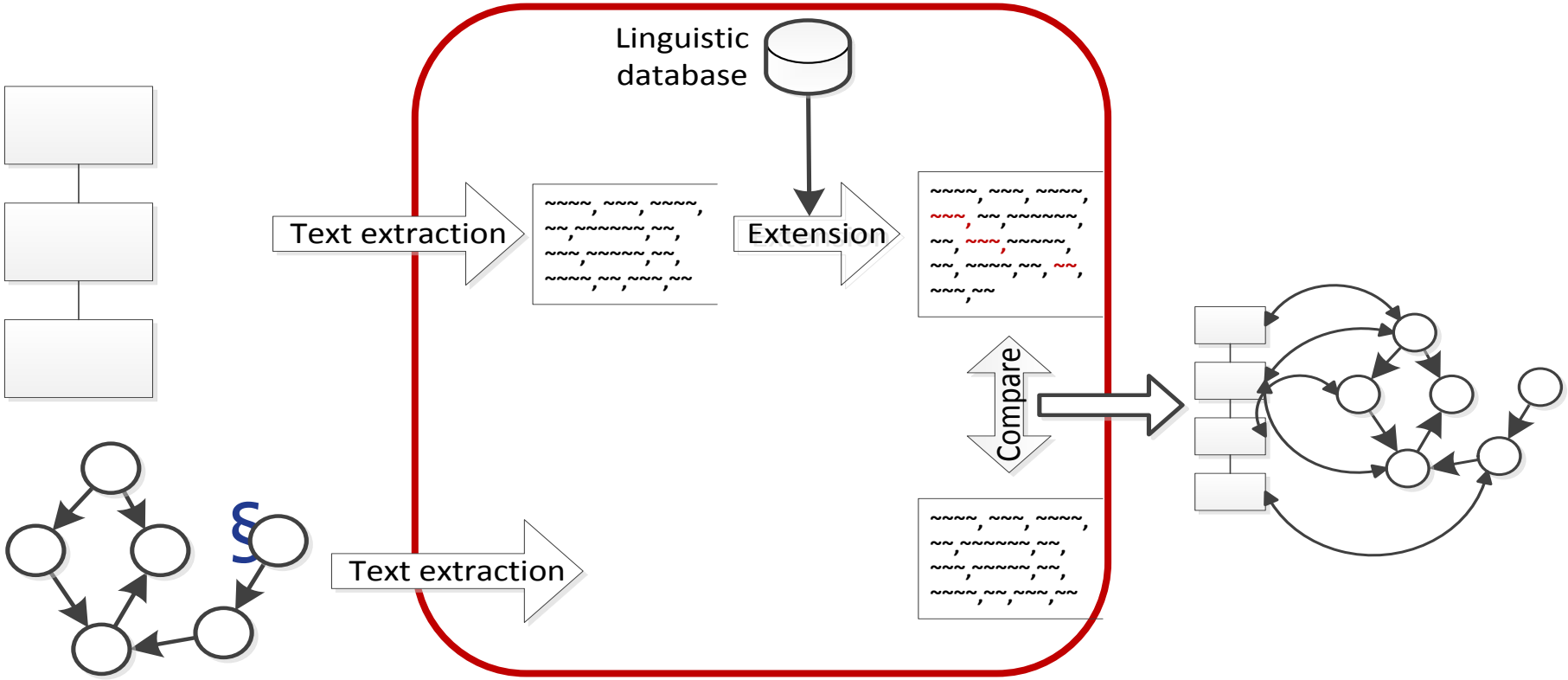
[Kunde stellt Anfrage zu Cloud-Service (233)]
4 Relevante Worte: [Information(200.0), Meldung(200.0), Nachricht 00.0), Internet(100.0)]
22 relevante Pattern:
B_5.10 : Internet Information Server (300
G_2.96 : Veraltete oder falsche Inform ngebot (200.0)
G_3.13 : Weitergabe falscher oder int 0.0)
G_3.44 : Sorglosigkeit im Umgang mi
...

Identifizierte Ausdrücke

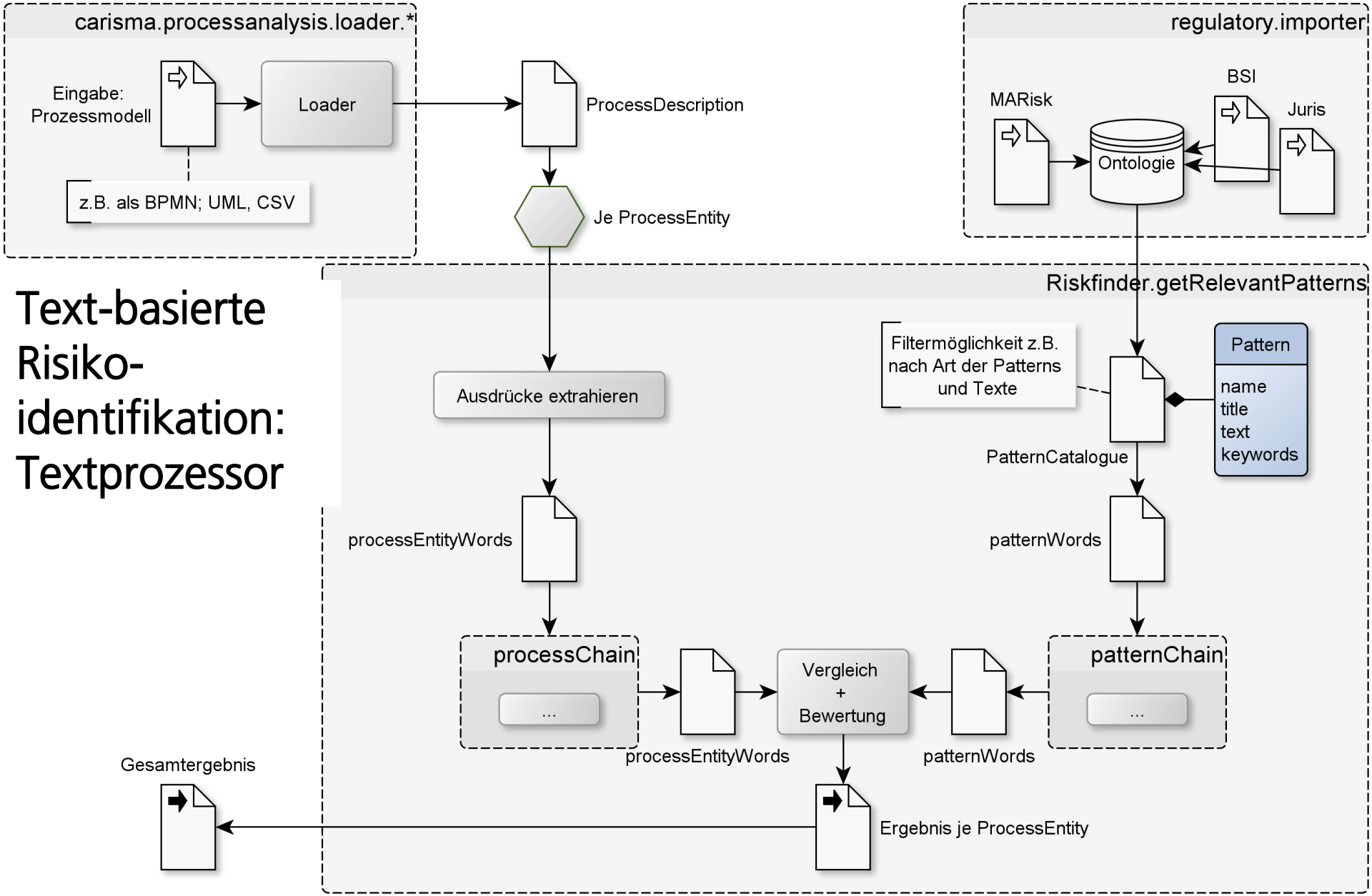
GP-Ebene: Umsetzung Textbasierte Risiko-Identifikation

Schlagwörtern wird **Schutzbedarf** zugeordnet.

Bsp. Sozialversicherungsnummer → personenbezogene Daten
→ hoher Schutzbedarf gemäß §3 Abs. 8 BDSG
→ darf nur innerhalb der EU verarbeitet werden



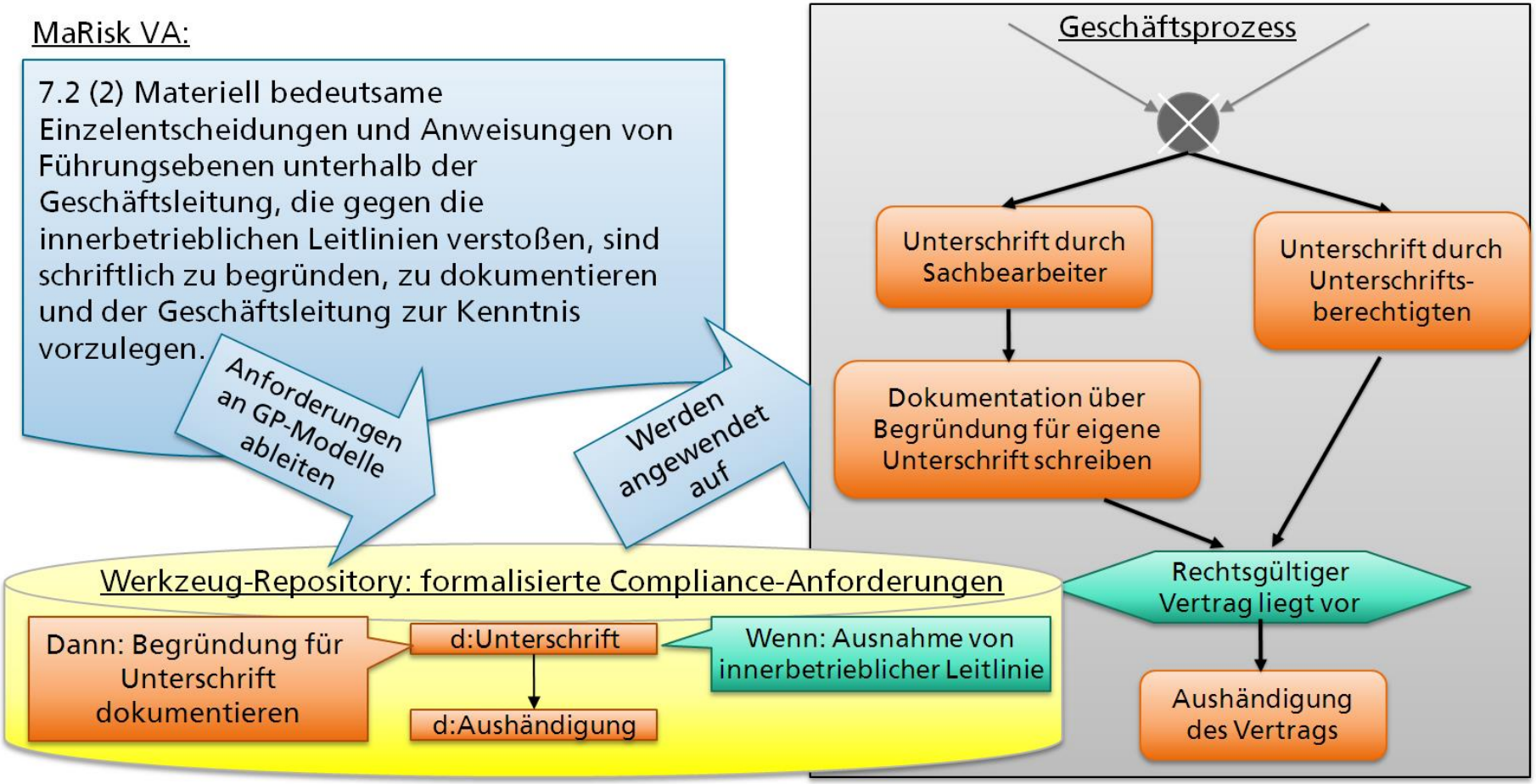
Text-basierte Risiko-identifikation: Textprozessor



J. Jürjens et al.. J. Inform. Management & Computer Security, 2013

GP-Ebene: Strukturbasierte Complianceanalyse

Jürjens et al., Int. Journal on Intelligent Systems 25(8): 813-840 (2010)



Logik-basierte Formalisierung:

```
formula four\_eyes\_principle ( a1:activity, a2:activity ) :=
forall [ p:person | ( !(execute(p, a1)) \/ !(execute(p, a2)) ) ];
```

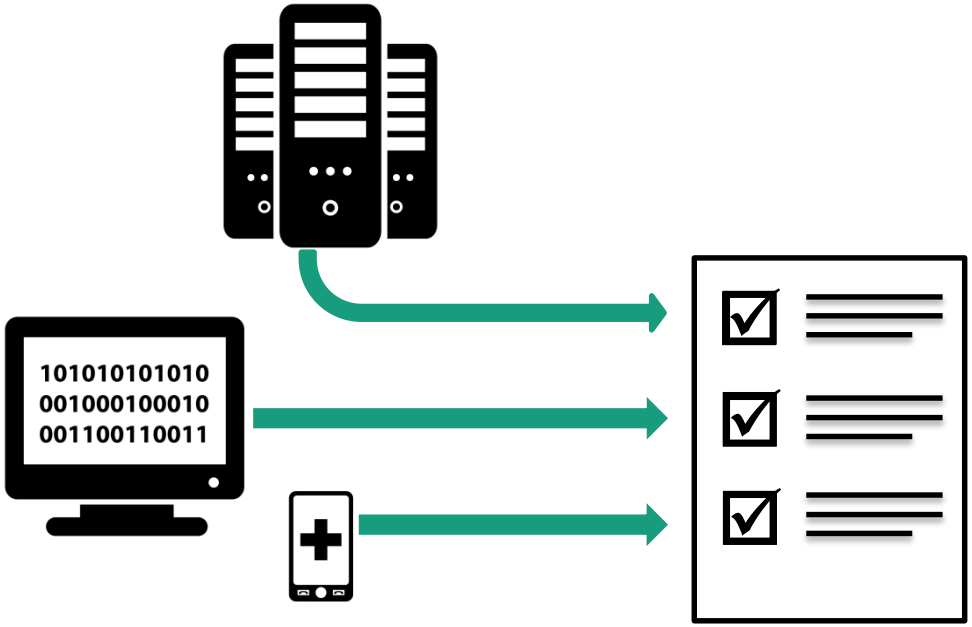
Roadmap

Herausforderungen

Lösungen

- Auswertungsschnitt-stellen & Automatische Validierung
- **Automatiserte Datenerhebung aus Drittsystemen**

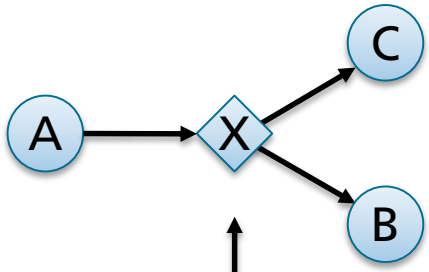
Erfahrungen



Compliance vs. Laufzeit-Daten

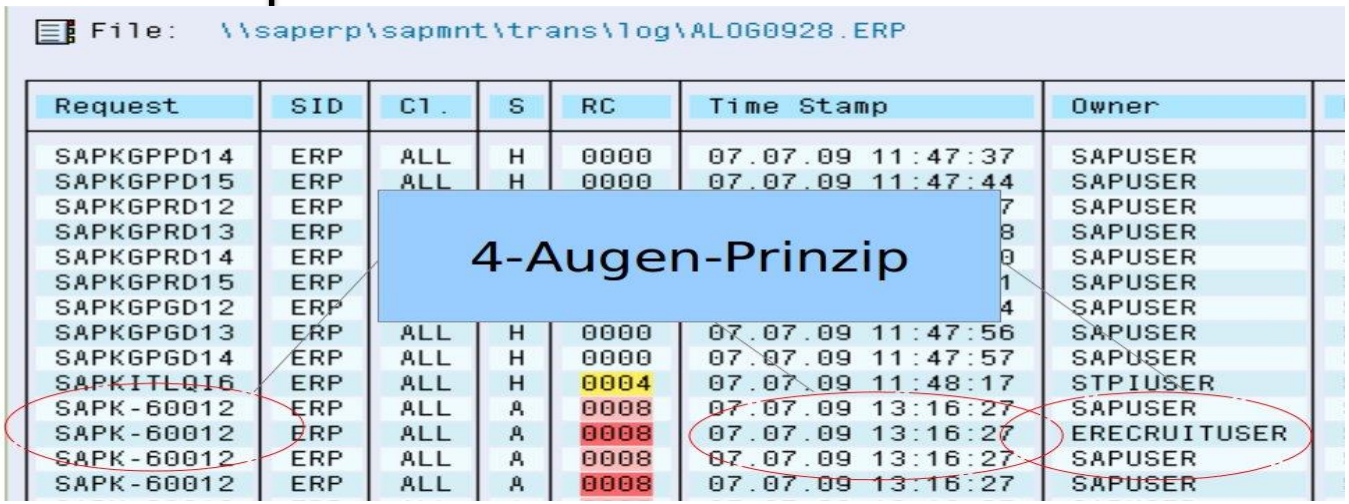
Jürjens et al., Journal on Computers & Security 29(3): 315-330 (2010)

Business Process Mining: Prozesse aus Logdaten rekonstruieren



Alternativ: **Compliance-Monitoring** auf Logdaten. Beispiel: 4-Augen-Prinzip

Ereignis-daten



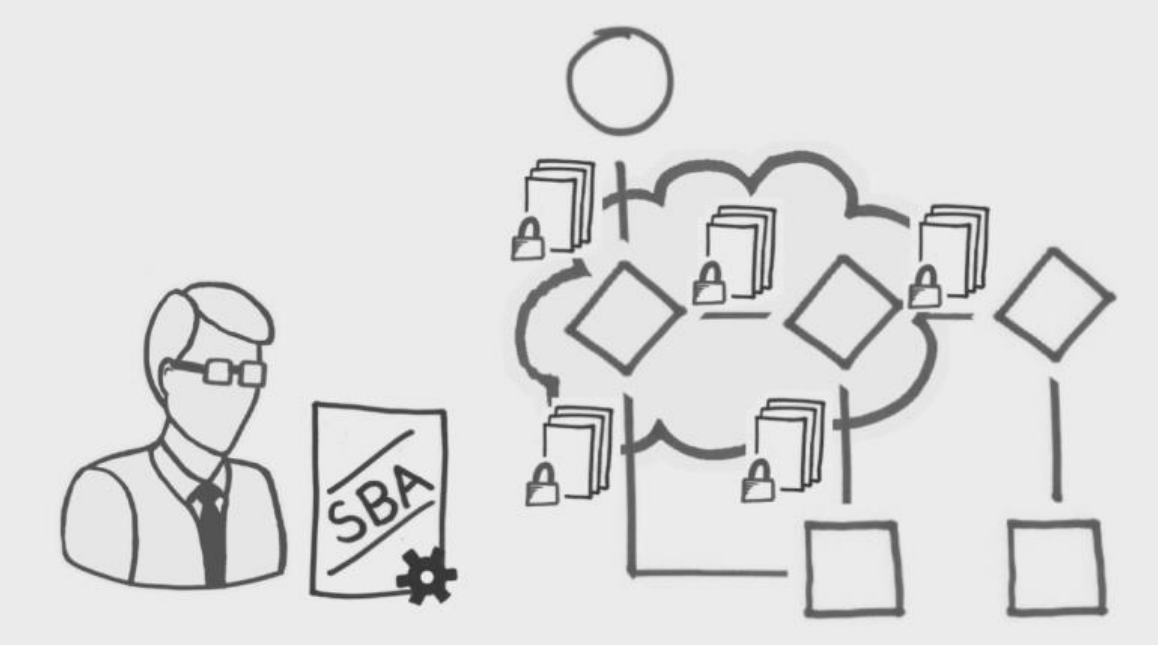
Request	SID	Cl.	S	RC	Time Stamp	Owner
SAPKGPPD14	ERP	ALL	H	0000	07.07.09 11:47:37	SAPUSER
SAPKGPPD15	ERP	ALL	H	0000	07.07.09 11:47:44	SAPUSER
SAPKGPRD12	ERP				7	SAPUSER
SAPKGPRD13	ERP				8	SAPUSER
SAPKGPRD14	ERP				0	SAPUSER
SAPKGPRD15	ERP				1	SAPUSER
SAPKGPGD12	ERP				4	SAPUSER
SAPKGPGD13	ERP	ALL	H	0000	07.07.09 11:47:56	SAPUSER
SAPKGPGD14	ERP	ALL	H	0000	07.07.09 11:47:57	SAPUSER
SAPKITLQI6	ERP	ALL	H	0004	07.07.09 11:48:17	STPIUSER
SAPK-60012	ERP	ALL	A	0008	07.07.09 13:16:27	SAPUSER
SAPK-60012	ERP	ALL	A	0008	07.07.09 13:16:27	ERECRUITUSER
SAPK-60012	ERP	ALL	A	0008	07.07.09 13:16:27	SAPUSER
SAPK-60012	ERP	ALL	A	0008	07.07.09 13:16:27	SAPUSER

Roadmap

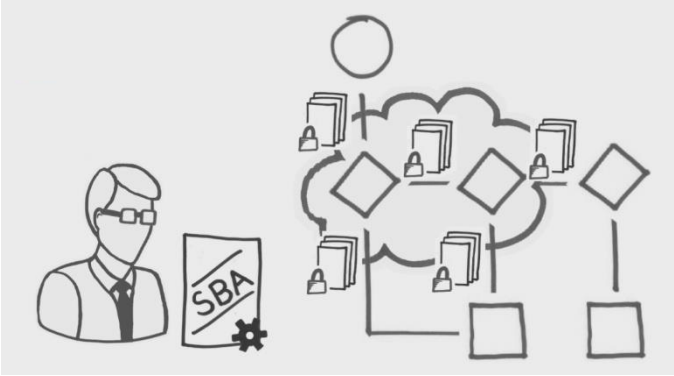
Herausforderungen

Lösungen

Erfahrungen

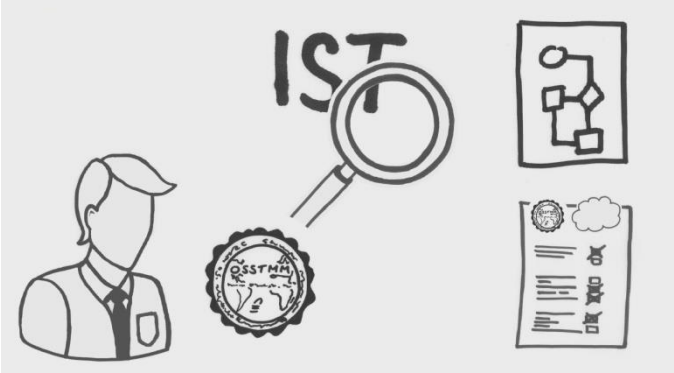


Leistungen / Angebote des Fraunhofer ISST



- **Machbarkeits-** und **Anforderungsanalysen** für technologische, organisatorische und rechtliche Vorgaben zu **Compliance**, **Risikomanagement**, **IT-Sicherheit**.
- **Ökonomische Bewertung** von **IT-Sicherheitsmaßnahmen** hinsichtlich ihres Einsatzes in konkreten IT-Systemen.
- **Beratung** zu **Compliance-** und **Sicherheitsaspekten** während **Entwicklung**, **Pflege** und **Einsatz** von IT-Systemen. Durchführung von **Risikoanalysen** und Unterstützung beim **Risikomanagement**.
- Entwicklung von **Analyse-** und **Monitoringwerkzeugen** zur Überwachung von Geschäftsprozessen und IT-Systemen auf **Compliance-** und **Sicherheitsanforderungen** (z.B. Datenschutz und Datensicherheit).

Einige Referenz-Projekte



- Elektronische Gesundheitskarte
- Sicherheitsrichtlinien für mobile Endgeräte
- Digitale Dokumentenverwaltung
- Digitale Geldbörse CEPS
- Sicherheitsanalyse Dokumentenmanagement
- Return-on-Security Investment-Analyse
- Sicherheitsanalyse für digitales Unterschriften-System
- Einführung IT-Sicherheitsrisikobewertung
- Update-Plattform für Smartcard-Software

Cloud-spezifisch:

- Zertifizierungen für Cloud-Sicherheit
- Sicherheitsuntersuchungen zur Cloud-Nutzung

Zusammenfassung

Sicherheit und **Compliance** in **Cloud**-basierten Umgebungen: komplexe und vielfältige Probleme.

Lösungen (und Tools) zur Bewältigung der Herausforderungen:

- **Analyse** der **Geschäftsprozesse** zur Auslagerung in Cloud (bzgl. **Sicherheit / Compliance**)
- Analyse / Überwachung der vom **Cloud-Anbieter** zugesicherten **Sicherheit / Compliance**

Kontakt: http://jan.jurjens.de