

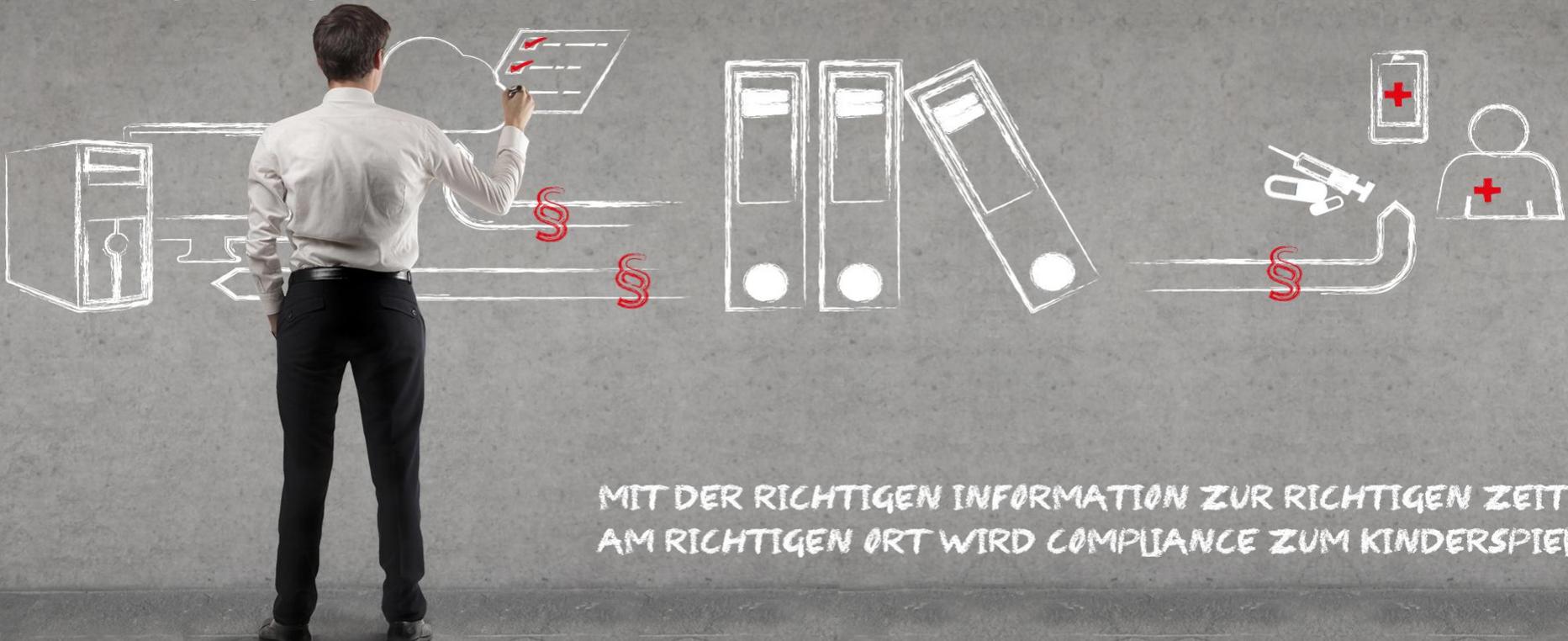
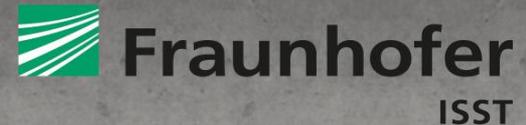
# Modellbasiertes Sicherheits-Testen für Cloud-basierte Prozesse

Prof. Dr. Jan Jürjens

Fraunhofer Institut für Software- und Systemtechnik ISST, Dortmund

<http://www.isst.fraunhofer.de>

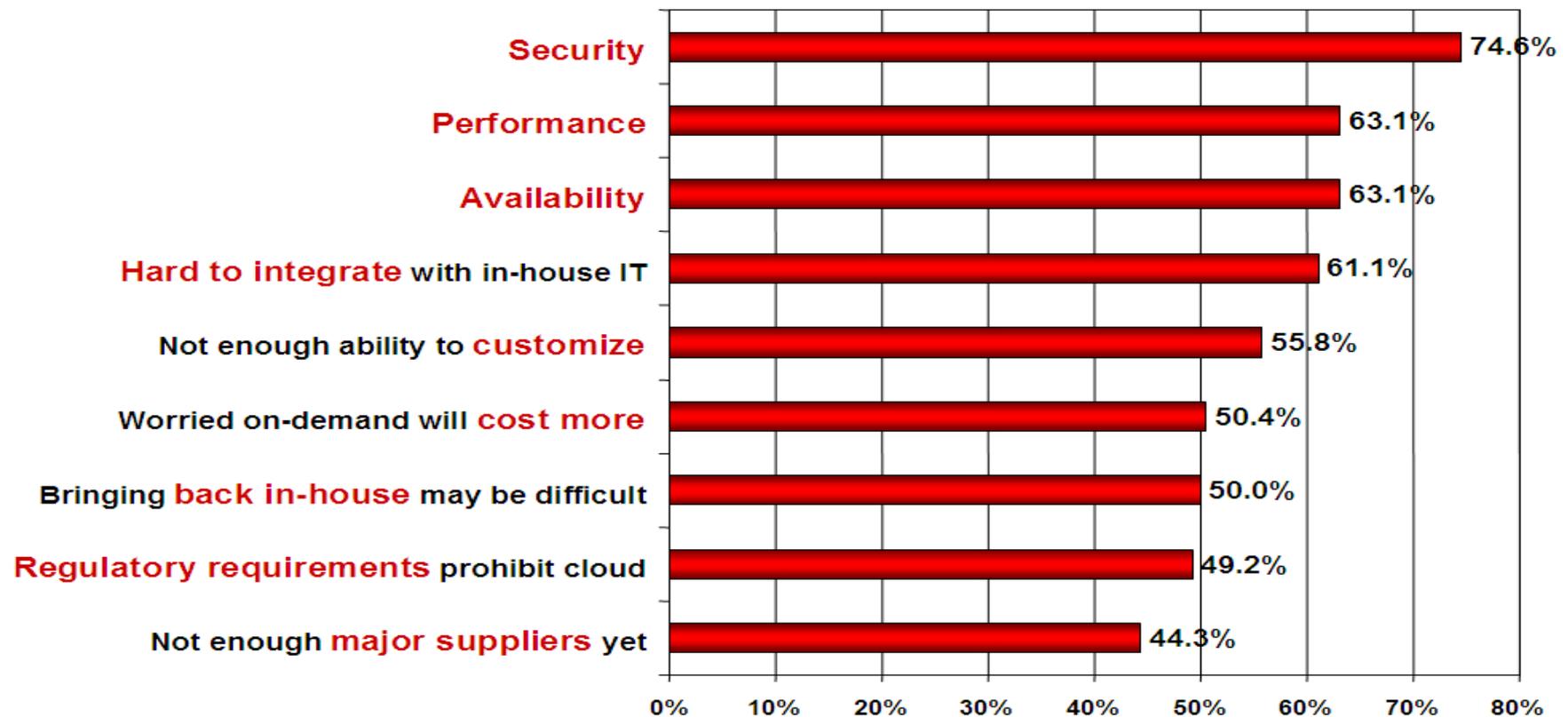
<http://jan.jurjens.de>



MIT DER RICHTIGEN INFORMATION ZUR RICHTIGEN ZEIT  
AM RICHTIGEN ORT WIRD COMPLIANCE ZUM KINDERSPIEL

# Herausforderung: Sicherheit und Compliance in der Cloud

## Umfrage: Größte Herausforderungen beim Einsatz von Clouds ?



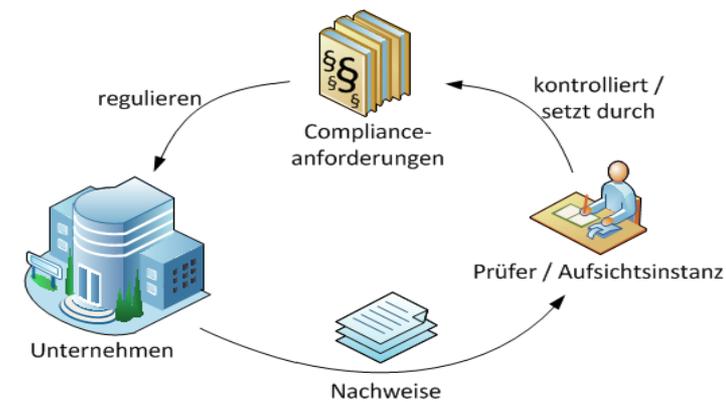
# Spezifische Sicherheitsprobleme bei Cloud Computing



- 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

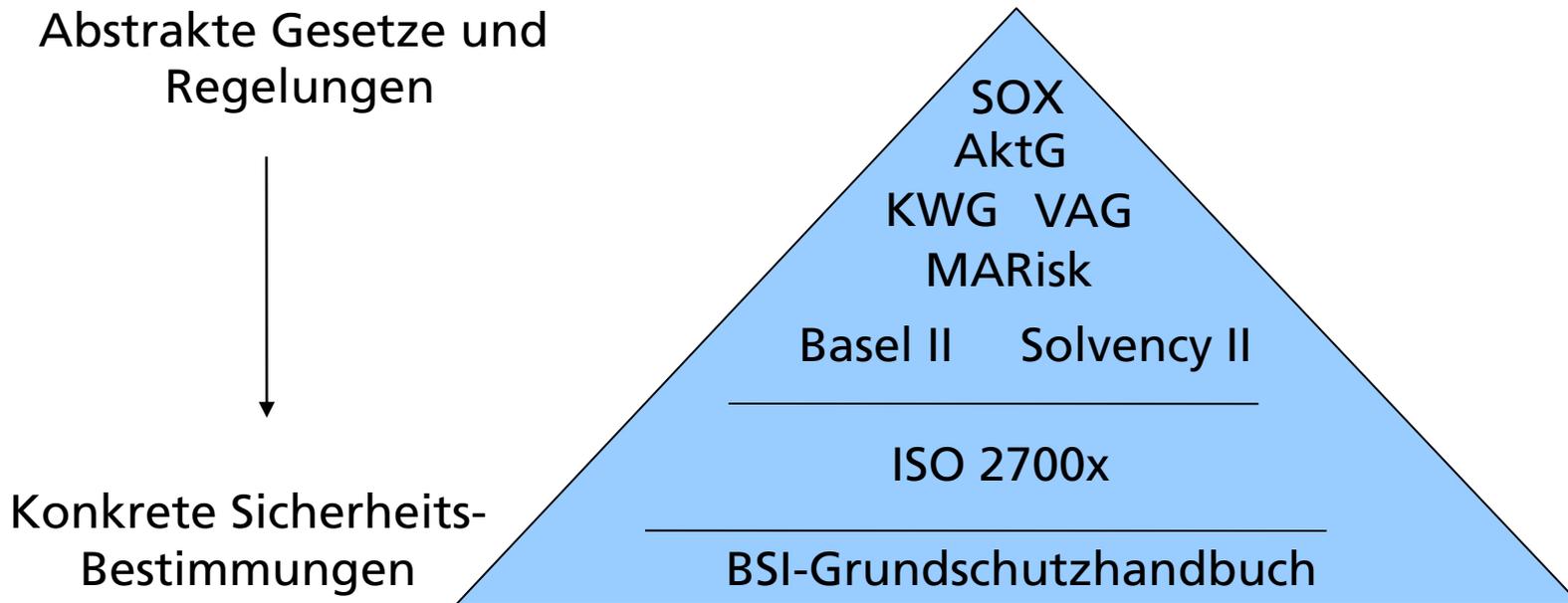
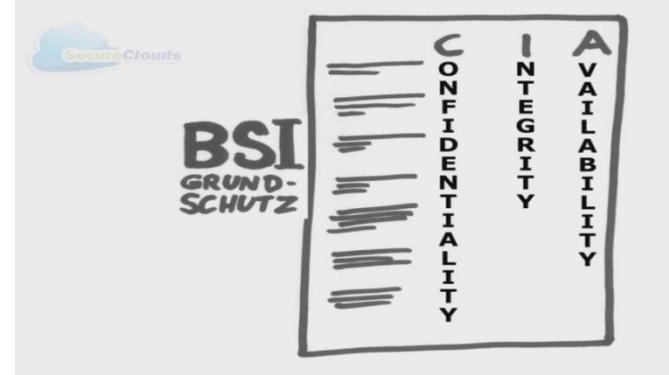
z.B. Finanzen: Solvency II, Basel III; Gesundheit: Medizinproduktegesetz (MPG); Pharma: Arzneimittelmarktneuordnungsgesetz (AMNOG)

## 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





# 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.

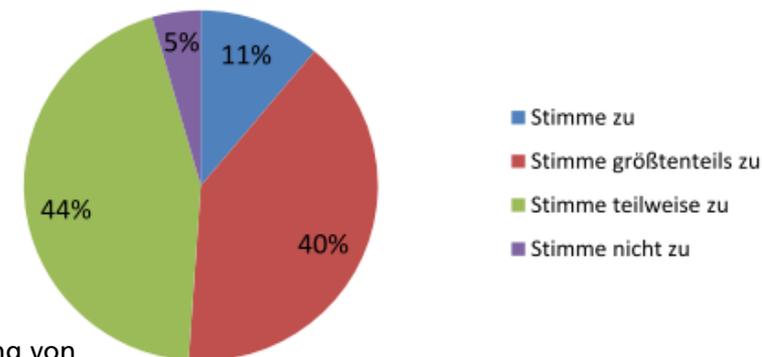
- Erforderliche Daten schwer manuell erfassbar.
- **Prüfung** einzelner Eigenschaften bereits **komplex** und umfangreich.
- Großer Bedarf an **Compliance-Werkzeugen** (1,3 Mrd.\$ [Forrester 2011])

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

**Schwachpunkte:**

- **Automatisierte Erfassung / Analyse** von Complianceanforderungen.
- **Überwachung** der Compliancevorgaben.
- **Derzeitige Risiko-Bewertungsmethoden** generell **nicht ausreichend**.<sup>1</sup>

Derzeitige Sicherheitsbewertungsverfahren sind ausreichend



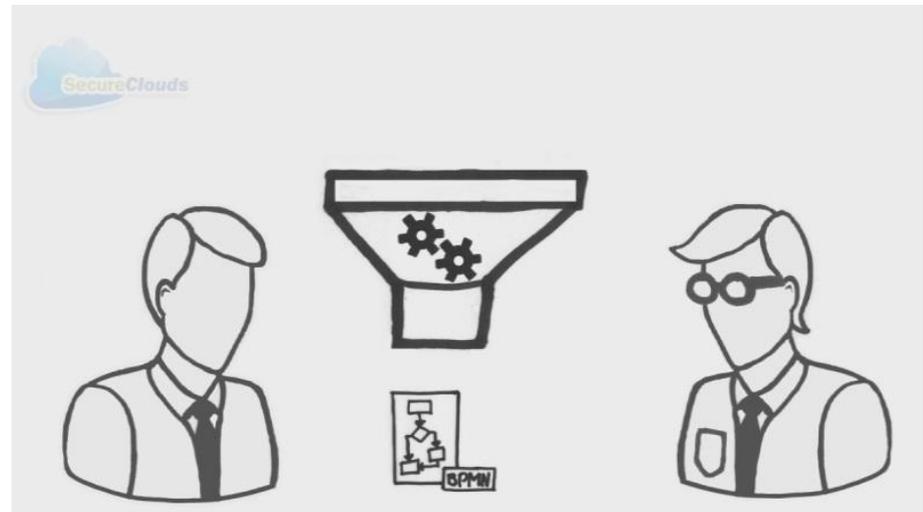
<sup>1</sup> S. Taubenberger, J. Jürjens: Durchführung von IT-Risikobewertungen und die Nutzung von Sicherheitsanforderungen in der Praxis. Studie, Fraunhofer ISST 2011 und DACH security 2011

# Roadmap

## Herausforderungen

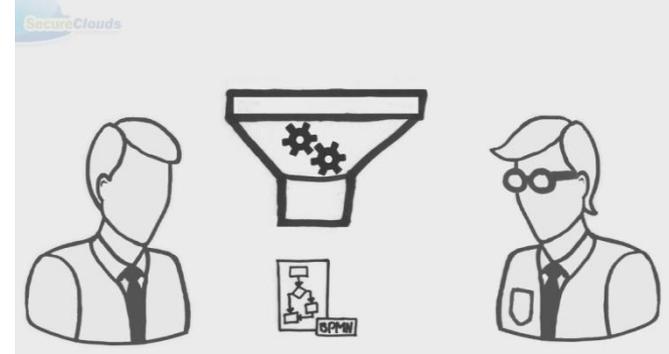
## Lösungen

- Auswertungsschnittstellen & Automatische Validierung
- Automatisierte Datenerhebung aus Drittsystemen



## Erfahrungen

# Lösung: Werkzeuggestützte Compliance-Analysen



## Ziele:

- Bewältigung der **Komplexität** und **Kostensparnis** 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 SecureClouds



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

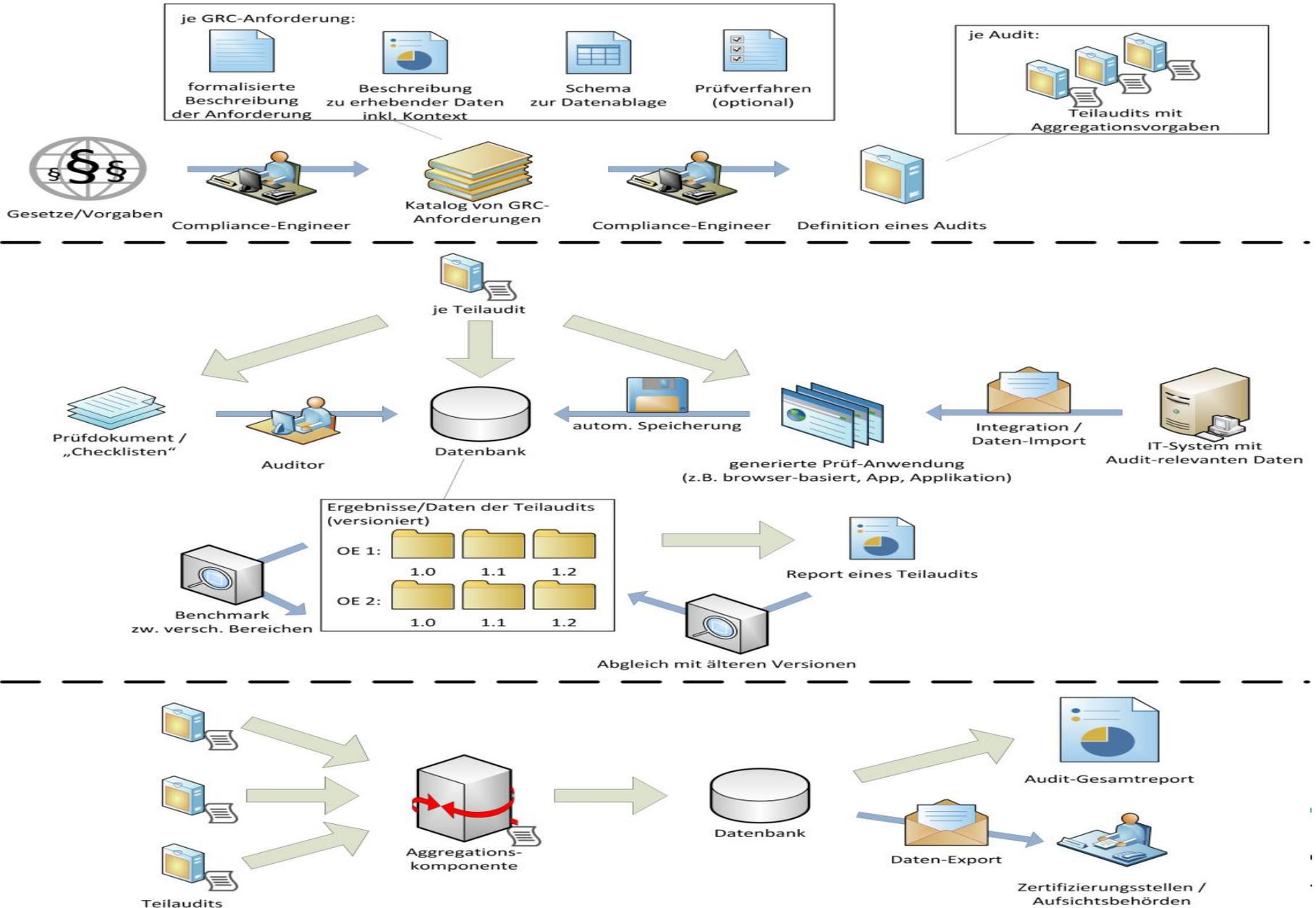
Unter Verwendung u.a.:

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



<http://secureclouds.de>

# Integrierte Compliance Management Plattform: Workflow



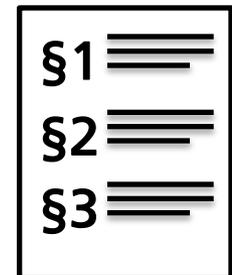
# Sicherheitsbedarfsanalyse: Unterstützte Regelwerke

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**

ISO 9001  
KHBV  
ÄApprO  
GOÄ  
IfSG  
HKG  
BÄO  
MPBetreibV  
HWG  
BDSG  
ISO 80001

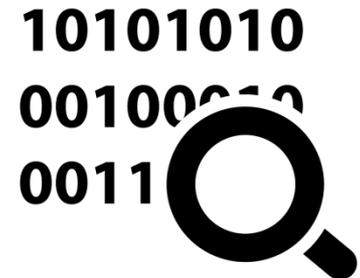
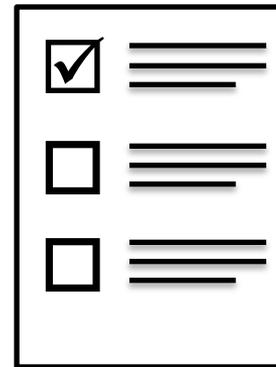


# Roadmap

Herausforderungen

Lösungen

- **Auswertungsschnittstellen & Automatische Validierung**
  - **Architekturebene**
  - **Geschäftsprozesse**
- **Automatisierte Datenerhebung aus Drittsystemen**



Erfahrungen

# Analysewerkzeug CARiSMA

## Sicherheitsanalysen auf GP-/Softwaremodellen

## Eclipse Plugin-Architektur

- Integriert etablierte Modellierungswerkzeuge, 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

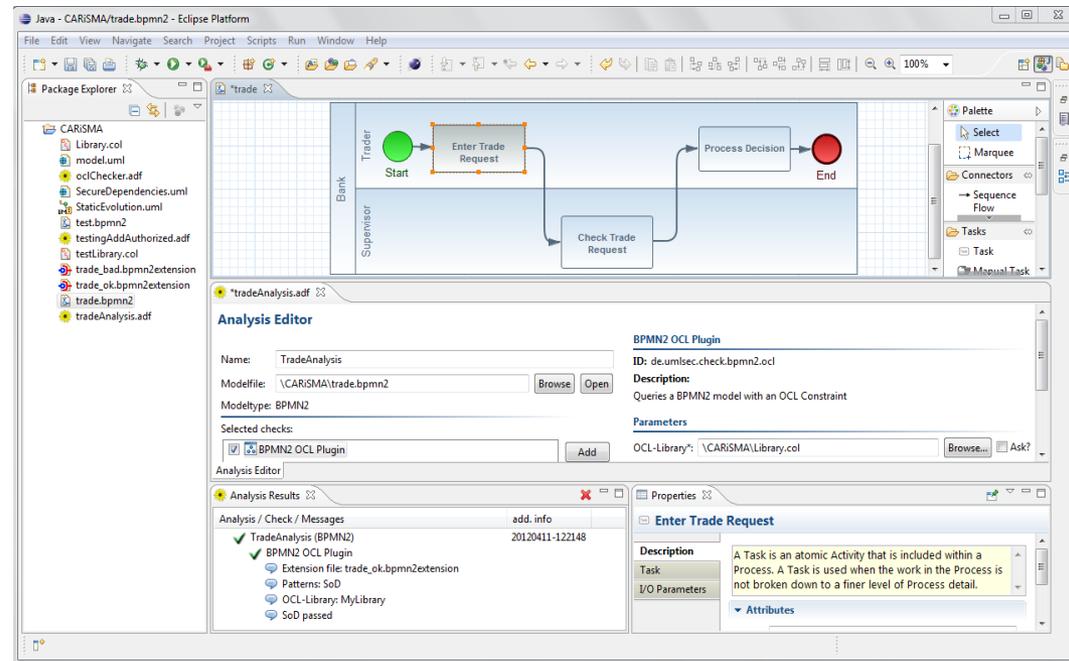
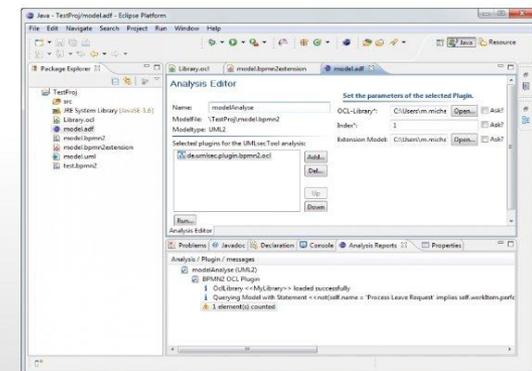
of software models.<sup>1)</sup>

Since CARiSMA is a reimplemented variant of the former **UMLsec** tool it natively supports UML models.

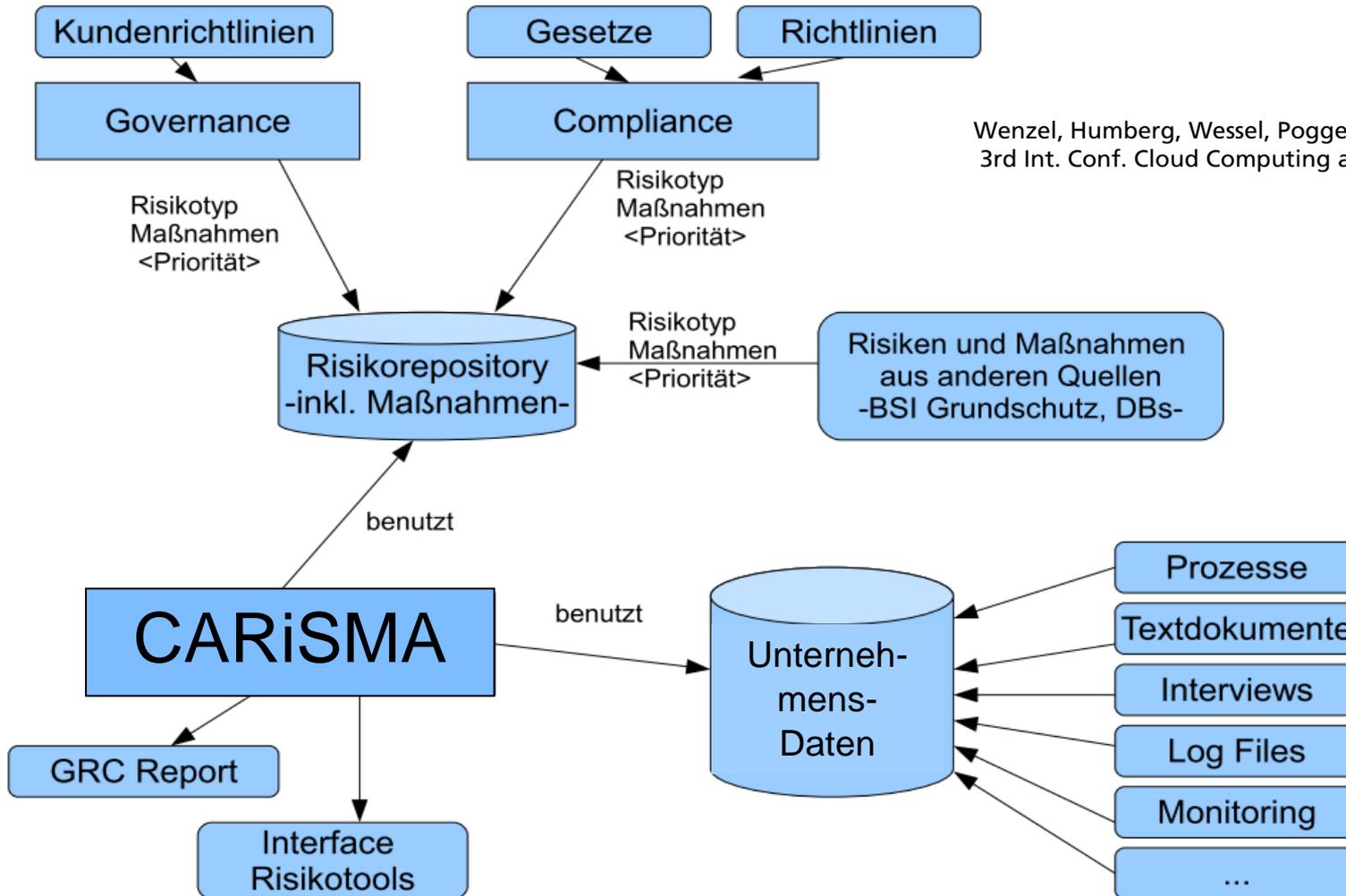
Due to its EMF-based implementation CARiSMA can also support **domain-specific modeling languages** such as BPMN.

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

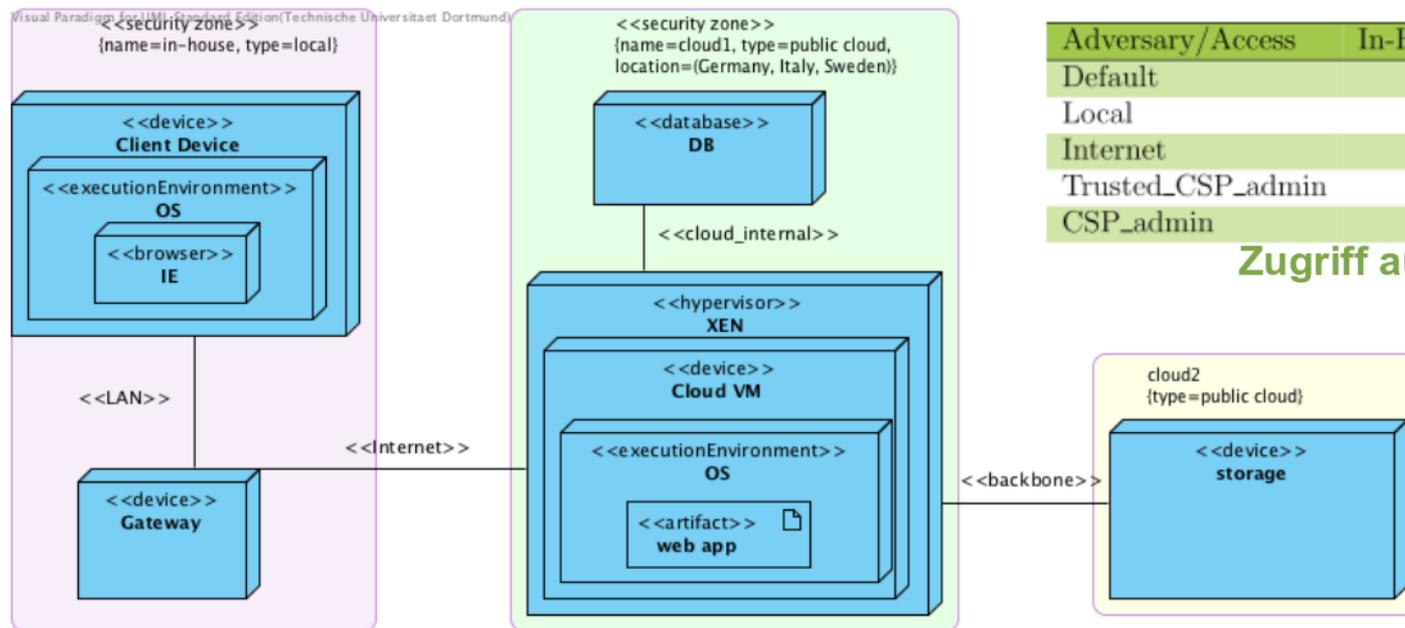


Wenzel, Humberg, Wessel, Poggenpohl, Ruhroth, Jürjens.  
3rd Int. Conf. Cloud Computing and Services Science, 2013

# 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.

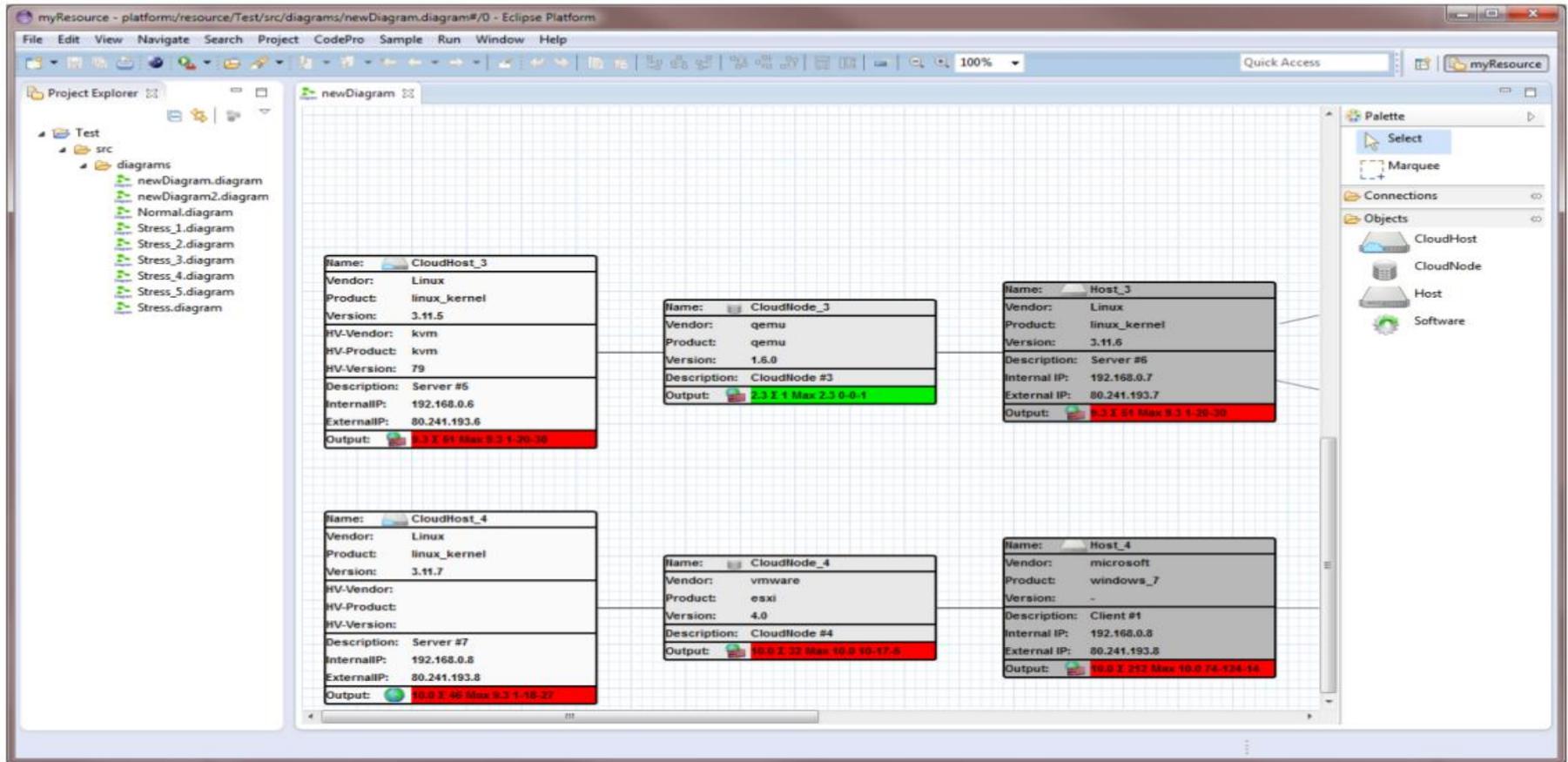


Adversary/Access	In-House	Cloud1	Cloud2
Default	-	-	-
Local	+	-	-
Internet	-	-	-
Trusted_CSP_admin	-	+	-
CSP_admin	-	-	+

Zugriff auf Knoten.

[N. Astahov 2014]

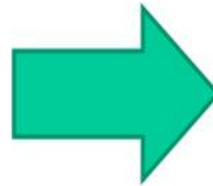
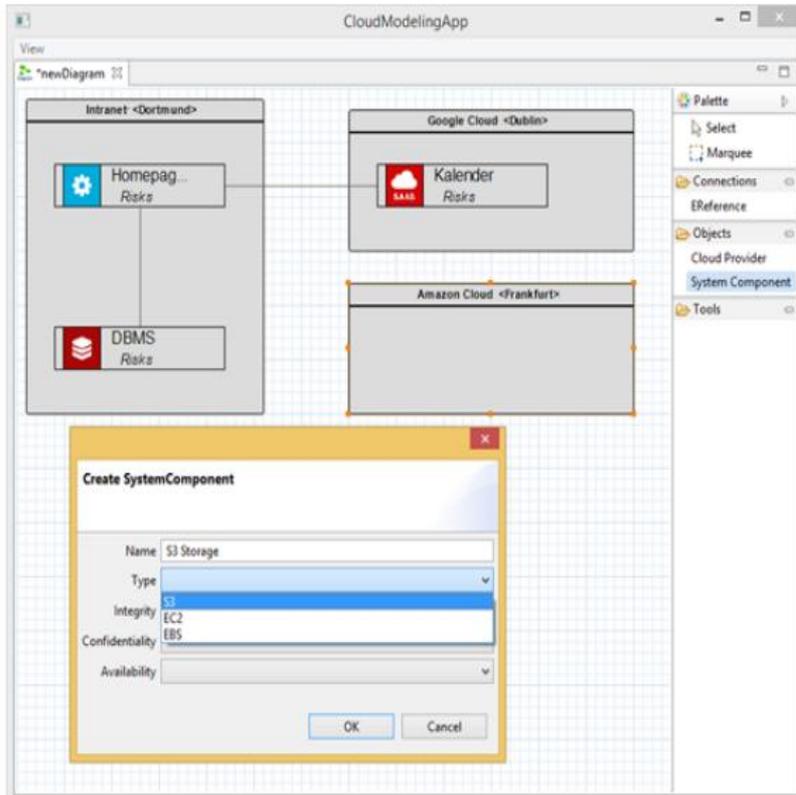
# Architekturebene: Exploit-Checking für Cloud-Umgebungen



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

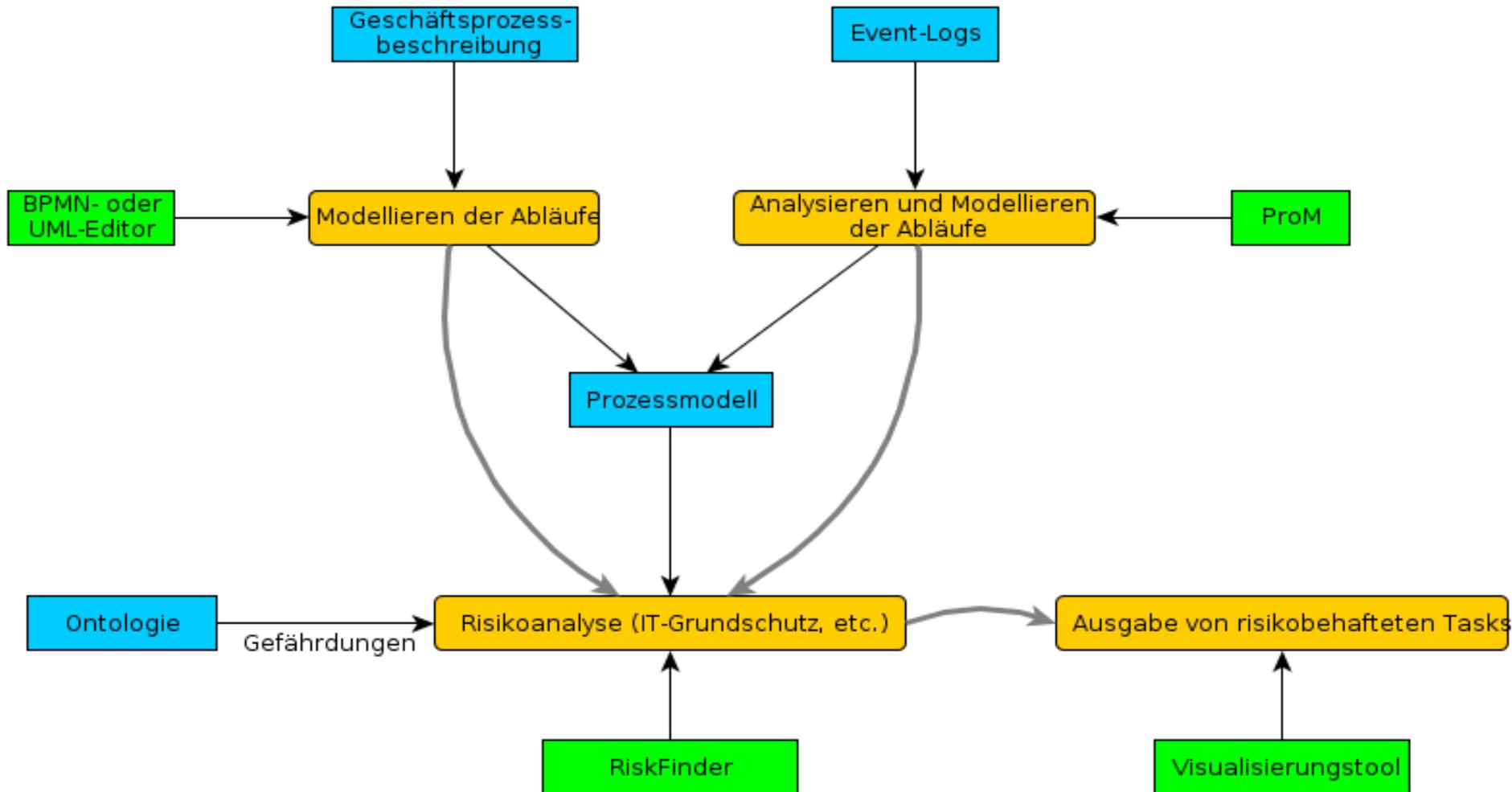


The screenshot shows the CloudModelingApp interface with a risk analysis table. The table has three columns: Risk Name, Risk Probability, and Risk Severity. The table contains two rows of data. Below the table, there is a dropdown menu showing 'S3 Risiko 2' and a 'New Risk' button. The dialog has 'OK' and 'Cancel' buttons.

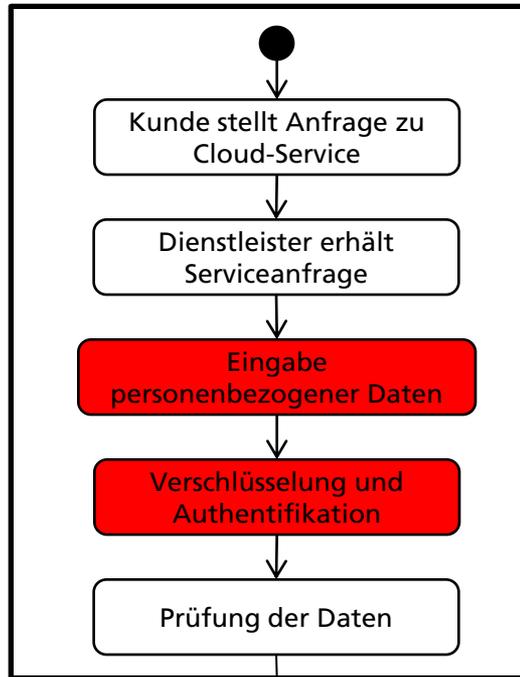
Risk Name	Risk Probability	Risk Severity
S3 Risiko 1	Medium	None
S3 Risiko 2	Medium	None

[F. Coerschulte 2014]

# Analyse der Geschäftsprozesse



# GP-Ebene: Textbasierte Risiko-Identifikation



**[Kunde stellt Anfrage zu Cloud-Service (233)]**  
 4 Relevante Worte: [Information(200.0), Meldung(200.0), Nachricht(100.0), Internet(100.0)]  
 22 relevante Pattern:  
 B\_5.10 : Internet Information Server (300.0)  
 G\_2.96 : Veraltete oder falsche Information (200.0)  
 G\_3.13 : Weitergabe falscher oder unrichtiger Informationen (200.0)  
 G\_3.44 : Sorglosigkeit im Umgang mit Informationen (200.0)  
 ...

Aktivität

Gefundene Pattern

Identifizierte Ausdrücke



**IT-Grundschutz-Kataloge**

Startseite IT-Grundschutz  
**Inhalt**

- Allgemeines
- Bausteine**
  - Übergreifende Aspekte
  - Infrastruktur
  - IT-Systeme
  - Netze
  - Anwendungen
- Gefährdungskataloge
- Maßnahmenkataloge
- Rollendefinitionen
- Glossar
- Index A-Z
- Baustein Datenschutz
- Hilfsmittel
- Überblickspapiere
- Bezugsquellen
- FAQ
- Registrierung / Newsletter
- Download
- Kontakt

Das BSI Themen Aktuelles Presse Publikationen

Startseite Themen IT-Grundschutz-Kataloge Inhalt Bausteine

## B 5.4 Webserver

### Beschreibung

Das Internet ist eines der zentralen Medien der heutigen Informationsgesellschaft. Daten werden von Servern bereitgestellt, die Daten, meist Dokumente in Form von Webseiten, ausliefern. Dies erfolgt typischerweise über die Protokolle HTTP (Hypertext Transfer Protocol), d. h. HTTP geschützt durch eine verschlüsselte Verbindung (HTTPS). Neben dem Internet wird die zunehmende Nutzung von Webservern für interne Informationen und Anwendungen in Firmen zunehmend wichtiger. In diesem Zusammenhang sind einfache und standardisierte Schnittstellen zwischen Servern und Client-Software (Webbrowser) für praktisch jede Betriebssystemumgebung erforderlich.

Die Bezeichnung *Webserver* (oder auch *WWW-Server*) wird meist sowohl für die Hardware als auch für den Betrieb des Servers verwendet. Die Bezeichnung *WWW-Server* ist jedoch nicht korrekt, da die Bezeichnung *WWW* nur ein Teil der Aufgaben des Servers ist. Die Bezeichnung *Webserver* ist daher präzisierender und sollte bevorzugt verwendet werden.

Da ein Webserver ein öffentlich zugängliches System darstellt, sind die sichere Installation und Konfiguration des Systems und seiner Konfiguration von großer Bedeutung. Die Sicherheit umfasst bei Webservern auch deswegen eine relativ große Anzahl von Maßnahmen, neben der reinen Webserver-Anwendung noch weitere Serveranwendungen, die auf dem Server erforderlich sind und deren sicherer Betrieb ebenfalls gewährleistet sein muss. Die Daten werden über ein Netzwerk (etwa per FTP oder SCP) auf den Server übertragen oder es wird

### Gefährdungslage

Für den IT-Grundschutz werden pauschal die folgenden Gefährdungen der Nutzung des Internets angenommen:

### Organisatorische Mängel

G 2.1	Fehlende oder unzureichende Regelungen
G 2.4	Unzureichende Kontrolle der Sicherheitsmaßnahmen
G 2.7	Unerlaubte Ausübung von Rechten
G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-F

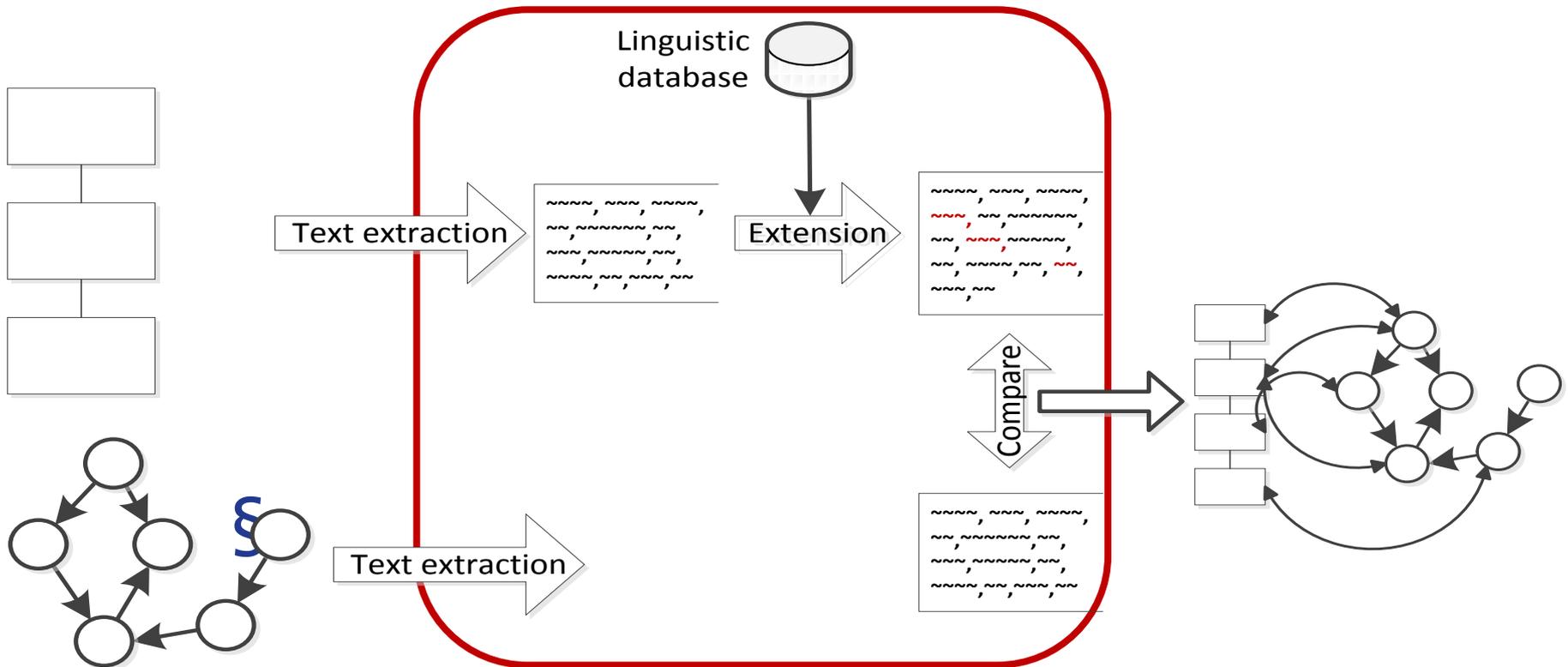
# GP-Ebene: Umsetzung Textbasierte Risiko-Identifikation

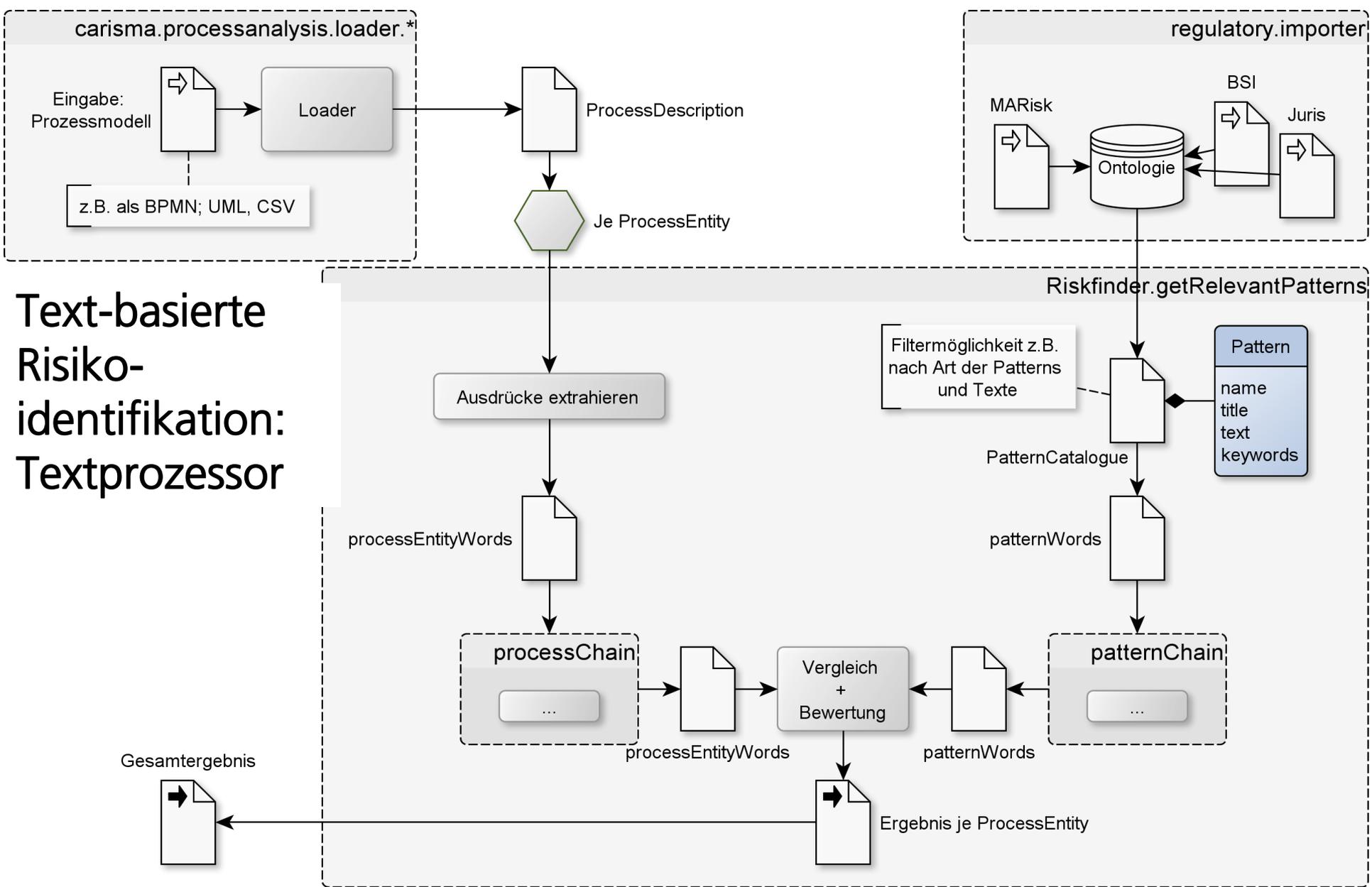
Schlagwörtern wird Schutzbedarf zugeordnet.

Bsp. Sozialversicherungsnummer → personenbezogene Daten

→ hoher Schutzbedarf gemäß §3 Abs. 8 BDSG

→ darf nur innerhalb der EU verarbeitet werden





# Text-basierte Risiko-identifikation: Textprozessor

# GP-Ebene: Strukturbasierte Complianceanalyse

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

## MaRisk VA:

7.2 (2) Materiell bedeutsame Einzelentscheidungen und Anweisungen von Führungsebenen unterhalb der Geschäftsleitung, die gegen die innerbetrieblichen Leitlinien verstoßen, sind schriftlich zu begründen, zu dokumentieren und der Geschäftsleitung zur Kenntnis vorzulegen.

Anforderungen an GP-Modelle ableiten

Werden angewendet auf

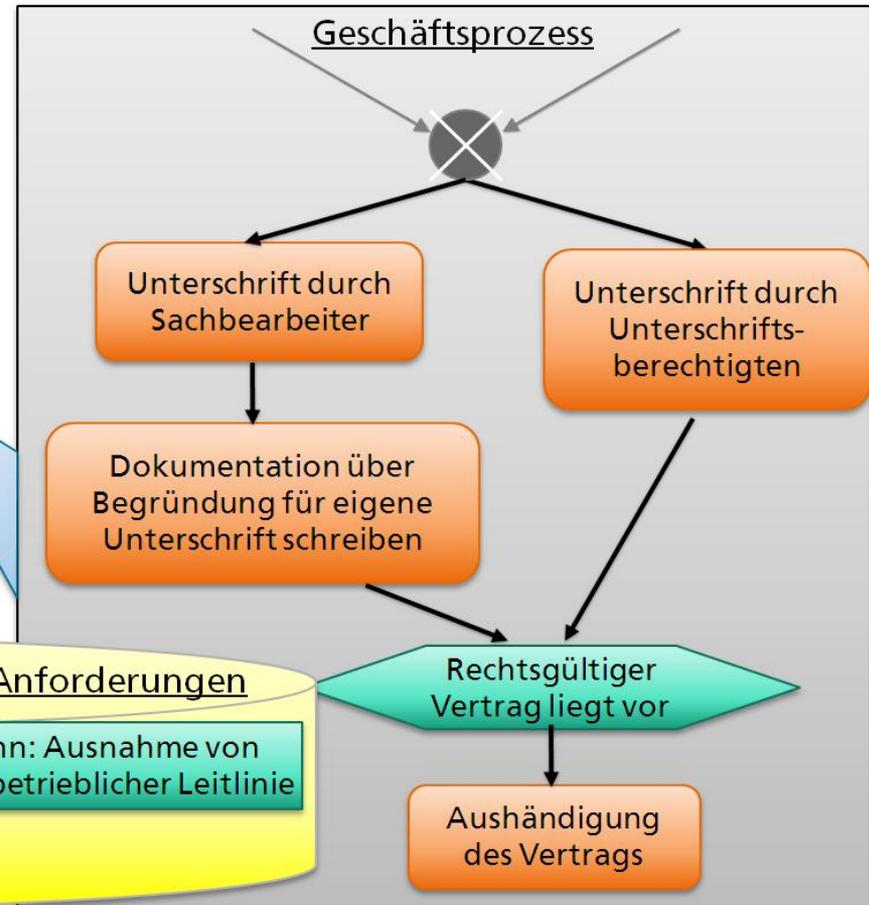
## Werkzeug-Repository: formalisierte Compliance-Anforderungen

Dann: Begründung für Unterschrift dokumentieren

d:Unterschrift

Wenn: Ausnahme von innerbetrieblicher Leitlinie

d:Aushändigung



## Logik-basierte Formalisierung:

```

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

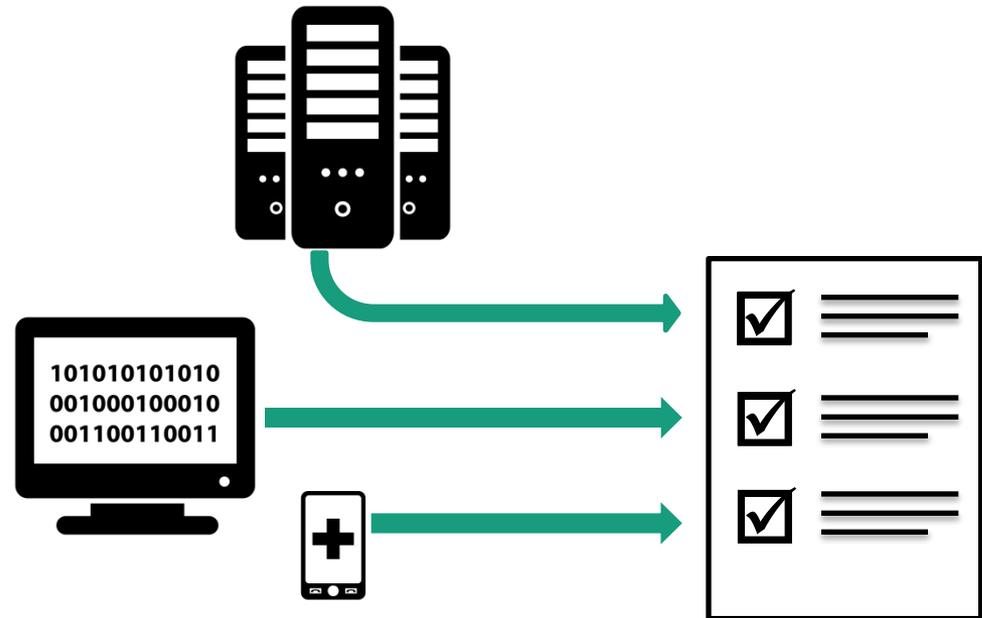
# Roadmap

Herausforderungen

Lösungen

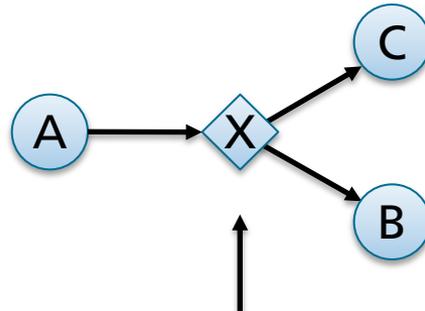
- Auswertungsschnittstellen & Automatische Validierung
- **Automatisierte Datenerhebung aus Drittsystemen**

Erfahrungen



# Compliance vs. Laufzeit-Daten

Business Process Mining: Prozesse aus Logdaten rekonstruieren



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

Ereignisdaten

File: \\saperp\sapmnt\trans\Log\AL060928.ERP

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					SAPUSER
SAPKGPRD13	ERP					SAPUSER
SAPKGPRD14	ERP					SAPUSER
SAPKGPRD15	ERP					SAPUSER
SAPKGPGD12	ERP					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
SAPKITLQ16	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

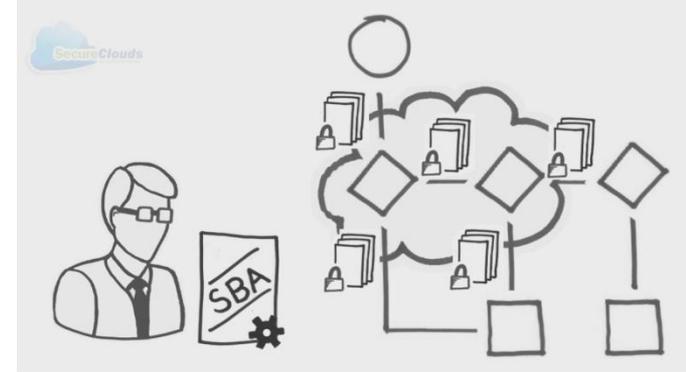
Herausforderungen

Lösungen

Erfahrungen



# Leistungen / Angebote des Fraunhofer ISST



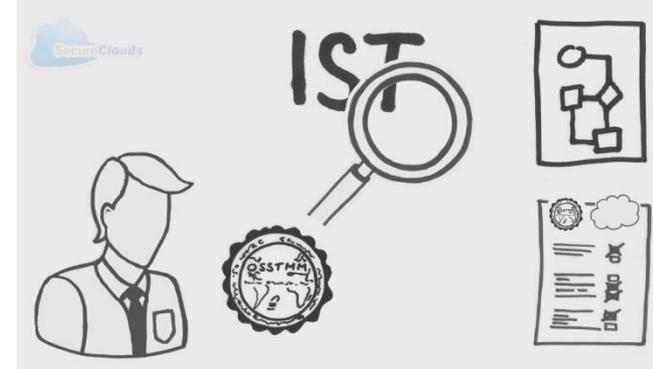
- **Machbarkeits- und Anforderungsanalysen** für technologische, organisatorische und rechtliche Vorgaben zu **Compliance, Risikomanagement, IT-Sicherheit**.
- **Ökonomische Bewertung** von IT-Sicherheitsmaßnahmen hinsichtlich ihres Einsatzes in konkreten IT-Systemen.
- **Beratung zu Compliance- und 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://www.isst.fraunhofer.de>  
<http://jan.jurjens.de>

