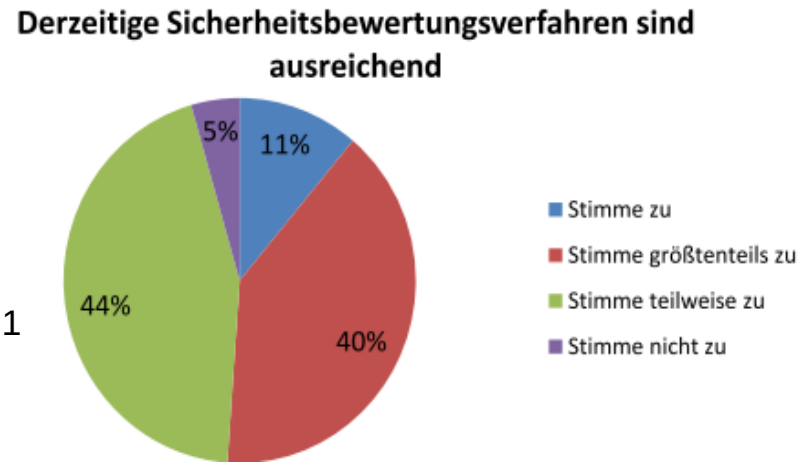
Geschäftsprozess-basiertes Compliance-Management

Jan Jürjens

TU Dortmund und Fraunhofer ISST

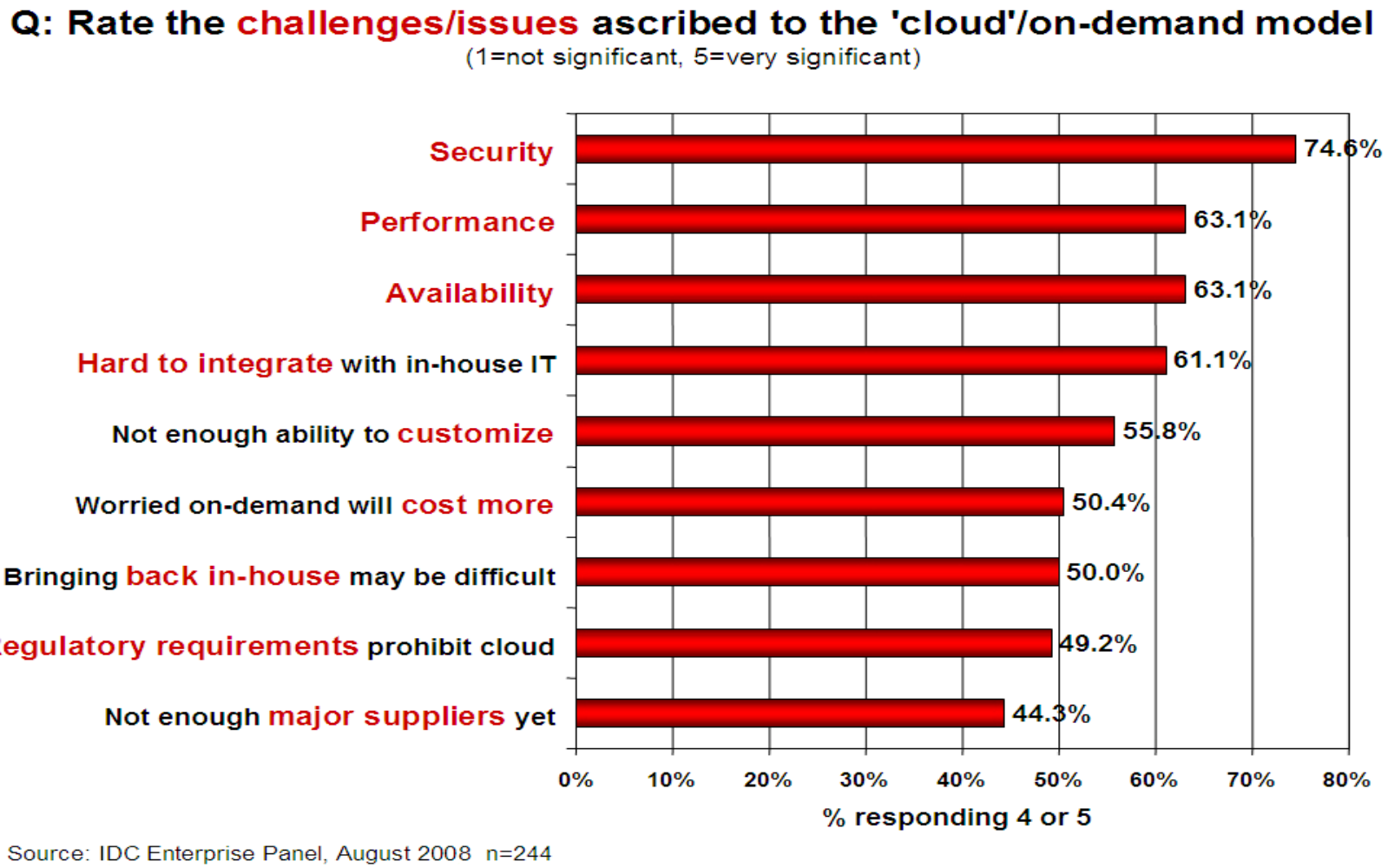
Herausforderung: Compliance

- Steigende Anforderungen für Unternehmen, die Konformität mit übergeordneten Regulierungswerken zu demonstrieren:
  - Ab 2013 müssen Versicherungen in der EU Solvency-II erfüllen => Mindestanforderungen an Risikomanagement, insbes. operationale Risken und IT-Sicherheitsrisken (MaRisk VA)
  - Ähnlich im Banken-Bereich: Basel III (bis 2018), MaRisk BA
  - Branchenunabhängig: Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KontraG); US: Sarbanes-Oxley
- Aufwendige und kostenintensive manuelle Arbeit.
- Derzeitige Risiko-Bewertungs-methoden sind dafür 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

Anwendungsgebiet: Clouds



Source: IDC Enterprise Panel, August 2008 n=244

Geschäftsprozess-basiertes Compliance-Management

Ziele:

- Bessere Überprüfbarkeit und Nachvollziehbarkeit von Compliance-relevanten Aktivitäten.
- Kostenersparnis für betroffene Unternehmen durch Werkzeugunterstützung und Konvergenz / Integration von vorhandenen Aktivitäten.

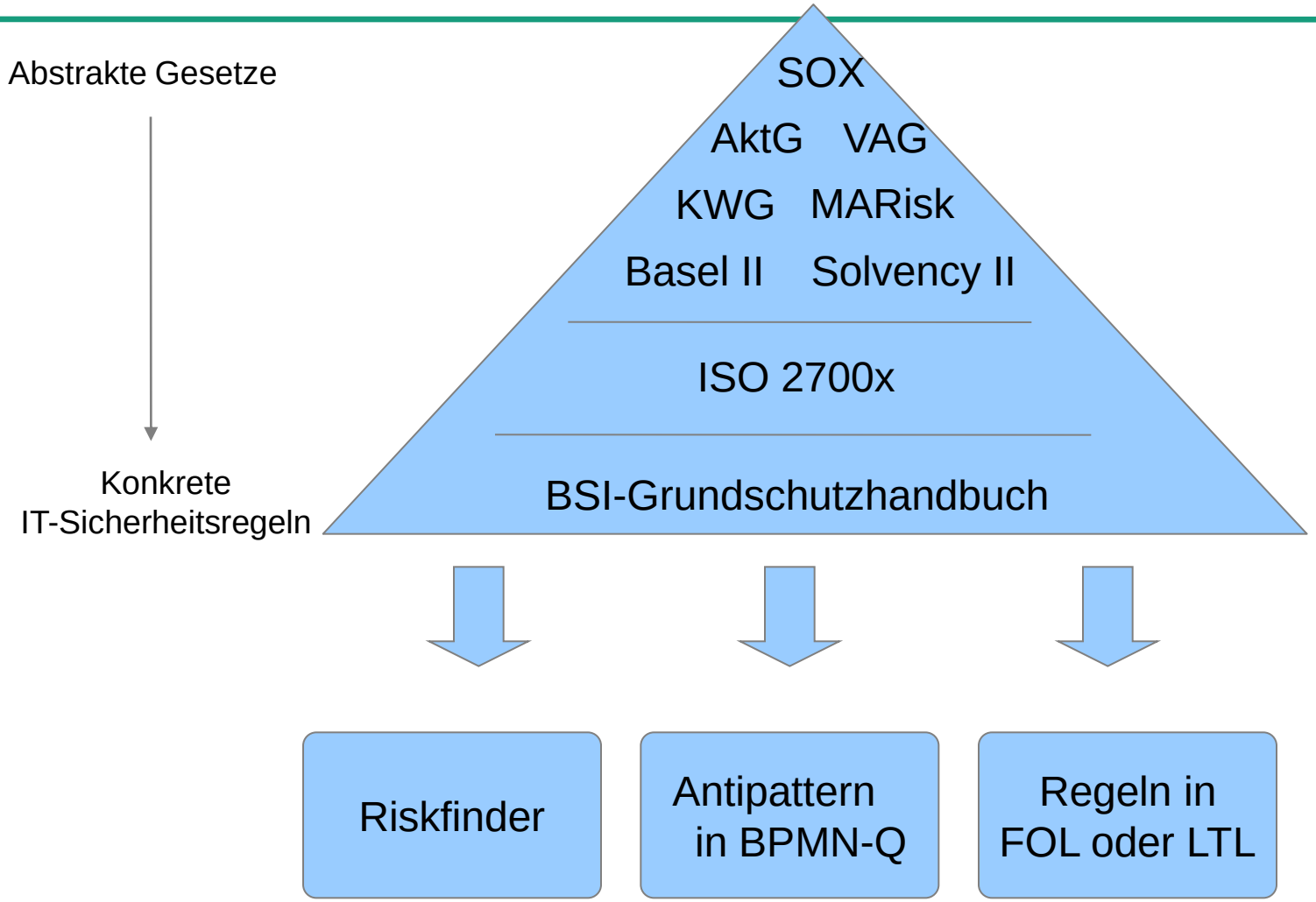
Idee:

- Entwicklung von automatischen Werkzeugen, die das Management von Compliance-Anforderungen auf Basis von vorhandenen Artefakten unterstützen.
- Insbesondere automatisierte IT-Sicherheits- und Risiko-Analysen auf der Basis von Textdokumenten, Schnittstellen-Spezifikationen, Geschäftsprozess-Modellen, Log-Daten und anderen Datenquellen.
- Insbesondere auch Anwendung auf den Einsatz von Cloud-Computing.

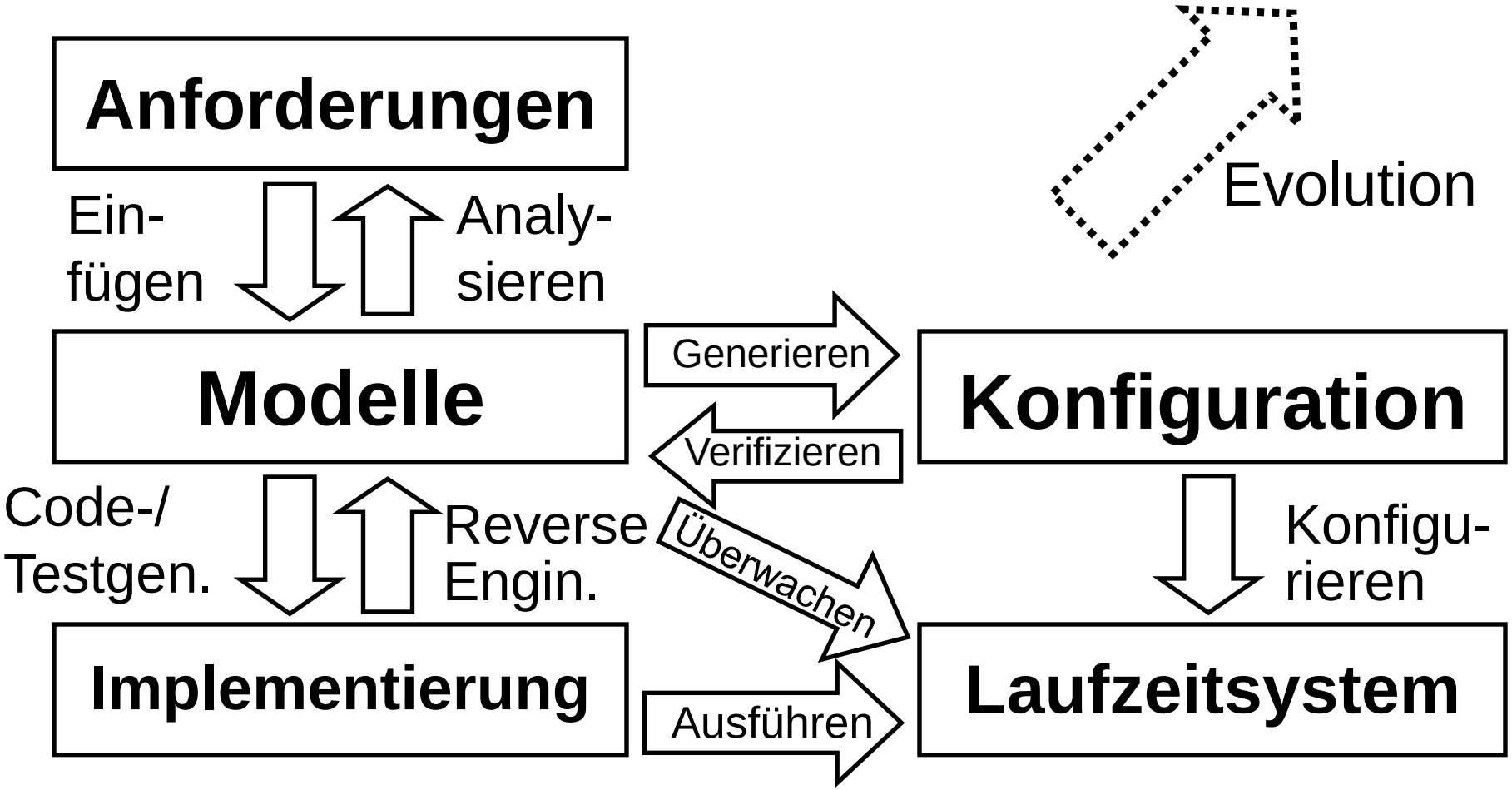
Compliance-Report

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

Compliance-Leitfaden / Methodik: Überblick



Modell-basiertes Compliance-Management



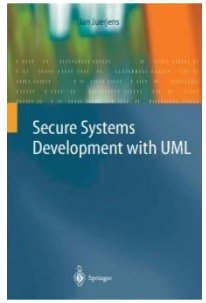
Compliance-Modellierung mit UMLsec

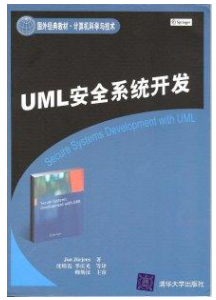
Ziel:

- Dokumentation und automatische Analyse von compliance-relevanten Informationen (z.B. Sicherheits-Eigenschaften und -Anforderungen) als Teil der Systemspezifikation.

Idee:

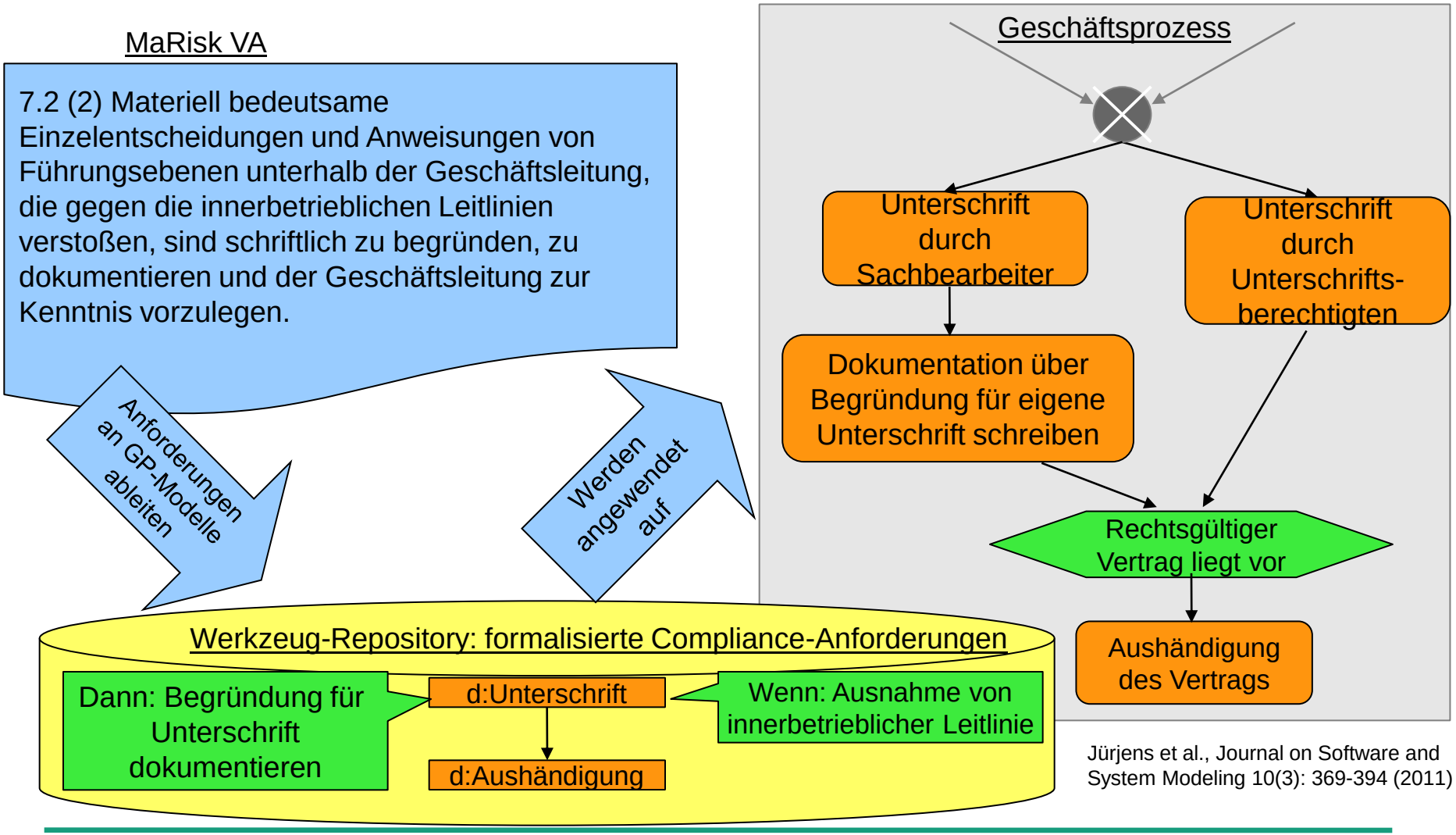
- UML für System-Modellierung.
- Sicherheitsinformationen als Markierungen (Stereotypen) einfügen, mithilfe der UML-Erweiterung UMLsec.
- Automatische Verifikation der Modelle gegen die Sicherheitsanforderungen auf Basis von formaler Semantik.





Jan Jürjens: Secure systems development with UML. Springer 2005. Chines. Übers. 2009

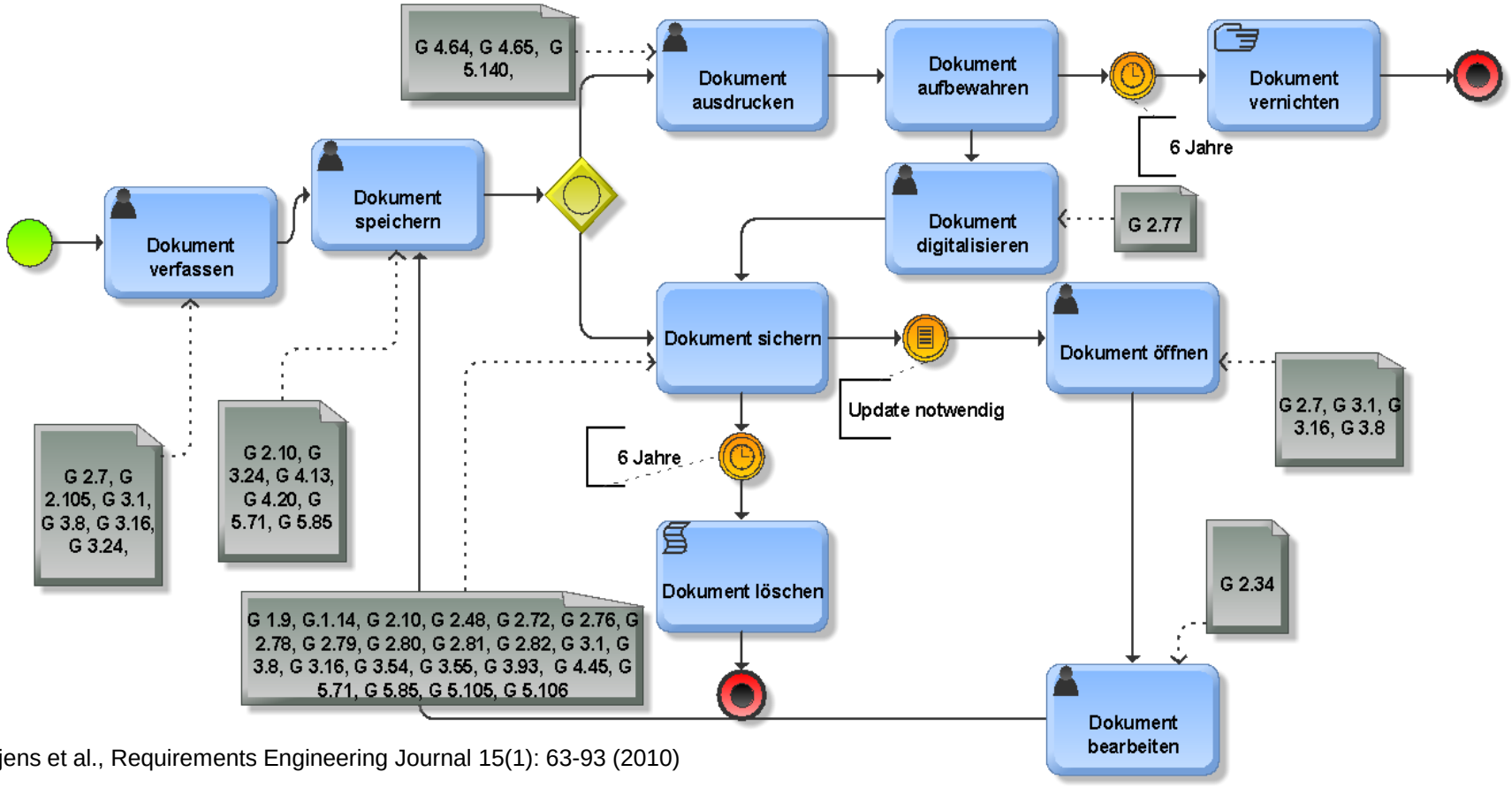
Vorgehen (1): Von Compliance nach IT-Sicherheit



Jürjens et al., Journal on Software and System Modeling 10(3): 369-394 (2011)

Vorgehen (2): Berücksichtigung von Sicherheitsstandards

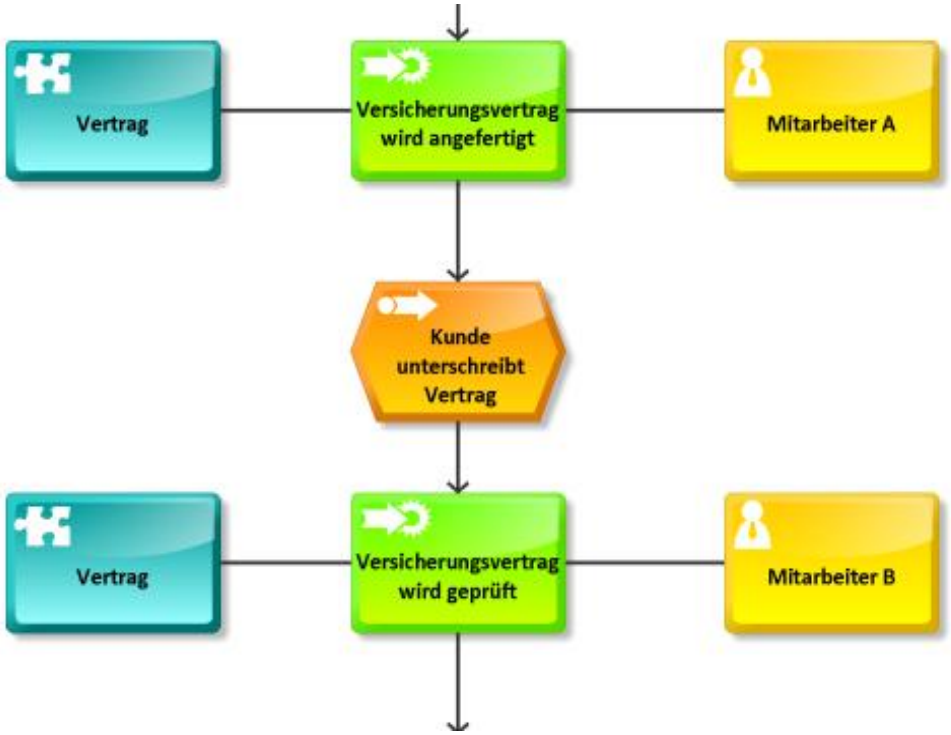
Werkzeuggestützte Annotation von GP-Modellen mit Risiken anhand des BSI-Grundschutzkataloges:



Jürjens et al., Requirements Engineering Journal 15(1): 63-93 (2010)

Vorgehen (3): Modell-basierte Compliance-Analyse

- Strukturanalyse eines Geschäftsprozesses auf Basis von Compliance-Mustern
- Beispiel: Für jedes Auftreten eines Vertragsabschlusses wird 4-Augen-Prinzip überprüft.




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

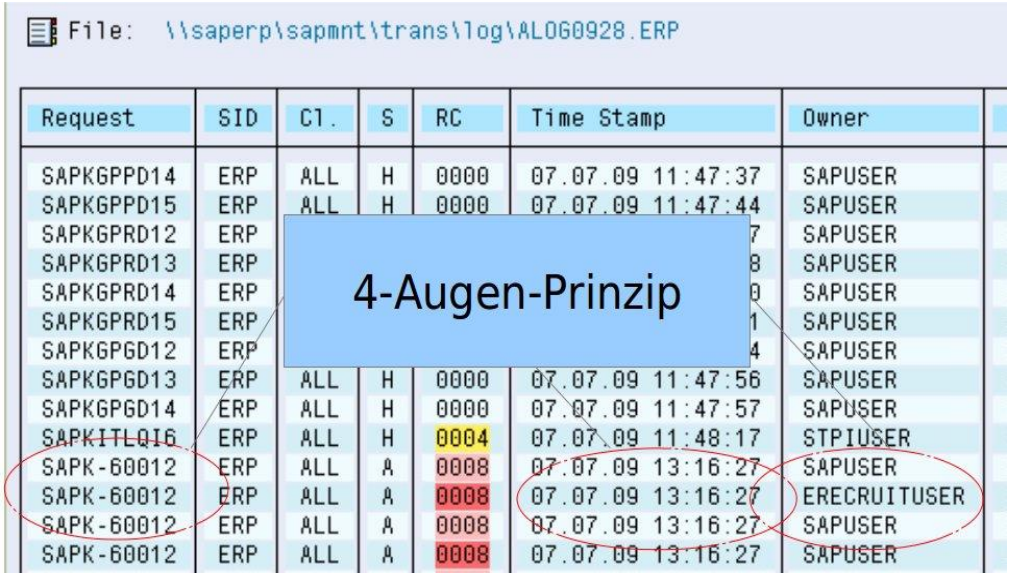
Jürjens et al., Int. Journal on Intelligent Systems 25(8): 813-840 (2010)

Vorgehen (4): Log-Daten-basierte Compliance-Analyse

Beispiel:

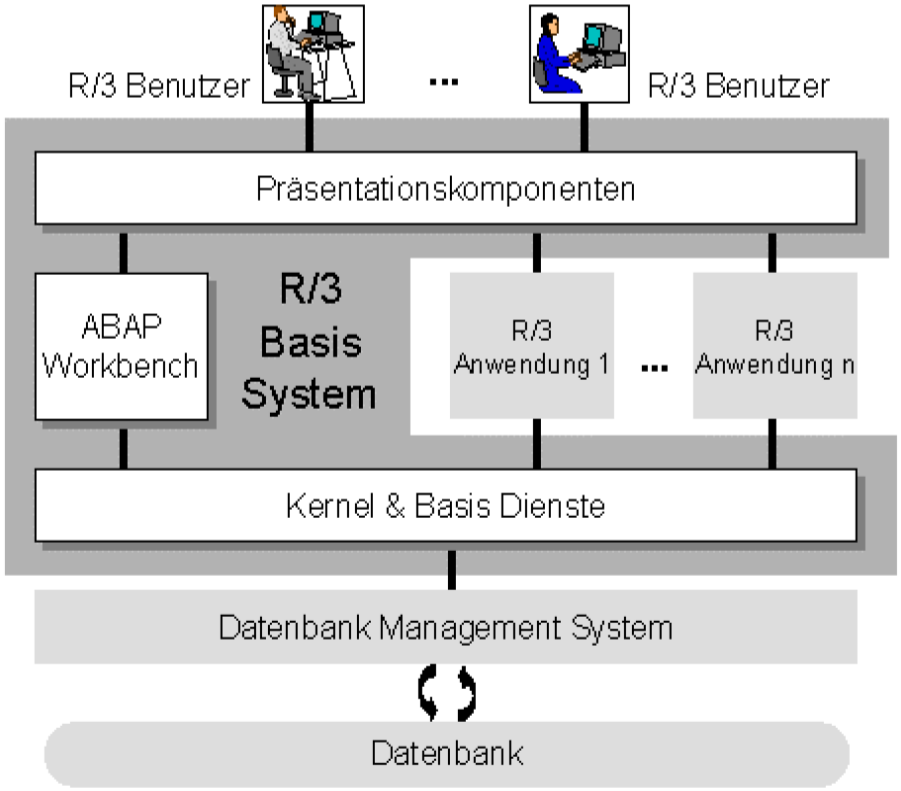
Überprüfung des 4-Augen-Prinzips anhand folgender Informationen:

- Request Ids stimmen überein
- Owner sind verschieden
- Auftrag wurde zum selben Zeitpunkt freigegeben



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

Vorgehen (5): Analyse von Berechtigungsdaten

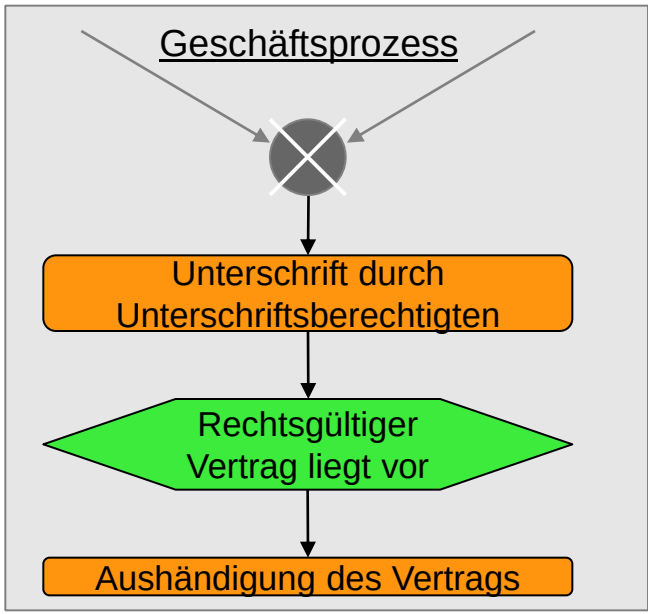


- SAP Berechtigungen auf Sicherheitsregeln prüfen. Geht nicht manuell:
  - Große Datenmengen (z.B. 60.000 Berechtigungen)
  - Komplexe Beziehungen zwischen Berechtigungen (Delegation)
  - Dynamische Änderungen (Urlaubsvertretung etc.)
- Automatische Analyse auf Produktionskopie erhöht Vertrauenswürdigkeit unabhängig von Administrator.
- Optionale Analyse gegenüber Geschäftsprozessmodellen.

Beispiel: Anwendung der MaRisk VA und BSI-Grundschutz (1)

MaRisk VA

7.2 (1) Organisatorische Rahmenbedingungen:
Das Unternehmen hat zur Umsetzung des 64a VAG bzw. des 104s VAG sicherzustellen, dass die mit wesentlichen Risiken behafteten Geschäftsaktivitäten auf der Grundlage von innerbetrieblichen Leitlinien betrieben werden...



Verwendet BSI Grundschutz

IT-Policy (BSI konform)

d:unterschreiben

d:aushändigen

Rollenüberpüfung: Berechtigung gegeben (BSI G3.1)

Werden angewendet auf

Abbildung MA-Risk VA auf Sicherheitsanforderungen

- Framework zur Abbildung von regulatorischer Compliance auf Security Policies

• Zwei Komponenten:

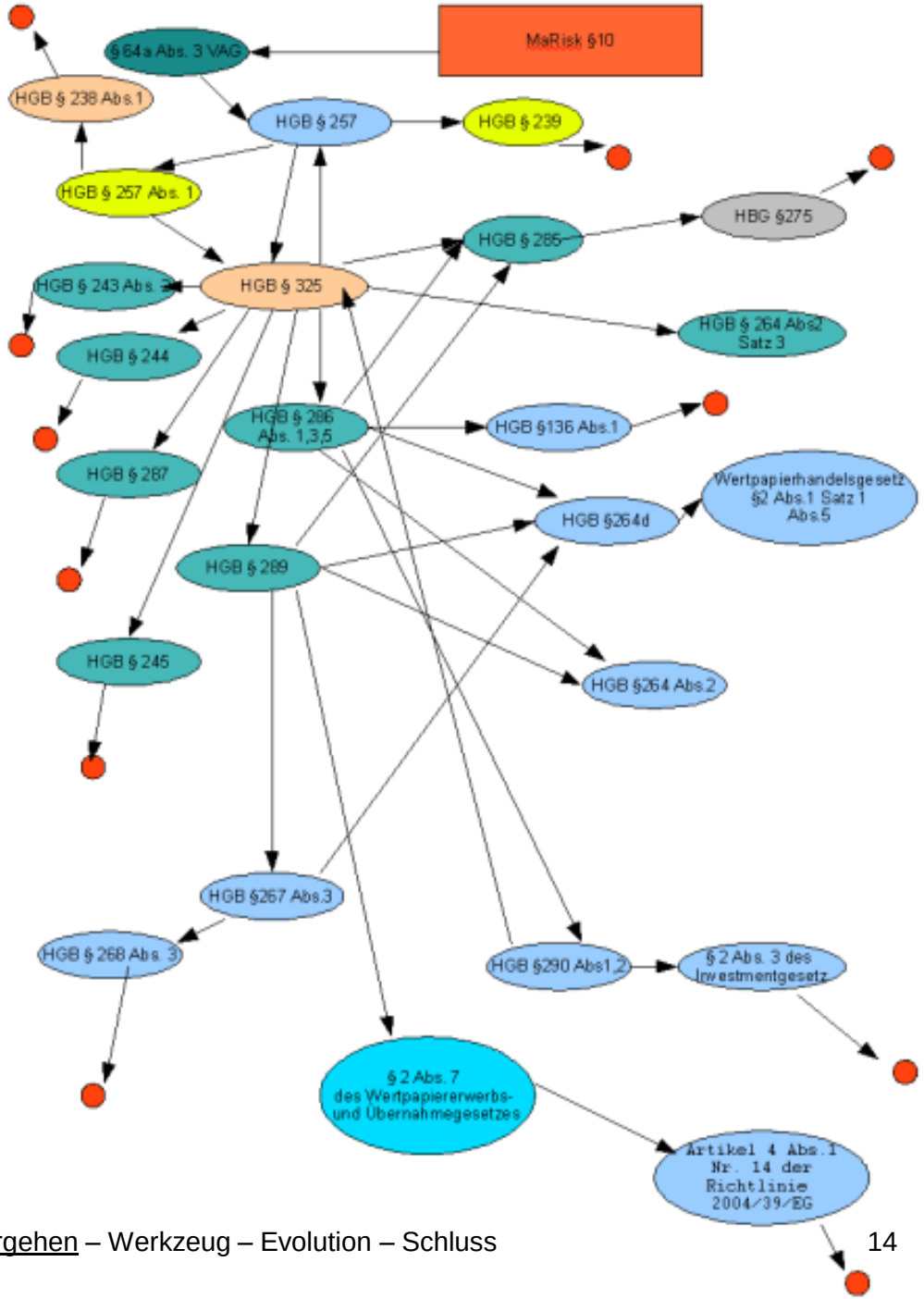
(welche Compliance-Anforderungen können auf *Security Policies* abgebildet werden?)

→ 1) die **Analysekomponente**

(wie wird die Abbildung vorgenommen?)

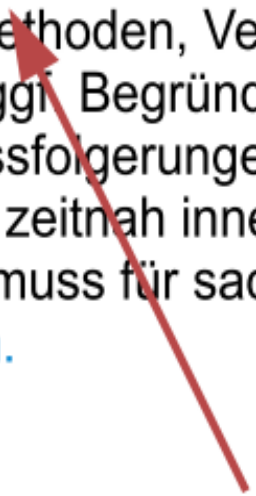
→ 2) die **Abbildungskomponente**

- Berücksichtigung von Cross-References ausgehend von MA-Risk VA



Beispiel: MaRisk VA 10

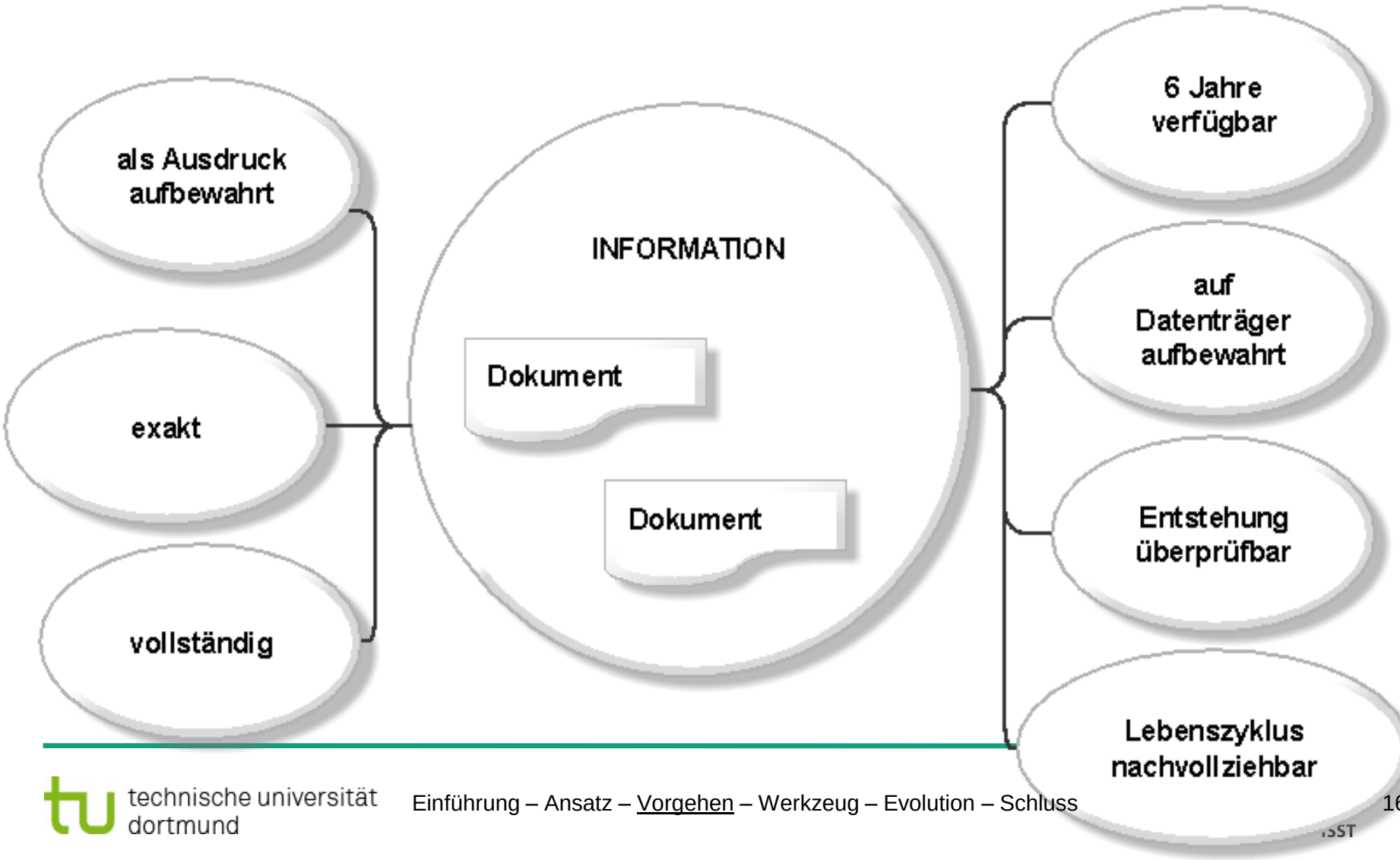
Alle für die Funktionsfähigkeit des Risikomanagements wesentlichen Informationen müssen den Entscheidungsträgern exakt und vollständig zur Verfügung stehen. Wie gesteuert werden soll, ist dabei in Abstimmung mit der Strategie des Unternehmens festzulegen. Hinsichtlich der Dokumentation gelten die Anforderungen des **§ 64a Abs. 3 VAG.** Die Dokumentation umfasst alle wesentlichen Formeln, Parameter, Methoden, Verfahren, Handlungen, Festlegungen, Entscheidungen und ggf. Begründungen sowie festgestellten Mängel und daraus gezogene Schlussfolgerungen. Wesentliche unterjährige Änderungen sind aufzuzeichnen und zeitnah innerhalb des Unternehmens zu kommunizieren. Die Dokumentation muss für sachverständige Dritte nachvollziehbar und überprüfbar sein.



CROSS-REFERENCE

Ergebnis der Analysekomponente

Ma-Risk VA 10:

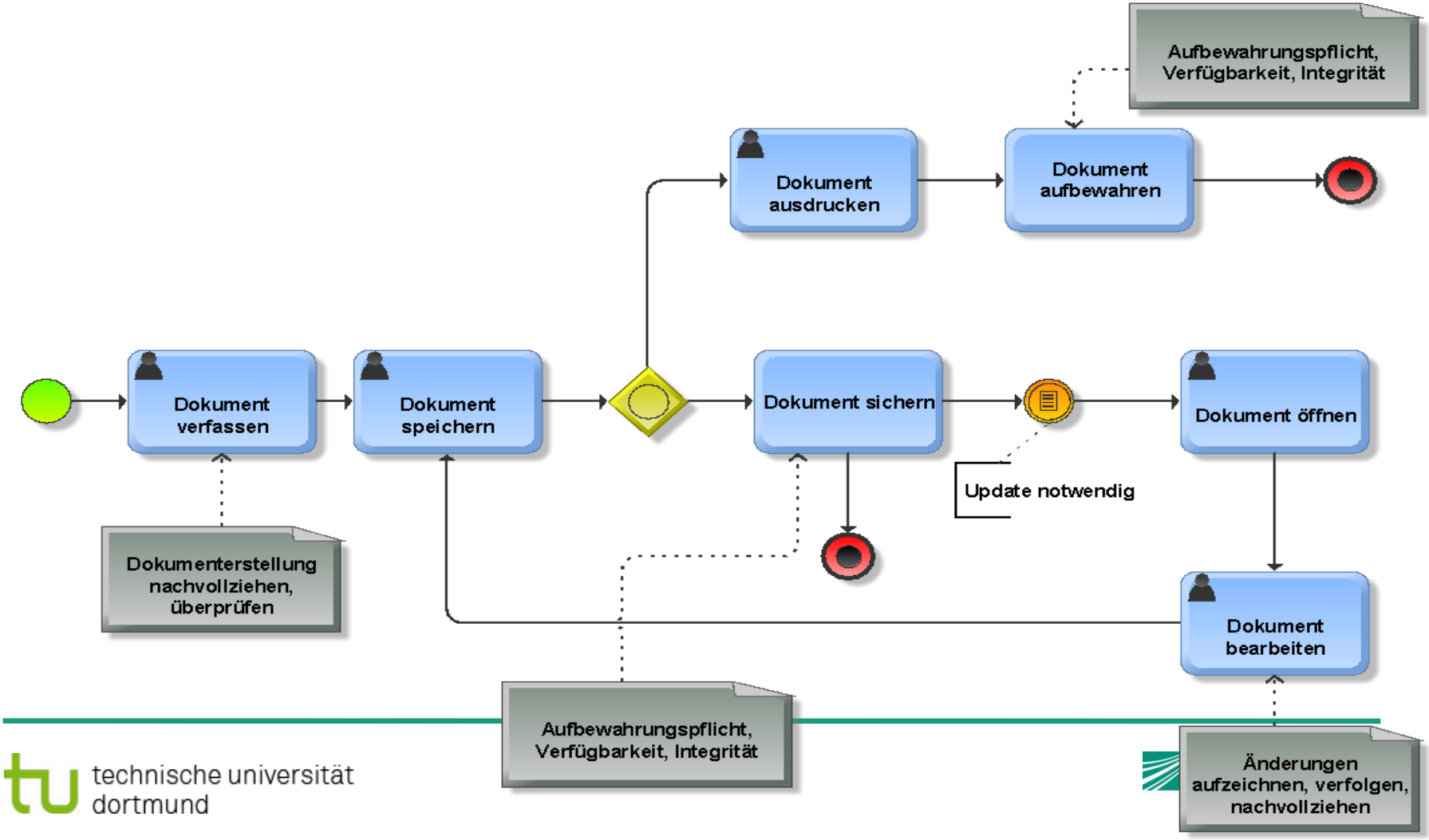


Ergebnis der Anwendung auf MaRisk VA 10

GESETZ	AKTVITÄT/ GP	IT-SECURITY-ANFORDERUNG	IT-SECURITY-ZIEL
MaRisk VA 10	Information	vollständig	Verfügbarkeit
MaRisk VA 10	Information	exakt	Integrität
MaRisk VA 10	Dokument ändern	Änderungen aufzeichnen	Autorisation Verbindlichkeit Authentifikation
MaRisk VA 10	Dokumentation	Änderungen nachvollziehbar	Verbindlichkeit Authentizität, Integrität
MaRisk VA 10	Dokumentation	Änderungen überprüfbar	Verbindlichkeit Authentizität, Integrität
VAG 64a Abs. 3	Dokumentation	Dokumentation 6 Jahre aufbewahren	Verfügbarkeit, Integrität Datensicherheit
VAG 64a Abs. 3	Dokumentation	Datensicherung Datenarchivierung	Verfügbarkeit, Integrität Datensicherheit
HGB 238 Abs. 1	Geschäftsvorfälle	Entstehen und Abwicklung verfolgbar	Verfügbarkeit
HGB 239	Dokument ändern	Änderungen aufzeichnen, Ursprünglicher Inhalt verfolgbar	Verfügbarkeit
HGB 239	Datenträger verwalten	Daten überprüfbar, lesbar	Verfügbarkeit
HGB 239	Ausgedruckte Dokumente verwalten	Dokumente verfügbar	Verfügbarkeit

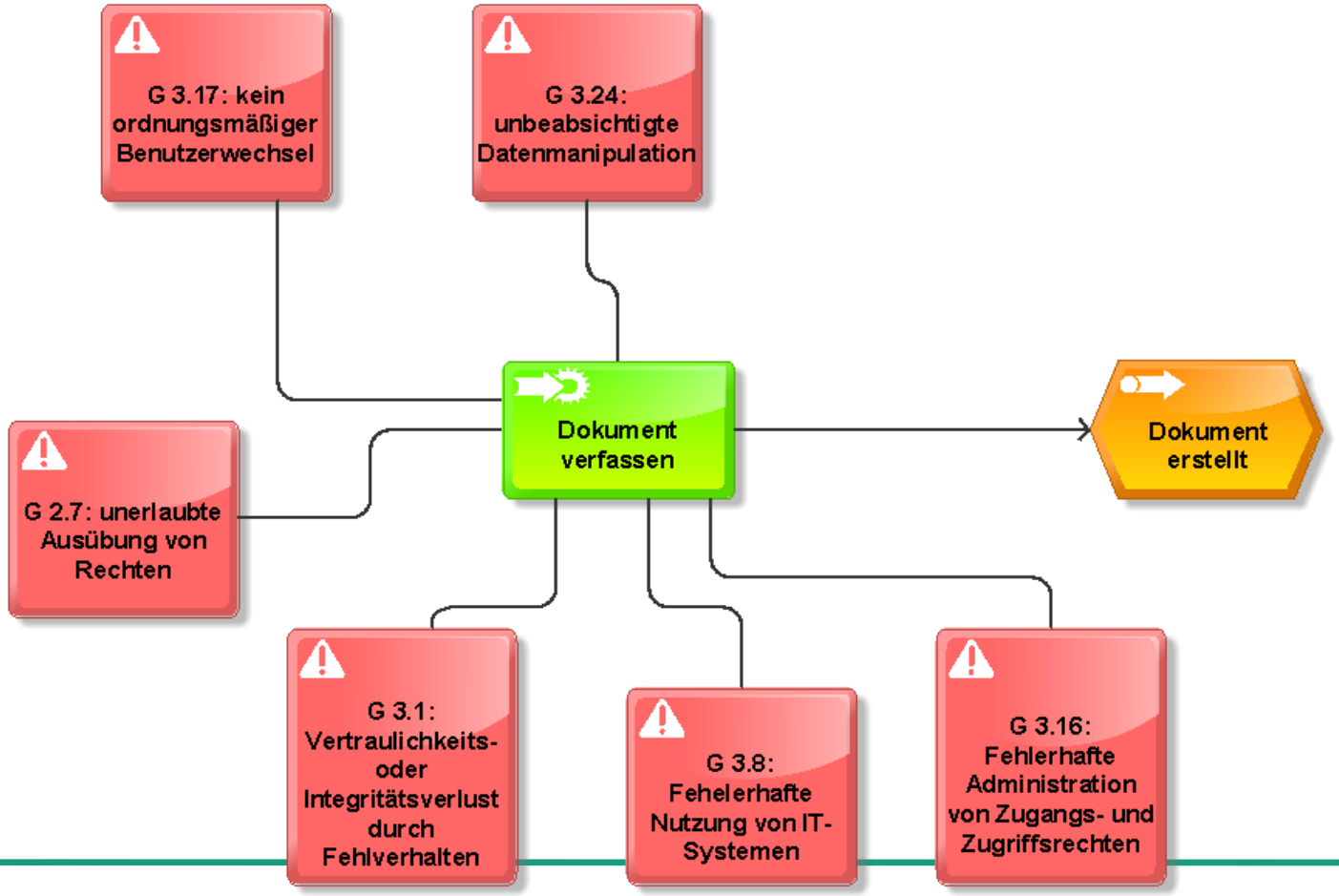
Beispiel

- BPMN-Geschäftsprozess „Dokumentieren“ annotiert mit Sicherheitsanforderungen resultierend aus MARisk VA



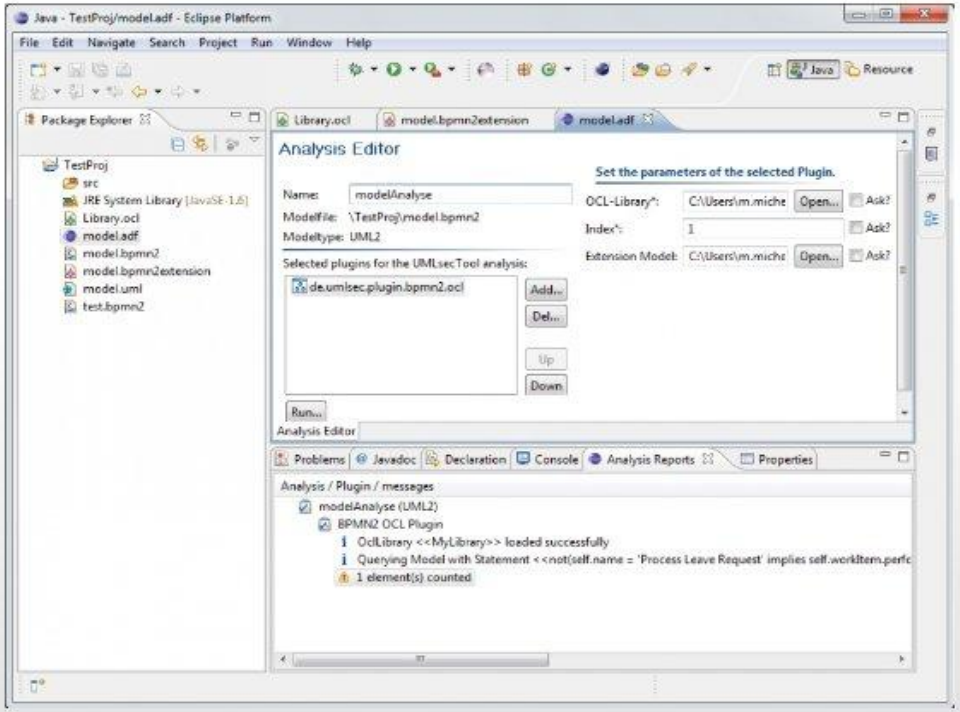
Beispiel: Aktivität

- Aus Sicherheitsanforderungen konkret abgeleitete Gefahren anhand des BSI-Grundschutzkataloges



Werkzeugunterstützung (s. 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

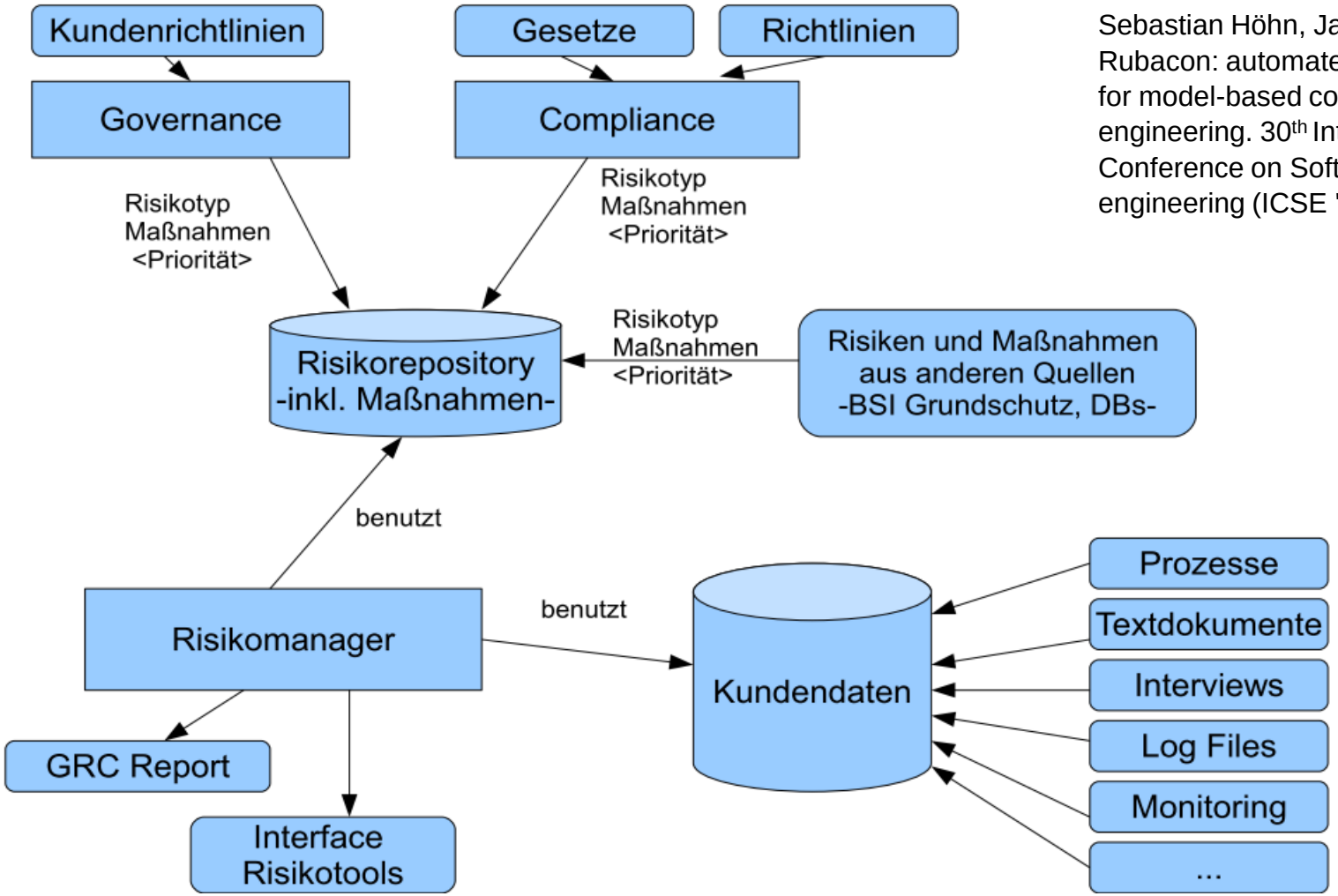
of software models.[1)]

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.

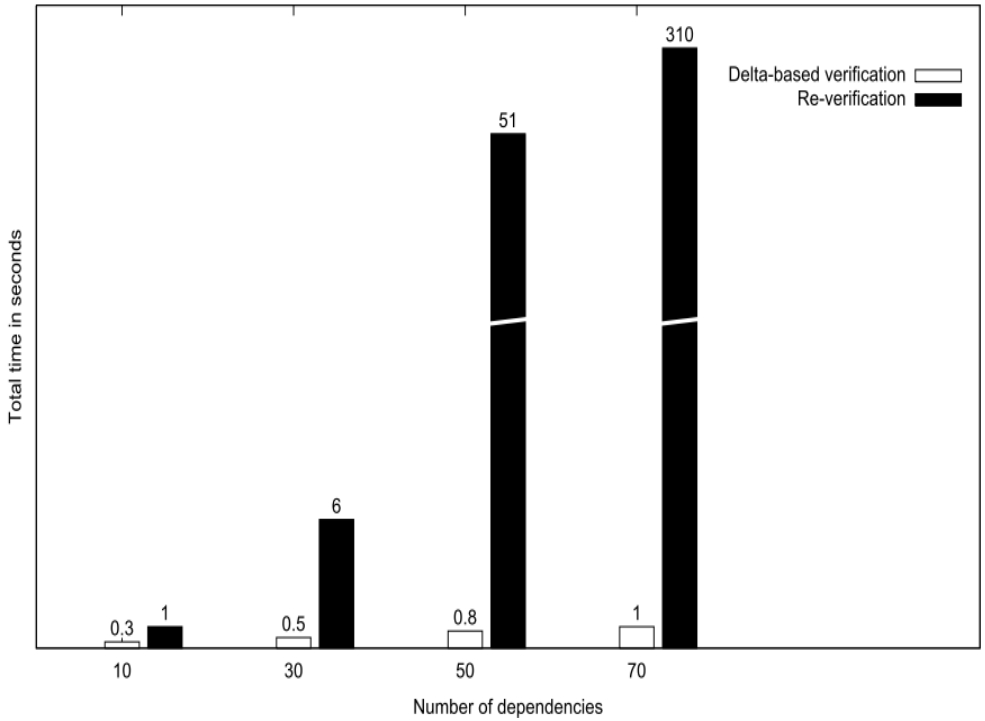
Werkzeugunterstützung: Workflow

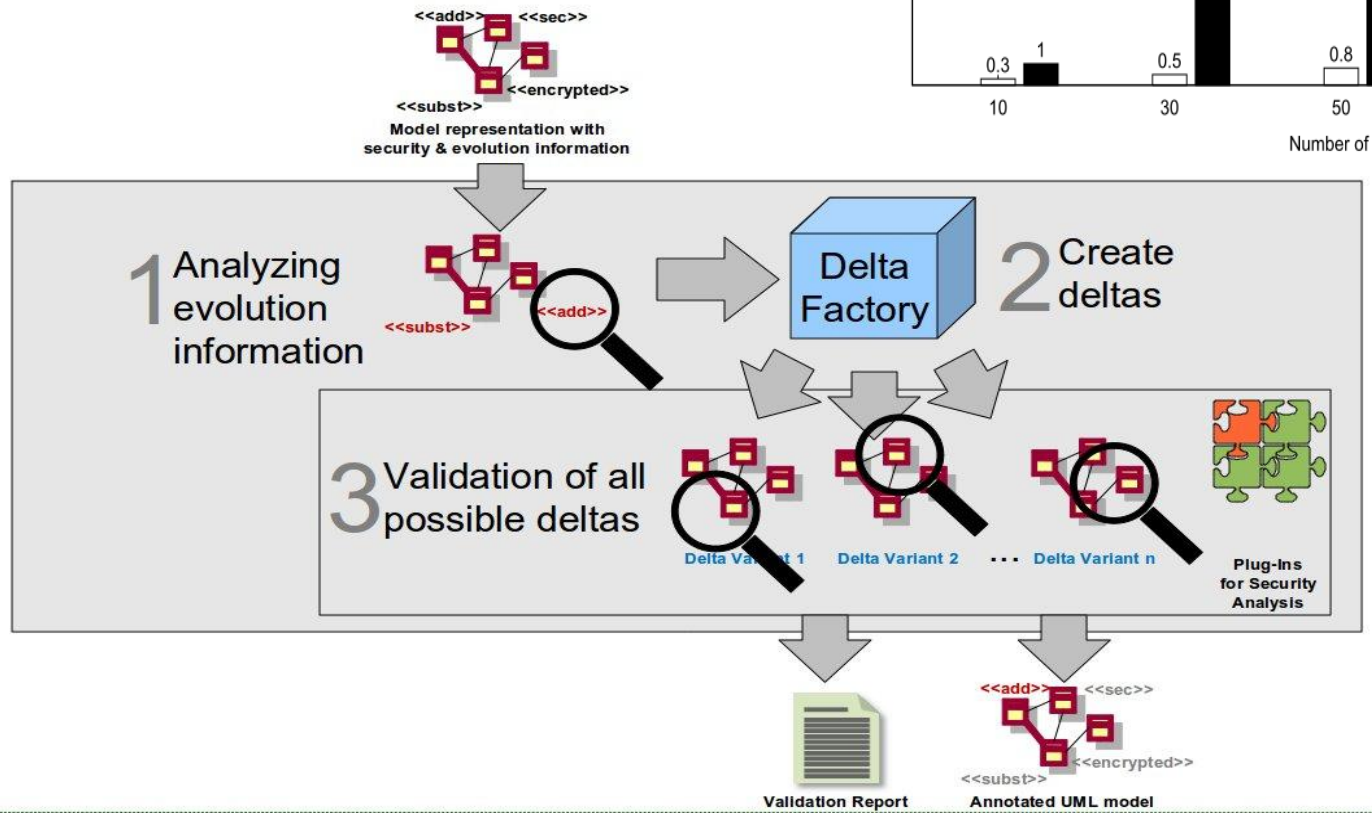


Sebastian Höhn, Jan Jürjens: Rubacon: automated support for model-based compliance engineering. 30th International Conference on Software engineering (ICSE '08). ACM

Werkzeugunterstützung: System-Evolution:

- Umsetzung der Evolutions-Analyse im Werkzeugprozess
- Resultierender Performanzgewinn





Jan Jürjens. 2011. Automated security hardening for evolving UML models. 33rd Int. Conf. on Software Engineering (ICSE '11). ACM.

A. Bauer, J. Jürjens, Y. Yu: Run-Time Security Traceability for Evolving Systems. Computer Journal 54(1): 58-87 (2011)

Anwendung: Mobile Kommunikation bei O_2

UMLsec-basierte Sicherheitsanalyse der Regulierungen für den Einsatz mobiler Endgeräte bei O_2 (Germany)

62 Sicherheitsanforderungen aus Security Policy extrahiert.

21 Geschäftsprozess-relevante Anforderungen in 8 Aktivitätsdiagrammen modelliert mithilfe der UMLsec-Stereotypen <<fair exchange>> and <<provable>>

10 Datensicherheits-Anforderungen (Vertraulichkeit, Integrität) in Deployment-Diagramm modelliert.

3 Anforderungen bzgl. Rollenbasierter Zugangskontrolle (RBAC) modelliert

15 Anforderungen bzgl. Sicherheit der Netzwerkdienste, und Einsatz von Firewalls und Antivirensoftware modelliert (mithilfe weiterer Erweiterung von UMLsec)

13 Anforderungen konnten nicht direkt in UMLsec modelliert werden

J. Jürjens, J. Schreck, P. Bartmann. 2008. Model-based security analysis for mobile communications. 30th International Conference on Software engineering (ICSE '08). ACM

Nr.	Sicherheitsanforderungen	<<Secure Links>>, Secure Links with XML	<<Fair Exchange>>	<<Provable>>	SecrecyIntegrity	TPTP-Datei z. Analyse v. Netzwerk-architekturen
1.9	Authentifizierung des Benutzers (Mitarbeiters) gegenüber dem Endgerät durch Chipkarten			X		
1.10	Verschlüsselung der auf den mobilen Endgeräten befindlichen Daten	X				
1.14	Keine zum Fernzugang parallele Verbindungen in andere Netze - Vermeidung der Kopplung mit unsicheren Netzen durch Umgehung der Firewall					X
1.26	Starke Verschlüsselung der Verbindung zwischen Endgerät und Fernzugangs-Server	X				
1.37	Bei O_2 übliche Virenschutzprogramme auf den Endgeräten					X
1.38	Aktualisierung des Virenschutzes über Fernzugang					

Anwendungsbeispiel: Internes Informationssystem

- MetaSearch Engine: Personalisierte Suche im Firmen-Intranet von BMW (passwort-geschützt).
- Einige Dokumente sehr sicherheitskritisch.

[ICSE 07]

- Über 1.000 potentielle Benutzer, 280.000 Dokumente, 20.000 Anfragen pro Tag.
- Nahtlos in unternehmensweite Sicherheitsarchitektur integriert. Bietet Sicherheitsdienste für Anwen-dungen (Benutzerauthentisierung, rollenbasierte Zugangskontrolle, globales Single-Sign-On), Ansatzpunkte für weitere Sicherheitsdienste.
- Erfolgreich mit UMLsec analysiert.

Weitere Anwendungen

- Gesundheitskarte: Architektur mit UMLsec untersucht, Schwachstellen aufgedeckt [Jour. Meth. Inform. Medicine 08]
- Internes Informationssystem [ICSE 07]
- Digitaler Formularschrank [SAFECOMP 03]
- Common Electronic Purse Specifications (Globaler Standard für elektr. Geldbörsen): mehrere Schwachstellen aufgedeckt [IFIPSEC 01, ASE 01]
- Biometrische Authentisierungssysteme: mehrere Schwachstellen aufgedeckt [ACSAC 05, Models 09]
- Gesundheitsinformationssysteme [Caise 09]
- Return-on-Security Investment Abschätzung
- Analyse Digitale-Signatur-Architektur
- IT-Sicherheits-Risikomodellierung
- Smart-card Software-Update Plattform

Aktuell:

- Cloud-Anwender Sicherheitsanalyse

Geplant:

- Cloud-Anbieter Sicherheitsanalyse
- Sicherheitsökonomische Analysen

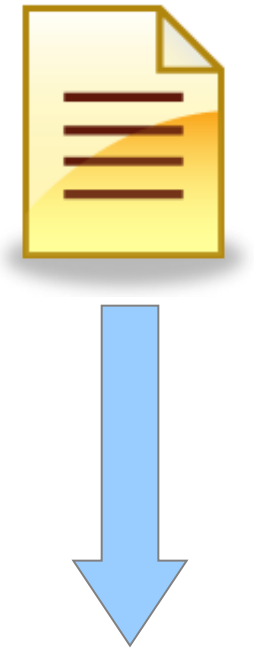
Ausblick: Anwendung von Data-Mining-Ansätzen auf Text-Dokumentation ?

Ein neuer Klient kommt in ein Versicherungsbüro der privaten Krankenversicherung Gesundheit & Co zu einem Versicherungsagenten (VA) mit dem Ziel, eine neue, private Krankenversicherung abzuschließen.

[…]
Der VA erfragt zuerst die **Daten** des Klienten; dies sind Name, Vorname, Geburtsdatum, Adresse, Bruttogehalt und den bisherigen Versicherungsstatus. Die **Daten** gibt der VA in seinen Computer ein, nachdem er ein entsprechendes Programm aufgerufen hat. Die Software berechnet nun aufgrund der eingegebenen **Daten** ein neues Versicherungsangebot. Dabei wird auch **überprüft**, ob sich der Klient überhaupt privat versichern **darf**. Hierzu wird eine Überprüfung durchgeführt; beträgt das Bruttoeinkommen **mehr als 48.000 Euro**, so ist eine private Versicherung möglich, andernfalls nicht. Weiterhin wird eine Auskunft von der **Schufa** eingeholt. Hierzu wird mit dem Schufa-Server kommuniziert. Dabei werden die nötigen **Daten** Name, Vorname, Geburtsdatum übermittelt. Der **Schufa**-Server liefert als Antwort eine Zahl (Wertebereich 1 bis 10). Liegt die Zahl **unter 5**, so steht dem Abschluss einer Versicherung nichts mehr im Wege. Andernfalls ist kein Versicherungsabschluss möglich.

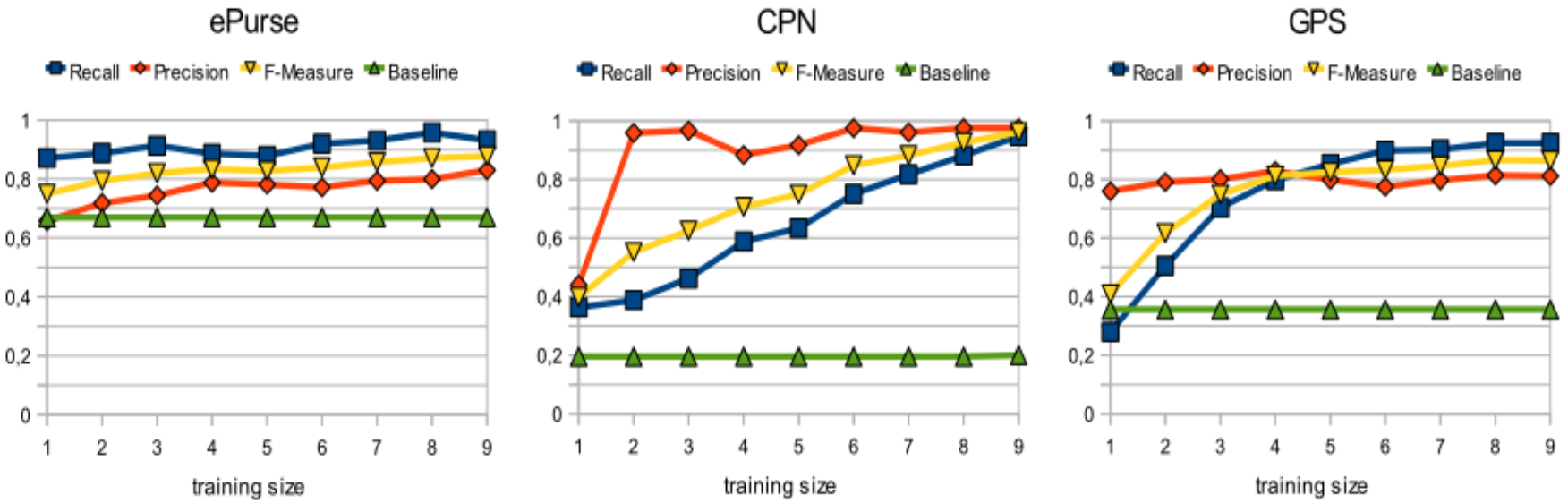
[…]
Der Klient prüft sie und unterschreibt. Die Antragsformulare werden zentral gesammelt und später an die Zentrale gefaxt. Aus **Datenschutzgründen** dürfen die Unterlagen **niemals länger als zwei Stunden** auf dem Sammelplatz liegen. In der Zentrale werden sie bearbeitet und die Versicherungspolice wird nach zwei Tagen an den Klienten geschickt.

[...]



Risikobewertung

Textmining: Erste Resultate



- Industrielle Anforderungsdokumente
  - Common Electronic Purse Specifications (ePurse)
  - Customer Premises Network specification (CPN)
  - Global Platform Specification (GPS)
- Metriken für Information Retrieval:
  - Recall: Trefferquote
  - Precision: Genauigkeit
  - F-Measure: Kombination P&R
  - Baseline: Alle Anforderungen als security relevant klassifiziert

K. Schneider, E. Knauss, S. Houmb, S. Islam, J. Jürjens: Enhancing Security Requirements Engineering by Organisational Learning. In: Requirements Engineering Journal (REJ)

Zusammenfassung: Modell-basiertes Compliance-Management

Problem: Steigende Anforderungen für Unternehmen, die Konformität mit übergeordneten Regulierungswerken zu demonstrieren.

Ziele: Verbesserung der Verlässlichkeit und Nachvollziehbarkeit von Aktivitäten im Compliance-Management sowie Kostenersparnis

Idee: Entwicklung von automatischen Werkzeugen, die das Management von Compliance-Anforderungen auf Basis von vorhandenen Artefakten unterstützen.
Automatisierte IT-Sicherheits- und Risiko-Analysen auf der Basis von Textdokumenten, Schnittstellen-Spezifikationen, Geschäftsprozess-Modellen, Log-Daten und anderen Datenquellen.

Ergebnisse: Erfolgreiche Validierung in mehreren industriellen Anwendungsprojekten.

Aktuelle Arbeiten:

- Anwendung auf den Einsatz von Cloud-Computing (Projekte SecureClouds, ClouDAT)
- Berücksichtigung ökonomischer Aspekte (Projekt Seconomics)

Compliance-Report

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