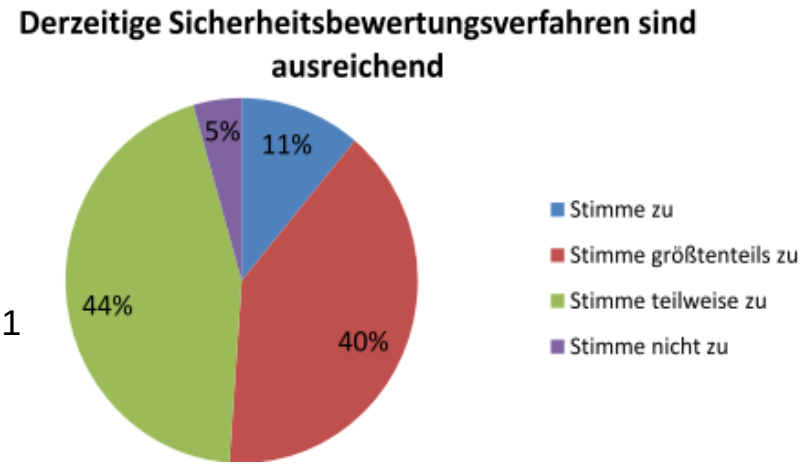
Den Nebel lichten: Von Compliance-Regularien zu testbaren Sicherheitsanforderungen

Prof. Dr. Jan Jürjens

TU Dortmund und Fraunhofer ISST

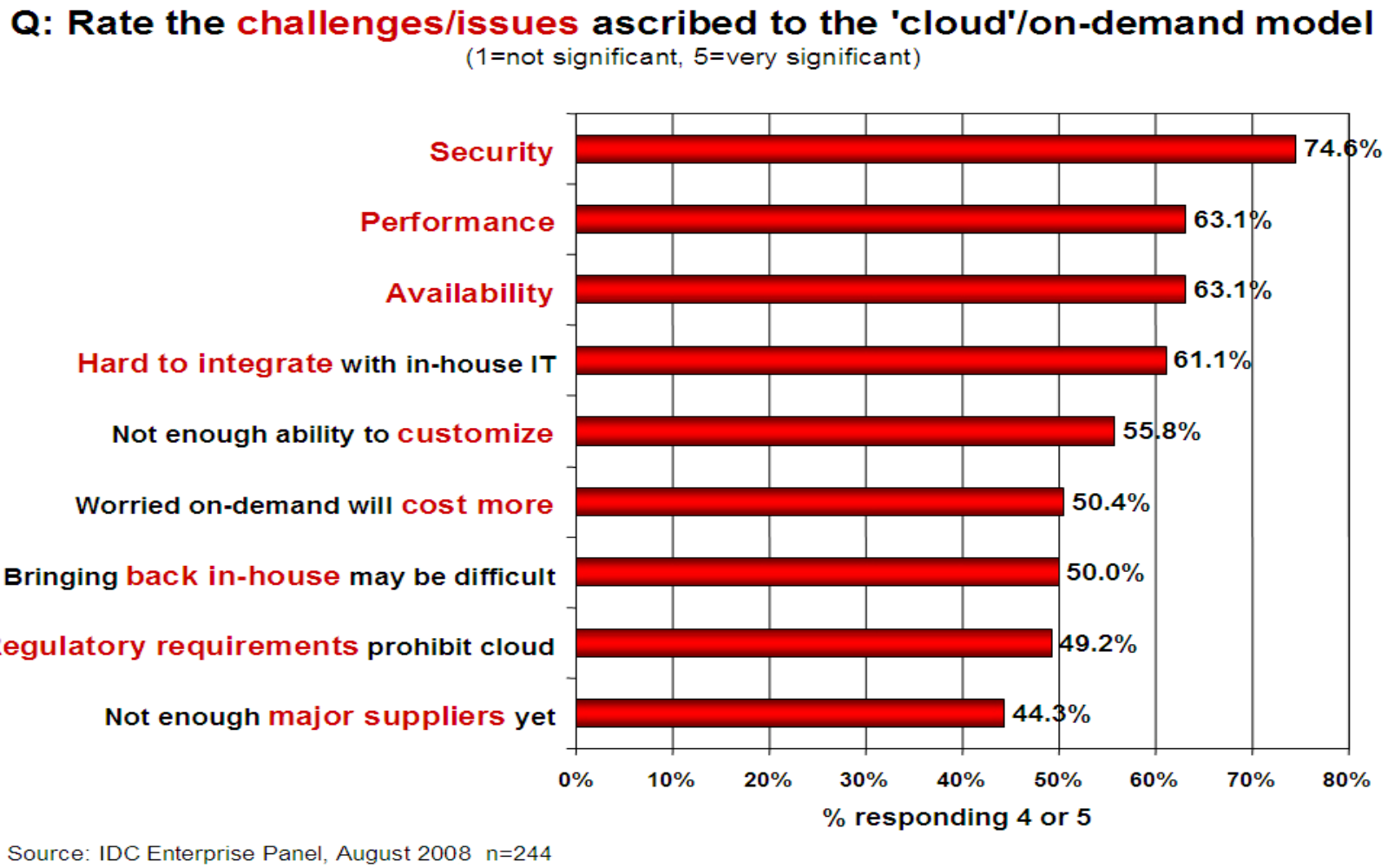
Herausforderung: Compliance

- 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.

Ansatz:

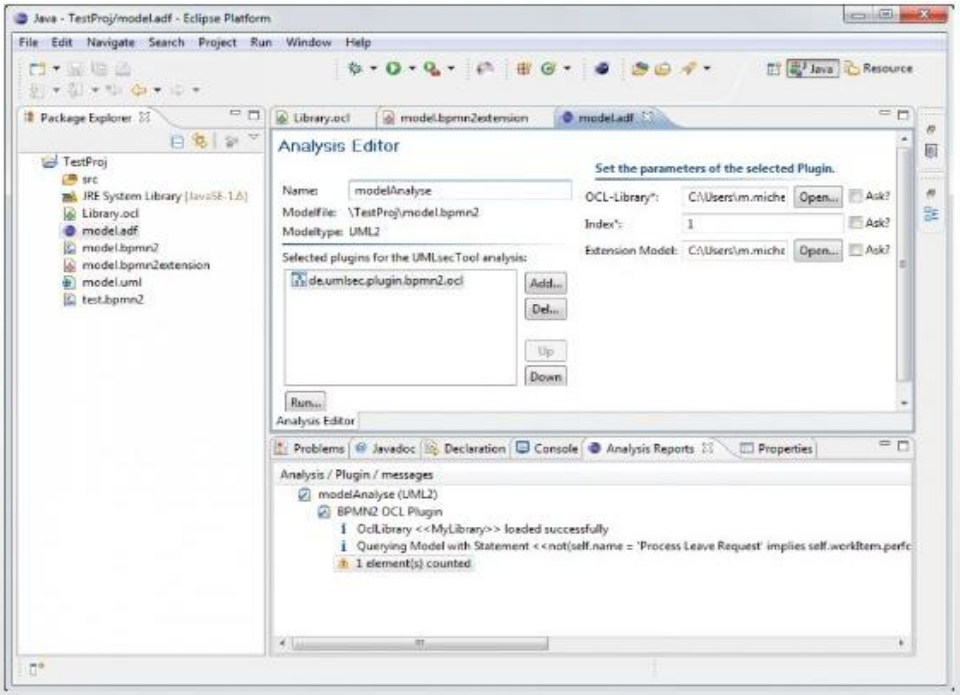
- Verwendung von automatischen Werkzeugen, die das Management von Compliance-Anforderungen auf Basis von vorhandenen Artefakten unterstützen.
- Insbesondere automatisierte IT-Sicherheits- und Risiko-Analysen auf der Basis von Textdokumenten, Schnittstellen-Spezifikationen, Geschäftsprozess-Modellen, 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

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)]

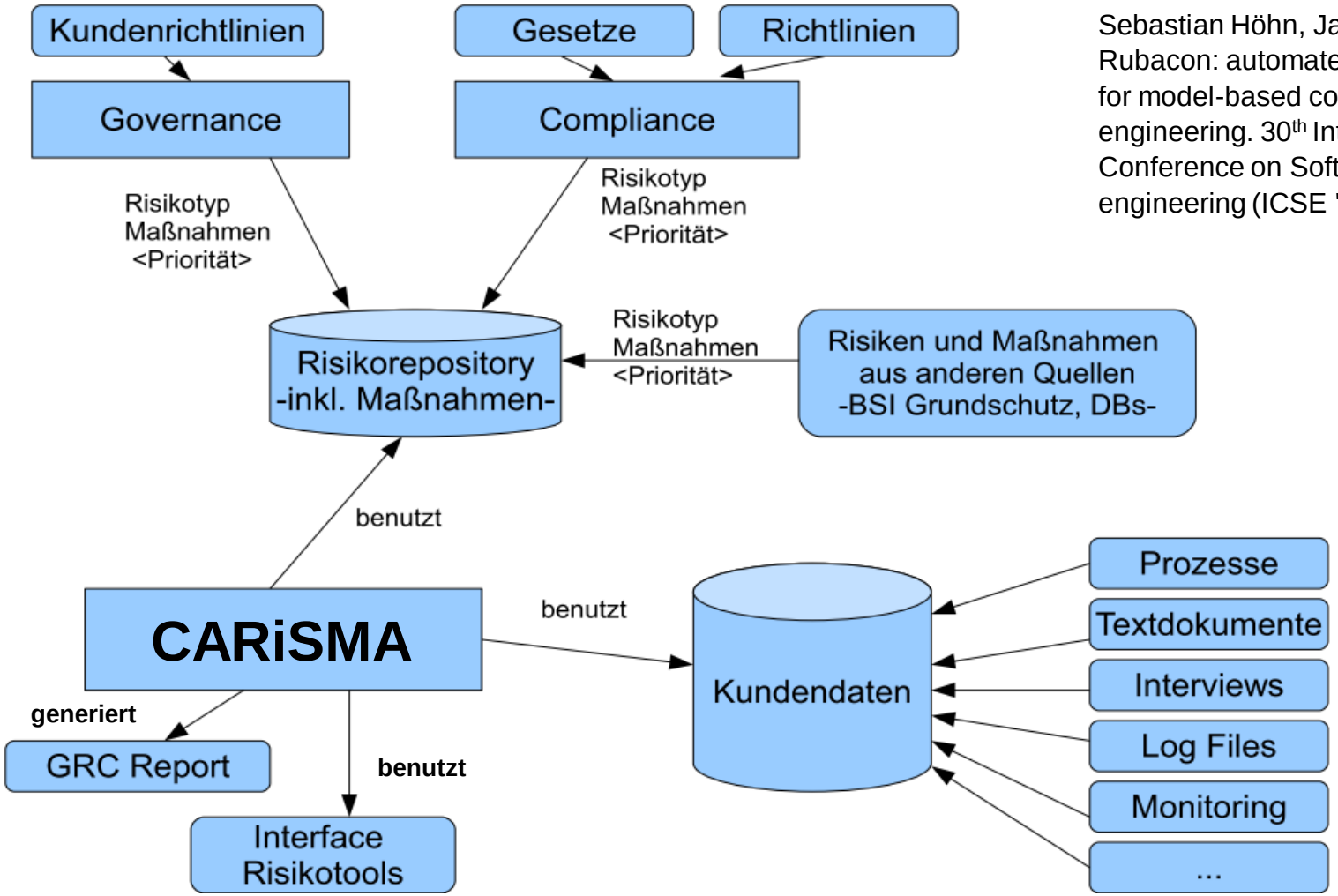
Since CARiSMA is a reimplemented variant of the former UMLsec tool it natively supports UML models. Due to its EMF-based implementation CARiSMA can also support **domain-specific modeling languages** such as BPMN.

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.

Open-source, Eclipse-style Lizenz (kann in kommerzielle Produkte eingebunden werden).

Werkzeugunterstützung: Workflow

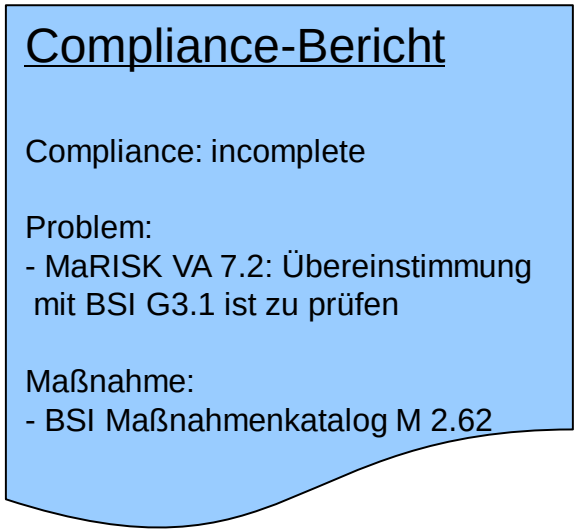


Sebastian Höhn, Jan Jürjens: Rubacon: automated support for model-based compliance engineering. 30th International Conference on Software engineering (ICSE '08). ACM

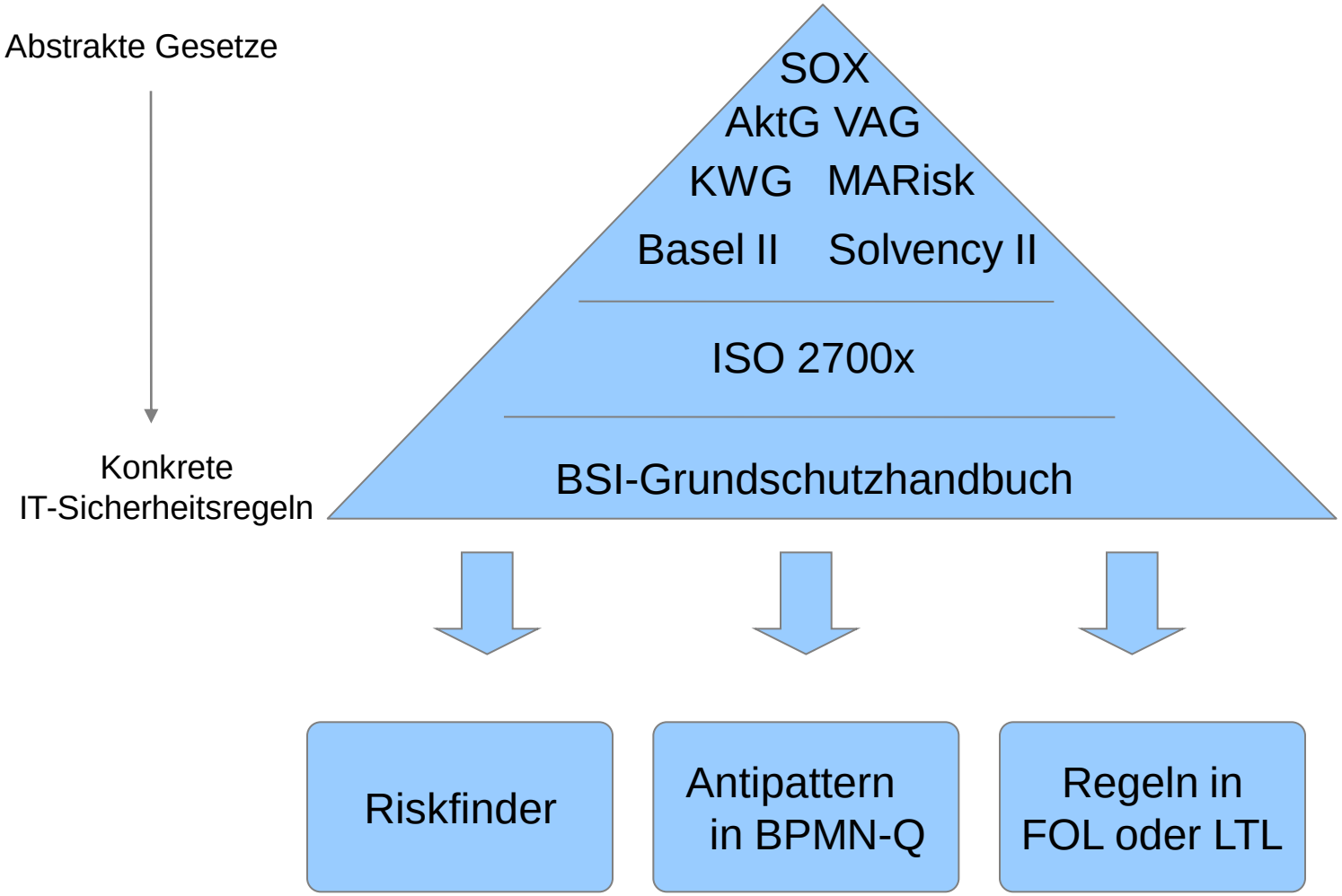
Nutzen

Automatisch generierter Compliance-Bericht:

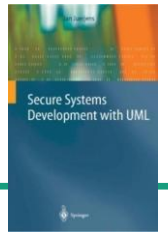
- Beispiel: „Compliant zu: MaRISK VA (ja / nein)“
- Führt weitere zu untersuchende Anforderungen auf
- Schlägt Maßnahmen zur Verbesserung der Übereinstimmung mit Compliance-Anforderungen vor:
  - Automatische Korrektur
  - Manuelle Korrektur

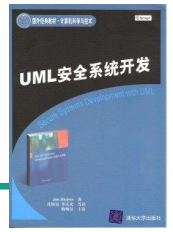


Compliance-Leitfaden / Methodik: Überblick

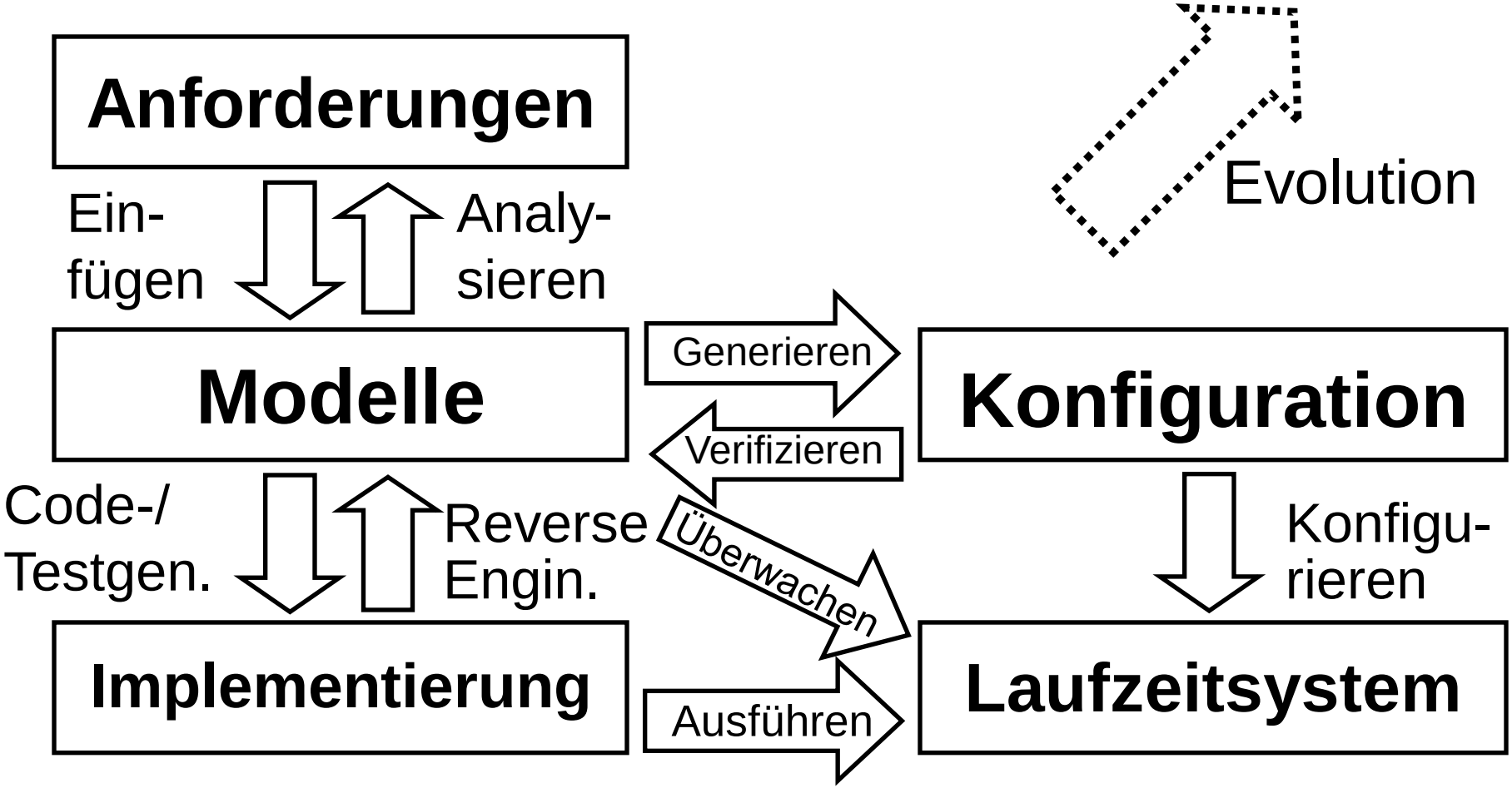


Modell-basiertes Compliance-Management





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



Vorgehen (1): Von Compliance nach IT-Sicherheit

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

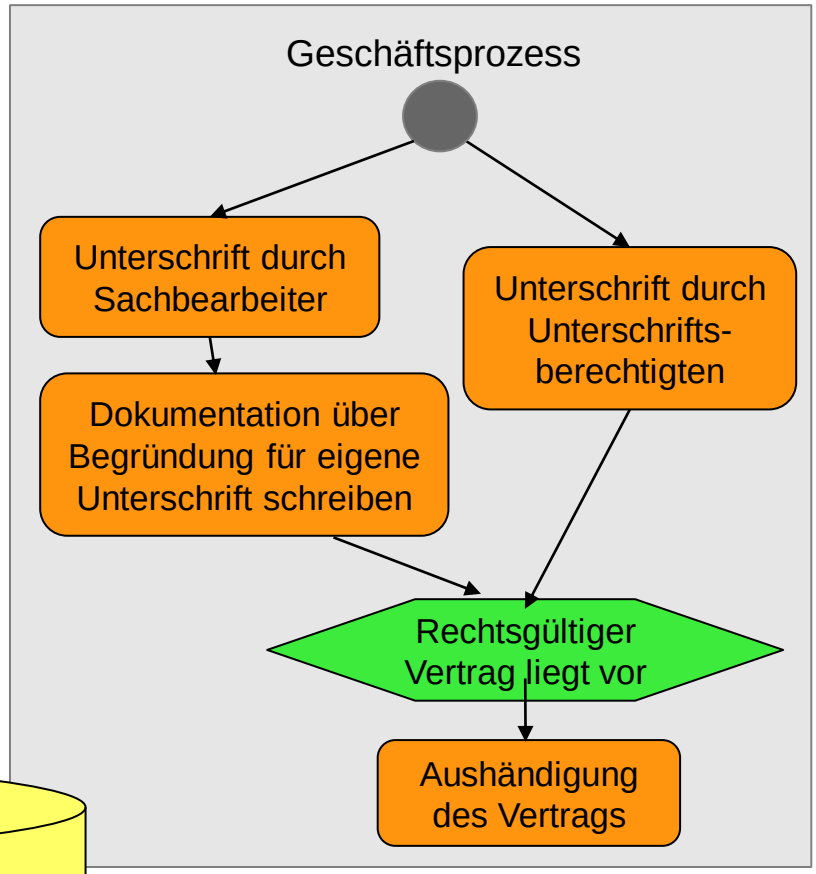
Werden angewendet auf

Werkzeug-Repository:
formalisierte Compliance-Anforderungen

Wenn: Ausnahme von innerbetrieblicher Leitlinie

Unterschrift

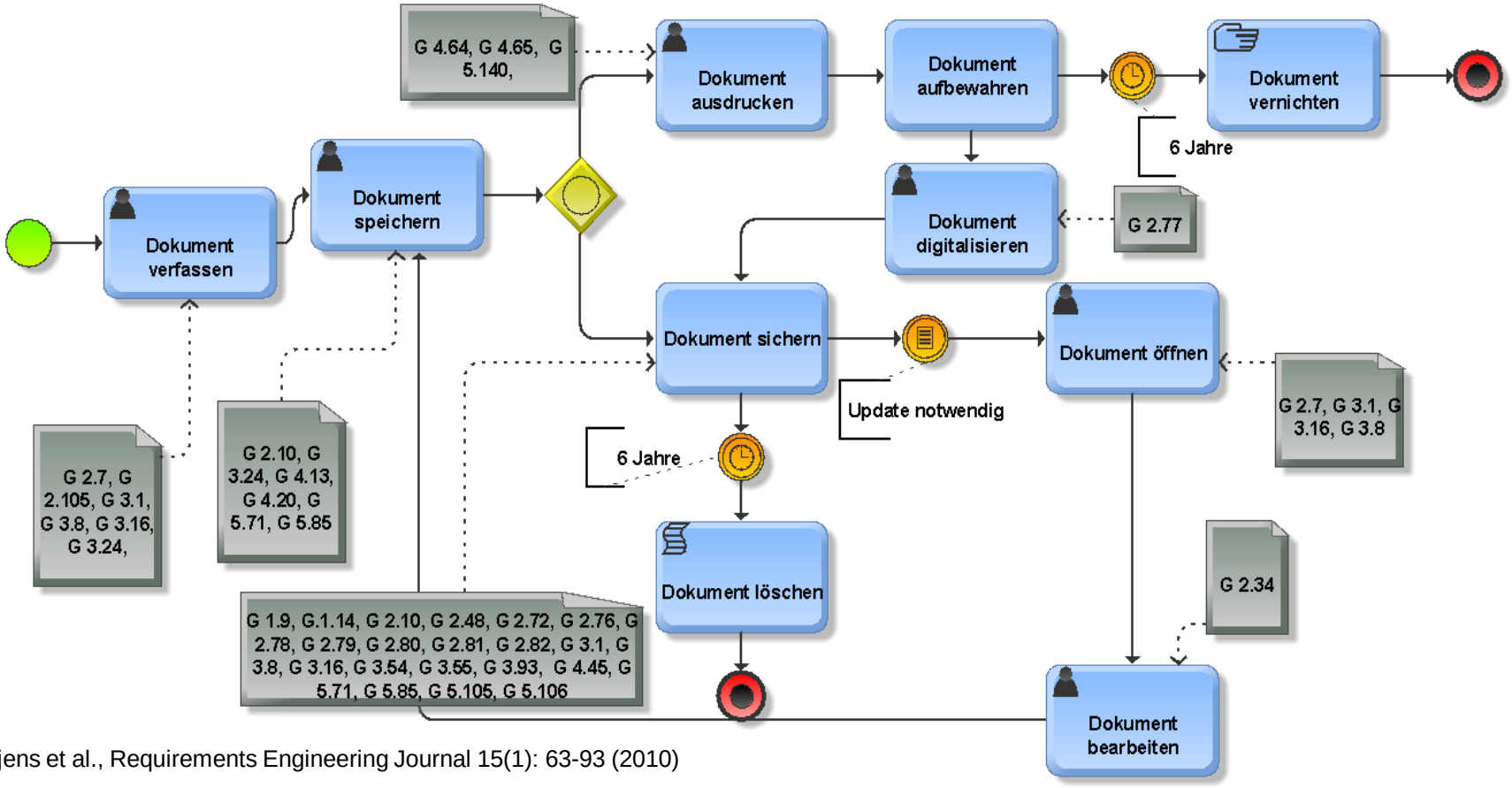
Dann: Begründung für Unterschrift dokumentieren



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

Vorgehen (2): Berücksichtigung von Sicherheitsstandards

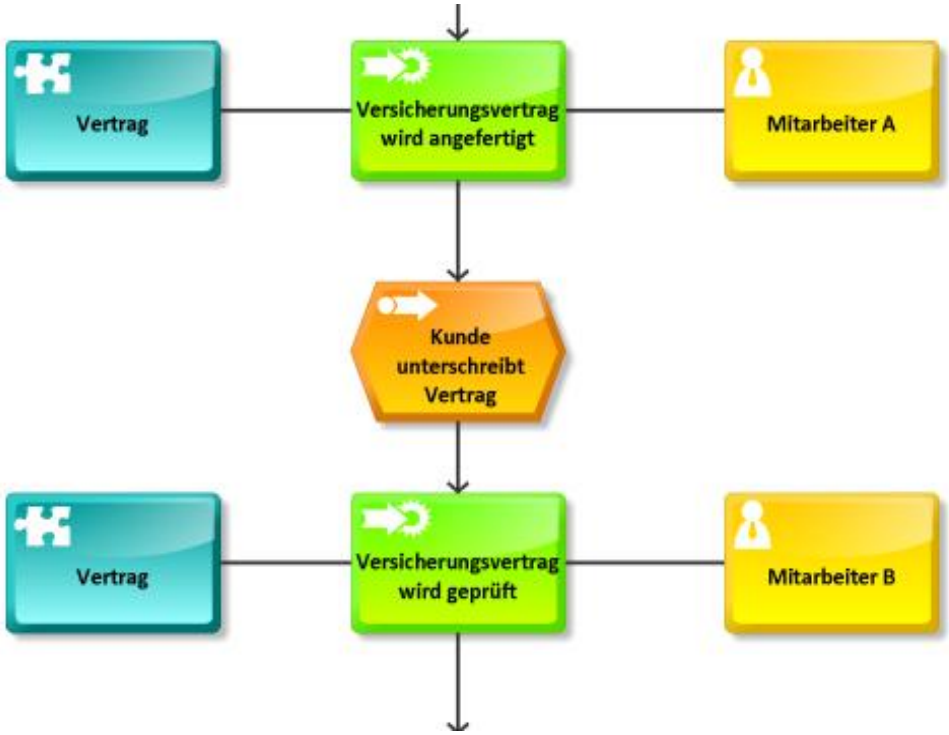
Werkzeuggestützte Annotation von GP-Modellen mit Risiken anhand des BSI-Grundschutzkataloges:



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 (werkzeugintern auf Basis von Formalisierung in Logik erster Stufe).



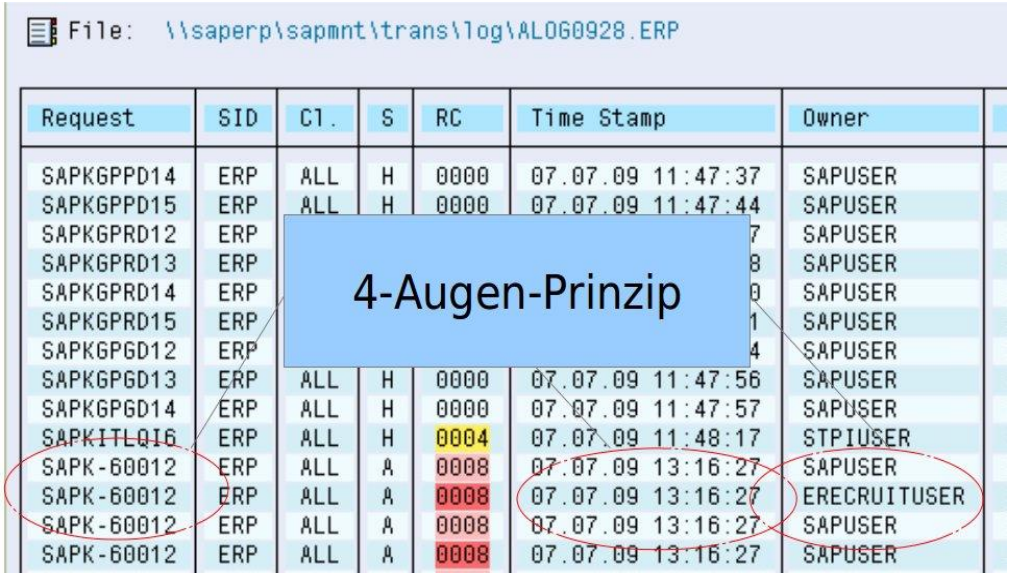
Jürjens et al., Int. Journal on Intelligent Systems 25(8): 813-840 (2010)

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

Beispiel:

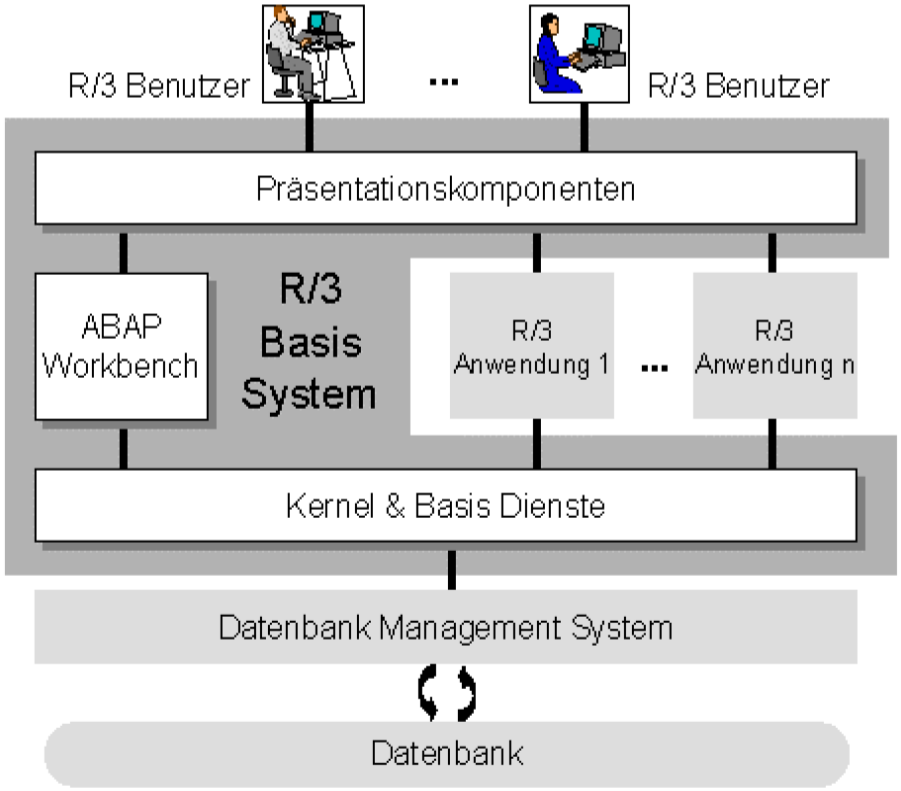
Überprüfung des 4-Augen-Prinzips anhand folgender Informationen:

- 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



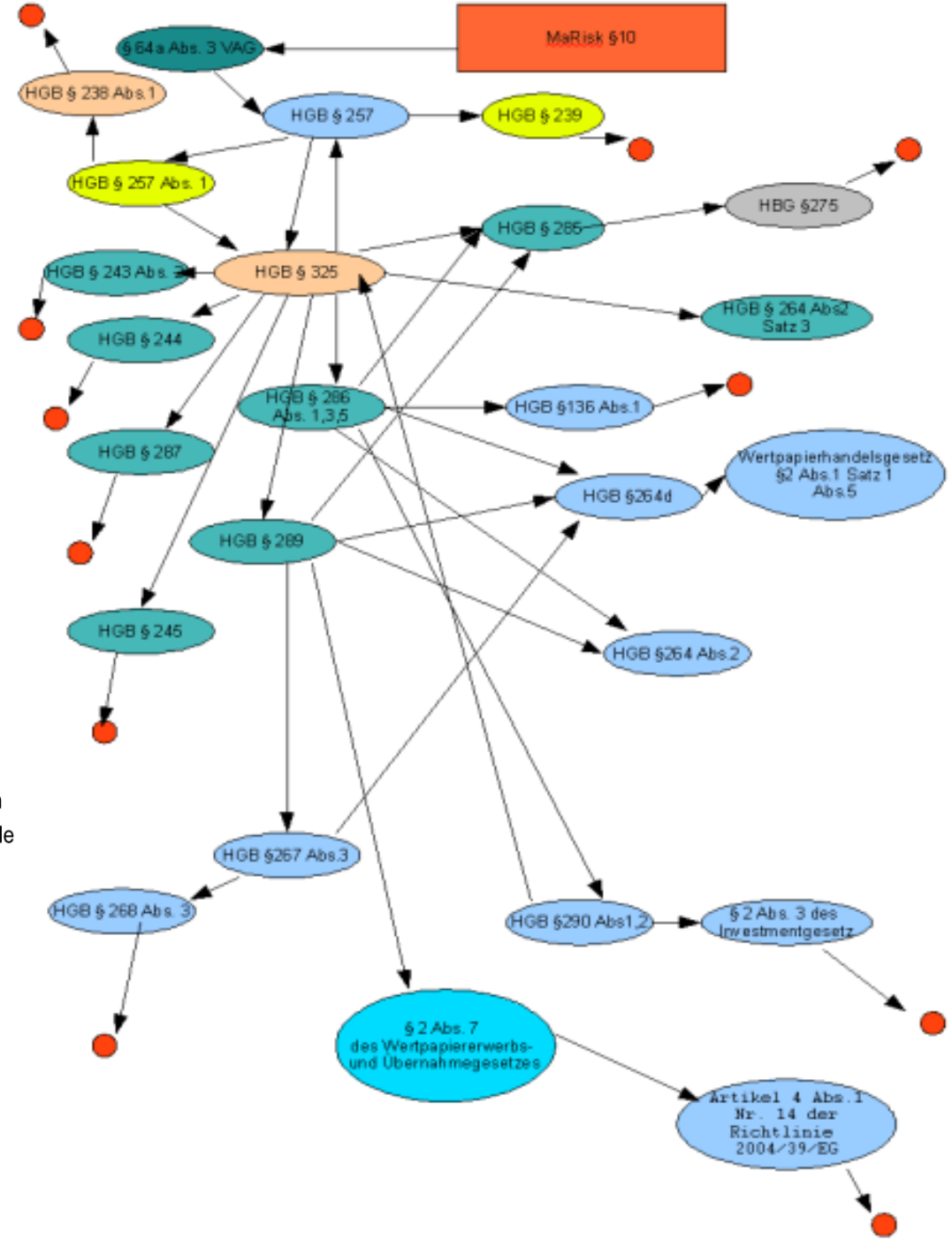
- SAP Berechtigungen auf Sicherheitsregeln prüfen. Geht nicht manuell:
  - Große Datenmengen (z.B. 60.000 Berechtigungen)
  - Komplexe Beziehungen zwischen Berechtigungen (Delegation)
  - Dynamische Änderungen (Urlaubsvertretung etc.)
- Automatische Analyse auf Produktionskopie erhöht Vertrauenswürdigkeit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

Compliance-Repository

- Werkzeuginternes Repository für Abbildung von Compliance- auf Sicherheits-Anforderungen
- Berücksichtigung von Verweisen. Hier als Beispiel: ausgehend von MA-Risk VA

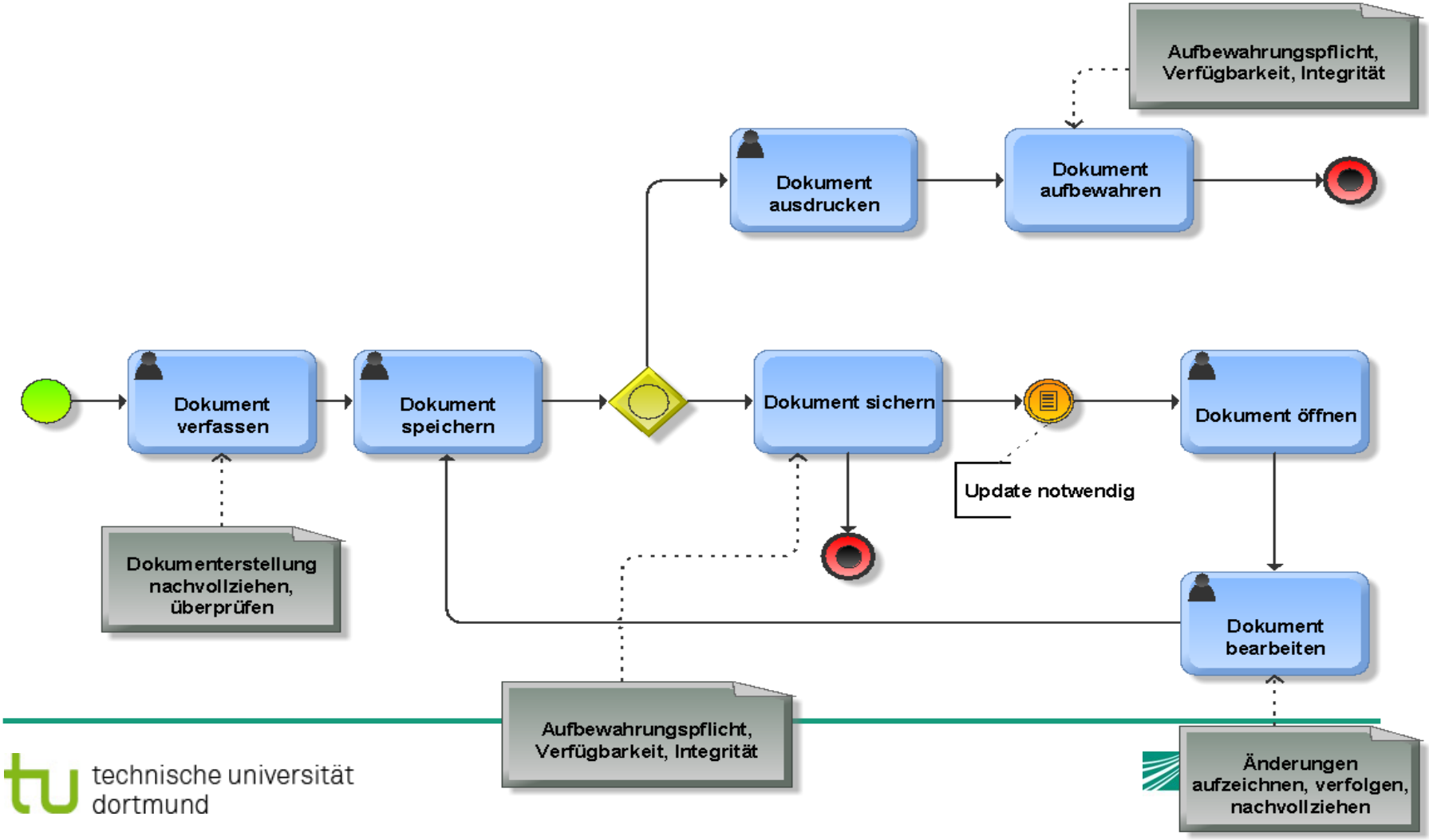
Alle für die Funktionsfähigkeit des Risikomanagements wesentlichen Informationen müssen den Entscheidungsträgern exakt und vollständig zur Verfügung stehen. Wie gesteuert werden soll, ist dabei in Abstimmung mit der Strategie des Unternehmens festzulegen. Hinsichtlich der Dokumentation gelten die Anforderungen 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



Beispiel

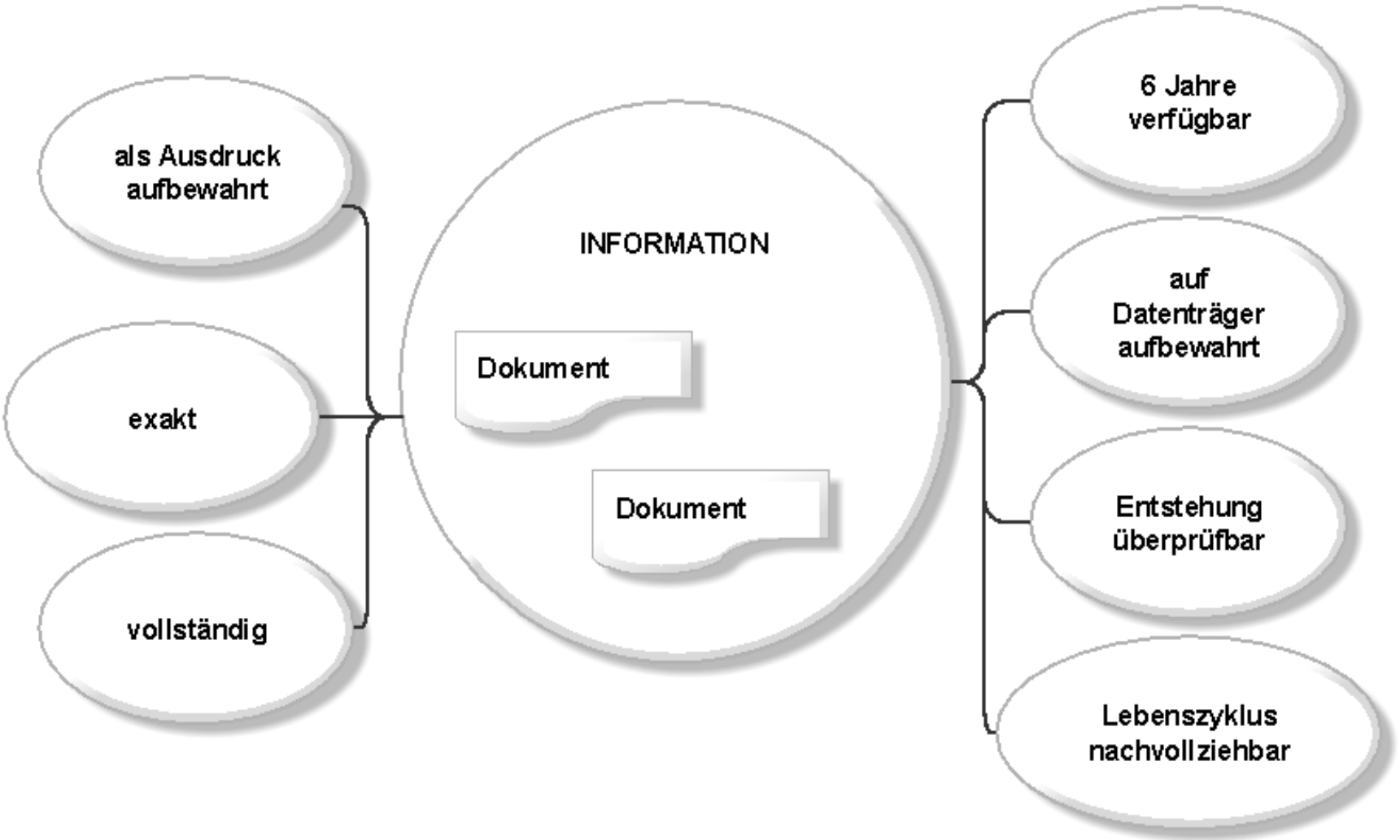
- BPMN-Geschäftsprozess „Dokumentieren“ annotiert mit Sicherheitsanforderungen resultierend aus MARisk VA



Beispiel-GP vs. 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

Ma-Risk VA 10: Dokumenten-Management



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					

Anwendung: Internes Informationssystem

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

[ICSE 07]

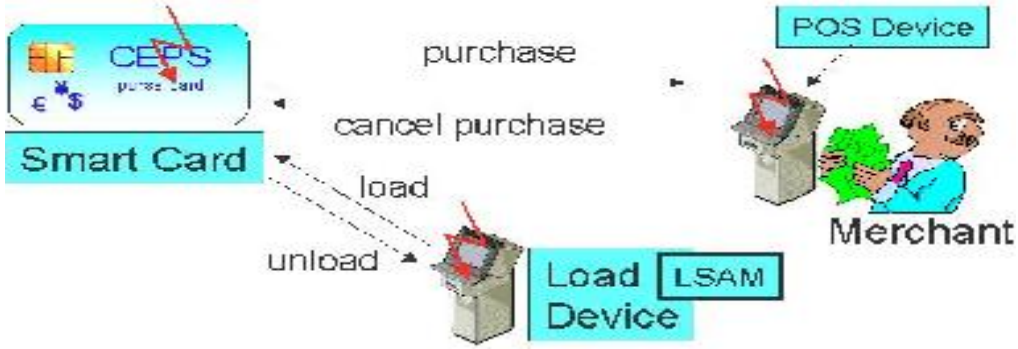
- Über 1.000 potentielle Benutzer, 280.000 Dokumente, 20.000 Anfragen pro Tag.
- Nahtlos in unternehmensweite Sicherheitsarchitektur integriert. Bietet Sicherheitsdienste für Anwen-dungen (Benutzerauthentisierung, rollenbasierte Zugangskontrolle, globales Single-Sign-On), Ansatzpunkte für weitere Sicherheitsdienste.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

Anwendung: Mobiles Bezahlsystem

Common Electronic Purse Specifications:
Globaler Standard für eGeldbörsen (Visa et al.).

Smartcard enthält Kontostand, sichert Transaktionen mithilfe Krypto.

Formale Analyse von Load und Purchase Protokollen:
signifikante Schwachstellen: Kauf-Umleitung, Betrug Ladegerätbetreiber vs. Bank.



Anwendung: Biometrische Authentisierung

Smartcard basiertes System.

Analysiert mit UMLsec parallel zur Entwicklung durch Firma in gemeinsamem Projekt.

Entdeckten drei signifikante Schwachstellen in verschiedenen Versionen (Fehlbedienungszähler umgangen durch Löschen / Wiederholen von Nachrichten; Smartcard unzureichend authentisiert durch Mischen von Sitzungen).

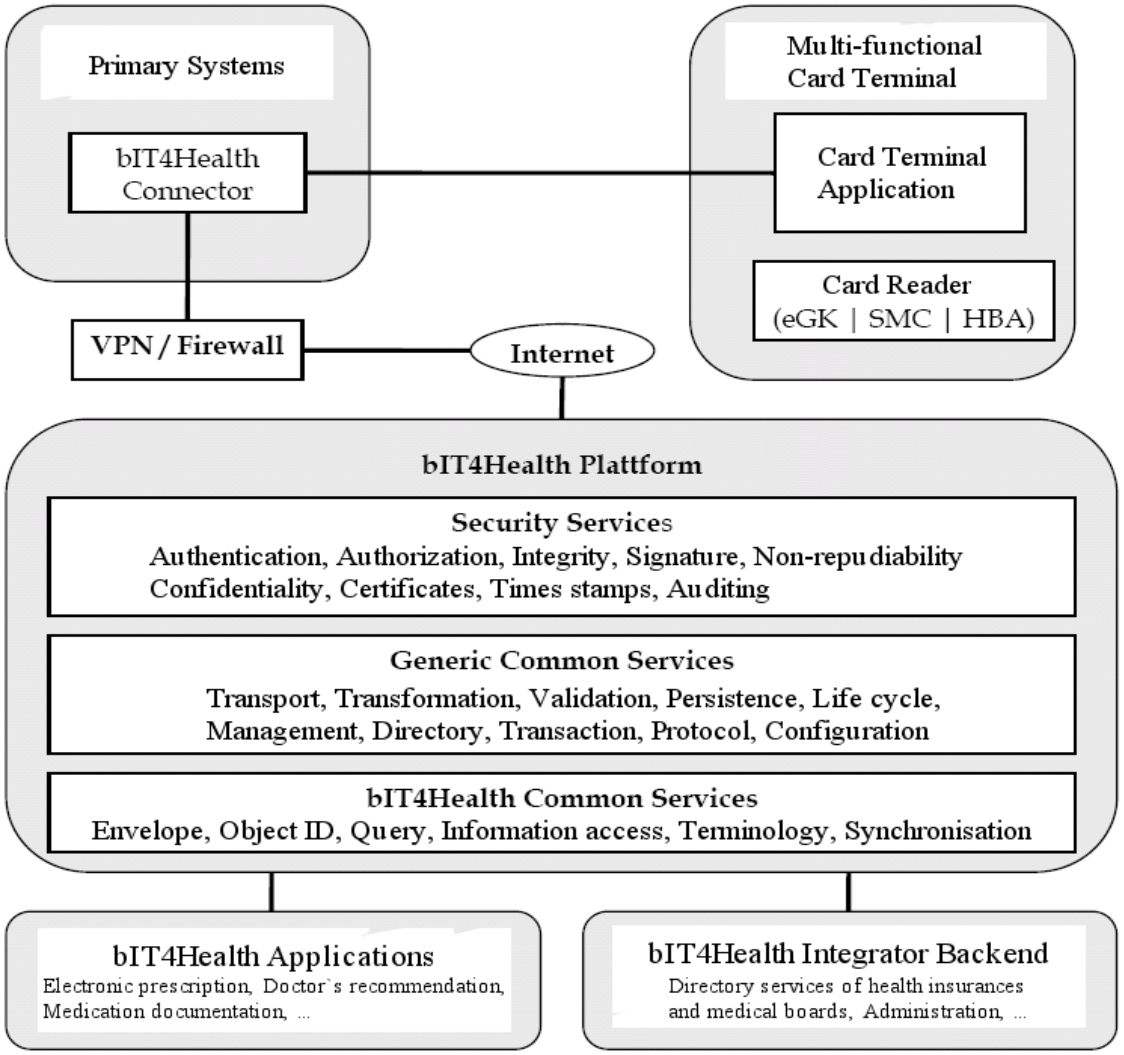
Endgültig entwickelte Version sicher.

Informationssysteme im Gesundheitsbereich: Die Gesundheitskarte

Architektur mit UMLsec analysiert

Einige Schwachstellen aufgedeckt (fehlender Vertraulichkeits-schutz für digitale Rezepte)

[Meth. Inform. Medicine 08]



Bank-Informationssystem bei der HVB

Modellbasierte Sicherheitsanalyse von webbasierter Bankanwendung (“digitaler Formularschrank”).

Geschichtete Architektur (SSL Protokoll, darauf Client Authentisierungs-Protokoll)

Anforderungen:

Vertraulichkeit

Authentisierung

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

Leistungen / Angebote des Fraunhofer ISST

- Vorbereitung und Durchführung von Compliance-Checks
- Erstellung von Compliance-Berichten
- Sicherheits- und Compliance-Analysen von Geschäftsprozessen (auf Basis der Prozessdokumentation falls vorhanden oder anhand von Interviews)
- Data Mining auf Log-Dateien zur Gewinnung von Geschäftsprozessmodellen
  - Compliance-Analysis der Prozessausführung
  - Automatische Generierung von Prozessmodellen

NB: Möglichkeit der Unterstützung als Pilotkunden in öffentlich geförderten Projekten.

Kooperationsmöglichkeiten

Unser Ansatz wird im Rahmen von öffentlich geförderten Forschungs- und Entwicklungsprojekten kontinuierlich weiterentwickelt. In diesem Zusammenhang gibt es verschiedene Kooperationsmöglichkeiten (ebenfalls öffentlich gefördert):

- Technologiepartner: Bei Interesse an einer Integration unseres Ansatzes mit der Methodik bzw. vorhandenen Werkzeugen zur Compliance- / Sicherheitsanalyse Ihres Unternehmens: Kooperation als gemeinsame Technologiepartner.
- Pilotanwender: Bei Interesse an einer Kooperation in einer Pilot-Anwendung neu entwickelter Ansätze und Werkzeuge: Kooperation als Pilotanwender.

Sprechen Sie mich an !

Zusammenfassung: Compliance & Sicherheit

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

Ansatz: Automatisierte Sicherheits- und Compliance-Analysen auf Basis von Textdokumenten, Schnittstellen-Spezifikationen, Geschäftsprozess-Modellen, Log-Daten und anderen Datenquellen.

Ergebnisse: Erfolgreicher Einsatz in Anwendungsprojekten.

Aktuelle Arbeiten:

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

Angebote: Durchführung von Sicherheits- / Complianceanalysen; Kooperation als Technologiepartner / Pilotanwender in öffentlich geförderten Projekten.

Kontakt: jan.juerjens@isst.fraunhofer.de

Compliance-Report

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

Herzlichen Dank für Ihre Fragen !

Kontakt: jan.juerjens@isst.fraunhofer.de