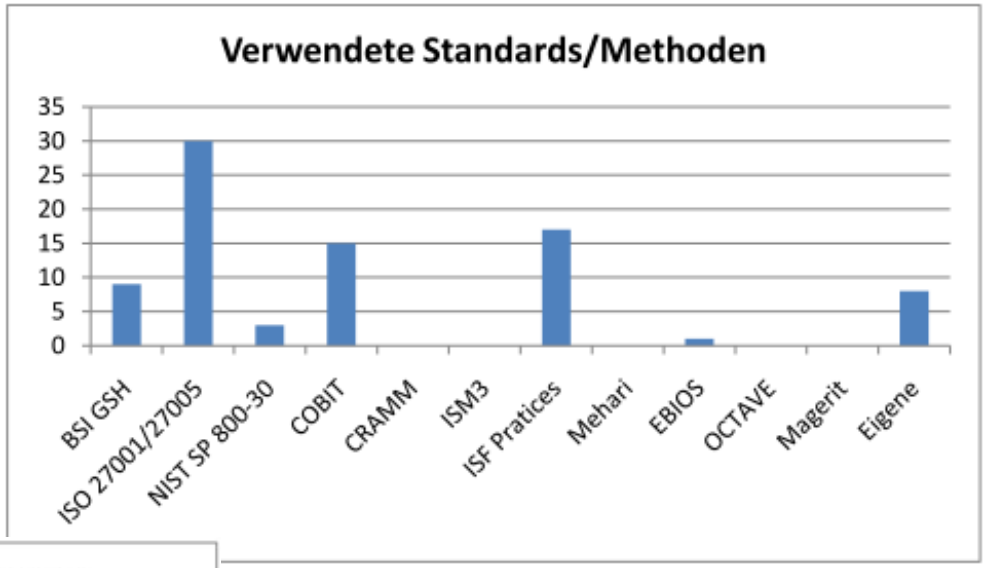
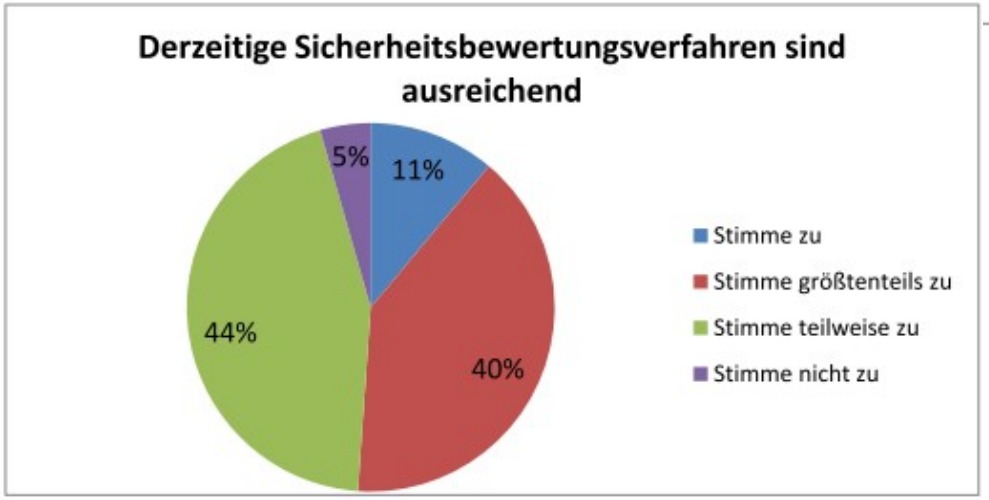
Werkzeuggestützte Identifikation von IT-Sicherheitsrisiken in Geschäftsprozessmodellen

Marc Peschke (Softlution)
Martin Hirsch (FH Dortmund)
Jan Jürjens (Fraunhofer ISST und TU Dortmund)
Stephan Braun (TU Dortmund)

Studie zu IT-Sicherheits-Risikomanagement I
(Stefan Taubenberger)

Derzeitige Risiko-bewertungsverfahren und -methoden sind nicht ausreichend





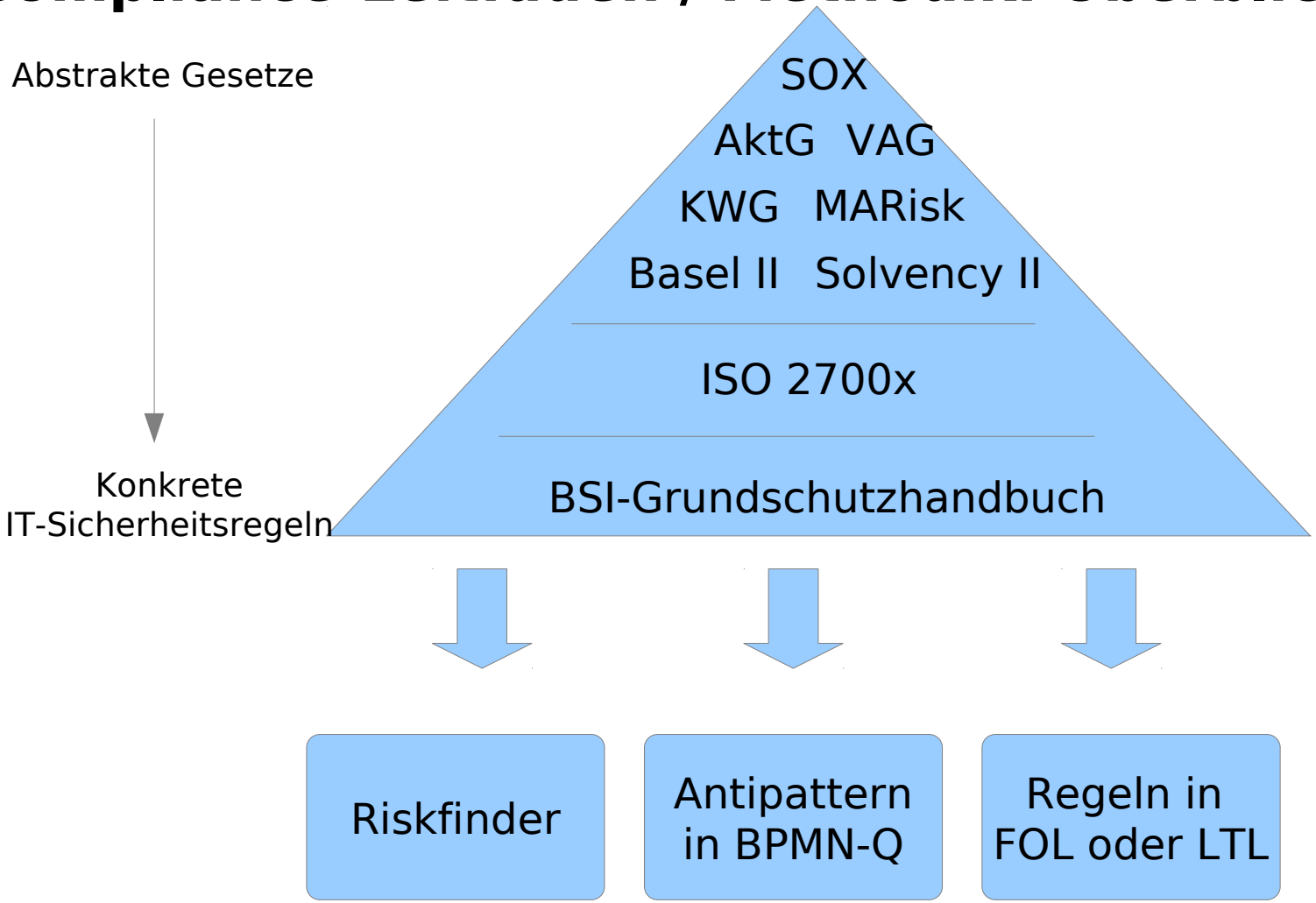
Idee: Geschäftsprozessbasierte Sicherheits-Risikoanalyse

- Entwicklung einer werkzeuggestützten Methode zur Abbildung von Geschäftsprozessen auf IT-Infrastrukturen unter Berücksichtigung von Governance-Risk-Compliance-Anforderungen (vgl. Basel II, Solvency II, ...).
- Analysen erfolgen auf der Basis von Textdokumenten, Schnittstellenspezifikationen, GP-Modellen, Log-Dateien etc
- Automatisierte Analyse auf operationale Risiken
  - Kategorisierung und automatische Risiko-Identifikation sowie -Bewertung
  - Integration mit weiteren Compliance- bzw. Betrugserkennungs-relevanten Analyse-Werkzeugen möglich

Vorteile

- Automatisierung von Standard GRC Aufgaben
  - RoI durch Reduzierung der manuellen Arbeiten
  - Fokussierung der Experten auf Spezialfälle
- Erstellung einer GRC Informationsbasis für Unternehmen
  - Datenquellen: Interviews, Text und Process Mining, Prozesse
- Bewertung von Risikomanagementkonzepten
  - Teilautomatisiert durch APEX Framework
- Hilfestellung bei Maßnahmen zur GRC Überwachung
  - Implementierung von Monitoring Tool z.B. in Web-Portalen
- Daten können ebenfalls im BPM Bereich eingesetzt werden

Compliance-Leitfaden / Methodik: Überblick



Beispiel: Anwendung der MaRisk VA und BSI-Grundschutz

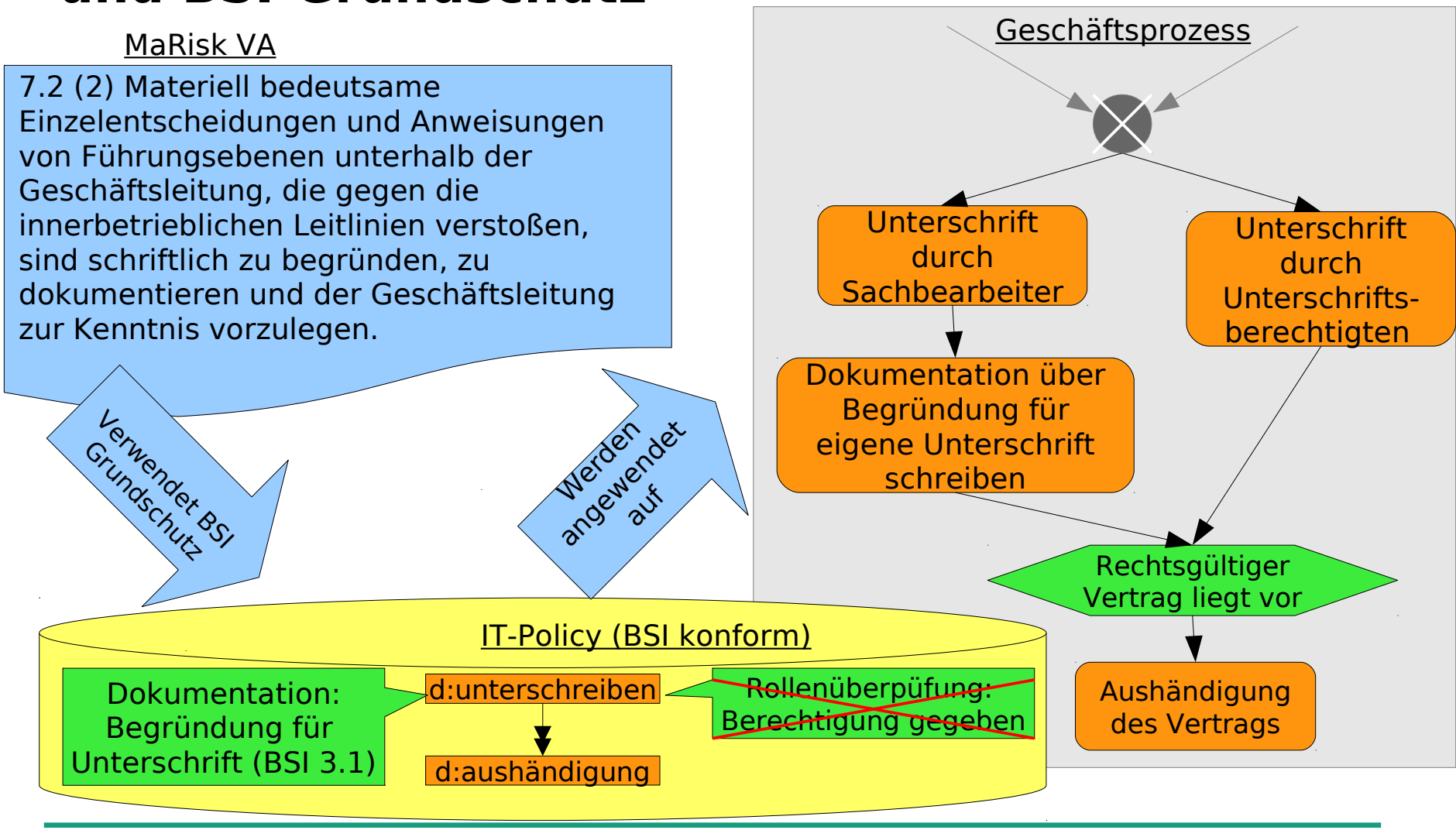
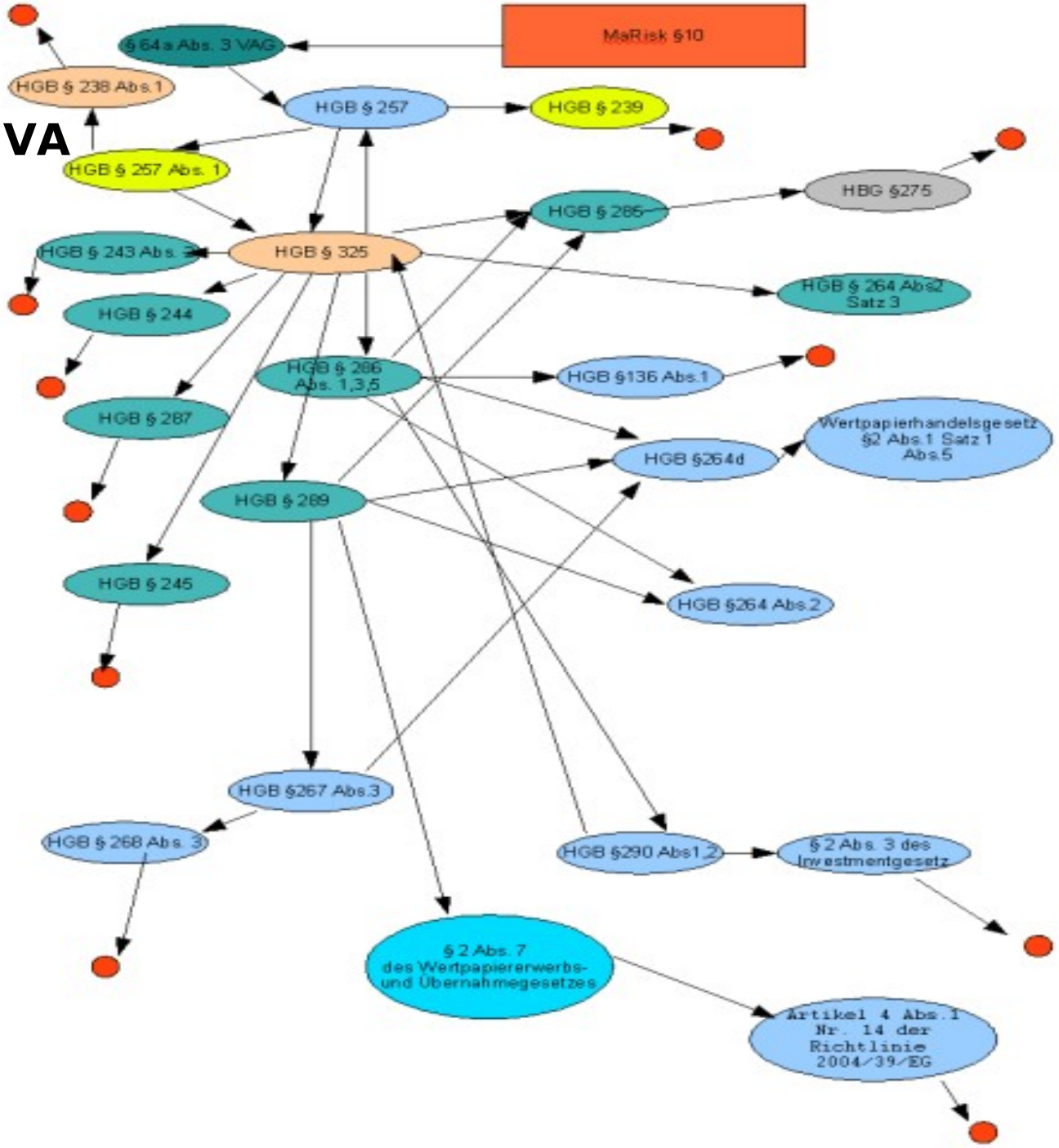


Abbildung MA-Risk VA auf Sicherheits-anforderungen

- Framework zur Abbildung von regulatorischer Compliance auf Security Policies
- Berücksichtigung von Cross-References ausgehend von MA-Risk VA

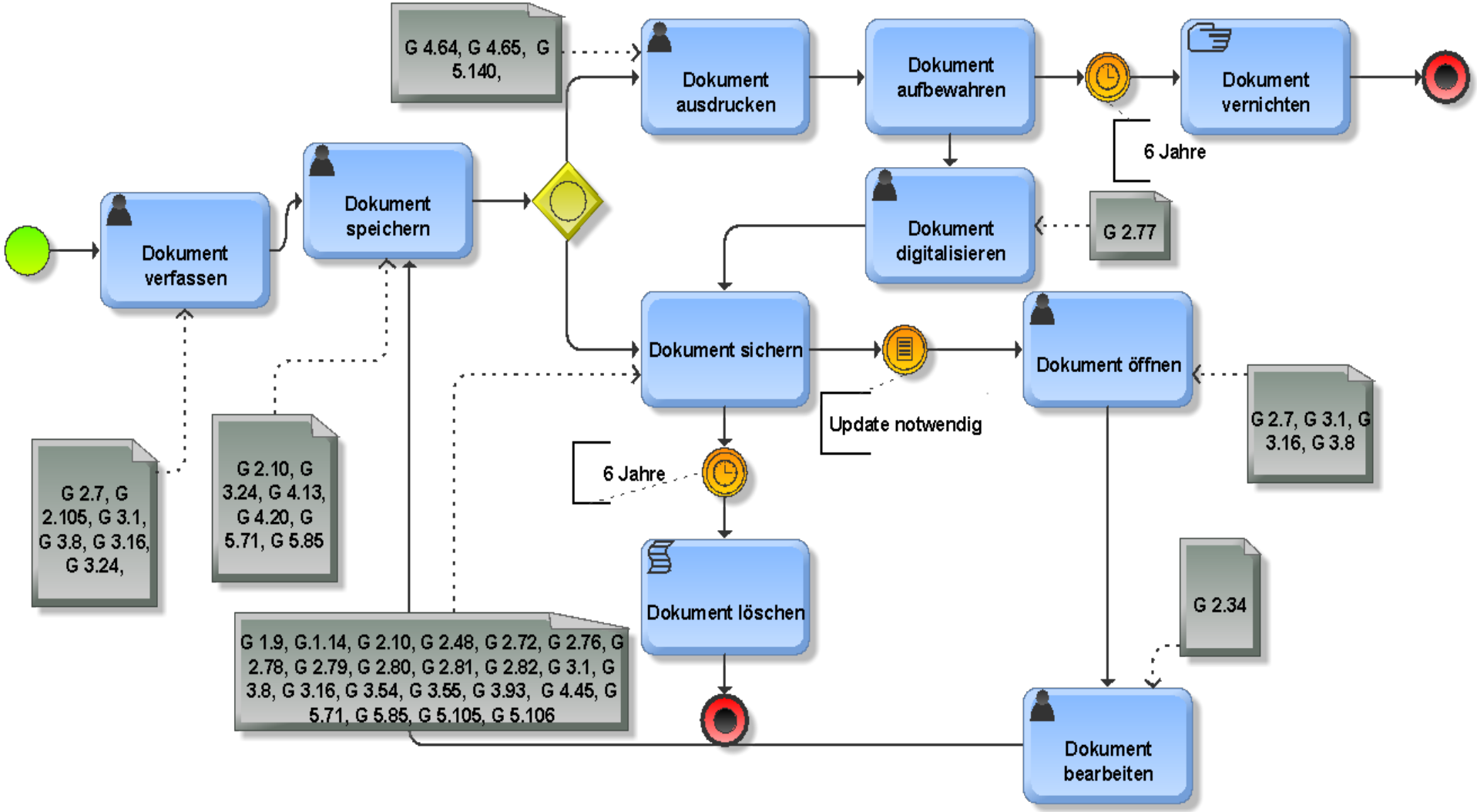


Ergebnis der Anwendung auf MaRisk VA §10

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 verwal-ten	Daten überprüfbar, lesbar	Verfügbarkeit
HGB §239	Ausgedruckte Doku-mente verwalten	Dokumente verfügbar	Verfügbarkeit

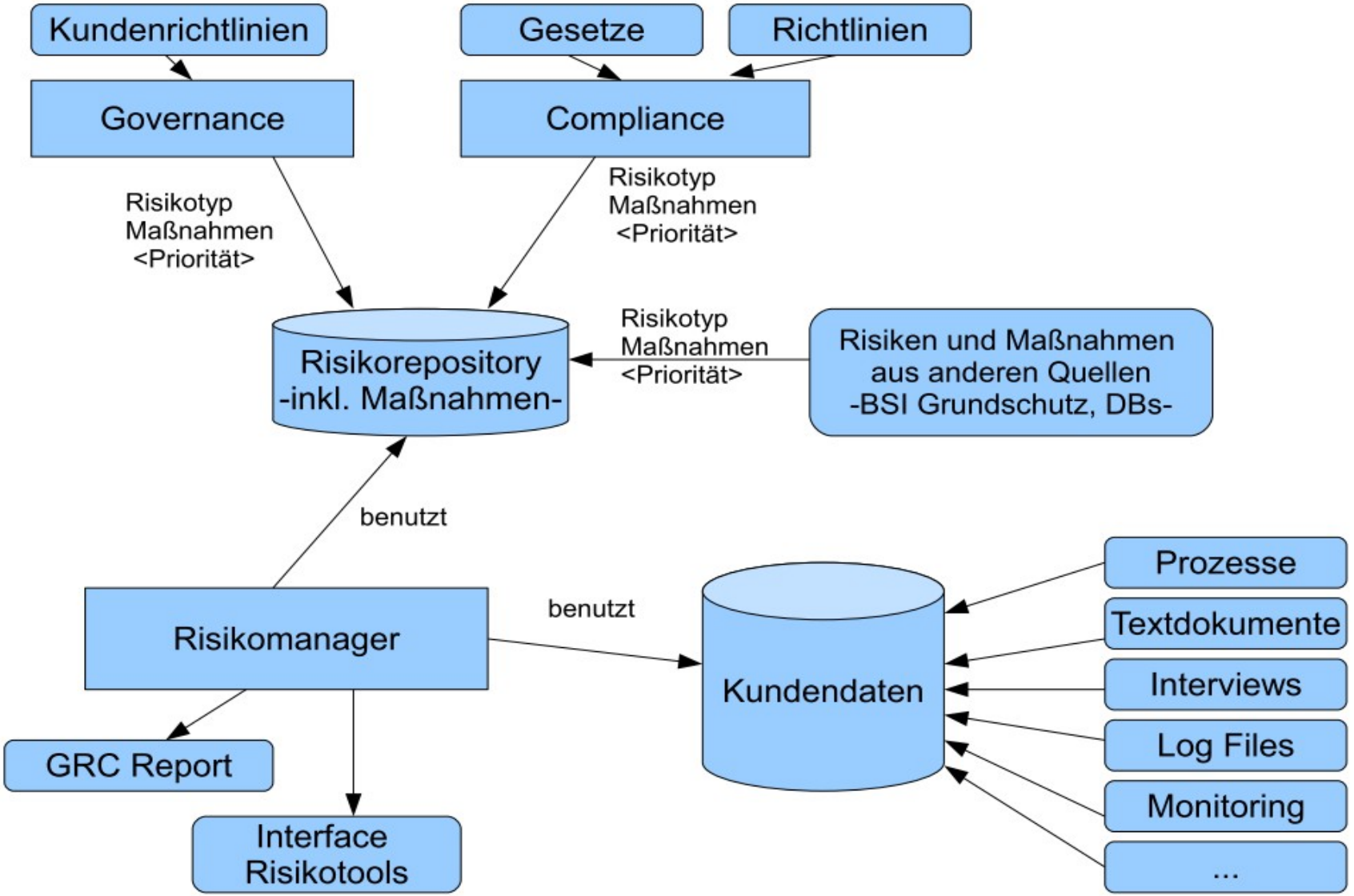
Beispiel: Prozess

- Aus Sicherheitsanforderungen konkret abgeleitete Gefahren anhand des BSI-Grundschutzkataloges



Werkzeug-Framework

Download: http://carisma.umlsec.de
Demo: http://www-jj.cs.tu-dortmund.de/jj/umlsectool/UMLsec-architecture-overview/gesamtablauf_de.html



Benefit

Ergebnis: Compliance-Report:

- Compliant nach (z.B.:) MaRISK VA (ja / nein)
- Eventuell nicht eingehaltene Vorschriften
- Mögliche Maßnahmen zur Behebung der Verstöße
  - Automatische Korrektur
  - Manuelle Korrektur

Compliance-Report

Compliant: NEIN

Verstöße:
- MaRISK VA 7.2: Einhaltung von BSI G3.1 nicht erfüllt

Maßnahmen:
- BSI Maßnahmenkatalog M 2.62

Einige Anwendungsprojekte mit Industriepartnern

- Gesundheitskarte: Architektur mit UMLsec untersucht, Schwachstellen aufgedeckt
- Sicherheits-Policen für mobile Architekturen
- Digitaler Formularschrank (HypoVereinsbank)
- Common Electronic Purse Specifications (Globaler Standard für elektr. Geldbörsen): mehrere Schwachstellen aufgedeckt
- Internes Informationssysteme (BMW)
- Return-on-Security Investment Abschätzung
- Analyse Digitale-Signatur-Architektur (Allianz)
- IT-Sicherheits-Risikomodellierung (Infineon)
- Smart-card Software-Update Plattform (Gemalto)

Aktuell:

- Cloud-Anwender Sicherheitsanalyse (adMERITia, LinogistiX)

Geplant:

- Cloud-Anbieter Sicherheitsanalyse (TÜV-IT, Itesys, LinogistiX)
- Sicherheitsökonomische Analysen (ATOS Origin u.a.)

Zusammenfassung

Alleinstellungsmerkmale des Apex Frameworks:

- Kostenreduzierung durch Automatisierung und Konvergenz der GRC-Aktivitäten
- Automatisierte Risiko-Identifikation
- Erstellung einer individuellen Risiko- und Maßnahmen-Datenbank für Kunden aus verschiedenen Datenquellen: Textdokumenten, Prozessen, Logfiles, Interviews, ...
- Automatisierter Abgleich von GRC-Regeln mit den erfassten Risikodaten und Maßnahmen
- Unterschiedliche Inputs möglich (Textdateien, Logfiles, Modelle)
- System-übergreifend und Plattform-unabhängig

Kontakt: http://jan.jurjens.de