

---

# Sicherheit und Compliance für IT-gestützte Prozesse

Jan Jürjens, TU Dortmund und Fraunhofer ISST

---

TU Dortmund, Fak. Informatik: Round-Table, 14. Dezember 2010

# Sicherheit und Compliance für IT-gestützte Prozesse

- Zunehmende Regulierungsanforderungen an Unternehmens-IT:
  - z.B. Versicherungen: Solvency-II (bis 2012)  
=> Mindestanforderungen an Risikomanagement (MaRisk VA)
  - Ähnlich in anderen Branchen (Banken: Basel II / III und MaRisk BA, allgemein: KontraG, US: Sarbanes-Oxley)
- Insbesondere steigende Anforderungen, die Etablierung eines adäquaten Risikomanagements gegenüber relevanten Regulierungsautoritäten (BAFin) zu demonstrieren: Aufwendige und kostenintensive manuelle Arbeit.
- Derzeitige Risikomanagementansätze konzentrieren sich oft auf externe Risiken und vernachlässigen das Risiko des Betrugs durch Mitarbeiter (spektakuläres Beispiel: Societe Generale 2008: 5 Mrd Euro Schaden). Vorhandene Lösungen und Aktivitäten unzureichend untereinander integriert.

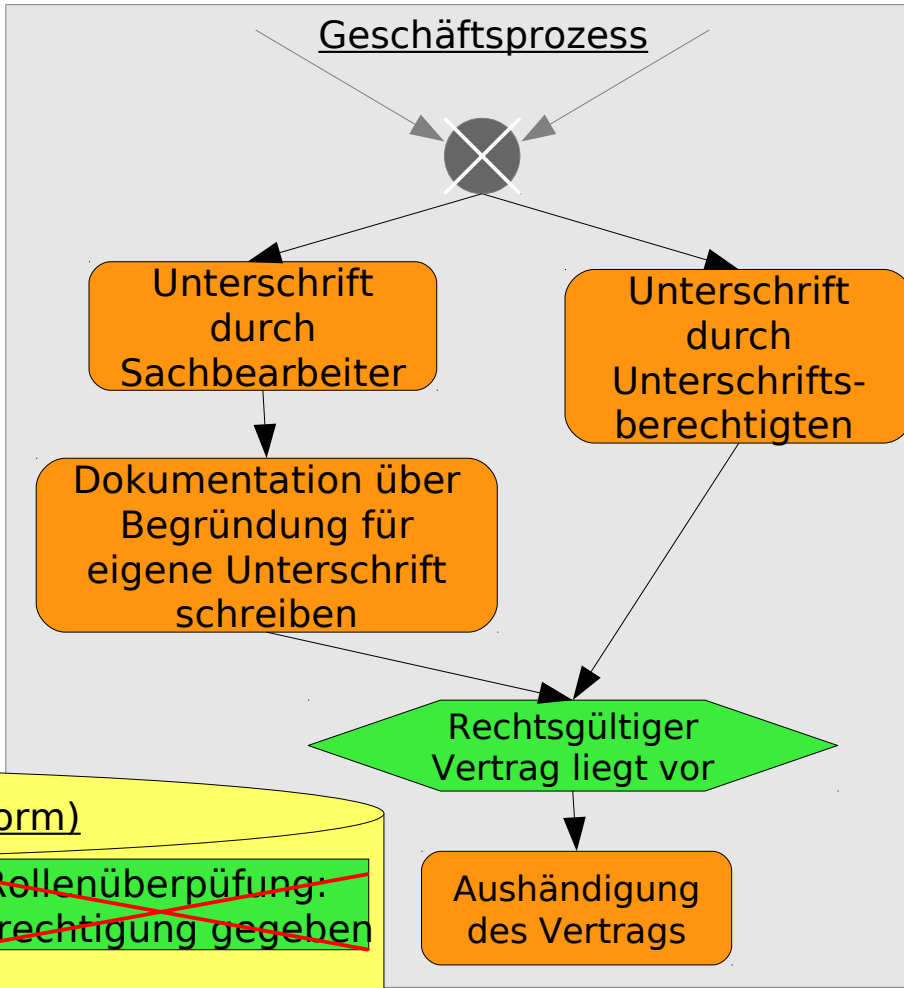
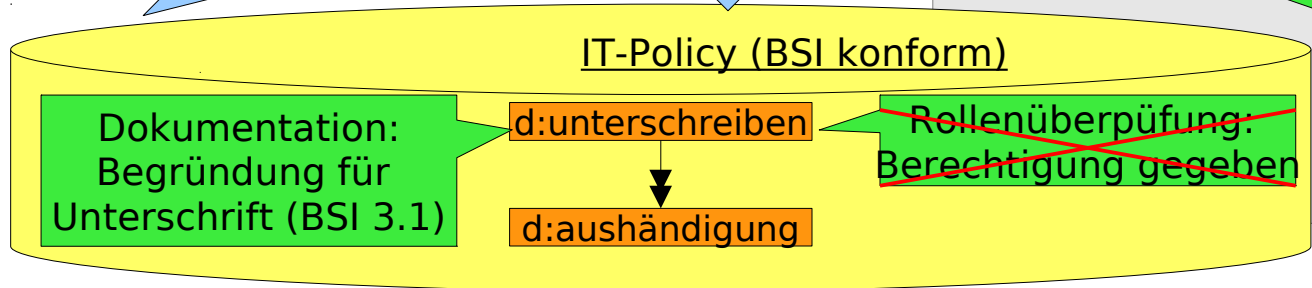
# Beispiel: MaRisk VA vs. BSI-Grundschutz

## 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.

Verwendet BSI Grundschutz

Werden angewendet auf



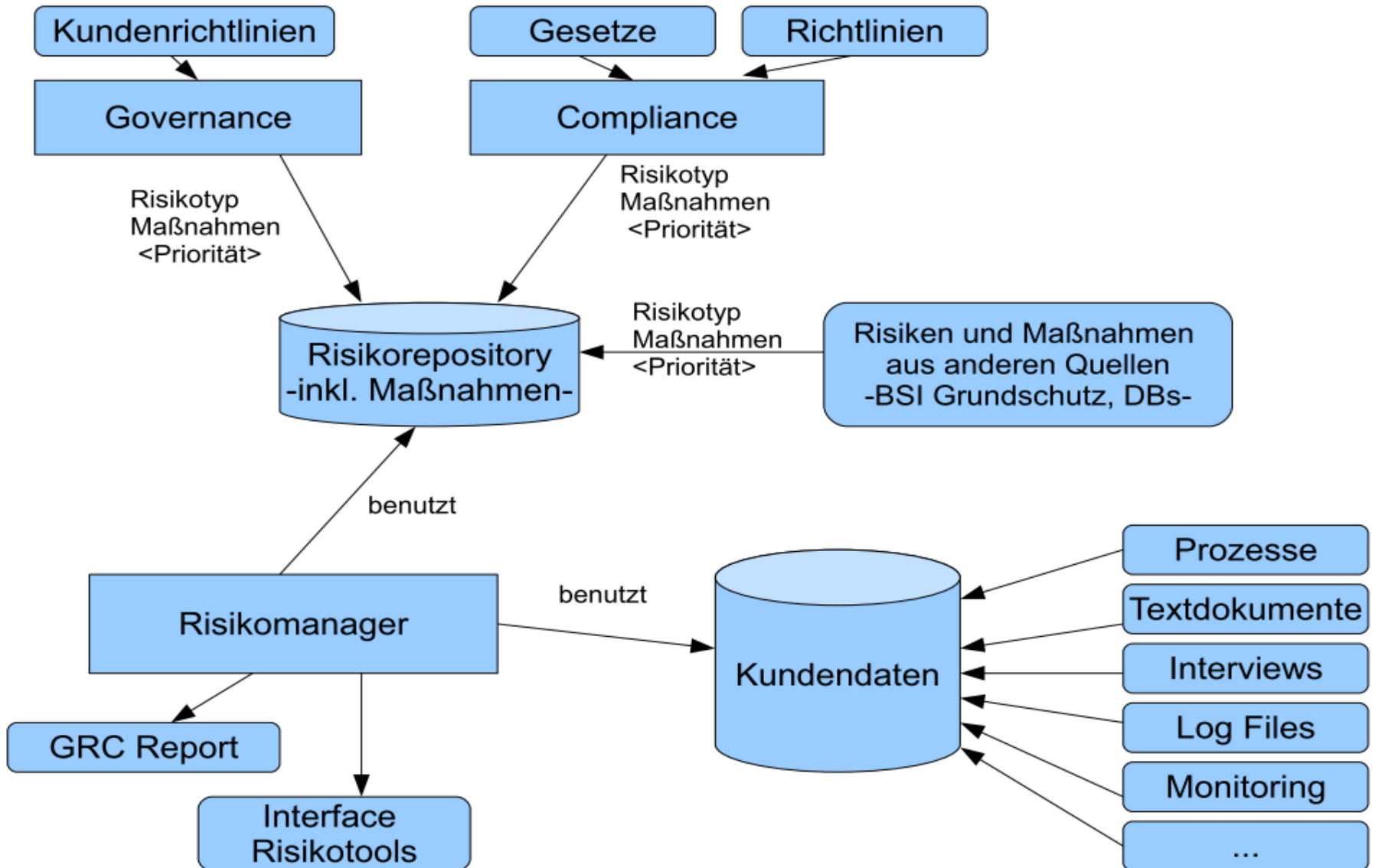
# Projekt: Architectures for Auditable Business Process Execution (APEX)

- Entwicklung einer werkzeuggestützten Methode zur Abbildung von Geschäftsprozessen auf IT-Infrastrukturen unter Berücksichtigung von Governance-Risk-Compliance-Anforderungen (vgl. Basel II, Solvency II, ...).
- Automatische Werkzeugen zur Unterstützung des Risikomanagements und seiner Dokumentation auf Basis von vorhandenen Artefakten (z.B. Textdokumente, Schnittstellenspezifikationen, GP-Modelle, Log-Dateien) bzw. Architekturen (z.B. web-basierte Unternehmensportale).
- Ziel: Kostenersparnis für betroffene Unternehmen durch Automatisierung und Konvergenz von GRC-Aktivitäten.
- Besonderer Schwerpunkt im Versicherungsbereich
- Kooperationen mit Werkzeugherstellern (auch domänenübergreifend)
- Weiterer Schwerpunkt: Cloud-Computing

# Idee des APEX Ansatzes

- 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

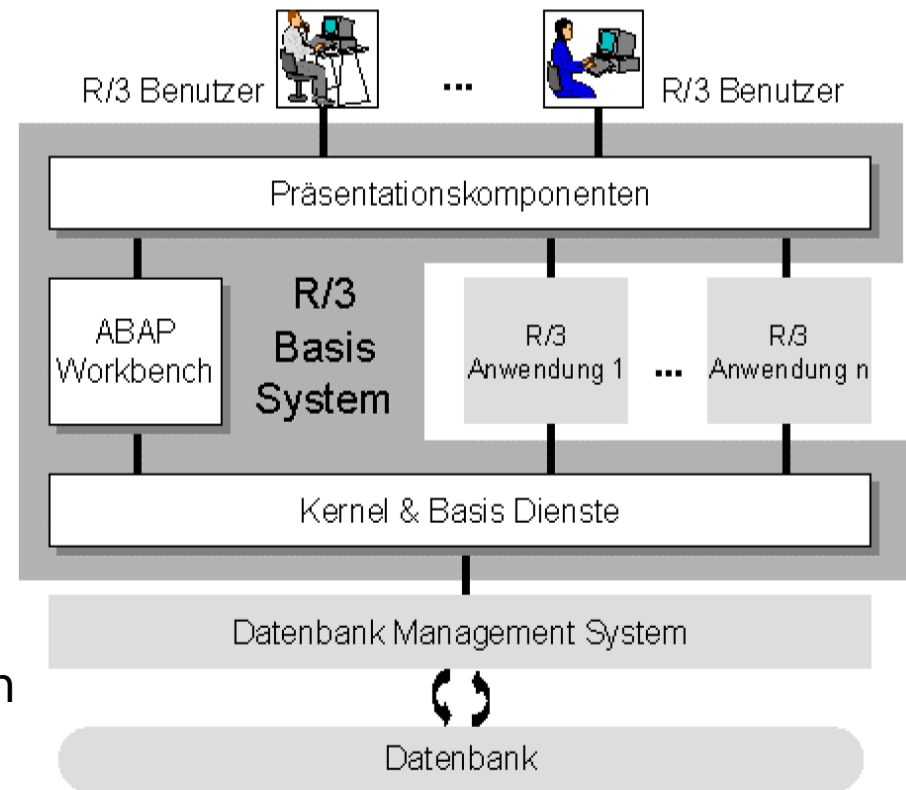
# APEX Framework





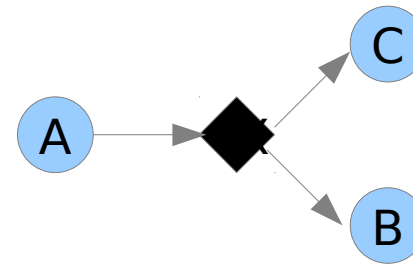
# Analyse von Berechtigungsdaten

- 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.



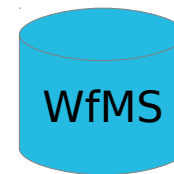
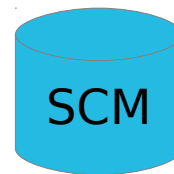
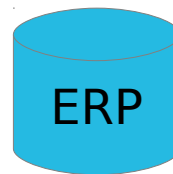
# Business Process Mining: Automatische Extraktion von GP-Dokumentation aus Laufzeitdaten

Analyse auf  
durch  
Reengineering  
gewonnenen  
Prozessen

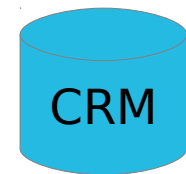


Prozess ID	Aktivitäts ID	Bearbeiter	Zeitstempel
1	A	John	9-3-10:15.01
2	A	Mike	9-3-10:15.12
1	B	Mike	9-3-10:16.07
2	C	Carol	9-3-10:18.25

Eventdaten

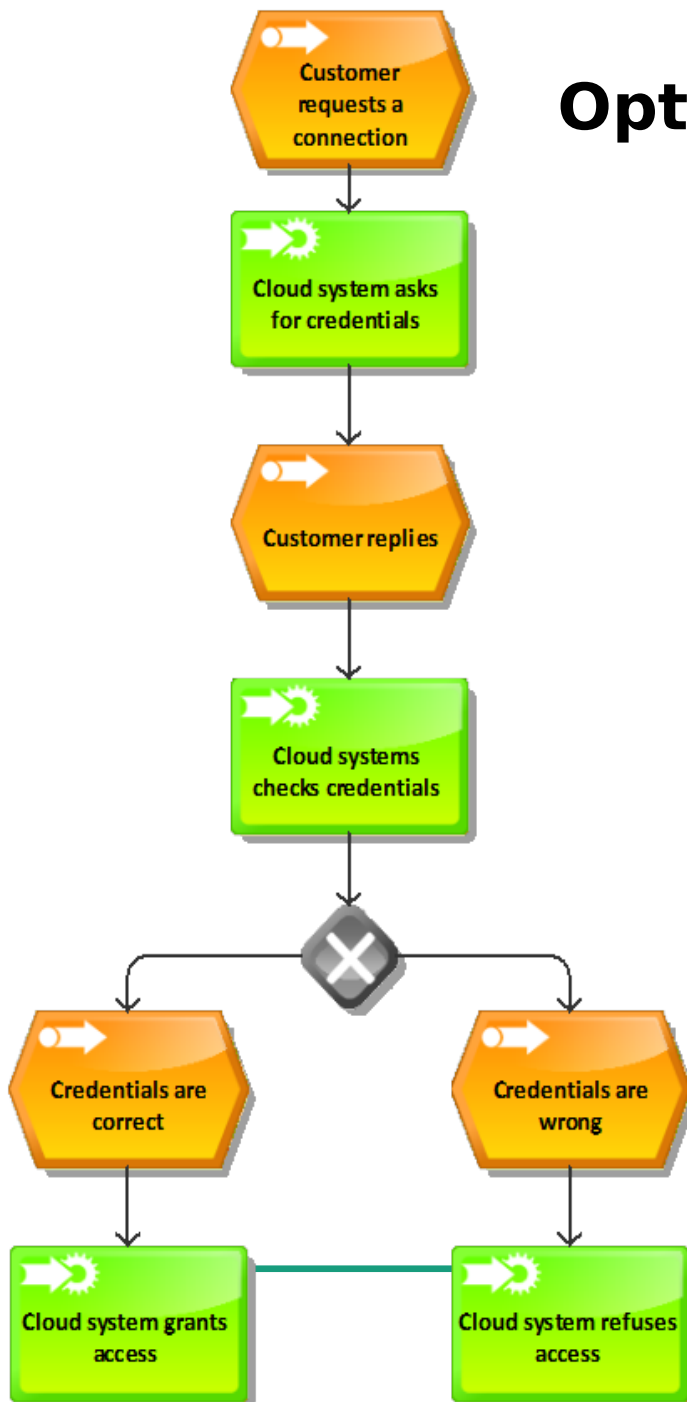


...



# Optional: Modell-Analysen

- Automatische Analyse von Geschäftsprozess-Modellen auf Compliance- und Sicherheitsanforderungen
- Falls GP-Modelle vorhanden oder mit BP-Mining extrahiert
- Zwei Ansätze:
  1. Text-basierte Analyse der Aktivitätsbezeichner zur automatisierten Risikoidentifikation
  2. Struktur-Analyse der Prozessmodelle auf Compliance-Verstoß-Muster



# Benefit

Automatisch generierter Compliance-Report:

- Zum Beispiel: Compliant nach 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

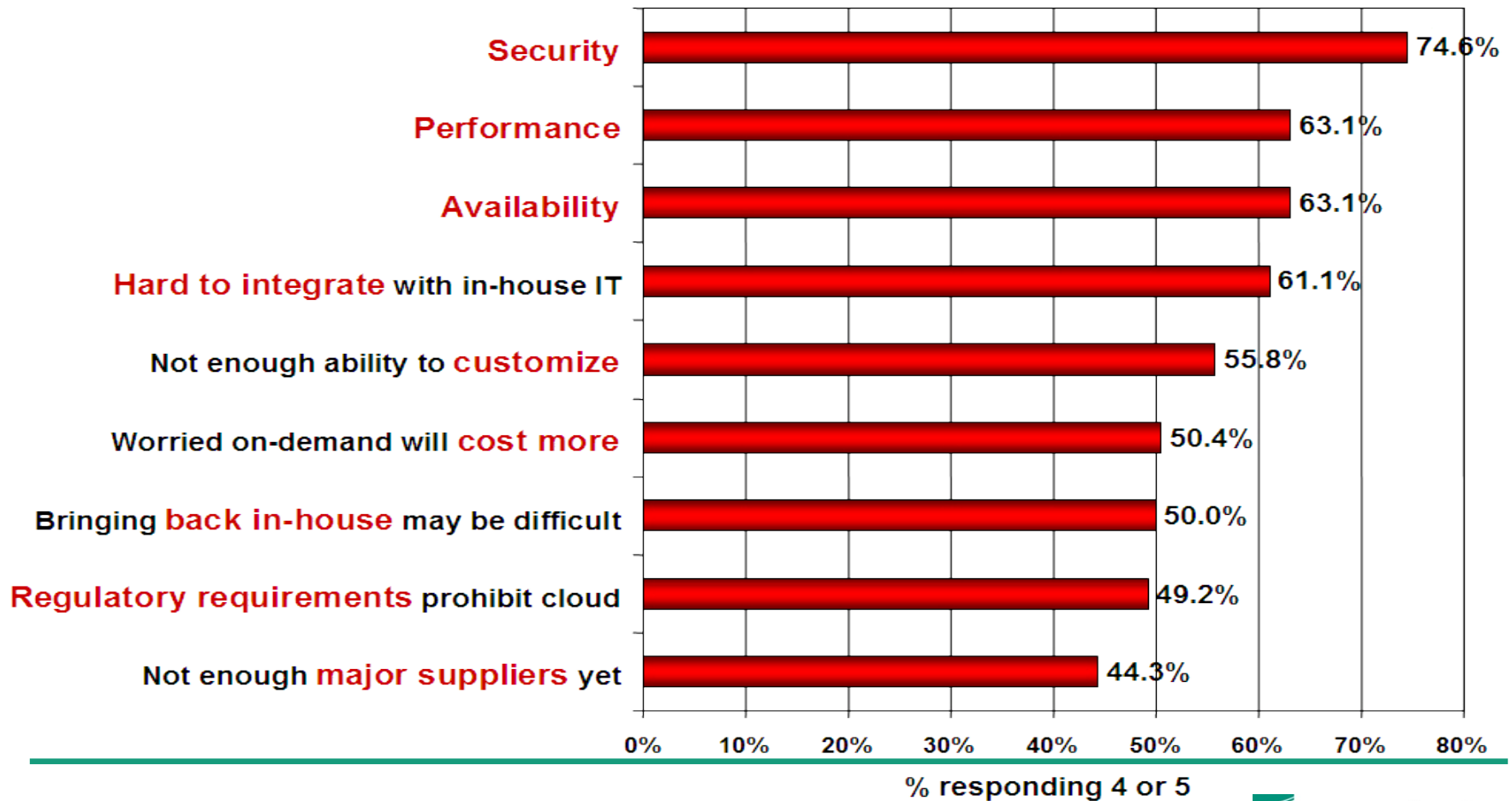
# Anwendungsfall: Cloud Computing

Governance	Risk	Compliance
<ul style="list-style-type: none"><li>■ Policy design</li><li>■ Classification schema for data and processes</li><li>■ Trust chain in a cloud</li></ul>	<ul style="list-style-type: none"><li>■ Risk strategy</li><li>■ Business Impact Analysis</li><li>■ Threat and Vulnerability Analysis</li><li>■ Risk Analysis Remediation</li></ul>	<ul style="list-style-type: none"><li>■ Policy enforcement</li><li>■ Legal compliance (SOX, SOLVENCY II)</li><li>■ Control implementation</li></ul>

The Cloud offers dynamic resource allocation  
→ For GRC in clouds we require the same dynamic

# Security & Compliance sind „Showstopper“

Q: Rate the **challenges/issues** ascribed to the 'cloud'/on-demand model  
(1=not significant, 5=very significant)



# Mögliche Kooperationen - Angebot

- Erstellung von Compliance Berichten mit Hilfe von hauseigenen Werkzeugen
- Analyse von Log-Daten
  - Auswertung bezüglich Compliance-Regularien
  - Erstellung von Modellen zwecks Dokumentation
- Beratung bei der Erstellung von Geschäftsprozessmodellen
- Beratung bei der Modellierung von Compliance Regularien

# Mögliche Kooperationen - Anknüpfungspunkte

Mögliche technische Anknüpfungspunkte:

- System-, Schnittstellen- oder GP-Dokumentation
- Schnittstellen zu Log-Daten

Aber: Ansätze unabhängig von der vorliegenden Architektur durch Erstellung von Architektur-spezifische Adaptern.

=> Flexibel einsetzbar, keine konkreten technischen Voraussetzungen.

# Einige Referenzprojekte

- Mobile Architekturen bei O2 (Germany)
- Digitaler Formularschrank bei HypoVereinsbank
- Common Electronic Purse Specifications (Globaler Standard für elektr. Geldbörsen, Visa International u.a.)
- Internes Informationssysteme bei BMW
- Return-on-Security Investment Abschätzung
- Analyse Digitale-Signatur-Architektur
- IT-Sicherheits-Risikomodellierung
- Plattform für Software-Update auf Smart-cards
- Geplant: Dokumentation und Analyse von Cloud-Computing Systemen



**BMW Group**



**Herzlichen Dank für Ihre  
Aufmerksamkeit.**

Kontakt: [jan.juerjens@isst.fraunhofer.de](mailto:jan.juerjens@isst.fraunhofer.de)