Informationssicherheit im Cloud Computing

Prof. Dr. Jan Jürjens

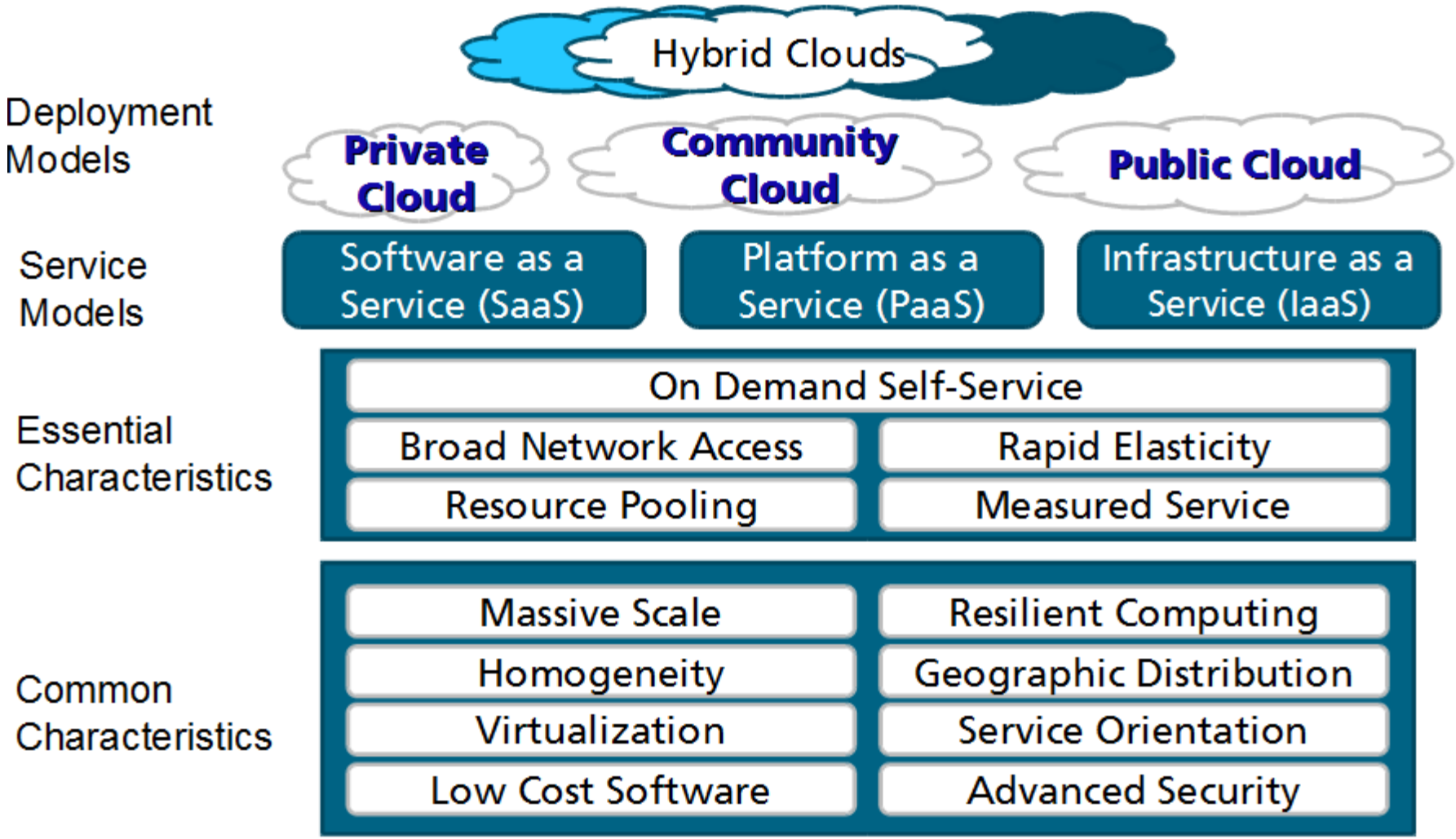
Fraunhofer Institut für Software- und Systemtechnik ISST, Dortmund

http://jan.jurjens.de

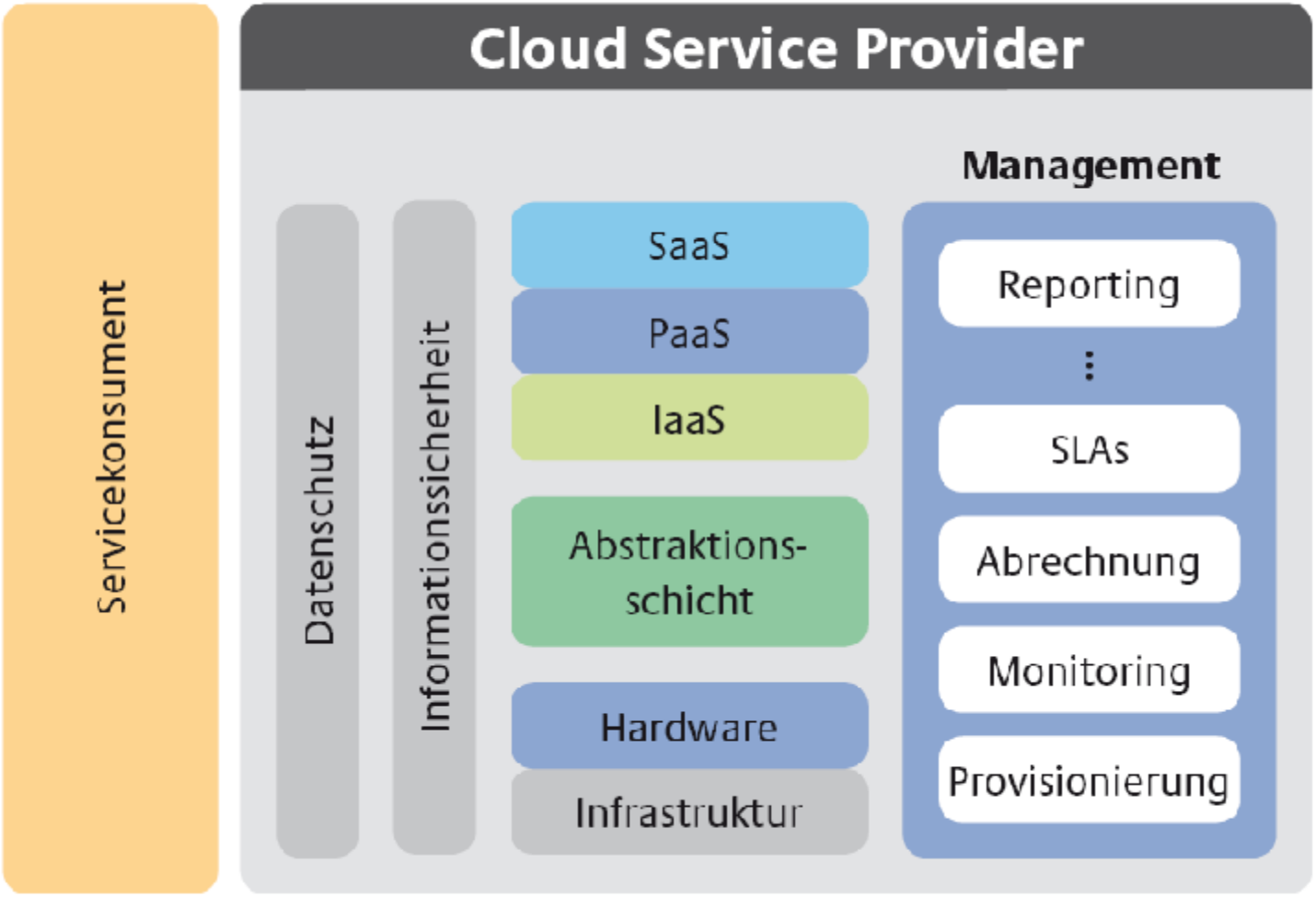
Übersicht

- Was sind die Herausforderungen?
- Was sind die Lösungen?
- Was sind die Werkzeuge?

The NIST Cloud Definition Framework



Das Cloud-Modell des BSI



(Quelle: BSI, Sicherheitsempfehlungen für Cloud Computing Anbieter, 2011)

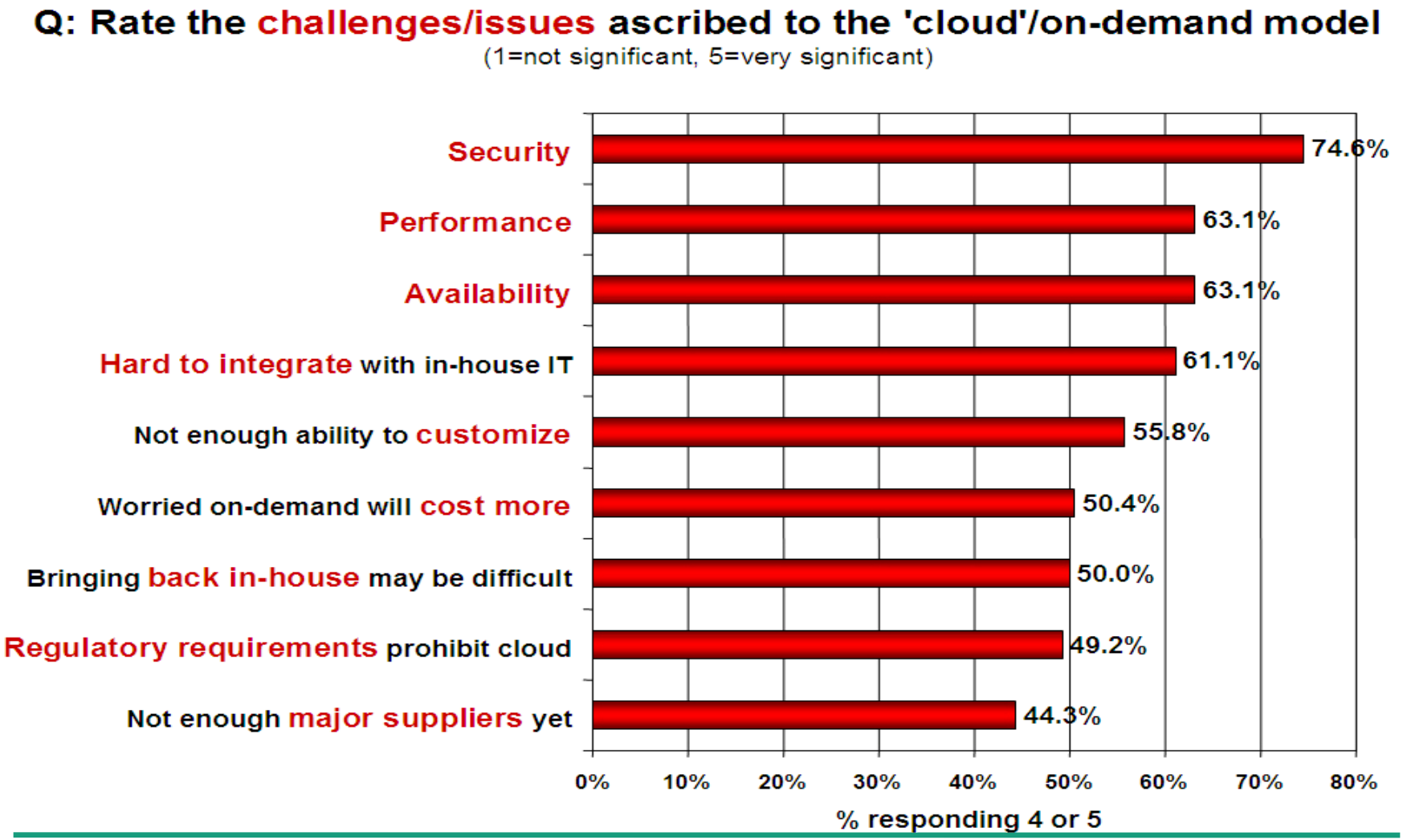
Fraunhofer ISST

Cloud Computing bietet Chancen

- Kostenersparnis
  - “Pay per use”-Modell
- Mehr Flexibilität durch Wahl des geeigneten Anbieters
  - Auch für einzelne Dienste

… Trotzdem wird Cloud Computing erst von wenigen Unternehmen genutzt

Sicherheit ist das Hauptproblem



Source: IDC Enterprise Panel, August 2008 n=244

Fraunhofer ISST

BSI Eckpunktepapier Cloud Computing

- Erweitert bestehende Standards um Cloud-spezifische Aspekte
- Hauptsächlich aus Sicht der Anbieter
- Schafft systematische Grundlage zur Untersuchung von Cloud-Angeboten

BSI Eckpunktepapier Cloud Computing (Forts.)

- Betrachtet elf Eckpunkte der Cloud Computing Sicherheit
  - Vorgestellt werden vor allem Ziele, weniger konkrete Lösungen
- Für (potentielle) Anwender vor allem interessant:
  - Vertragliche Gestaltung von Cloud-Angeboten
    - Kontrollmöglichkeiten für Nutzer
  - Portabilität und Interoperabilität
  - Sicherheitsprüfung und –nachweis (Zertifizierung)

Sicherheitsziele beim Cloud Computing

Vertraulichkeit	Verarbeitete Daten in Clouds sind unverschlüsselt Verschlüsselte Speicherung in Cloud Verschlüsselter Datenaustausch mit Cloud
Verfügbarkeit	Neben „klassischen IT-Problemen“: Cloud nur über Internetverbindung Schutz virtueller Maschinen vor Datenkorruption Redundanz von Rechen- und Speicherresourcen, geographisch verteilt
Integrität	Unerwünschte und unerkannte Veränderung von Daten in Cloud verhindern
Authentizität	von Cloud-Systemen gegenüber User… … und umgekehrt
Nicht-Abstreitbarkeit	Transaktionen in Clouds erfordern Signaturen Unabhängiger Check der Signaturen
Datenschutz	Einhaltung gesetzlicher Regelungen (Standort beachten) Erstellung von Benutzerprofilen verhindern Konflikt mit Nicht-Abstreitbarkeit

BSI: Drei Kategorien für Anforderungen

Basisanforderungen (B)

- Von jedem Cloud-Provider zu erfüllen

Hohe Vertraulichkeit (C+)

- Basisanforderungen + zusätzliche Maßnahmen
- Bei Daten mit hohem Schutzbedarf der Vertraulichkeit

Hohe Verfügbarkeit (A+)

- Basisanforderungen + zusätzliche Maßnahmen
- Bei Daten mit hohem Schutzbedarf der Verfügbarkeit

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)

Compliance: Bedeutung und Herausforderung

- "Compliance" ist die Einhaltung von Regularien (z.B. Gesetze oder betriebliche Bestimmungen).
- Etablierung von Compliance-Regelungen ist notwendig:
  - Einhaltung von EU-Richtlinien Basel II (=> III), Solvency II
  - Einhaltung von MaRisk der BaFin
  - Auf US-Markt: SOX
  - Bundesdatenschutzgesetz (besonders problematisch für Clouds)
- Heute: Hoher Aufwand, teuer und langwierig
- Für Standardaufgaben werden Spezialisten benötigt, besondere Fälle bleiben häufig unbeachtet, z.B. Fehlverhalten des Personals (spektakuläres Beispiel: Societe Generale 2008: 5 Mrd. Euro Verlust).

Compliance

- Herausforderung: Manuellen Aufwand reduzieren
  - Dadurch mehr Zeit für Konzentration auf wichtige GRC-Probleme
- Die automatische Prüfung von Sicherheitszielen fördert das Vertrauen zwischen Cloud-Anbieter und Nutzer.
- Compliance-Checks können die Geschäftsprozesse des Cloud-Anwenders auch auf legale Probleme hin prüfen:
  - SOX, EURO-SOX, BASEL II, SOLVENCY II
- Compliance von Geschäftsprozessen kann auf zwei Arten erreicht werden:
  - Compliance by design
  - Compliance Validierung

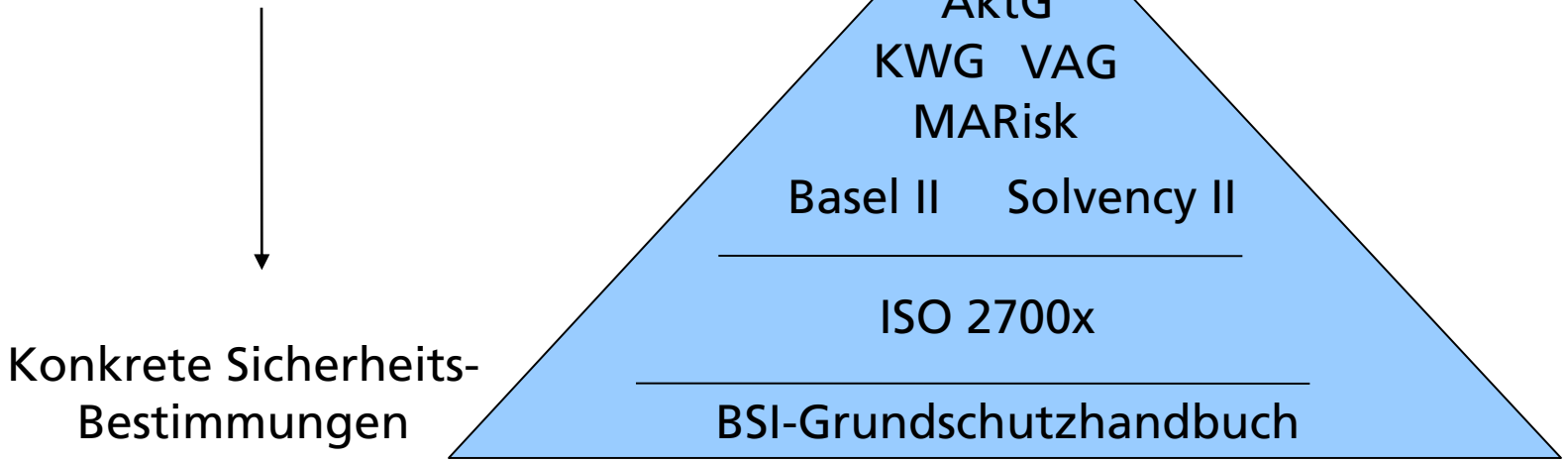
Sicherheit vs. Governance, Risk und Compliance (GRC)

- Governance, Risk und Compliance (GRC)
  - Governance: Unternehmensinterne Richtlinien
  - Compliance: Externe Richtlinien, z.B. SOX, EURO-SOX, BASEL II, SOLVENCY II
  - Risk: Risiko-Management unter Beachtung aller Richtlinien
- Sicherheit
  - Abstrakte Sicherheits-Ziele, z.B. Anwendung von CIA auf Unternehmen

Sicherheit und Compliance sind ähnlich, aber verschieden.

Sicherheit vs. Compliance: Regularien und Standards

Abstrakte Gesetze und Regelungen



Konkrete Sicherheits-Bestimmungen

GRC in Clouds

Governance	Risk	Compliance
■ Erstellung von Verfahren/Richtlinien ■ Klassifikationsschema für Daten und Prozesse ■ Vertrauens-beziehungen (trust chains) in der Cloud	■ Risiko-Strategie ■ Business Impact Analyse ■ Analyse von Bedrohungen und Schwachstellen ■ Risk Analysis Remediation	■ Umsetzung von Verfahren/Richtlinien ■ Legale Compliance (SOX, SOLVENCY II) ■ Implementierung von Kontrollen

Die Cloud stellt dynamisch Ressourcen bereit
→ Dieselbe Dynamik wird für GRC in Clouds benötigt

Compliance-Szenarien in der Cloud

- **Kunde -> Cloud:**
  - Sicherheits-Compliance:
    - Sicherheitsprozesse der Cloud auf Compliance mit SLA
  - Legale Compliance:
    - Überprüfung der Geschäftsprozesse auf Compliance mit SOX und MaRisk
- **Cloud -> Cloud:**
  - Vertrags-Compliance:
    - Überprüfung der Interaktion zweier Geschäftspartner in der Cloud
- **Cloud -> Kunde:**
  - Sicherheits-Compliance:
    - Überprüfung der Kundenprozesse auf Verstoß gegen Verhaltensbestimmungen

Übersicht

- Was sind die Herausforderungen?
- Was sind die Lösungen?
- Was sind die Werkzeuge?

Voraussetzungen

- Systematisches Vorgehen nur bei klaren Gegebenheiten
- Eine Möglichkeit: Anerkannte Standards für IT-Sicherheit
  - ISO 2700x-Normen
  - BSI Grundschutz-Standards und Kataloge
  - Seit 2011: BSI Eckpunktepapier Cloud Computing

Vertragliche Gestaltung: Service Level Agreements (SLA)

- Transparenz schafft Vertrauen beim Kunden
- Genaue Beschreibung der angebotenen Leistung und deren Beschränkungen!
- Vergleich verschiedener SLAs mit Anforderungen.
  - Bietet der Provider überhaupt ein SLA an?
- Was bedeuten die Werte? Z.B. 99.8% jährliche Verfügbarkeit:
  - Die Cloud ist ~17,5 Stunden pro Jahr offline!
- Ist die Cloud in verschiedene Sicherheitszonen unterteilt?
  - Muss ich meine Daten vor der Übertragung in die Cloud aufteilen?
  - Sollte ich die Übertragung vertraulicher Daten in die Cloud vermeiden?

Vertragliche Gestaltung: Kontrollmöglichkeiten

- Auch hier: Transparenz schafft Vertrauen
- Welche Möglichkeiten sind vorgesehen?
- Was sind die Strafen für Verletzungen der SLA?
  - Kann der Kunde die Leistung der Cloud überwachen?
  - Existiert ein Frühwarnsystem?

Portabilität und Interoperabilität

- Ein Vorteil der Cloud: Flexibilität
  - Daher: Festlegung auf bestimmten Anbieter vermeiden („Vendor Lock-In“)
- Vorhandene Daten müssen übernommen werden
  - Etablierte Austauschformate helfen
- Auch ein Ende der Cloud-Nutzung sollte ohne großen Aufwand möglich sein!

Sicherheitsprüfung und -nachweis

- Sicherheitsprüfungen sind regelmäßig durchzuführen…
  - vom Anbieter
  - vom Kunden
  - von unabhängigen Dritten
- Allgemein: Zertifikate!
  - ISO 27001
    - Definiert umfassende Anforderungen an IT-Sicherheitsmanagement
    - Auch auf Basis der BSI-Standards möglich
  - SAS 70 Type II
    - Bewertung interner Kontrollmechanismen
  - TRUSTe
    - Einhaltung von Datenschutzrichtlinien

Einige Beispiele: Sicherheits-Zertifikate

Vendor	TRUSTe	Safe Harbor	SAS 70 Type II	ISO/IEC 27001
Microsoft	x	x	x	x
Google	x		x	
Amazon	x	x	x	x
Salesforce	x	x	x	x
PingIdentity			x	
Postini		x	x	
CohesiveFT				
Scalr				
RightScale				
IBM	x	x	x	x
GoGrid	x		x	
FlexiScale				
Rackspace	x			
LongJump				

(Quelle: Fraunhofer SIT, Cloud Computing Sicherheit, 2009)

Übersicht

- Was sind die Herausforderungen?
- Was sind die Lösungen?
- Was sind die Werkzeuge?

Eine einfache Checkliste für eine Cloud

- Ist die Sicherheit des Anbieters dokumentiert?
  - Wie werden Sicherheitslevel eingehalten?
- Ist eine einfache Beendigung der Cloudnutzung möglich?
- Welche Garantien und Service Level Agreements (SLA) existieren?
  - Können diese an die Bedürfnisse des Kunden angepasst werden?
  - Welche Vertragsstrafen sind in den Standard-SLAs vorgesehen?
  - Wie kann der Anbieter die Einhaltung der SLA überwachen und durchsetzen?
  - Wo ist der Standort der Cloud, welche Gesetze gelten dort?
  - Kann die Anwendung von deutschem Recht erzwungen werden (“Rechtswahl”)? Insbesondere Datenschutzbestimmungen!

Einige Beispiele

- Physikalische Sicherheit des Rechenzentrums:
  - Googles Security Operations Center
  - Amazon: Zwei-Faktor Authentifizierung
- Angriffe auf Netzwerkebene, z.B. Denial-of-Service:
  - Amazon nutzt „Denial-of-Service Prevention“, genaue Methode ist geheim
  - Microsoft nutzt Load-Balancer und Intrusion Prevention Systems
- Backup-Lösungen:
  - Google, Amazon sichern Daten an unterschiedlichen Standorten
  - FlexiScale legt Backups an, aber Nutzer kann die Daten nicht (selbst) wiederherstellen
- Amazon speichert Daten dauerhaft: nach 5 Minuten sind diese in der Cloud

Verwandte Standards

Fraunhofer ISST

Compliance: Herausforderungen bewältigen

- Wie können Aufgaben im Bereich GRC automatisiert werden?
  - Reduktion des RoI durch Reduktion des manuellen Aufwandes
  - Experten konzentrieren sich auf Spezialfälle
- Wie kann innerhalb eines Unternehmens eine Wissensbasis über GRC aufgebaut werden?
  - Datenquellen: Interviews, Texte, Prozesse, Process mining
  - Wie kann die Evaluierung von Konzepten des Risikomanagements organisiert werden?
  - Idealerweise (teil-)automatisiert durch Werkzeugunterstützung
- Wie kann die Überwachung von GRC unterstützt werden?
  - Einsatz von Überwachungs-Werkzeugen, z.B. in Web-Portalen
- Ideal: Wiederverwendung der Informationen zur Prozessoptimierung

Was sind die Werkzeuge?

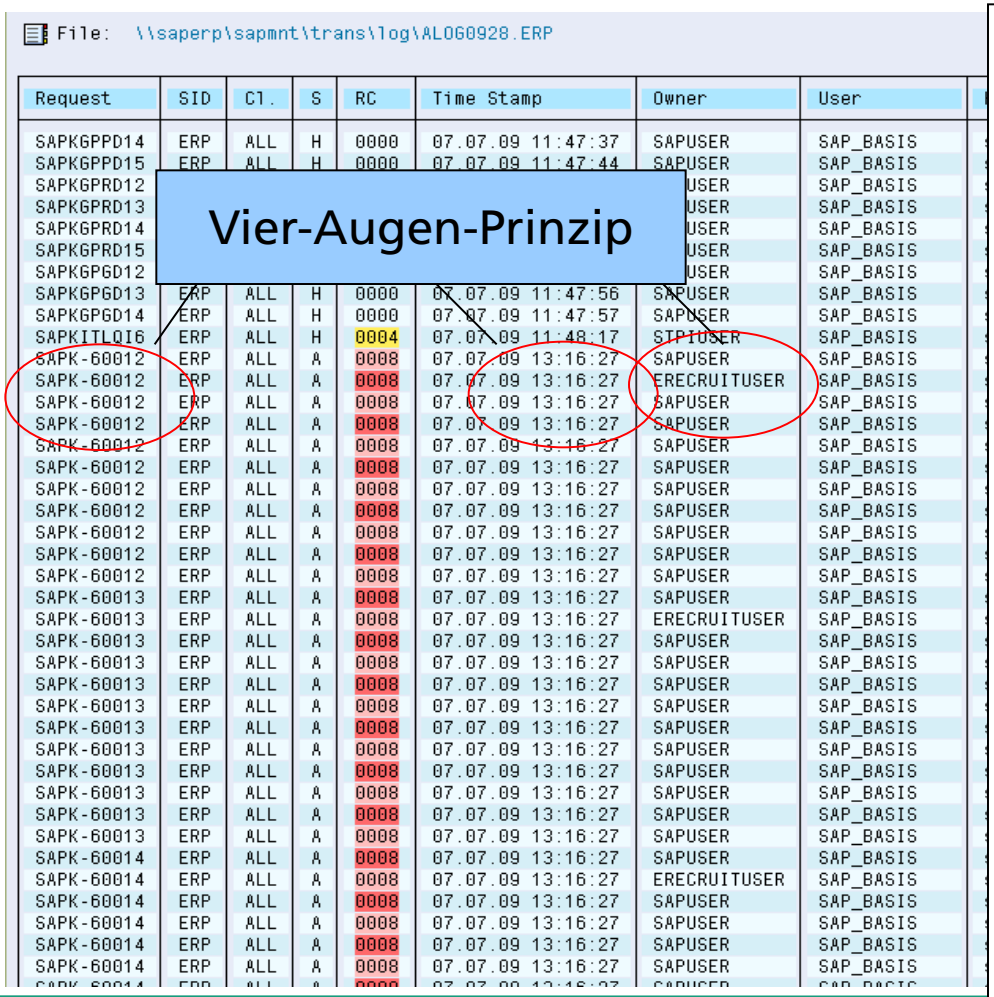
Welche Werkzeugunterstützung gibt es für:

- 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

Möglichkeiten:

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

Untersuchung von Log-Daten



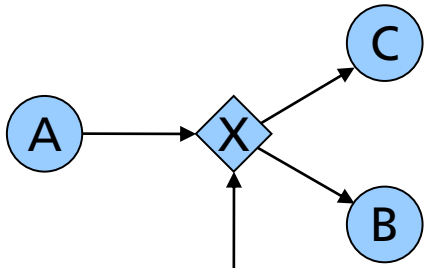
File: \\saperp\sapmnt\trans\log\ALOG0928.ERP

Request	SID	Cl.	S	RC	Time Stamp	Owner	User
SAPKGPPD14	ERP	ALL	H	0000	07.07.09 11:47:37	SAPUSER	SAP_BASIS
SAPKGPPD15	ERP	ALL	H	0000	07.07.09 11:47:44	SAPUSER	SAP_BASIS
SAPKGPRD12						USER	SAP_BASIS
SAPKGPRD13						USER	SAP_BASIS
SAPKGPRD14						USER	SAP_BASIS
SAPKGPRD15						USER	SAP_BASIS
SAPKGPGD12						USER	SAP_BASIS
SAPKGPGD13	ERP	ALL	H	0000	07.07.09 11:47:56	SAPUSER	SAP_BASIS
SAPKGPGD14	ERP	ALL	H	0000	07.07.09 11:47:57	SAPUSER	SAP_BASIS
SAPKITLQI6	ERP	ALL	H	0004	07.07.09 11:48:17	STPIUSER	SAP_BASIS
SAPK-60012	ERP	ALL	A	0008	07.07.09 13:16:27	SAPUSER	SAP_BASIS
SAPK-60012	ERP	ALL	A	0008	07.07.09 13:16:27	ERECRUITUSER	SAP_BASIS
SAPK-60012	ERP	ALL	A	0008	07.07.09 13:16:27	SAPUSER	SAP_BASIS
SAPK-60012	ERP	ALL	A	0008	07.07.09 13:16:27	SAPUSER	SAP_BASIS
SAPK-60012	ERP	ALL	A	0008	07.07.09 13:16:27	SAPUSER	SAP_BASIS
SAPK-60012	ERP	ALL	A	0008	07.07.09 13:16:27	SAPUSER	SAP_BASIS
SAPK-60012	ERP	ALL	A	0008	07.07.09 13:16:27	SAPUSER	SAP_BASIS
SAPK-60012	ERP	ALL	A	0008	07.07.09 13:16:27	SAPUSER	SAP_BASIS
SAPK-60012	ERP	ALL	A	0008	07.07.09 13:16:27	SAPUSER	SAP_BASIS
SAPK-60012	ERP	ALL	A	0008	07.07.09 13:16:27	SAPUSER	SAP_BASIS
SAPK-60012	ERP	ALL	A	0008	07.07.09 13:16:27	SAPUSER	SAP_BASIS
SAPK-60013	ERP	ALL	A	0008	07.07.09 13:16:27	SAPUSER	SAP_BASIS
SAPK-60013	ERP	ALL	A	0008	07.07.09 13:16:27	ERECRUITUSER	SAP_BASIS
SAPK-60013	ERP	ALL	A	0008	07.07.09 13:16:27	SAPUSER	SAP_BASIS
SAPK-60013	ERP	ALL	A	0008	07.07.09 13:16:27	SAPUSER	SAP_BASIS
SAPK-60013	ERP	ALL	A	0008	07.07.09 13:16:27	SAPUSER	SAP_BASIS
SAPK-60013	ERP	ALL	A	0008	07.07.09 13:16:27	SAPUSER	SAP_BASIS
SAPK-60013	ERP	ALL	A	0008	07.07.09 13:16:27	SAPUSER	SAP_BASIS
SAPK-60013	ERP	ALL	A	0008	07.07.09 13:16:27	SAPUSER	SAP_BASIS
SAPK-60013	ERP	ALL	A	0008	07.07.09 13:16:27	SAPUSER	SAP_BASIS
SAPK-60013	ERP	ALL	A	0008	07.07.09 13:16:27	SAPUSER	SAP_BASIS
SAPK-60013	ERP	ALL	A	0008	07.07.09 13:16:27	SAPUSER	SAP_BASIS
SAPK-60013	ERP	ALL	A	0008	07.07.09 13:16:27	SAPUSER	SAP_BASIS
SAPK-60014	ERP	ALL	A	0008	07.07.09 13:16:27	SAPUSER	SAP_BASIS
SAPK-60014	ERP	ALL	A	0008	07.07.09 13:16:27	ERECRUITUSER	SAP_BASIS
SAPK-60014	ERP	ALL	A	0008	07.07.09 13:16:27	SAPUSER	SAP_BASIS
SAPK-60014	ERP	ALL	A	0008	07.07.09 13:16:27	SAPUSER	SAP_BASIS
SAPK-60014	ERP	ALL	A	0008	07.07.09 13:16:27	SAPUSER	SAP_BASIS
SAPK-60014	ERP	ALL	A	0008	07.07.09 13:16:27	SAPUSER	SAP_BASIS

- Identifikation des Vier-Augen-Prinzips mit Hilfe der folgenden Informationen:
- Vorgangsnummern stimmen überein
- Nutzer sind verschieden
- Aktionen wurden zum selben Zeitpunkt abgeschlossen

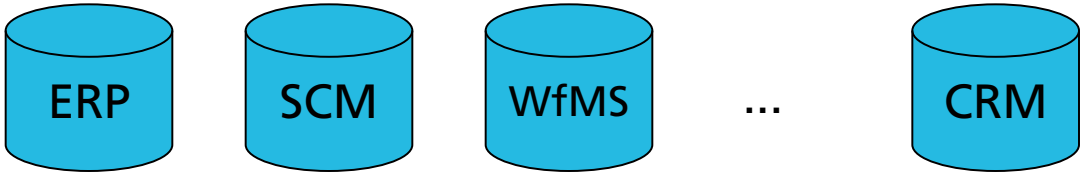
Business Process Mining

Analyse von Prozessen, die aus Log-Daten rekonstruiert wurden



Ereignis-Daten

Process ID	Activity ID	Consultant	Time Stampe
1	A	John	9-3-10:15.01
2	A	Mike	9-3-10:15.12
3	B	Mike	9-3-10:16.07
4	C	Carol	9-3-10:18.25

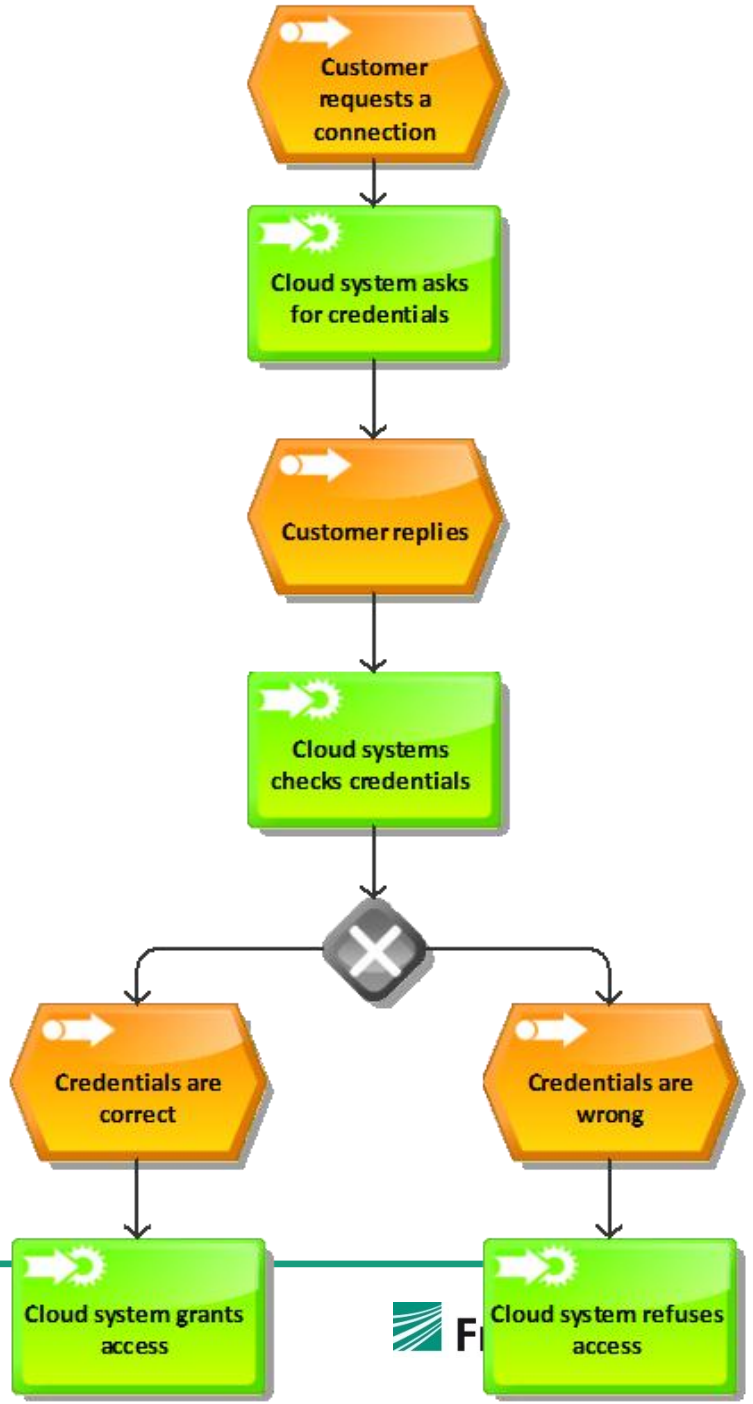


Business Process Analysis

- Automatisierte Compliance-Analyse
- Zwei Ansätze:

1. Text-basierte Analyse der Aktivitäts-Bezeichner zur automatischen Identifikation von Risiken

2. Strukturelle Analyse des Prozessmodells auf Muster, die Compliance verletzen



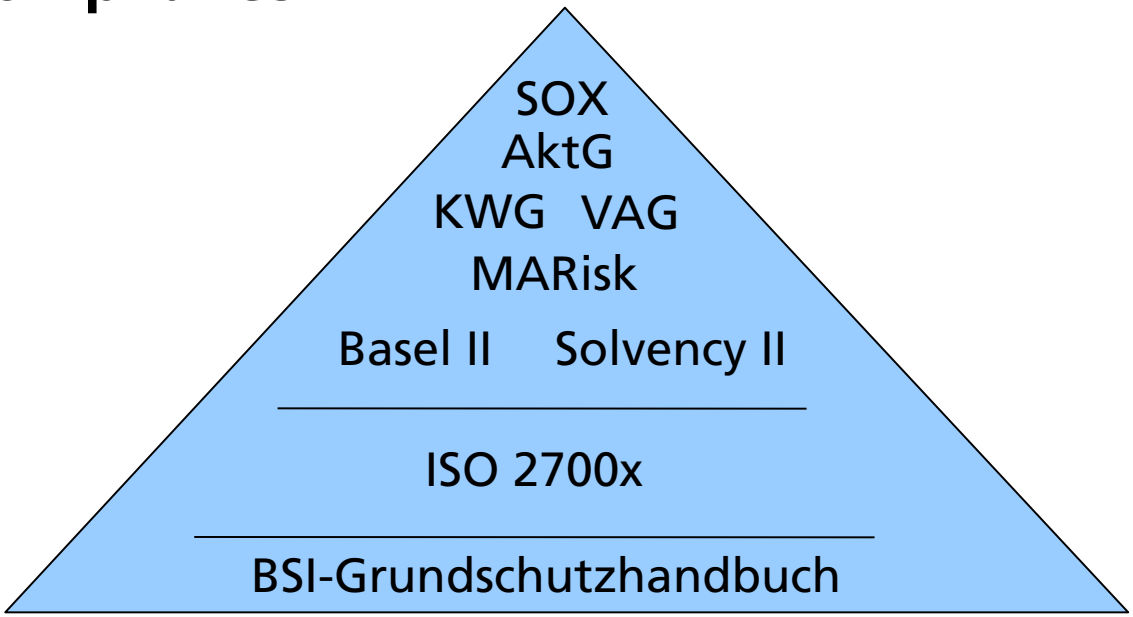
Projekt SecureClouds (http://secureclouds.de)

- Werkzeuggestützte Methode zur Umsetzung von Geschäftsprozessen auf IT-Infrastrukturen unter Beachtung von Compliance-Anforderungen (z.B. Basel II, Solvency II, ...).
- Analyse wird auf Basis von Textdokumenten, Modellen und anderen Datenquellen durchgeführt
- Governance, Risk, Compliance (GRC) und Maßnahmen, insbesondere für Cloud Computing in KMUs und Großunternehmen.

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung
DLR
Projektträger im DLR

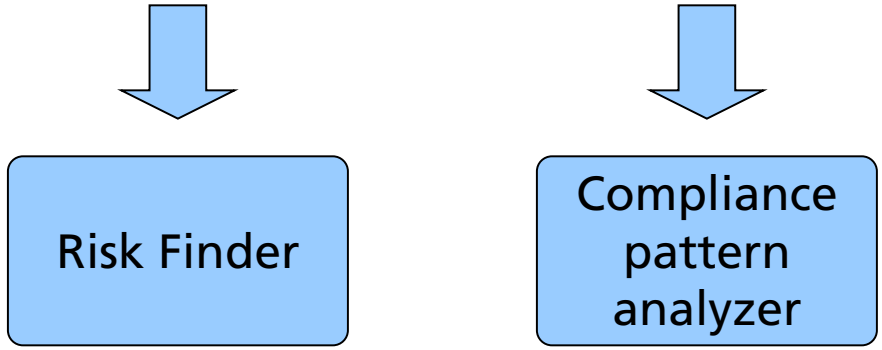
Werkzeuggestützte Analyse und Umsetzung von Sicherheit und Compliance

Abstrakte Gesetze und Regularien



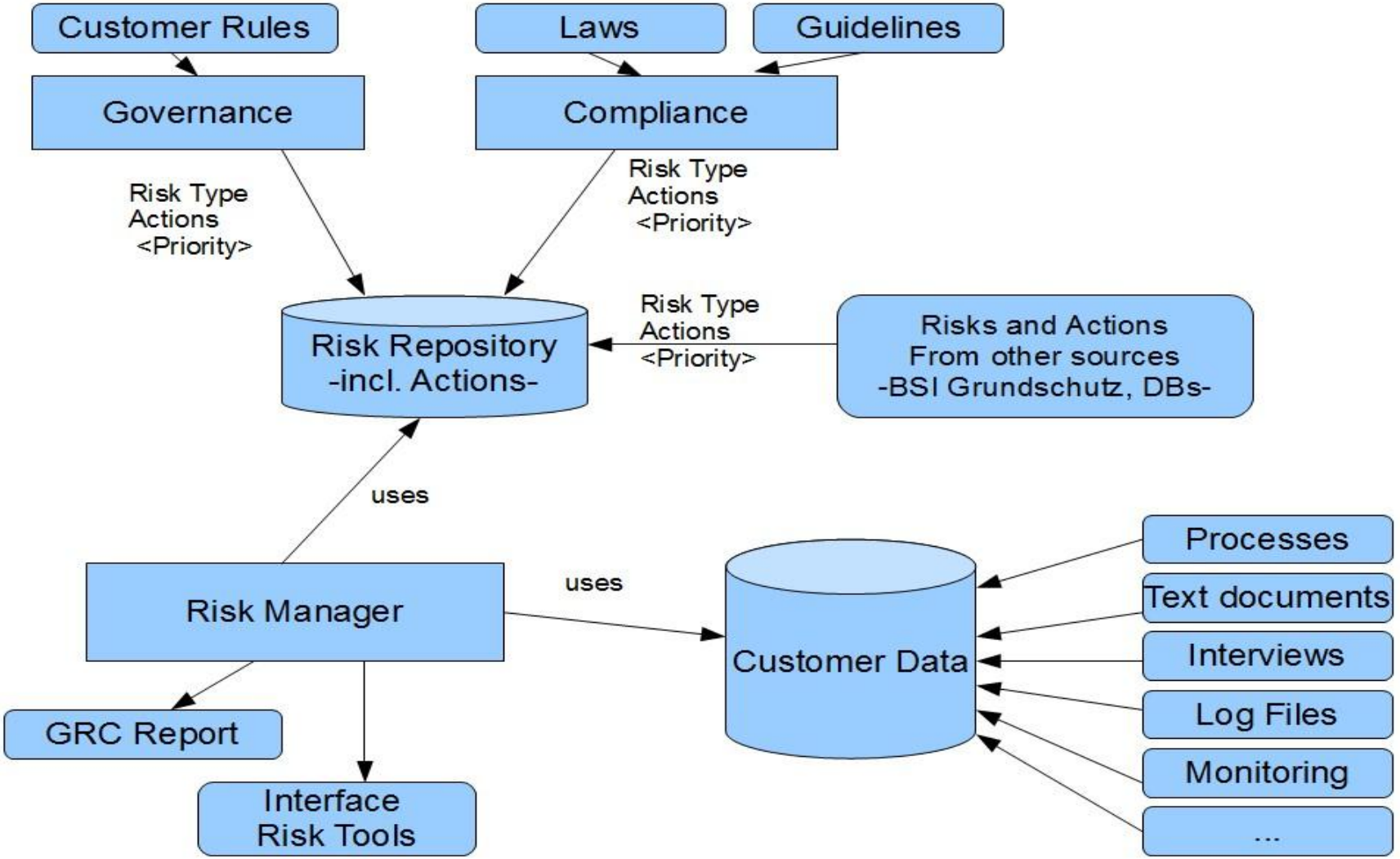
Konkrete Sicherheits-Bestimmungen

SecureClouds Tools



Fraunhofer ISST

Die SecureClouds-Werkzeugarchitektur



Nutzen

Automatisch generierter Compliance-Bericht:

- Grundlage sind Sicherheitsstandards, z.B. BSI Sicherheitsempfehlungen oder MaRisk
- 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-Bericht

Compliance: incomplete

Problem:
- MaRISK VA 7.2: Übereinstimmung mit BSI G3.1 ist zu prüfen

Maßnahme:
- BSI Maßnahmenkatalog M 2.62

Leistungen/Angebote des Fraunhofer ISST

- Erstellung von Compliance-Berichten mit Werkzeugunterstützung
- Data Mining auf Log-Dateien
  - Compliance-Analysis der Prozessausführung
  - Automatische Generierung von Prozessmodellen
- Sicherheits- und Compliance-Analysen von Geschäftsprozessen auf Basis der Prozessdokumentation
- Vorbereitung und Durchführung von Compliance-Checks

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

Projekte

- Elektronische Gesundheitskarte
- Mobile Architekturen und Verfahren (O2 Deutschland)
- Digitale Dokumentenverwaltung (HypoVereinsbank)
- Digitales Bezahlprotokoll CEPS (Visa International)
- Sicherheitsanalyse Intranet-System (BMW)
- Return-on-Security Investment-Analyse (Münchener Rück)
- Sicherheitsanalyse für digitales Unterschriften-System (Allianz)
- Untersuchung zu IT-Sicherheitsrisiko (Infineon)
- Update-Plattform für Smartcard-Software (Gemalto)
- Zertifizierung für Cloud-Sicherheit (TÜV-IT, Itesys, LinogistiX)
- Sicherheitsuntersuchung zur Cloud-Nutzung (adMERITia, LinogistiX)

Fazit

- Sicherheit und Compliance in Cloud-basierten Umgebungen sind komplexe und vielfältige Probleme.
  - So vielfältig wie Clouds selbst (vgl. NIST-Definition)
- Es gibt Lösungen (und Tools) zur Bewältigung der Herausforderungen.
  - Analyse der eigenen Geschäftsprozesse auf Eignung zur Auslagerung in eine Cloud (bzgl. Sicherheit / Compliance)
  - Analyse / Überwachung der vom Cloud-Anbieter zugesicherten Sicherheit / Compliance

Kontakt: http://jan.jurjens.de

Informationen: http://www.isst.fraunhofer.de/geschaeftsfelder/insuranceandfinance/refpro/gruppe-apex