IT-Risikomanagement im Cloud Computing: Status Quo und aktuelle Entwicklungen

CAST-Workshop Cloud Security

Michael Adelmeyer, M.Sc., CISA, michael.adelmeyer@uos.de

Unternehmensrechnung und Wirtschaftsinformatik

UNIVERSITÄT OSNABRÜCK

Agenda

1. Cloud Computing: Definition und Motivation
2. Risiken im Cloud Computing
3. Management von Cloud-Risiken
4. Aktuelle Entwicklungen
5. Zusammenfassung

Agenda

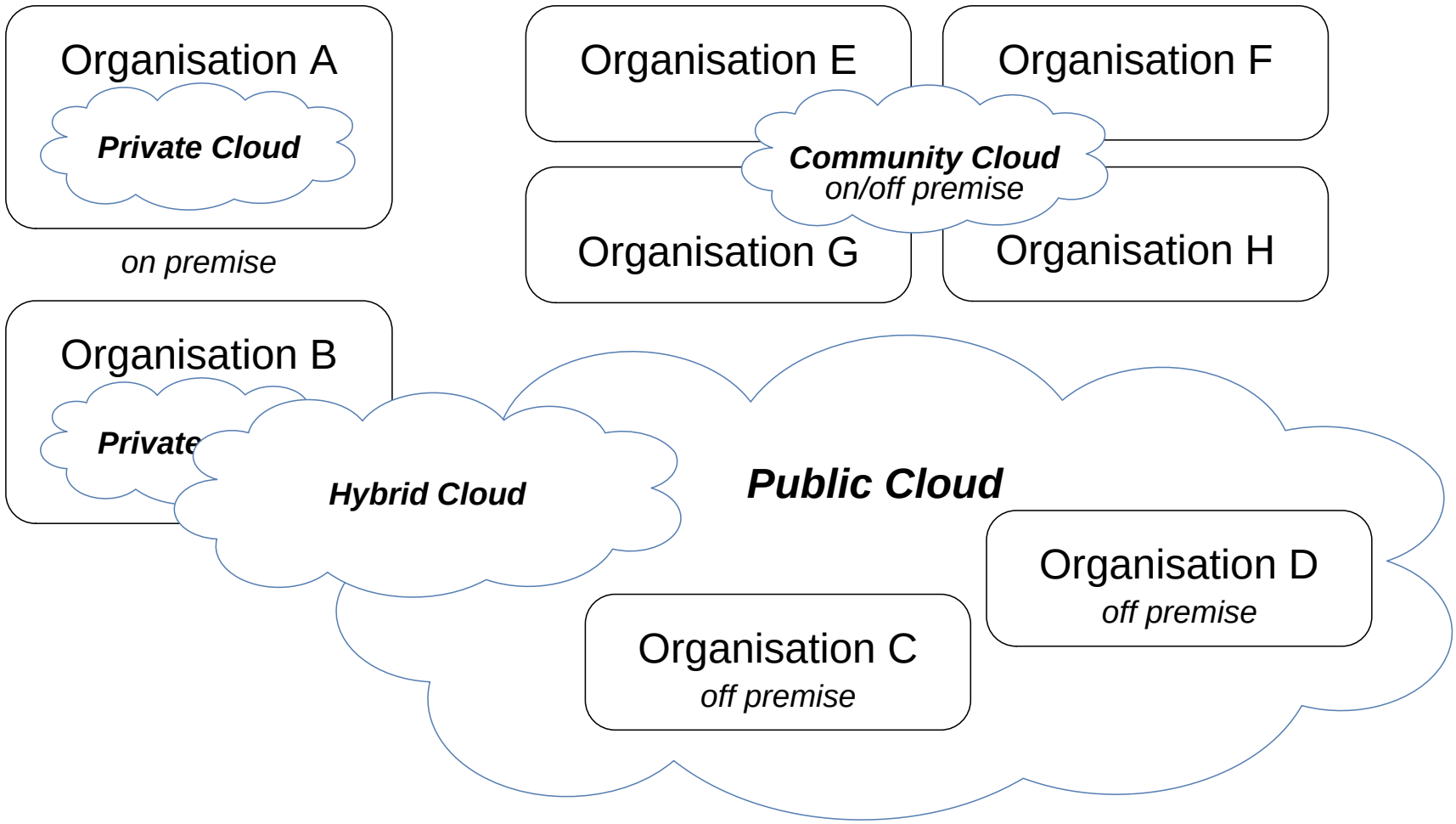
1. **Cloud Computing: Definition und Motivation**
2. Risiken im Cloud Computing
3. Management von Cloud-Risiken
4. Aktuelle Entwicklungen
5. Zusammenfassung

Definition Cloud Computing

- „Cloud Computing ist ein Modell, welches bei Bedarf einen **allgegenwärtigen**, komfortablen Netzwerkzugang zu zusammengefassten, **konfigurierbaren** Computerressourcen (bspw. Netzwerke, Server, Speicherplatz, Anwendungen und Dienstleistungen) bietet, die schnell zur Verfügung gestellt und wieder freigegeben werden können, mit **minimalem Verwaltungsaufwand** bzw. Interaktion mit dem Anbieter“
- 5-4-3-Definition des National Institute of Standards and Technology (NIST):
  - **5 Charakteristika (Essential Characteristics):** on-demand self-service; broad network access; resource pooling; rapid elasticity; measured service;
  - **4 Bereitstellungsmodelle (Deployment Models):** public / private / hybrid / community cloud (on / off premise)
  - **3 Servicemodelle (Service Models):** Infrastructure / Platform / Software as a Service (IaaS, PaaS, SaaS)

Quelle: NIST 2011

4 Bereitstellungsmodelle



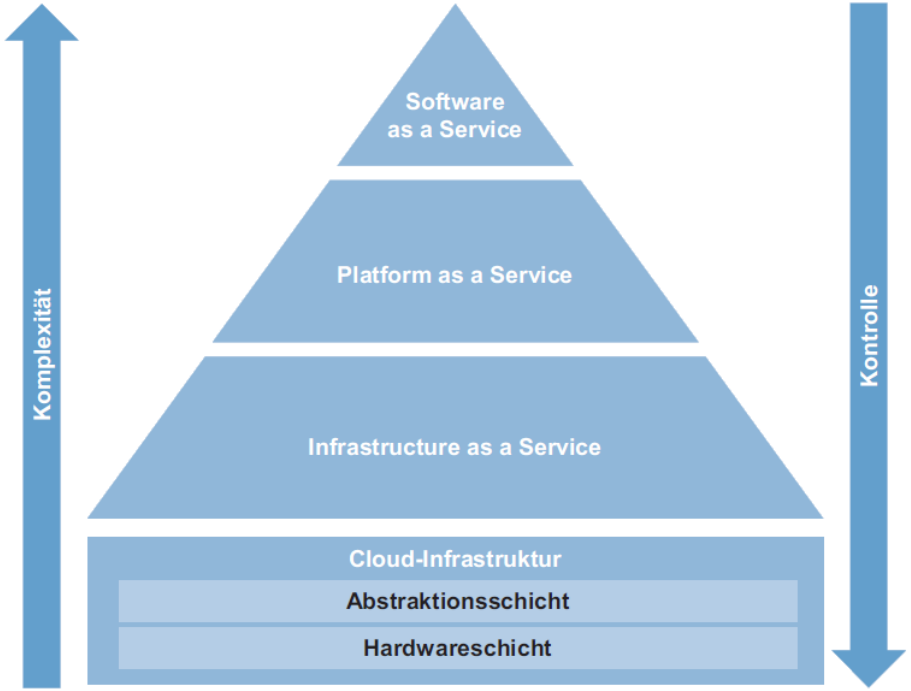
Quelle: NIST 2011

3 Servicemodelle

- **Infrastructure as a Service (IaaS):** Bezug grundlegender Hardware-Ressourcen wie Speicher-, Rechen- oder Netzwerkkapazitäten
- **Platform as a Service (PaaS):** Nutzung von Programmierungs- bzw. Laufzeitumgebungen, auf denen eigene Anwendungen entwickelt oder ausgeführt werden können
- **Software as a Service (SaaS):** Bereitstellung von Anwendungs-programmen über einen web-basierten Zugriff

→ Keine Verwaltung der zugrunde liegenden Infrastruktur durch den Benutzer

→ Kontrolle lediglich im Rahmen der ihm zur Verfügung gestellten Abstraktionsebene



Quellen: Adelmeyer et al. 2017b, Martens et al. 2011, NIST 2011

Motivation

- **Probleme bei klassischen IT-Investitionen**
  - Häufig geringe Ressourcennutzung
  - Überdimensionierung für Lastspitzen notwendig
  - Keine schnelle Skalierung möglich
- **Vorteile von Cloud Computing**
  - Keine Kapitalbindung („pay-as-you-go“ Modell)
  - Flexible und rapide Skalierung
  - Remote-Zugriff
- **erhöhte Risiken/Anforderungen**
  - Informationssicherheit (Vertraulichkeit, Verfügbarkeit, Integrität)
  - Schutz (personenbezogener) Daten
  - Gesetzliche Vorgaben
- Steigende Relevanz: Umsatzsteigerung von 58,6 (2009) auf 383,36 Mrd. USD (Prognose 2020) mit Cloud Computing weltweit

Quellen: Armbrust et al. 2010, Statista 2017

Agenda

1. Cloud Computing: Definition und Motivation
2. **Risiken im Cloud Computing**
3. Management von Cloud-Risiken
4. Aktuelle Entwicklungen
5. Zusammenfassung

Risiken im Cloud Computing

- IT-Risiken im Cloud Computing grundsätzlich verwandt mit denen des klassischen Outsourcings oder Outtaskings
- Fokus Cloud-bezogener Risiken stärker auf **Datenschutz- und Datensicherheitsaspekten**
- Entstehende Risiken stark abhängig von Anbieter, Bereitstellungs- und Servicemodell
  - Bei Einsatz einer Private Cloud entstehende Risiken minimal, Hoheit über Daten und Anwendungen verbleibt im Unternehmen
  - Je höher das Abstraktionslevel in Bezug auf die Servicebereitstellung, desto geringer die Kontrolle des Nutzers

→ **Detaillierte Betrachtung auf Einzelrisikoebene hat für den jeweiligen Anwendungsfall individuell zu erfolgen**

Quellen: Ackermann 2013, Adelmeyer et al. 2017b, Knoll 2014, Königs 2017

Cloud-spezifische Risiken

Externe Risiken

Beispiel: Wegnahme des Cloud-Services vom Markt / Insolvenz des Anbieters

Wirtschaftliche Risiken

Beispiel: versteckte Kosten oder Vendor-Lock-in / Backsourcing Problematik

Methodische Risiken

Beispiel: Mangelhafte Projekt-dokumentation

Soziokulturelle Risiken

Beispiel: Missachtung der Privatsphäre

Rechtliche Risiken

Beispiel: Mangelhafter Vertrag mit dem Cloud-Anbieter

Organisatorische Risiken

Beispiel: Hohe Abhängigkeit vom Cloud-Anbieter

Technische Risiken

Beispiel: Mangelhafte Maßnahmen zur Einhaltung von Datensicherheit

Quelle: Teuteberg 2015

Warum IT-Risikomanagement im Cloud Computing?

- Externe Verarbeitung oder Speicherung von (sensiblen) Unternehmensdaten
- Beachtung von Compliance-Richtlinien und gesetzlichen Vorgaben
- Ausweitung des Risikomanagement auf das Unternehmen des Dienstleisters → Anpassung und Erhöhung der Komplexität
- Sourcingentscheidungen werden häufig nicht ausreichend analysiert
- Neuartige Risikofaktoren → z. B. versteckte Kosten/Vendor-Lock-in/Backsourcing-Problematik
- IT-Sicherheits- und Risikomanagement sind im Cloud Computing und IT-Outsourcing von hoher Relevanz

→ **(Proaktives) IT-Risikomanagement erforderlich**

Quellen: Ackermann 2013, Armbrust et al. 2010, Martens et al. 2011

Agenda

1. Cloud Computing: Definition und Motivation
2. Risiken im Cloud Computing
3. **Management von Cloud-Risiken**
4. Aktuelle Entwicklungen
5. Zusammenfassung

IT-Risikomanagement im Cloud Computing

- IT-Risikomanagement im Kontext von Cloud Computing (CC) umfasst jede Kommunikation, die der **Identifikation**, der **Bewertung**, der **Steuerung** und der **Überwachung** von IT-Risiken im CC dient

- Beteiligte **Akteure** sind das Top-Management, Projektleiter, Anbieter von Cloud-Services, Mediatoren, Investoren, interne und externe Berater sowie die Endanwender

- Die **Risikokommunikation** zielt dabei insbesondere auf die Vermittlung von Wissen über Risikopotentiale, das Erkennen sowie die Vermeidung von Konflikten bei Auseinandersetzungen bzw. unterschiedlichen Einschätzungen der Akteure bei der **Bewertung und Steuerung der Risiken** ab

Gestaltung des IT-Risikomanagements

- Ausgestaltung **abhängig von Einsatzgebiet, Service-Art bzw. Phase**
- Vorhandene Theorien und Konzepte des IT-Risikomanagements im klassischen IT-Outsourcing grds. auf CC übertragbar (Unterschied: Automatisierungsgrad)
- **Nutzerperspektive**: Kontrolle über vertragliche Ausgestaltung, Service Level Agreements (SLAs), Key Performance Indicators (KPIs) oder entsprechende Zertifikate
- **Anbieter-/Betreiberperspektive**: Signaling (Zertifikate), direkte Kontrolle der Risiken, Umsetzung individueller Kundenanforderungen (bspw. Banken)
- Unterstützung des Risikomanagements im Cloud Computing durch div. Methoden
  - Qualitativ: Erfassung nicht direkt messbarer Risiken
  - Quantitativ: mathematisch-statistische Verfahren, erfordern hinreichend große Datenbasis
- Integration entsprechender **Standards, Best Practices und Frameworks** in bestehende Risikomanagementprozesse
- **Betrachtung des kompletten Cloud-Lebenszyklus**

Quellen: Adelmeyer et al. 2017a, Königs 2017, Teuteberg 2015

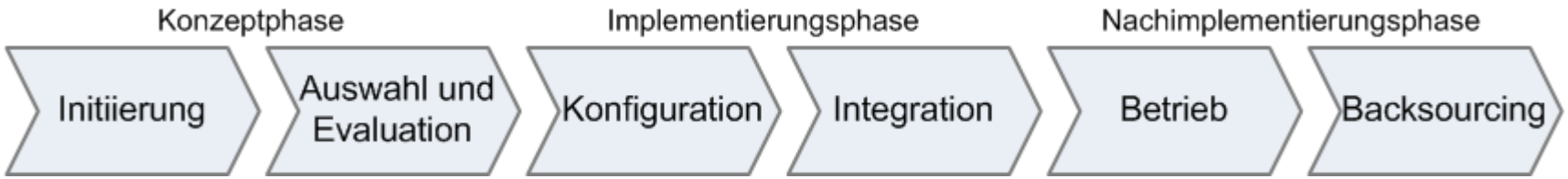
Phasen des Risikomanagements

1. **Umfeldanalyse (Risikostrategie):** Durchführung Umfeldanalyse, Definition Risikostrategie
2. **Risikoidentifikation:** Identifikation von Risiken im Kontext des Cloud Computing
3. **Risikoanalyse:** Bestimmen von Eintrittswahrscheinlichkeiten und Schadensausmaßen
4. **Risikoevaluierung:** Monetarisierung, Bewertung und Priorisierung von Risiken
5. **Risikobehandlung:** Maßnahmenplanung und Umsetzung, um angemessen auf Störereignisse und zukünftige Risiken reagieren zu können, Zuweisung Risikobegegnungsstrategien
6. **Risikoüberwachung:** Kontinuierliche Überwachung der Cloud Computing-Prozesse mit dem Ziel, Störungen vor deren Eintreten zu antizipieren

Quelle: Junginger 2005

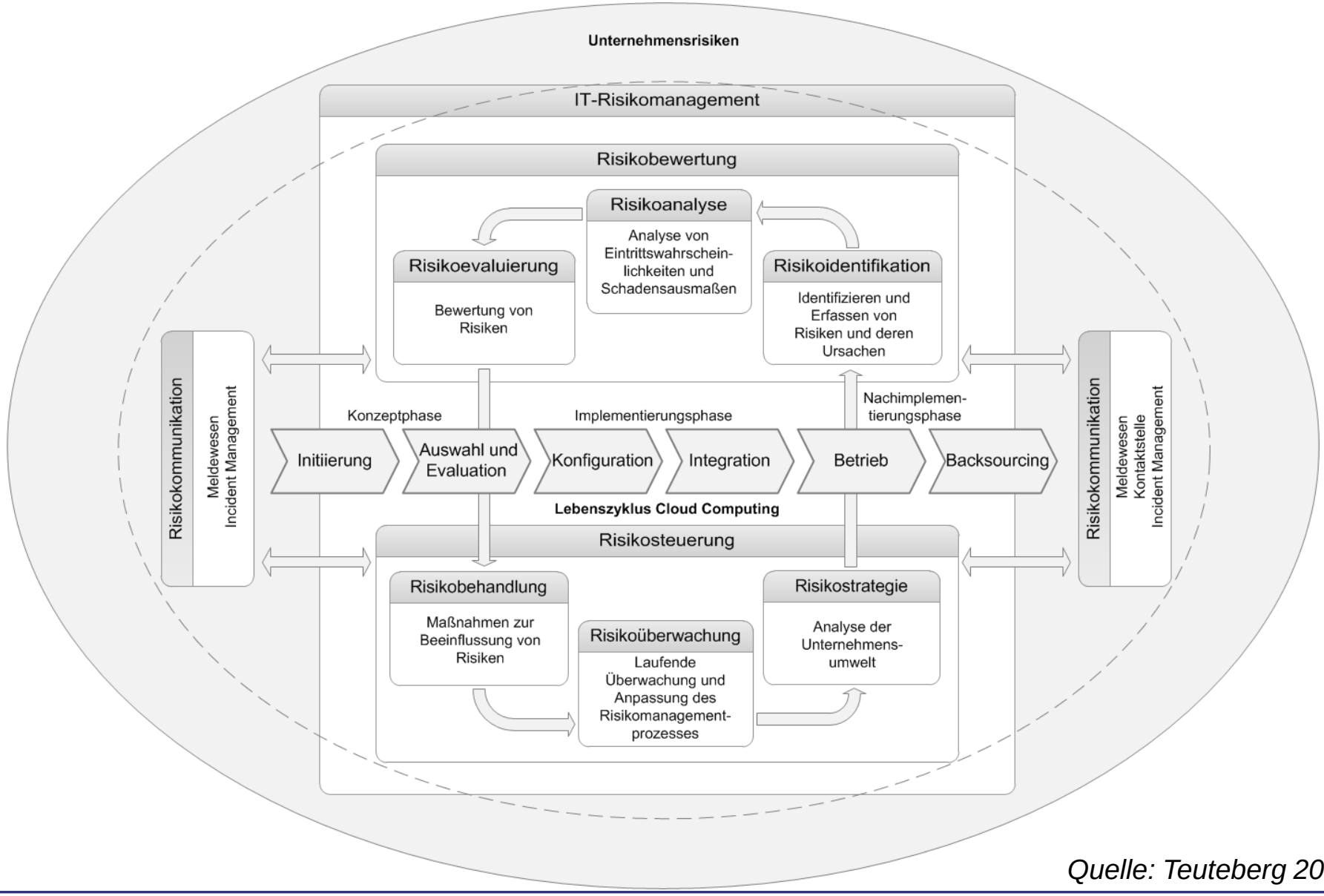
Cloud-Lebenszyklus

- **Initiierung:** strategische Überlegungen in Bezug auf das Outsourcingvorhaben und Anbietersuche
- **Auswahl und Evaluation:** Auswertung der Entscheidungsalternativen und Auswahlentscheidung
- **Konfiguration und Integration:** Anpassung der Funktionalitäten an die unternehmensspezifischen Gegebenheiten und Integration des Cloud-Services in die IT-Systemlandschaft
- **Betrieb:** organisatorische Aufgaben und Überwachung des Dienstleisters
- **Backsourcing:** Bewertung des vorhandenen Serviceportfolios



Quelle: Teuteberg 2015

IT-Risikomanagement im Cloud Computing



Quelle: Teuteberg 2015

Anwendbare Standards und Richtlinien

- **ISO 31000** als Basis-Norm zum Risikomanagement
- **ISO/IEC 270xx-Familie**
  - ISO/IEC 27001 als De-facto-Basisstandard für das Management von Informationssicherheit
  - ISO/IEC 27005 Management von Informationssicherheitsrisiken
  - ISO/IEC 27017/27018 berücksichtigen Cloud-Spezifika
- **SOC 2, IDW PS 951, SSAE 16/18 und ISAE 3402**
  - Beurteilung interner Kontrollen bei Dienstleistern
  - Integrität der Daten im Rahmen der Finanzberichterstattung
- **COSO/COBIT**
  - Steuerung der IT bzw. Einhaltung von Compliance-Anforderungen
- **IT Infrastructure Library (ITIL)**
  - Serviceperspektive, insbesondere Fokus auf Verfügbarkeit
- u.v.m.

Quelle: Adelmeyer et al. 2017b, Königs 2017

Ausgewählte Kontroll-Frameworks

- BSI **Cloud Computing Compliance Controls Catalogue** (C5)
  - Richtet sich an Anbieter, deren Prüfer und Kunden
  - Fokus auf Informationssicherheit
- Cloud Security Alliance (CSA) **Cloud Controls Matrix** (CCM) v3.0.1
  - Deckt zentrale IT-Sicherheitskonzepte und -prinzipien ab
  - Basiert auf Standards, wie bspw. ISO 27000
- Information Systems Audit and Control Association (ISACA) **Cloud Computing Management Audit/Assurance Program**
  - Beurteilung interner Kontrollen von Anbietern durch Stakeholder
  - Anzupassende Basis für individuelle Überprüfungen
- European Network and Information Security Agency (ENISA) **Cloud Computing Security Risk Assessment**
  - Analyse von Informationssicherheitsrisiken im Kontext von CC

Agenda

1. Cloud Computing: Definition und Motivation
2. Risiken im Cloud Computing
3. Management von Cloud-Risiken
4. **Aktuelle Entwicklungen**
5. Zusammenfassung

IT Sicherheitsgesetz

- Verabschiedet am 12.06.2015
- Als Artikelgesetz eine Erweiterung bestehender Gesetze
- Adressaten des IT-Sicherheitsgesetzes (IT-SiG)
  - Bundesamt für Sicherheit in der Informationstechnik (BSI)
  - Betreiber von Webangeboten
  - Telekommunikationsunternehmen
  - **Betreiber Kritischer Infrastrukturen (kurz: KRITIS)**
- KRITIS sollen dazu verpflichtet werden ihre IT besser vor Cyber-Attacken zu schützen
- Verpflichtung zu angemessenen Sicherheitsmaßnahmen (Einhaltung des Stands der Technik), Audits und Meldepflichten für Vorfälle

→ Integration der Anforderungen in das (IT-)Risikomanagement

CC Risikomanagement im Kontext vom IT-SiG

Beim IT-Risikomanagement von Cloud-Dienstleistungen im Kontext des IT-SiG sind verschiedene Fälle zu unterscheiden:

1. KRITIS lagert Prozesse und Funktionen an einen Cloud-Dienstleister aus
2. KRITIS ist selbst Betreiber einer Cloud
3. Betrachtung des Cloud-Betreibers als Dienstleister von KRITIS

Quelle: Adelmeyer et al. 2017a

1. KRITIS lagert an einen Cloud-Dienstleister aus

- Bei Auslagerung von für die Funktionen der KRITIS maßgeblichen Systemen oder Prozessen (z. B. Rechenzentrums- oder IT Sicherheitsfunktionen) entstehen **Risiken im Kontext des IT-SiG**
- KRITIS-Betreiber ist im Falle von Verstößen gegen das IT-SiG primär verantwortlich
  → **Überwachung der IT-Risiken beim Dienstleister** erforderlich (z. B. durch entsprechende SLAs oder KPIs)
- Erfüllung der Anforderungen des IT-SiG durch Dienstleister sollte vertraglich festgelegt werden
- Absicherung durch Audits/Zertifikate (bspw. ISO 27001)
  - jedoch: Scope und zugrundeliegende Kriterien überprüfen
  - Orientierung an Best Practices des UP KRITIS oder TeleTrusT Handreichung zum geforderten Stand der Technik

Quelle: Adelmeyer et al. 2017a

2. KRITIS ist selbst Betreiber einer Cloud

- Aufbau eines Managementsystems für Informationssicherheit (**ISMS**) notwendig (z. B. nach ISO 27001)
- Identifikation und Beurteilung von Risiken anhand **bestehender Frameworks**, wie bspw.
  - CSA Cloud Controls Matrix
  - BSI-Sicherheitsempfehlungen für CC-Anbieter oder BSI C5
- Aufgaben des unternehmensinternen IT-Risikomanagements
  - Beurteilung und Überwachung der Risiken
  - Meldungspflichtige Vorfälle müssen identifiziert, kategorisiert und bewertet werden
- Betrieb der Cloud auf Basis von
  - gängigen Standards und Best Practices
  - den KRITIS-Betreiber betreffenden B3S (branchenspezifische Standards)

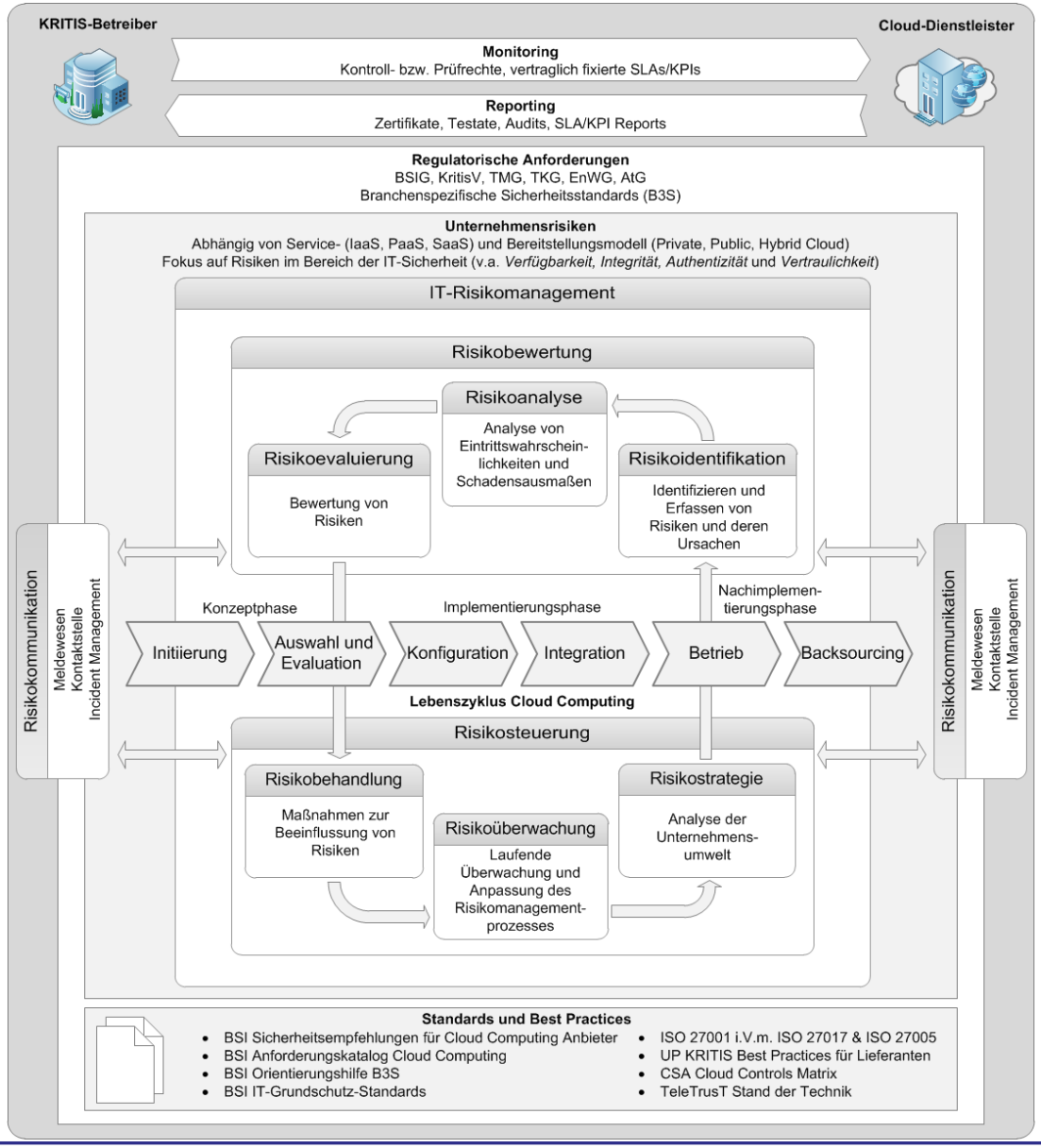
Quelle: Adelmeyer et al. 2017a

3. Cloud-Betreiber ist Dienstleister von KRITIS

- Cloud-Dienstleister muss meldepflichtige Vorfälle unverzüglich an den KRITIS-Betreiber melden
- Erreichbarkeit und die Funktionsfähigkeit der Kommunikationsstrukturen muss sichergestellt werden
- **Einhaltung der jeweiligen B3S**
  - Sofern ein Kunde (KRITIS) davon betroffen ist
  - Anforderungen auch im eigenen Unternehmen beachten, um Wettbewerbsvorteile zu erzielen
- Integration in das unternehmensinterne IT-Risiko- und Incident-Management, ggf. Zertifizierung sinnvoll
- Überprüfungen der Cloud-Dienste durch das BSI möglich bzw. zu erwarten (§ 7a Abs. 1 BSIG)

Quelle: Adelmeyer et al. 2017a

CC Risikomanagement im Kontext des IT-SiG



Adelmeyer et al. 2017a

Handlungsempfehlungen für KRITIS-Betreiber

Analyse bestehender Outsourcings

Überprüfung, ob eine Störung der ausgelagerten Systeme den Betrieb der KRITIS maßgeblich gefährden kann. Zudem: Prüfung von Vertragswerk/Zertifizierungen

Auswahl/Bewertung der Dienstleister

Beachtung der Kriterien aus dem IT-SiG. Orientierung für KRITIS an den Zertifikaten der Cloud-Dienstleister (z. B. ISO 27001)

Vertragsgestaltung mit Cloud-Dienstleister

Interne und durch das IT-SiG ergebene Anforderungen lassen sich über die Vertragsgestaltung an den Cloud-Dienstleister übertragen

Prüfrecht und Audits

Prüfrecht des KRITIS-Betreibers beim Dienstleister über Einhaltung der Anforderungen des IT-SiG sollten vertraglich fixiert werden

Koordination meldepflichtiger Vorfälle

Es müssen klare Strukturen und Prozesse mit Cloud-Dienstleistern entworfen und implementiert werden; Incidents müssen zeitgerecht gemeldet werden

Kooperation und Kommunikation

Insbesondere die Aufrechterhaltung des „Stands der Technik“ macht eine regelmäßige Kommunikation notwendig

Ausfallbedingte Kosten

Ermittlung der ausfallbedingten Kosten

Quelle: Adelmeyer et al. 2017a

Handlungsempfehlungen für Cloud-Betreiber

Klassifikation bzw. Kundenstammanalyse

Klassifikation anhand der festgelegten Schwellenwerte, proaktive Analyse des Kundenstamms hinsichtlich potentiell betroffener Kunden

Analyse bestehender Maßnahmen

Maßnahmen und Kontrollmechanismen im Rahmen der IT-Sicherheit sollen auf Basis von ISO 270xx evaluiert, entsprechende Vorkehrungen getroffen und Risiken identifiziert werden

Personal

Aufbau von Personal/Verantwortlichkeiten. Zudem muss bzgl. der Meldepflicht Personal für die Bewertung der Kritikalität und Meldung der Vorfälle vorhanden sein

Meldestruktur und Incident Management

Zur Meldung bzw. Eskalation relevanter Vorfälle müssen Verantwortlichkeiten und Prozesse geschaffen werden

Mitarbeit bei Branchenstandards

Potentiell betroffene Cloud-Betreiber sollten sich bei ihren Verbänden für ein vertretbares Niveau der branchenspezifischen Regelungen einsetzen

Dienstlokalisierung

Kontrollbedarf über Speicherort und Verarbeitung von Daten für KRITIS-Betreiber steigt. Sicherstellung der Compliance durch inländische Cloud-Dienstleistungen

Quelle: Adelmeyer et al. 2017a

EU Datenschutzgrundverordnung (DSGVO)

- Verabschiedet am 14. April 2016 durch die EU
- Anforderungen verbindlich ab 25. Mai 2018 umzusetzen
- Verbindliche Verordnung zur EU-weiten Harmonisierung der Vorschriften zum Schutz der Grundrechte und Grundfreiheiten bei der Verarbeitung personenbezogener Daten
- **Sechs Verarbeitungsgrundsätze**
  - Rechtmäßigkeit/Transparenz
  - Zweckbindung
  - Datenminimierung
  - Richtigkeit
  - Speicherbegrenzung
  - Integrität und Vertraulichkeit
- **Risikoorientierte Ausgestaltung der Anforderungen**

CC im Kontext von EU-DSGVO

- Datensicherheit: Cloud-Nutzer und Anbieter müssen geeignete Schutzmaßnahmen ergreifen (Artikel 32 Abs. 1 DSGVO)

„Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen **Eintrittswahrscheinlichkeit und Schwere des Risikos** für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein **dem Risiko angemessenes Schutzniveau** zu gewährleisten […]“

- Cloud-Nutzer bleiben als Auftraggeber der Datenverarbeitung hauptverantwortlich für den Schutz der Daten (Artikel 28 DSGVO)
  - Risikominimierung durch Risiko-Analysen und datenschutzrechtliche Prüfungen im Vorfeld
  - Hinreichende, „genehmigte“ Garantien des Dienstleisters notwendig
  - Kontrolle schwierig, daher müssen Cloud-Nutzer Provider genau auswählen, bspw. anhand von Zertifikaten (Artikel 32 DSGVO)

  → Cloud-Zertifizierungen bekommen einen neuen Stellenwert

CC im Kontext von EU-DSGVO

- Cloud-Migration muss gewährleistet werden („**Recht auf Datenübertragbarkeit**“)
- Nutzer haben unter bestimmten Voraussetzungen das Recht auf eine Kopie ihrer Daten in einem marktüblichen und maschinenlesbaren Format
- Ausländische Cloud-Anbieter müssen sich ebenfalls an die Vorgaben der DSGVO halten („Marktortprinzip“)
- Recht auf Löschung personenbezogener Daten in Clouds komplex
- Datenübermittlung in Drittstaaten unter folgenden Voraussetzungen möglich:
  - angemessenes Schutzniveau
  - geeignete Garantien, durchsetzbare Rechte und wirksame Rechtsbehelfe (z. B. „Binding Corporate Rules“) oder Standarddatenschutzklauseln

CC Risikomanagement im Kontext von EU-DSGVO

- **Bedeutung für das IT-Risikomanagement**
  - Individuelle Analyse der betroffenen Bereiche und Auswirkungen
  - Ist-Analyse sowie Ableitung von Maßnahmen
  - Umsetzungsplanung
- **Risikoorientiertes Monitoring und Umsetzung** der geforderten
  - Rechenschaftspflicht („Accountability“)
  - Technisch-organisatorischen Maßnahmen
  - Meldung von Datenschutzvorfällen an Behörden/Betroffene
- Berücksichtigung der Spezifika von Cloud-Dienstleistungen bei der Auftragsdatenverarbeitung, insbesondere rechtlicher Risiken
- Cloud-Anbieter trägt Teilverantwortung
- Erweiterung oder Integration der Anforderungen an den Datenschutz in bestehende IT-Risikomanagementprozesse

Agenda

1. Cloud Computing: Definition und Motivation
2. Risiken im Cloud Computing
3. Management von Cloud-Risiken
4. Aktuelle Entwicklungen
5. **Zusammenfassung**

Zusammenfassung

- Verbreitung und Relevanz von Cloud Computing steigt aufgrund vielfältiger Vorteile
- Einsatz geht mit Risiken einher, abhängig von der Art des Cloud-Services
- Management der Risiken über alle Phasen des Cloud-Lebenszyklus essentiell
- Verschiedene Methoden zum IT-Risikomanagement sind individuell einzusetzen
- Identifikation und Management der Cloud-Risiken mit Hilfe von Standards und Frameworks
- Anforderungen an Cloud-Dienste durch aktuelle gesetzliche Entwicklungen müssen entsprechend berücksichtigt und in das IT-Risikomanagement integriert werden

Michael Adelmeyer, M.Sc., CISA

Universität Osnabrück

Institut für Informationsmanagement und Unternehmensführung

Fachgebiet für Unternehmensrechnung und Wirtschaftsinformatik

Katharinenstr. 1, 49074 Osnabrück

www.uwi.uni-osnabrueck.de

michael.adelmeyer@uni-osnabrueck.de

Literatur

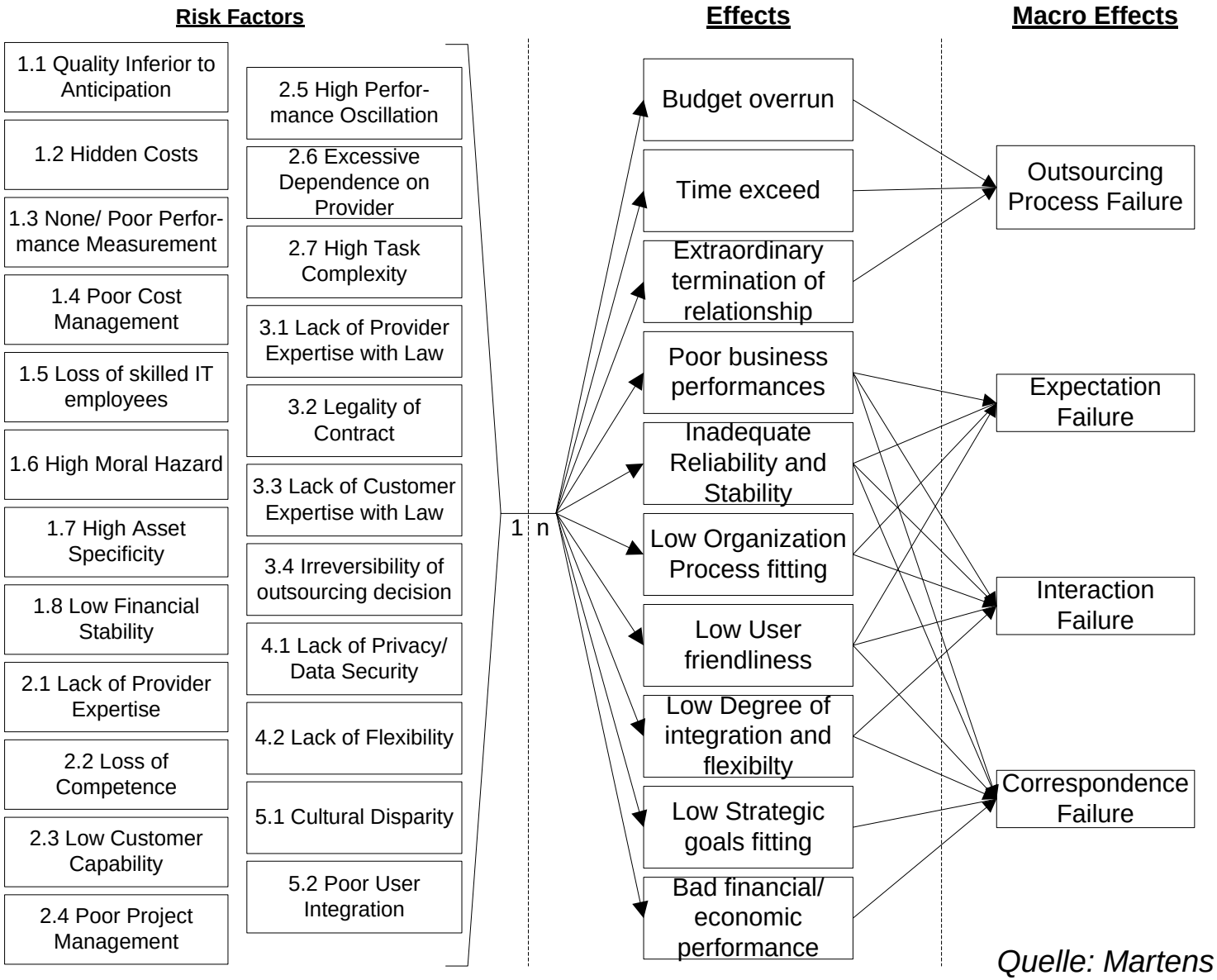
- Ackermann, T. (2012). IT security risk management: perceived IT security risks in the context of cloud computing. Springer Science & Business Media
- Adelmeyer, M.; Petrick, C.; Teuteberg, F. (2017a). IT-Risikomanagement von Cloud-Dienstleistungen im Kontext des IT-Sicherheitsgesetzes, HMD – Praxis der Wirtschaftsinformatik 54(1), S. 111-123
- Adelmeyer, M.; Walterbusch, M.; Lang, J.; Teuteberg, F. (2017b). Datenschutz und Datensicherheit im Cloud Computing, Die Wirtschaftsprüfung (WPg), Nr. 01
- Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., ... & Zaharia, M. (2010). A view of cloud computing. Communications of the ACM, 53(4), 50-58
- Junginger, M. (2005). Wertorientierte Steuerung von Risiken im Informationsmanagement. Springer-Verlag
- Knoll, M. (2014). Praxisorientiertes IT-Risikomanagement: Konzeption. Implementierung und Überprüfung, Heidelberg
- Königs, H. P. (2017). Risikomanagement bei Nutzung und Angebot Cloud-Computing. In IT-Risikomanagement mit System (pp. 381-404). Springer Fachmedien Wiesbaden

Literatur

- Martens, B.; Teuteberg, F. (2009). Why Risk Management Matters in IT Outsourcing – A Systematic Literature Review and Elements of a Research Agenda; In: Proceedings of the 17th European Conference on Information Systems
- Martens, B.; Teuteberg, F. (2011). Risk and Compliance Management for Cloud Computing Services: Designing a Reference Model, in: Proceedings of the Seventeenth Americas Conference on Information Systems
- NIST (2011). The NIST Definition of Cloud Computing
- Statista (2017). Umsatz mit Cloud Computing weltweit von 2009 bis 2016 und Prognose bis 2020 (in Milliarden US-Dollar). Abrufbar unter: https://de.statista.com/statistik/daten/studie/195760/umfrage/umsatz-mit-cloud-computing-weltweit-seit-2009/ (Stand 08.06.2017)
- Teuteberg, F. (2015). Kennzahlengestütztes Risikomanagement zum Monitoring von IT-Outsourcing-Aktivitäten am Beispiel des Cloud Computing, Controlling, Jg. 27, Nr. 6, S. 290-299, 2015

Backup

Risiken im IT-Outsourcing



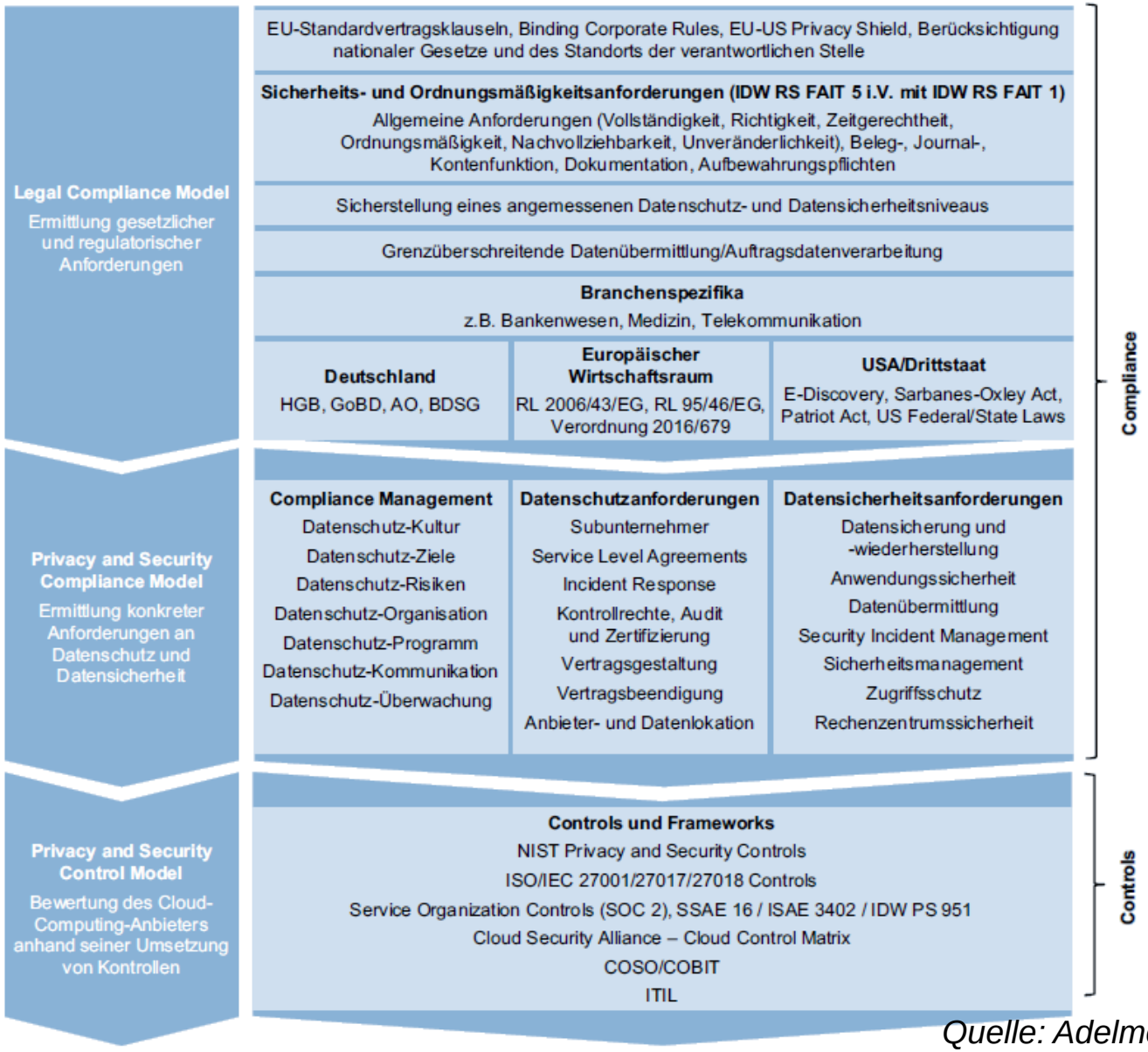
Quelle: Martens et al. 2009

Cloud Controls Matrix v3.0.1 - Domänen

- Application & Interface Security
- Audit Assurance & Compliance
- Business Continuity Mgmt & Op Resilience
- Change Control & Configuration Management
- Data Security & Information Lifecycle Mgmt
- Datacenter Security
- Encryption & Key Management
- Governance & Risk Management
- Human Resources Security
- Identity & Access Management
- Infrastructure & Virtualization
- Interoperability & Portability
- Mobile Security
- Sec. Incident Mgmt, E-Disc & Cloud Forensics
- Supply Chain Mgmt, Transparency & Accountability
- Threat & Vulnerability Management

16 Domänen
133 Kontrollen

Beurteilung von Datenschutz und Datensicherheit



Quelle: Adelmeyer et al. 2017b

Ausgewählte Methoden zur Unterstützung des Risikomanagements

Methoden	Risikoidentifikation	Risikoanalyse, -bewertung und -priorisierung
quantitativ	▪ Trendexploration ▪ Ertragsvolitalitätsanalyse (Earnings-at-Risk) ▪ Netzplantechnik ▪ …	▪ Nutzwertanalyse ▪ Key Performance Indikatoren/Kennzahlensysteme ▪ Value-at-Risk ▪ Total Cost of Ownership ▪ Methoden der Investitionsrechnung ▪ Analytische Entscheidungsmodelle ▪ Monte-Carlo-Simulation ▪ Sensitivitätsanalyse ▪ Risiko-Portfolio ▪ System Dynamics ▪ …
qualitativ	▪ Brainstorming und andere Kreativitätstechniken ▪ Risikochecklisten ▪ Dokumentenanalyse ▪ Experten-/Mitarbeiterbefragungen ▪ Prozess-/Ausfalleffekt-analysen ▪ Szenarioanalyse ▪ Risikodatenbanken ▪ Delphi-Studien ▪ Fehlermöglichkeits- und Einflussanalyse (FMEA) ▪ …	▪ Experten-/Mitarbeiterbefragungen ▪ Stärken-/Schwächenanalyse (z. B. SWOT) ▪ Konkurrentenanalyse ▪ Semi-formale Reifegrad-, Referenz- sowie Prozessmodelle ▪ Produktlebenszyklusanalyse ▪ Heuristische Ansätze ("Daumenregeln") ▪ Bewertung basierend auf vergangenen Erfahrungen (Historische Analogiemethode) ▪ …

Quelle: Teuteberg 2015