



universität
wien

MASTERARBEIT / MASTER'S THESIS

Titel der Masterarbeit / Title of the Master's Thesis

Ein Privacy Driven Governance Model
für Cloud Computing

verfasst von / submitted by

Ahmet Sehalic, BSc

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of
Diplom-Ingenieur (Dipl.-Ing.)

Wien 2018 / Vienna 2018

Studienkennzahl lt. Studienblatt /
degree programme code as it appears on
the student record sheet:

A 066 926

Studienrichtung lt. Studienblatt /
degree programme as it appears on
the student record sheet:

Masterstudium Wirtschaftsinformatik/Business Informatics

Betreut von / Supervisor:

Univ-Prof. Dipl.-Ing. DDr. Gerald Quirchmayr

Widmung und Danksagung

Ich bedanke mich bei meinem Betreuer Herrn Univ.-Prof. Dipl.-Ing. DDr. Gerald Quirchmayr, der mir während der Ausarbeitung meiner Forschungsarbeit, durch seine ruhige und freundliche Haltung, stets ermutigend mit konstruktiven und aufbauenden Ratschlägen zur Seite stand.

Ich bedanke mich vor allem bei meiner Frau, Aida Sehalic, für Ihr Verständnis, aufmerksames Korrekturlesen der Masterarbeit, für die Unterstützung während des Studiums sowie für alle Tipps, die Sie mir gegeben hat.

Ich bedanke mich noch bei der Frau Michelle Miller für Ihre Verbesserungsvorschläge und aufmerksames Korrekturlesen der Masterarbeit.

Eidesstattliche Erklärung

Ich erkläre hiermit, dass ich die vorliegende Arbeit selbstständig verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und mich auch sonst keiner unerlaubten Hilfe bedient habe. Die aus fremden Quellen direkt oder indirekt übernommenen Gedanken sind als solche kenntlich gemacht. Ich versichere, dass ich diese Masterarbeit bisher weder im Inland noch im Ausland zur Begutachtung in irgendeiner Form als Prüfungsarbeit vorgelegt habe. Sollte dennoch eine Urheberrechtsverletzung bekannt werden, ersuche ich um Meldung bei mir.

Wien, September 2018

Ahmet Sehalic

Unterschrift

Handwritten signature of Ahmet Sehalic in black ink.

Gender Erklärung

Aus Gründen der besseren Lesbarkeit wird in dieser Diplomarbeit die Sprachform des generischen Maskulinums angewendet.

Es wird an dieser Stelle darauf hingewiesen, dass die ausschließliche Verwendung der männlichen Form geschlechtsunabhängig verstanden werden soll.

Zusammenfassung

Diese Masterarbeit befasst sich mit der Entwicklung eines Privacy-Driven Governance Modells für Cloud Computing Infrastrukturen. Die Analyse der gegenwärtigen Situation fokussiert auf Cloud Computing, seine Eigenschaften, Arten von Cloud Services, Lifecycle- oder Artefact Governance, sowie den für diese Arbeit wesentlichen Aspekten serviceorientierter Architekturen und den nötigen Sicherheitsmaßnahmen für das zu entwickelnde Modell. Im anwendungsorientierten Teil wird ein Privacy-Driven Modell für Cloud Computing erstellt und mit einer konkreten Technologie verglichen. Abschließend wird die Frage der Anwendung des Modells auf zukünftige Technologien erörtert.

Abstract

This master thesis deals with the development of a privacy protection-oriented governance model for cloud computing. The analytical part focusses on cloud computing, its characteristics, types of cloud services, lifecycle vs. artifact governance, as well as relevant aspects of service-oriented architectures, and security measures for the envisaged model. Subsequently, a privacy-driven model for cloud computing is developed and compared with an existing technology. Ultimately, the applicability of the model to future technologies will be discussed.

Keywords: Cloud computing, cloud services, privacy-driven governance model, SOA, Governance

Inhaltverzeichnis

Widmung und Danksagung	4
Eidesstattliche Erklärung	5
Gender Erklärung	6
Zusammenfassung	7
Abstract	7
Inhaltverzeichnis	8
Einleitung	13
<i>Gliederung der Arbeit</i>	13
 1. Einordnung des Cloud Computing	16
1.1 Historische Entwicklung	16
1.2 Begriffsdefinition	18
1.3 Warum Cloud Computing?	23
 2. Essentielle Eigenschaften von Cloud Computing	24
2.1 On-Demand Service	24
2.2 Zugriff über das (Inter)-Net	24
2.3 Ressourcenpools	25
2.4 Skalierbarkeit	25
2.5 Messbarkeit der Services	26
2.6 Open Cloud Manifesto	27
 3. Cloud-App-Plattformen	28
3.1 Typen und Ebenen von Clouds	28

Inhaltverzeichnis

3.2 IaaS.....	30
3.3 PaaS	31
3.4 Cloud-Anwendungsplattformen.....	32
3.4.1 Domain-agnostic orientation	33
3.4.2 Domain-specific orientation.....	33
3.5 SaaS	34
3.6 Cloud Service Broker	35
3.7 „as a Service“	36
3.8 IaaS, PaaS, und SaaS: Unterschiede und Ähnlichkeiten.....	36
3.9 SPI	38
4. Typen von Cloud Services.....	39
4.1 Private Cloud.....	40
4.2 Public Cloud	41
4.3 Hybrid Cloud	42
4.4 Community Cloud.....	43
4.5 Trusted Cloud.....	44
5. Motivation für Policy-Driven Governance in Cloud Application Platforms.....	47
5.1 Definitionen der Governance	47
5.2 Cloud Governance vs. Cloud Management.....	54
5.3 Abgrenzung Cloud Governance - SOA Governance	55
5.4 Policy-Driven Governance in Cloud Application Platforms	58

Inhaltverzeichnis

6. Lifecycle vs. Artefact Governance	64
6.1 Lifecycle Governance	64
6.2 Prozess- & Artefact Governance	65
6.3 Einschränkungen	67
6.4 Ontologie-basierter Ansatz, Ziel, Datenschutz	68
6.5 Forschungsstand.....	69
7. SOA.....	71
7.1 Problemverständnis	71
7.2 Wechselwirkung zwischen Business und IT	73
7.3 Die Essenz von SOA-Governance.....	75
7.3.1 Was ist Governance?.....	75
7.3.2 Was ist IT Governance?	78
7.4 Was ist SOA?.....	78
7.5 Säulen der Serviceorientierung.....	85
7.6 SOA Stufen der Organisatorische Reife	87
7.7. Key Governance Themen	88
7.7.1 Collect the right metrics	88
7.7.2 Transparenz.....	88
7.7.3 Compliance	88
7.8 Governance, Risk und Compliance	90
7.9 SOA Governance - Häufigste Fehler	93

Inhaltverzeichnis

8. Sicherheitsmaßnahmen.....	95
8.1 Vulnerabilities.....	99
8.2 Missbrauchsgefahren.....	100
8.3 Empfehlungen für die Policies	101
8.3.2 Data Loss Prevention.....	101
8.3.3 Data Leak Protection (DLP).....	103
8.3.4 Data at rest.....	103
8.3.5 Daten in Bewegung (Data in motion (network)).....	104
8.3.6 Data in use (end-point)	105
9. Compliances Challenges	106
9.1 Audit.....	106
9.2 Digital Rights Management (DRM)	106
10. Entwicklung eines Governance Modells	107
10.1 Bestehende Governance Modelle.....	107
10.2 Anforderungen für ein wirksames Governance Modell.....	114
10.2.1 GDPR.....	116
10.2.2 GDPR-Schlüsseländerungen.....	117
10.2.3 Individuelle Rechte und Rechtsmittel.....	118
10.2.4 ISO/IEC 27000 family - Information security management systems (ISMS)	119
11. Privacy-Driven Governance Modell	121
11.1 Konstruktion eines Governance Modells	121

11.2 Was ist Perfect Forward Secrecy?.....	133
11.3 Reality Check / Praxis Test – Anwendungsbeispiel für MS Windows Azure	134
11.4 Zukünftige Anwendung des Modells	137
12. Conclusio	140
12.1 Diskussion der Ergebnisse	140
12.2 Lessons learned	141
13. Abbildungsverzeichnis	143
14. Tabellenverzeichnis	146
15. Literaturverzeichnis	147
16. Abkürzungsverzeichnis	156

Einleitung

Cloud Computing ist ein Thema, das in der Gegenwart nicht nur immer präsenter, sondern auch immer komplexer wird. Mit seiner Verbreitung steigt der Bedarf daran, die privacy-driven Governance besser verstehen und implementieren zu wollen. Diese Komplexität der Cloud-Computing-Umgebung führt dazu, dass die unerwünschten Sicherheitsrisiken steigen. Somit wird die Wahrscheinlichkeit für die Entstehung von potenziellen Fehlern, die für das System insgesamt gefährlicher werden, immer größer. Um herauszufinden, wie diese Sicherheitsrisiken minimiert und bessere datenschutzorientierte Governance angeboten werden kann, wird in dieser Arbeit ein privacy-driven Governance Modell für Cloud Computing erstellt und analysiert. Um diesem Ziel möglichst nahe zu kommen, werden in den nachstehenden Kapiteln die wichtigsten Fragen fundiert beantwortet und die Inhalte der Arbeit wie folgt aufgebaut.

Gliederung der Arbeit

Das erste Kapitel beschreibt die historische Entwicklung von Cloud Computing. Außerdem wird versucht mit Hilfe der gängigen Literatur Cloud Computing genau zu definieren.

Im zweiten Kapitel werden Essentielle Eigenschaften von Cloud Computing genannt und beschrieben.

Das dritte Kapitel setzt sich mit der Arten und Ebenen von Clouds beschäftigt und die Unterschiede und Ähnlichkeiten analysiert. Die Cloud-Anwendungsplattformen werden zusammen mit dem Cloud Service Broker dargestellt.

Einleitung

Das vierte Kapitel befasst sich mit der Analyse und dem Vergleich der unterschiedlichen Arten von Cloud Services

Es werden auch die Begriffe, wie z.B. Trusted Cloud dargestellt. Des Weiteren wird gezeigt, wofür Trusted Cloud wichtig ist.

Kapitel 5 widmet sich der Frage, warum policy-driven Governance in Cloud-Applikation-Plattform gebraucht werden? Dabei wird Cloud Governance sowohl mit Cloud Management als auch mit SOA Governance verglichen.

Im sechsten Kapitel diskutiert über die unterschiedlichen Anwendungsmöglichkeiten und Beschränkungen von Lifecycle- und Artefact Governance.

Im Rahmen des siebten Kapitels wird serviceorientierte Architektur und Key-Governance thematisiert.

Die Analyse der Sicherheitsmaßnahmen sowie von Vulnerabilities, Threads, Data Loss und Data Leak Prevention erfolgt im achten Kapitel. Hier werden außerdem Empfehlungen für die Policies gegeben. Die Compliances Challenges werden kurz im neunten Kapitel besprochen.

Das Kapitel 10 befasst sich parallel mit der Modellentwicklung und mit den bereits bestehenden Governance Modellen sowie Anforderungen für ein wirksames Governance Modell

Aufbauend auf der Forschungsarbeit wird im Kapitel 11 ein privacy-driven Governance Modell gebaut. Es wird sowohl ein Praxistest mit

einem Anwendungsbeispiel durchgeführt als auch ein Ausblick auf die Anwendung des Modells in Zukunft gegeben.

Das zwölfte und letzte Kapitel schließt die Arbeit mit der Diskussion der Ergebnisse ab.

1. Einordnung des Cloud Computing

In diesem Kapitel wird der Entstehungs- und Entwicklungsprozess von Cloud Computing beschrieben und der Begriff Cloud Computing definiert. Es wird auch eine Auflistung von verfügbaren Typen und Ebenen gegeben.

1.1 Historische Entwicklung

Nach dem Zweiten Weltkrieg wurden in den Vereinigten Staaten große Mainframerechner in den Schulen, Regierungsgebäuden und großen Konzernen installiert. Mainframerechner waren aufgrund hoher Hardwarekosten schwierig zu skalieren und zu erstellen. In der Nachkriegszeit waren diese Institutionen in den USA die Einzigen, denn nur dort war es möglich, diese Rechner installieren und betreuen zu können. Aufgrund ihrer ausserordentlichen Größe war es nicht möglich, eine Vielzahl von diesen Geräten in nur einer Institution zu platzieren. Aus diesem Grund wurden die so genannten „dummen Terminale“ entwickelt, die an die Mainframerechner angeschlossen waren. Auf diesen Rechnern konnte einer Vielzahl der Nutzer und Nutzerinnen der Zugriff auf die notwendigen Ressourcen, welche auf dem Rechner gespeichert wurden, ermöglicht werden. Allerdings waren die Hardwarekosten vergleichsweise sehr hoch und die auftretenden Probleme äusserst schwer zu skalieren. [ego13]

In den 60er waren die Mainframerechner beachtlich effizient und boten den Benutzern eine besonders akzeptable Performance an.

1. Einordnung des Cloud Computing

Die Benutzer waren nicht im Besitz über die volle Kontrolle der Performance von Mainframeapplikationen. Die Performance wurde von der Benutzerzahl, die den Mainframe in einem zeitlichen Moment zeitgleich genützt haben, abhängig. Es fehlte die Möglichkeit die volle Kontrolle über die eigenen PC-Ressourcen zu übernehmen. [ego13]

Ein paar Jahre später entwickeln die Forscher am MIT¹ die Idee, „eine Computerleistung über ein vorhandenes Netzwerk als Dienst anzubieten.“ [gfg14] In einem Vortrag aus dem Jahr 1961 sagte McCarthy den berühmten Satz „*Computation kann eines Tages als öffentlicher Dienst organisiert werden*“².

Im Jahr 1966 wurde „Intergalactic Computer Network“, eine Idee von J.C.R Licklider, eingeführt. [kdv10]

In dem selben Jahr veröffentlichte der kanadischer Ingenieur Douglass Parkhill das Buch „The Challenge of the Computer Utility“, in welchem er die Idee von Computing als „public utility“ mit zentralisiertem „facility“ beschrieb und zu welchem sich viele externe Benutzer über das Netzwerk verbinden konnten.[ego13]

Erst viele Jahre später (2002) entwickelte Amazon zunächst Web Service. Nach weiteren 4 Jahren folgen Elastic Computer Cloud (EC2). [wpcc09] Diese zwei Technologien waren große Schritte in der Cloud Computing Entwicklung, die heute bekannt sind. [kdv10]
Cloud Computing kombiniert das Beste aus der Mainframe-Ära

¹ Massachusetts Institute of Technology

² [car61]

1. Einordnung des Cloud Computing

mit dem Besten aus der PC-fähigen Client-Server-Ära und geht der Internet-Ära zusammen. Heute besteht die Möglichkeit, ohne Hardware zu kaufen oder Rechenzentren zu bauen, Cloud Computing im großen Maßstab mit einem Pay-As-You-Go-Abrechnungsmodell und Geschwindigkeiten, die nie zuvor erreicht wurden, anzubieten. [ego13]

Der erste gesprochene Verweis auf den Begriff "Cloud Computing" im modernen Sinn stammt von Eric Schmidt, CEO³ von Google im August 2006: "Es beginnt mit der Prämisse, dass sich die Datendienste und die Architektur auf Servern befinden sollten. Wir nennen es Cloud Computing - sie sollten irgendwo in einer "Wolke" sein."⁴ Ein paar Wochen später kündigte Amazon sein Angebot Elastic Compute Cloud (EC2) an und der Begriff unterlag breiter Akzeptanz. [dko16]

1.2 Begriffsdefinition

Inzwischen sind unterschiedliche Cloud-Computing-Definitionen und Interpretationen aus diversen Quellen bekannt. Der Begriff „Cloud Computing“ stammt nach [ego13] aus den Netzwerkdiagrammen, in welchen Cloud-Form genutzt werden, um die bestimmten Netzwerktypen zu beschreiben, unabhängig davon, ob es sich um Internet- oder Intranet-Netzwerke handelt. [ego13]

³ Chief executive officer

⁴ "Konversation mit Eric Schmidt gehostet von Danny Sullivan" veröffentlicht in *Search Engine Strategies Conference*, 2006.

1. Einordnung des Cloud Computing

Die anderen Quellen sehen Cloud Computing als eine Gruppe von Applikationen, die als Services in Kombination mit dem Datenzentrum für Hardware und Software, das die Applikationen ermöglicht, dienen. Cloud Computing geht davon aus, dass jede Softwareapplikation oder Systemkomponente einen Service erhält oder ein Teil vom Service ist. [ego13]

Laut [ego13] besteht Cloud Computing sowohl aus technologischen als auch aus Businesskomponenten. Bestimmte Technologien, wie Open-Source Software, Virtualisierungen, verteilter Speicher, verteilte Datenbanken und Überwachungssysteme bilden die Eckpfeiler der Cloud Infrastruktur.

Unter Cloud Computing wird das Konzept der Bereitstellung von Ressourcen und Services über Internet-Technologien verstanden. Als Informationsressource können die Benutzer nicht nur Software- sondern auch Speicherkapazitäten und CPU-Zeit erwerben. Es bietet Unternehmen die Möglichkeit ihre Business-Anwendungen und E-Mail-Server nicht auf der eigenen IT-Infrastruktur zu realisieren, sondern diese in die Cloud auszulagern. Dadurch entfallen Investitionen im Hard- und Softwarebereich für die in Anspruch nehmenden Unternehmen. [mgt09]

Ein Cloud-Service beschreibt daher die Implementierung eines Geschäftsprozesses, der durch eine Reihe von verwandten, funktionalen Komponenten und Ressourcen bereitgestellt wird und seinen Verbrauchern Business-Werte bietet. [rup16]

1. Einordnung des Cloud Computing

Aus den zahlreichen Definitionen, die über Cloud Computing bis heute in der Forschungsliteratur erschienen sind, sei die Definition vom NIST⁵ zu erwähnen.

NIST gibt dabei die Definitionsempfehlungen an einer Spezialpublikation, welche im September 2011 veröffentlicht wurde. Vor allen der vier Betriebsmodellen, drei verschiedenen Servicemodellen und fünf essentiellen Eigenschaften definiert NIST Cloud Computing sinngemäß in dieser Publikation folgendermaßen: [nis11]

NIST sieht das Cloud Computing als ein Modell (Abbildung 1), das allgegenwärtig geeignete Netzwerkzugriffe auf Anforderung (On-Demand) von gemeinsamen Ansammlungen der konfigurierten Computing-Ressourcen (z. B. Netzwerken, Servers, Speicher, Applikationen und Dienstleistungen) ermöglichen kann und eine hohe und schnelle Skalierbarkeit besitzt. [nis11]

⁵ National Institute of Standards and Technology

1. Einordnung des Cloud Computing

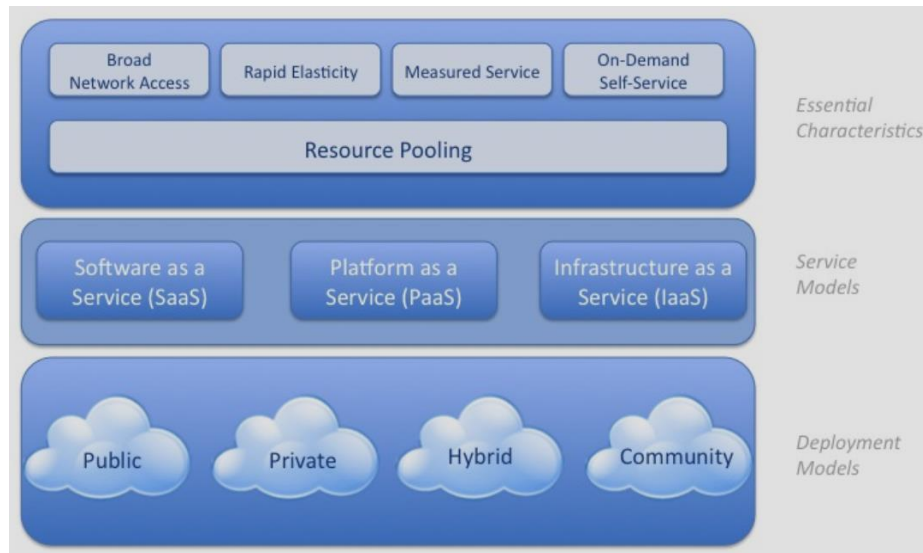


*Abbildung 1: NIST Ein visuelles Modell von Cloud Computing
Definition [csa09]*

Das Modell ermöglicht laufende Verfügbarkeit von allen essentiellen Eigenschaften einer Cloud. Mit einem minimalen Managementbedarf von Dienstleistungsanbietern werden dem Cloud-Nutzer schnell und bedarfsgerecht notwendige Funktionen, wie Speicherbedarf oder Rechenleistung, zur Verfügung gestellt. [rup16]

Diese Definition wird auch von ENISA⁶ verwendet.

⁶ European Network und Information Security Agency

1. Einordnung des Cloud Computing

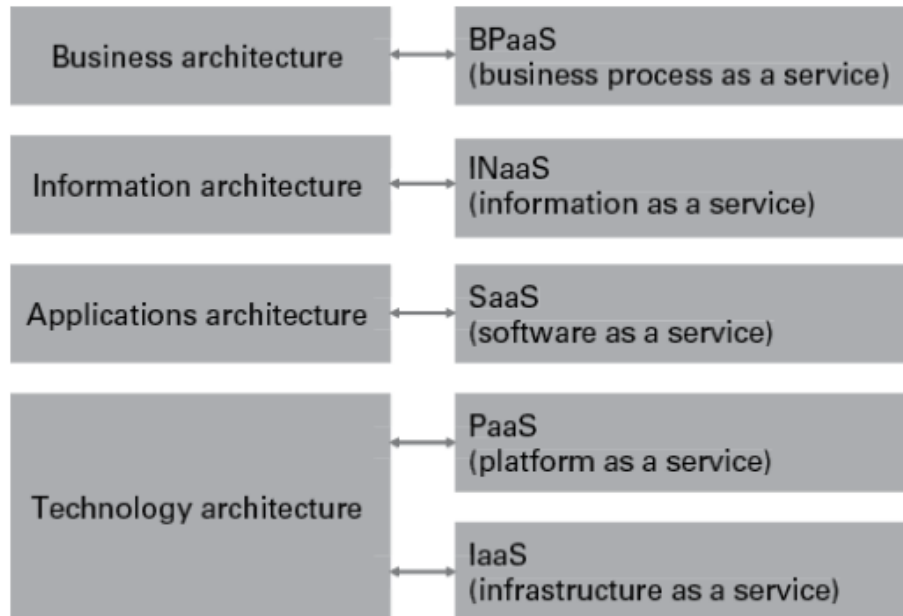


*Abbildung 2: Enterprise Architecture Stack
und erweitertes Cloud Service-Modell [rup16]*

Die IT-Unternehmensarchitektur erkennt vier Architekturdomänen, welche in der linken Spalte von Abbildung 2 dargestellt werden. Diese vier Architekturdomänen sind Technologiearchitektur, Anwendungsarchitektur, Informations- oder Datenarchitektur und Business-Architektur. [rup16]

Bei der Technologiearchitektur handelt es sich um die IT-Infrastruktur, Middleware sowie Betriebssysteme. Die Anwendungsarchitektur betrifft Softwareanwendungen, ihre Interaktionen und Beziehungen zu Geschäftsprozessen. Die Datenarchitektur definiert die Daten Assets und deren Management sowie die Business-Architektur. Die Datenarchitektur wandelt auch die Geschäftsstrategie in IT-Strategie.

1. Einordnung des Cloud Computing

Jede dieser Domänen bildet sich in der Unternehmensarchitektur ab und richtet sich nach den Cloud-Service-Modellen aus, welche in der rechten Spalte von Abbildung 2 dargestellt sind. [rup16]

1.3 Warum Cloud Computing?

Im anschließenden Hauptkapitel „Essentielle Eigenschaften von Cloud Computing“ werden nur einige von den elementarsten Gründen erwähnt, warum die Unternehmen Cloud Computing nutzen sollen.

Elastizität, On-Demand Service, Zugriff über das (Inter)-Net, Ressourcenpools, Skalierbarkeit und Messbarkeit der Services sind die Eigenschaften, die auf oben gestellte Frage eine Antwort geben können.

[ego13]

2. Essentielle Eigenschaften von Cloud Computing

„Cloud Computing ist ein Modell, das den allgegenwärtigen, bequemen, bedarfsgesteuerten Netzwerkzugriff auf einen gemeinsam genutzten Pool konfigurierbarer Rechenressourcen ermöglicht (z. B. Netzwerke, Servers, Storage, Applikationen und Services).“ [nis11]
Diese können schnell bereitgestellt und mit minimalem Verwaltungsaufwand oder Interaktion mit dem Dienstanbieter freigegeben werden. [nis11]

Cloud-Services zeigen fünf wesentliche Merkmale auf, welche ihre grundsätzliche Beziehung zu traditionellen Computing-Ansätzen näher beschreiben sowie auch in welchen ihre Unterschiede liegen. [nis11]

2.1 On-Demand Service

On-Demand Service bietet dem Benutzer die Möglichkeit an, selbst zu entscheiden, wann er Rechenleistung oder Netzwerkspeicher vom Cloud-Anbieter verwenden möchte. [gfg14]. Der Prozess wird ohne die Wechselwirkung mit einem humanoiden Nutzer verlangt. [bsi10]
[mgt09]

2.2 Zugriff über das (Inter)-Net

Der Zugriff wird auf Cloud Services über das Netzwerk mittels der standardisierten Mechanismen vorgesehen. Dabei wird dem Benutzer

2. Essentielle Eigenschaften von Cloud Computing

ein Nutzungsspektrum von unterschiedlichen Geräten, wie bspw. Smartphones, Laptops, PDAs⁷, IoT⁸-Geräte, angeboten, mit denen er die Cloud Services nutzen kann. [mgt09]

2.3 Ressourcenpools

Die typischen Ressourcenbeispiele sind Lagerung, Verarbeitung, Speicher, Netzwerkbandbreite und virtuelle Maschinen. [gfg14][nis11] Diese Rechenressourcen des Anbieters können gepolt werden, um mehrere Kunden mit einem mandantentauglichen Modell bedienen zu können. Die Kunden werden in diesem Modell dynamisch verschiedene physische und virtuelle Ressourcen zugewiesen und je nach Verbrauchsnachfrage werden sie neu zugeteilt. [nis11]

Diese sind in einem Ressourcenpool zusammengefasst und können i.d.R., über eine virtualisierte Ebene, ortsunabhängig verwendet werden. Somit können mehrere Benutzer dieselbe Infrastruktur benutzen. [mgt09]

Sogar private Clouds neigen dazu, die Ressourcen zwischen verschiedenen Teilen, ein und derselben Organisation zu bündeln. [nis11]

2.4 Skalierbarkeit

Die Benutzer erwarten unter anderem den Service, die Rechenkapazität nach oben oder nach unten zu skalieren. [ego13] Mit Hilfe der Ska-

⁷ Personal digital assistant

⁸ Internet of Things Geräte

2. Essentielle Eigenschaften von Cloud Computing

lierbarkeit werden auch potenzielle Wachstumsbeschränkungen von Cloudanwendungen vermieden. [gfg14][mgt09]

Die potenziellen Probleme mit rasant steigenden Nachfragen werden durch Skalierbarkeit kurzfristig gelöst. Dem Benutzer werden problemlos, der Nachfrage entsprechende, Ressourcen zur Verfügung gestellt. [gfg14][mgt09]

2.5 Messbarkeit der Services

„Cloud-Systeme steuern und optimieren die Ressourcennutzung automatisch.“ Die Dosierfähigkeit ist auf einer gewissen Abstraktionsebene von der Art der Bedienung (Speicher, Bandbreite oder aktive Benutzerkontos) abhängig. [nis11]

Die NIST-Definition listet fünf Merkmale des Cloud-Computing auf, die in der zweiten Spalte von Tabelle 1 aufgeführt sind: ubiquitärer Zugriff, On-Demand-Verfügbarkeit basierend auf Self-Service des Verbrauchers, Bündelung von Ressourcen, schnelle Elastizität und gemessene Dienstnutzung:

	Characteristic	Description	Parameter
1.	Broad network access	Consume services from anywhere	Where

2. Essentielle Eigenschaften von Cloud Computing

2.	On-demand self-service	Consume services when you want	When
3.	Resource pooling and virtualization	Pool the infrastructure, virtual platforms, and applications	How
4.	Rapid elasticity	Share pooled resources to enable horizontal scalability	How
5.	Measured Service	Pay for the service you consume as you consume it	How much

Tabelle 1: Fünf Charakteristiken des Cloud Computings [rup16]

2.6 Open Cloud Manifesto

Obgleich in dieser Arbeit aus Kapazitätsgründen das Thema Open Cloud Manifesto⁹ nicht tiefer diskutiert wird, bleibt zu erwähnen, dass Open Cloud Manifesto im Jahr 2009 von einer Gruppe von Unternehmen (IBM, Intel, Google) entwickelt wurde, mit dem Ziel die Methode vorzuschlagen, die dann für die Verwendung, in der Regelung, von Cloud-Computing-Services genutzt werden können.

Cloud Computing ist in Open Cloud Manifesto mit einer Reihe von Charakteristiken und Wertvorstellungen definiert. [kdv10]

⁹ www.opencloudmanifesto.org

3. Cloud-App-Plattformen

3.1 Typen und Ebenen von Clouds

Cloud-Services werden in drei Kategorien eingeteilt:

- SaaS (Software as a service),
- PaaS (Platform as a service) und
- IaaS (Infrastructure as a service).

Alle drei Kategorien können in privaten, öffentlichen und hybriden Cloud Umgebungen implementiert werden und werden nachfolgend detailliert erklärt. [ego13]

In der Tabelle 2 ist die Einteilung der Hauptkategorien, als auch die Unterteilung in den Ebenen ersichtlich.

3. Cloud-App-Plattformen

• Applications • Data	• Applications • Data	• Applications • Data	
• Runtime • Middleware • O/S	• Runtime • Middleware • O/S	• Runtime • Middleware • O/S	Cloud Customer Responsibility
• Virtualization • Servers	• Virtualization • Servers	• Virtualization • Servers	Cloud Provider Responsibility
• Storage • Networking	• Storage • Networking	• Storage • Networking	
IaaS	PaaS	SaaS	

Tabelle 2: Cloud-Service/Modelle und die Zuständigkeit [Ifu15]

3.2 IaaS

IaaS stellt Basis für infrastrukturelle Komponenten für Clients, dabei bestehen diese unter anderem aus virtuellen Maschinen, Speicher, Netzwerke, Firewalls und Loadbalancer. Außerdem zählen alle Infrastrukturkomponenten wie Server, Rechenleistung, Speicher- und Netzkapazitäten zu dieser Betrachtung mit. [ego13] Darüber hinaus wird die gesamte Rechenzentrums- und Netzinfrastruktur zur Verfügung gestellt. Der Benutzer (der Kunde) kann diese Ressourcen über das Netz per Service benutzen. [Han10]

IaaS liefert PC-Infrastruktur as a Service. [csa11] Es geht um eine virtualisierte Umgebung samt notwendigem Rechenzentrum und Software.

Die Klienten kaufen allein die Ressourcen als vollständig ausgelagerten Service. [kav14]

Typische Beispiele sind Amazon EC2¹⁰ und S3¹¹ oder Microsoft Windows Azure Virtual Machines.

Amazon Web Services ist beispielweise einer der größten IaaS-Anbieter.

¹⁰ Amazon Elastic Compute Cloud

¹¹ Amazon Simple Storage Service

3.3 PaaS

Nach dem IaaS ist die PaaS die nächste Ebene des Cloud Computing. PaaS liefert vordefinierte Applikation-Plattform für Klienten.

Was IaaS für Infrastruktur ist, ist PaaS für die Anwendungen. PaaS setzt direkt auf IaaS auf und abstrahieren einen Großteil der Standardanwendung wie Stack-Level-Funktionen und es stellt diese Funktionen als Service zur Verfügung.

Zum Beispiel, wenn die Entwickler High-Scaling Systeme entwerfen, muss häufig eine beachtliche Menge an Programmcode geschrieben werden, um Caching, asynchrones Messaging, Datenbank-Skalierung und viel mehr zu behandeln.

Viele PaaS-Lösungen bieten Fähigkeiten wie Caching, asynchrones Messaging, Datenbank-Skalierung und vieles mehr als Service an. Die Entwickler können sich auf Business-Logik konzentrieren und verlieren keine unnötige Zeit für die Codierung der obengenannten Services.

[kav14]

Im Hintergrund skaliert PaaS automatisch in Abhängigkeit von Applikationsanforderungen die benötigten infrastrukturellen Komponenten. PaaS Lösungen liefern ein API¹², welches einen Satz von Funktionen für die Lösungsentwicklung und für programmierbares Plattformmanagement beinhaltet. [ego13]

¹² Application programming interface

3. Cloud-App-Plattformen

Über die Programmierschnittstellen, die sogenannten API's, werden Dienste wie Datenbanken sowie weitere Software bereitgestellt.

[han10]

Einige Beispiele sind Google AppEngine und Amazon Web Services, die neben IaaS- auch einige PaaS-Lösungen anbietet.

Die CSA¹³ erwähnt, dass PaaS-Dienste vollständig über das Internet verfügbar sind.

Ein weiterer großer Vorteil von PaaS ist, dass diese Plattformen sich mit zahlreichen Drittanbieter-Software Lösungen integrieren lassen, die vielfach als Plugins, Add-Ons oder Erweiterungen bezeichnet werden. Hier sind einige Beispiele für Kategorien von Erweiterungen, die in den meisten ausgereiften PaaS-Lösungen zu finden sind: Datenbanken, Logging, Monitoring, Security, Caching, Search, E-Mail, Analytics und Payments. [kav14]

3.4 Cloud-Anwendungsplattformen

Die Vorteile, welche Anwendungsentwickler durch die Einführung eines PaaS-Angebots erhalten können, sind von den Eigenschaften der jeweiligen Plattform abhängig. In groben Zügen können Cloud-Anwendungsentwicklungsplattformen, die als PaaS-Angebote bereitgestellt werden, als Plattformen mit domänenunabhängiger oder domänenspezifischer Ausrichtung klassifiziert werden. [dco16]

¹³ The Cloud Security Alliance

3. Cloud-App-Plattformen

3.4.1 Domain-agnostic orientation

Diese Cloud-Anwendungsplattformen stellen Computerinfrastruktur und einen Server-Software-Stack für die Entwicklung und Bereitstellung von webbasierten Anwendungen bereit. Die Anwendungsplattform verwendet eine bestimmte Programmiersprache oder ein Framework, unabhängig von einer bestimmten Anwendungsdomäne. Beispiele hierfür sind Google App Engine, Microsoft Azure und Heroku. [dko16]

3.4.2 Domain-specific orientation

Diese Cloud-Anwendungsplattformen bieten auch analoge Funktionen für die Entwicklung und Ausführung von Anwendungen wie Cloud-Anwendungsplattform unter 3.4.1 beschrieben wurde an.

Der einzige Unterschied ist in zusätzlichen Komponenten und Anwendungsprogrammierschnittstellen (APIs), welche auf eine bestimmte Domäne spezialisiert sind.

Beispiele für solche Plattformen sind SAP PaaS für E-Commerce, Force.com für Kundenbeziehungsmanagement, Intuit Developer für das Rechnungswesen und Zoho Creator für situative Anwendungen.

Ein wichtiger Vorteil insbesondere von Cloud-Anwendungsplattformen für Entwickler von kommerziellen Anwendungen (ISVs) ist, dass sie es einfacher machen, Anwendungen zu vermarkten und an potenzielle Benutzer zu verteilen. [dko16]

3.5 SaaS

Software as a Service liefert Online Software Lösungen. SaaS Software Anbieter besitzt komplette Kontrolle über die Applikationssoftware. Die Beispiele für SaaS Applikationen umfassen Online-Email, Projektmanagement System, ERP (Enterprise Ressource Planung) CRMs (Customer Relationship Management) und die Plattformen für soziale Medien. [eg013]

SaaS ist ein Cloud Computing Typ der PaaS sehr ähnlich ist. Es werden jedoch nicht nur Programmierschnittstellen, sondern auch die vollständige Software des Cloud-Anbieters zur Verfügung gestellt.

Vorteilhaft sind vergleichsweise überschaubare Kosten, da SaaS dem „Economies-of-scale“¹⁴ Modell folgt. Das Modell basiert auf Volumengeschäft mit einem niedrigen Preis.

Einer der bekanntesten Vertreter für SaaS ist Google mit seinen Webapplikationen¹⁵ [mgt09]

Diese Infrastruktur besteht aus: Netzwerk, Server, Betriebssystem, Speicher oder aus einzelnen Anwendungsmöglichkeiten inkludiert mit denkbaren Ausnahmen von eingeschränkten benutzerspezifischen Anwendungskonfigurationseinstellungen. [kav14]

¹⁴ “Eine Economy of Scale ist eine Wirtschaftssprache, die große Einheiten bedeutet, egal ob Unternehmen, Non-Profit-Organisationen oder Regierungen, die Ausgaben einfach wegen ihrer Masse senken können.“ [rsa15]

¹⁵ <http://google.com/apps/>

3.6 Cloud Service Broker

Das NIST-Modell befasst sich nur am Rande mit den neu entstehenden Service-Modelldefinitionen von Cloud-Service-Brokern und Anbietern.

Diese Cloud-Service-Broker und Anbieter bieten die Vermittlungs-, Überwachungs-, Umwandlungs-, Portabilitäts-, Governance-, Bereitstellungs- und Integrationsdienste an. Sie verhandeln Beziehungen zwischen verschiedenen Cloud-Anbietern und Kunden.

Die Innovationen treiben kurzfristig die schnelle Entwicklung von Lösungen an, während Verbraucher und Anbieter von Cloud-Diensten unterschiedliche Methoden der Interaktion mit Cloud-Diensten in Form von APIs und Schnittstellen besitzen. Cloud-Service-Broker werden zu einer wichtigen Komponente im gesamten Cloud-Ökosystem.

In Cloud-Service-Broker werden diese, möglicherweise inkompatiblen, Funktionen und Schnittstellen abstrahieren. Im Auftrag von Kunden soll Cloud-Service-Broker in der Lage sein, einen Proxy zu bieten und das Problem mit einer semantischen Fähigkeit längerfristig zu lösen.

Diese Fähigkeit ermöglicht dem Verbraucher fließend und agil, das Modell das für seine speziellen Bedürfnisse am besten geeignet ist, zu nutzen. [csa11]

3.7 „as a Service“

Es können viele weitere „as a Service-“ Angebote Kunden angeboten werden, wie z. B. BP (Business Process) as a Service, Backend as a Service (BaaS), High Performance Computing as a Service (DICaaS), Network-as-a-Service (NaaS), Anything-as-a-Service (XaaS), u.v.m..

Die Cloudebeneen besitzen unterschiedliche Sicherheitsstufen und Verwaltungsmöglichkeiten. IaaS, PaaS und SaaS bieten den Kunden verschiedene Kontrollmechanismen. Bei PaaS hat der Kunde nur Kontrolle über seine auf der Plattform angebotenen Anwendungen, bei IaaS volle Kontrolle über das System, welches ihm innerhalb seines zugelassenen Bereichs zur Verfügung gestellt wird, während ihm bei SaaS noch mehr Kontrolle über den zugelassenen Bereich vom Cloud Service Provider zugesprochen wird. [bsi11]

3.8 IaaS, PaaS, und SaaS: Unterschiede und Ähnlichkeiten

Laut bekannten Definitionen können Cloud Delivery Modelle nach folgenden Charakteristiken aufgeteilt werden:

- SaaS: Software Applikationen (hier sind nicht die Applikationen mit APIs inkludiert)
- PaaS: Ausführungslaufzeiten ohne direkten Zugriff auf das Betriebssystem (Datenbanken, Entwicklungsplattformen und Applikationsservers)

3. Cloud-App-Plattformen

- IaaS: Virtuelle Maschinen, Server, Speicher, Netzwerkzubehör, Hardware und Betriebssysteme. [ego13]

Für die nahe Zukunft bleiben alle drei Cloud-Delivery-Modelle vorhanden. Es ist zu erwarten, dass der IaaS-Marktanteil mit der Zeit sinkt. Die potenziellen Kunden erkennen, dass sie mehr Ressourceneinsparungen von Software und Plattformdiensten anstelle von Infrastruktur erwirtschaften können.

Aus bestimmten technischen Gründen und Abhängigkeiten bleiben die IaaS Cloud-Dienste jedoch noch für einige Zeit wirksam präsent.

Als Anbieter, welcher für seine Kunden bessere Produktivitätstools anbieten möchte, ergänzt er diese IaaS mit PaaS- und SaaS-Services. Daher wird sich die Linie zwischen Cloud-Delivery-Modelle vermischen.

Es kann festgestellt werden, dass Cloud-Delivery-Modellklassifizierungen nicht nur von technischen Merkmalen, sondern auch von der Benutzerwahrnehmung abhängig sind. [ego13]

3.9 SPI

SPI ist ein Akronym für die häufigsten Modelle der Cloud Computing Services (Abbildung 3):

- SaaS - Software as a Service,
- PaaS - Platform as a Service und
- IaaS - Infrastructure as a Service.

Servicemodelle können im Hinblick auf erhöhte Abstraktionsstufen betrachtet werden. Die höchste Form der Abstraktion ist Geschäftsprozess als Service Niveau.

Es ist zu beachten, dass jede höhere Ebene die darunterliegenden Ebenen enthält. Das heißt, dass Software as a Service (SaaS) Software, die eine Business Function und gleichzeitig eine Plattform als Service (PaaS) bereitstellt, beinhaltet. [rup16]

4. Typen von Cloud Services

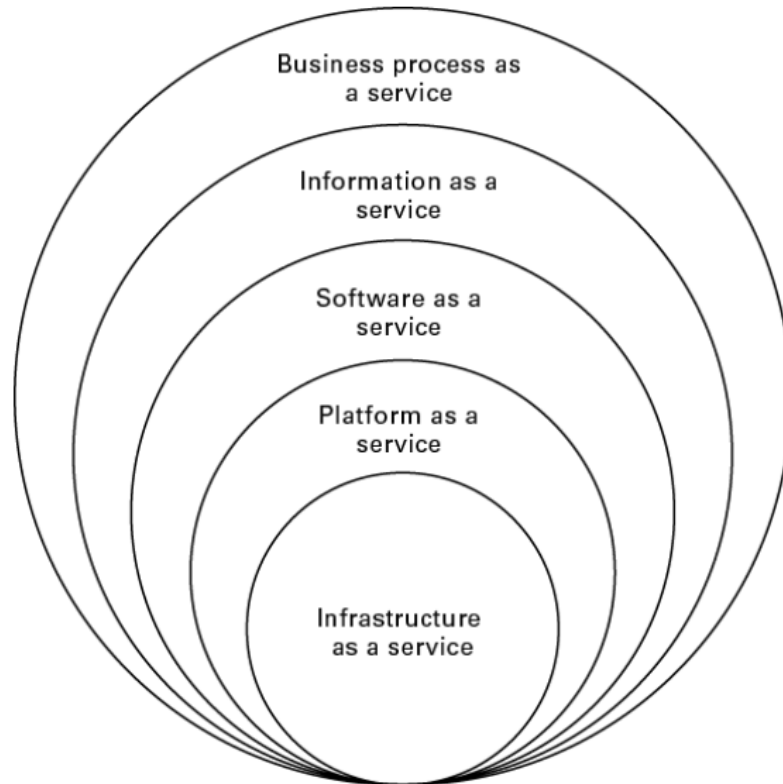


Abbildung 3: Fünf Ebenen der Abstraktion [rup16]

4. Typen von Cloud Services

Cloud Services unterscheiden sich nach dem Ort, an dem der Cloud Service realisiert wird, und den implementierten Sicherheitsaspekten:

- Private Cloud
- Public Cloud
- Hybrid Cloud
- Community Cloud

4. Typen von Cloud Services

	SaaS	PaaS	IaaS
Private Cloud		Apprenda, Stackato	VMware, Hyper-V, OpenStack, CloudStack
Community Cloud		NYSE Capital Markets Community Platform	NYSE Capital Markets Community Platform
Public Cloud	Salesforce.com, QuickBooks online, Office 365	Google AppEngine, Microsoft Azure, VMware, CloudFoundry	Amazon EC2, Rackspace
Hybrid Cloud		Custom CloudFoundry	Custom, Rackspace

Tabelle 3: Service- und Bereitstellungsmodelle bilden eine Matrix [dro12]

4.1 Private Cloud

Cloud Benutzer, Cloud Provider und Ressource Owner sind der Teil eines Unternehmens. Im Vordergrund steht, dass die Cloud Benutzer und Cloud Provider zu einer Firma gehören. Es ist auch möglich, dass die Infrastruktur von einem Dienstleister verwaltet und betrieben wird [gfg14].

4. Typen von Cloud Services

Eine private Cloud ist daher eine, die Dienste über ein LAN oder ein WAN liefert und den Verbrauch dieser Dienste auf eine ausgewählte Gruppe von Benutzern beschränkt. [rup16]

In begrenzten Fällen können private Cloud-Services über das Internet mit Zugriffsbeschränkungen geliefert werden, so dass nur private Einrichtungen Zugang zu diesen Diensten erhalten können. In der Praxis können Datenintegrität und Sicherheitsprobleme der Dienstleistung über das Internet für private Clouds schwierig werden. [rup16]

4.2 Public Cloud

Cloud Services werden von einem externen Anbieter angeboten und verwaltet. Die physikalischen Ressourcen einer Cloud liegen nicht beim Cloud Benutzer. Public Cloud Services können entweder kostenlos¹⁶ sein oder auch als Pay-per-Use angeboten werden. Solche Cloud-Lösungen können von einer großen Gruppe genutzt werden. [clo10]

Die öffentliche Cloud hat die Anwendbarkeit über die verschiedenen Abstraktionsebenen. So finden Sie öffentliche Clouds, welche Infrastruktur, Plattform, Software, Informationen oder Geschäftsprozesse als Service bereitstellen. [rup16]

¹⁶ free-of-charge

4. Typen von Cloud Services

4.3 Hybrid Cloud

Hybrid Cloud ist eine Mischung aus mindestens zwei Arten einer Cloud. Meistens werden die Eigenschaften von Private- und Public Cloud verwendet. [rup16]

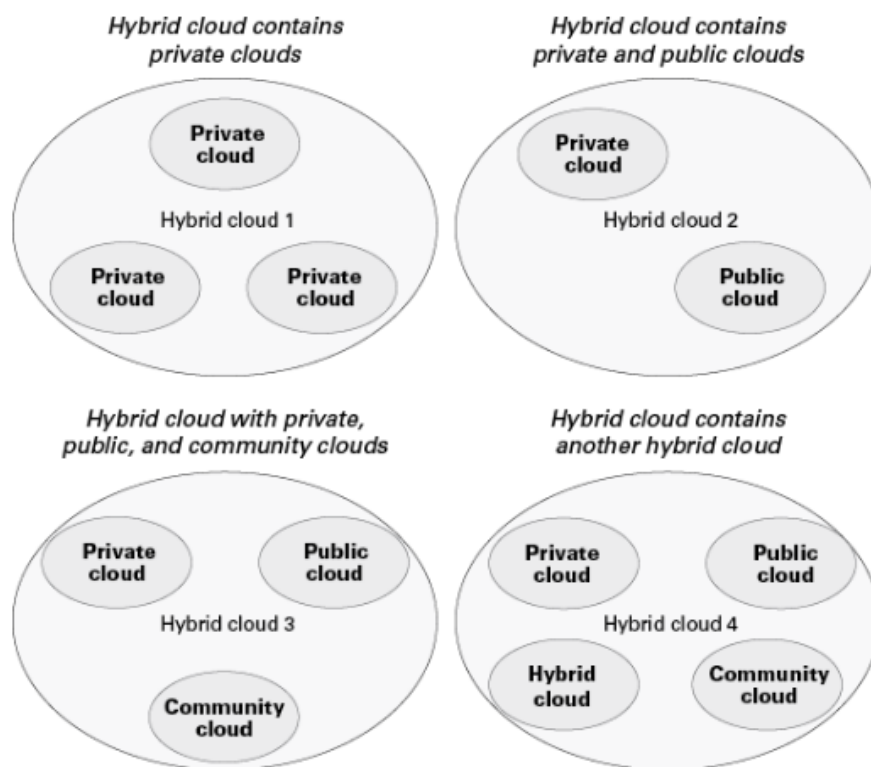


Abbildung 4: Hybrid Cloud sorten [rup16]

Beispiel: Es ist möglich eine private Cloud zu haben, die IAAS ist und ist ein public Cloud, die PaaS innerhalb einer Hybrid Clouds ist.

4. Typen von Cloud Services

Während die private Cloud Datenschutz, höhere Performance und transparente Service-Level-Ziele bietet, bietet die Public Cloud ein Standard-Service, welche Flexibilität und Kosteneffizienz verleiht, da die Firma das Rad nicht neu erfinden muss, durch eigene Erstellung von Textverarbeitungs-Cloud-Services. [rup16]

4.4 Community Cloud

Die Community-Cloud ist eine breitere Version einer privaten Cloud. Diese unterstützt eine Gemeinschaft, die gemeinsame Interessen oder die gemeinsame Anliegen wie Sicherheitsanforderungen, Datenschutz, Aufgaben in einem regulatorischen Umfeld, Geschäftsmodelle und Bedürfnisse der Endbenutzer verfolgt. [rup16]

Cloud-Ressourcen werden nur für eine Community bzw. Organisation angeboten. Die Verwaltung kann die Community selbst betreiben oder zu einem Dienstleister auslagern. [gfg14]

Eine Community-Cloud kann sogar eine geographische Region haben, zum Beispiel eine Community-Cloud der Europäischen Union oder eine nordamerikanische Cloud.

Die Community-Cloud teilt die gleiche Cloud-Infrastruktur, wenn es sich um eine IaaS-Community-Cloud handelt, die gleiche Cloud-Software, wenn es sich um eine SaaS-Community oder um dieselben Cloud-Geschäftsprozesse handelt, wenn es sich um eine BPaaS¹⁷-Community-Cloud handelt. Im Gegensatz zu einer privaten Cloud werden Community-Cloud-Services in der Regel über das Internet geliefert und unterliegen in der Regel einem Betriebskostenmodell. [rup16]

¹⁷ Business Process as a Service

4. Typen von Cloud Services

4.5 Trusted Cloud

Der Verein „Kompetenznetzwerk Trusted Cloud“ ist für den Aufbau und die Weiterentwicklung von Trusted Cloud¹⁸ verantwortlich.

Zielgruppe sind kleine und mittlere Unternehmen. In der Abbildung 4 ist ersichtlich, dass Deutschland sowie auch Österreich in diesem Bereich besonders weit hinter den anderen EU-Ländern liegen. [tcl17]¹⁹

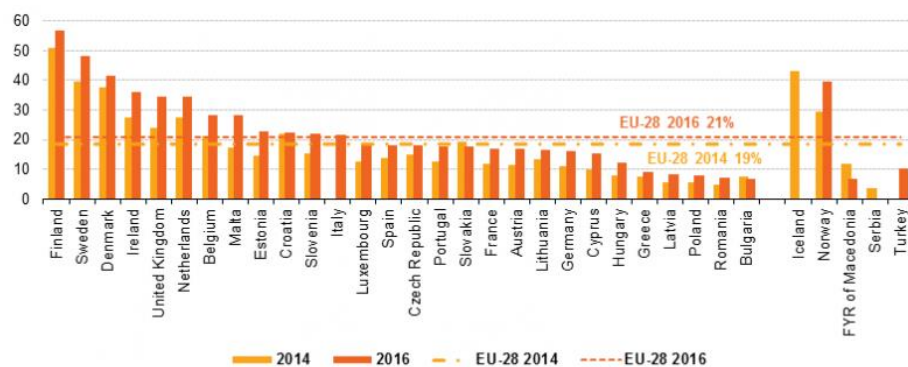


Abbildung 5: Nutzung von Cloud Computing-Diensten, 2014 und 2016
[Eur17]

Im Frühjahr 2011 hat das BMWi²⁰ Booz & Company beauftragt, die Studie "Standardisierung im Cloud Computing" in Zusammenarbeit mit dem FZI²¹ durchzuführen. Diese Studie ist in den Kontext des Cloud Computing Aktionsprogramms (siehe Abbildung 6, das vom BMWi ins Leben gerufen wurde und durch eine Allianz von Industrie, Wissenschaft und Regierung geführt wird, eingebettet.

¹⁸ <https://www.trusted-cloud.de/>

¹⁹ Bundesamt für Statistik Deutschland 2017

²⁰ Bundesministerium für Wirtschaft und Technologie in Deutschland

²¹ Forschungszentrums für Informatik

4. Typen von Cloud Services

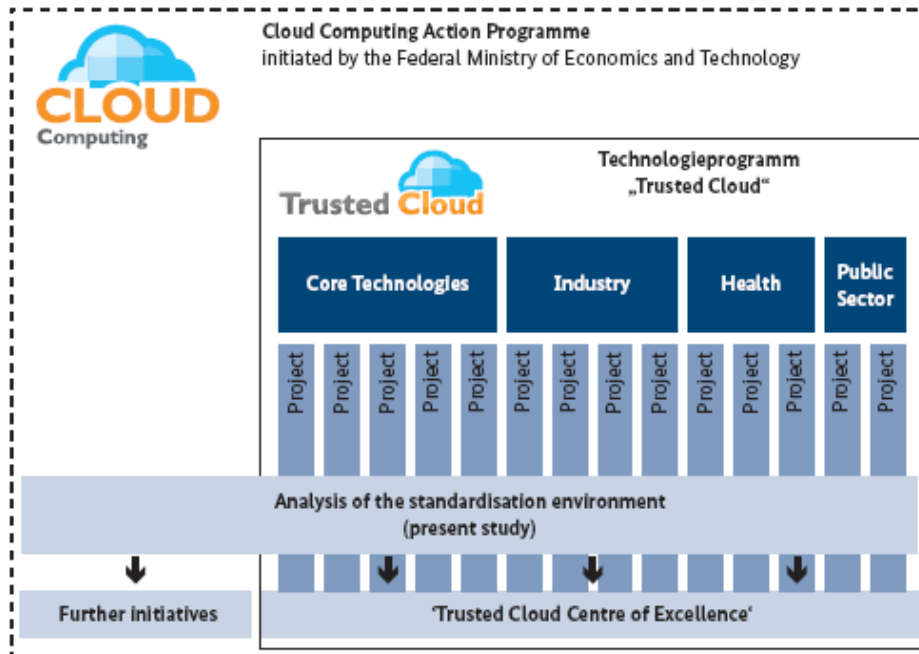


Abbildung 6: Cloud Computing Aktionsprogramm [tcl17]²²

Das Aktionsprogramm umfasst das BMWi Trusted Cloud Technology Programm²³, das darauf abzielt Förderung von Forschungs- und Entwicklungsaktivitäten für effiziente und innovative Cloud-Infrastrukturen und sichere als auch vertrauenswürdige Cloud-basierte Dienste zu nutzen[tcl17]²⁴

²² BMWI, ANALYSE VON BOOZ & COMPANY UND FZI

²³ <https://www.bmw.de/Redaktion/DE/Publikationen/Digitale-Welt/Trusted-Cloud-Cloud-Computing.html>

²⁴ Bundesamt für Statistik Deutschland 2017

4. Typen von Cloud Services

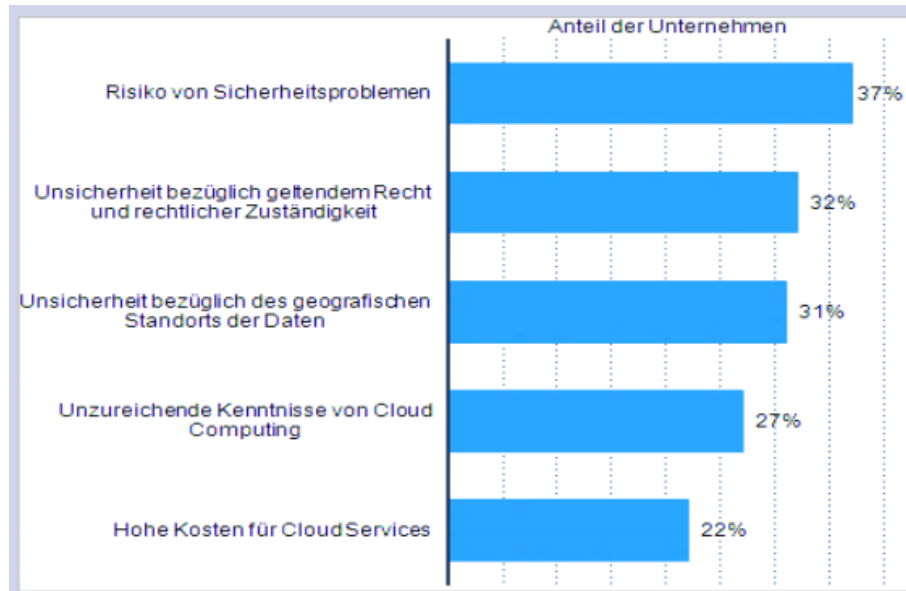


Abbildung 7: Gründe für Unternehmen in Deutschland, keine Cloud-Dienste [tcl17]

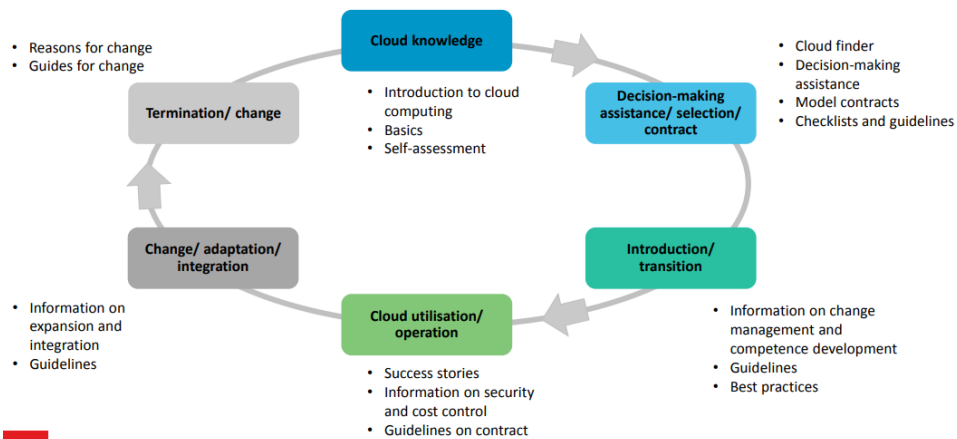


Abbildung 8: Support während des gesamten Lebenszyklus der Cloud Service-Nutzung [tcl17]

5. Motivation für Policy-Driven Governance in Cloud Application Platforms

5.1 Definitionen der Governance

Governance ist ein breiter Begriff, der in verschiedenen Kontexten verwendet wird. Das englische Verb *govern* stammt aus dem griechischen Verb *kybernan* (κυβερνάν), was so viel bedeutet wie "to direct", "to steer" [mwd16]. Die deutsche Übersetzung lautet „steuern“, oder „lenken“.

Der Politikwissenschaftler Mark Bevir²⁵ definiert Governance als "alle Regierungsprozesse, ob von einer Regierung, einem Markt oder einem Netzwerk übernommen, ob über eine Familie, einen Stamm, eine formelle oder informelle Organisation oder ein Territorium und ob durch Gesetze, Normen, Macht oder Sprache" [mb12].

Nach Ansicht von IBM [bmt06] umfasst die Enterprise Governance zwei Komponenten:

"Aufbau von Verantwortungsketten, Autorität und Kommunikation, um Menschen mit Entscheidungsrechten zu stärken.

Etablierung von Mess-, Policy- und Kontrollmechanismen, um Menschen in die Lage zu versetzen, ihre Rollen und Verantwortlichkeiten wahrzunehmen. " [bmt06]

²⁵ <http://polisci.berkeley.edu/people/person/mark-bevir>

5. Motivation für Policy-Driven Governance in Cloud Application Platforms

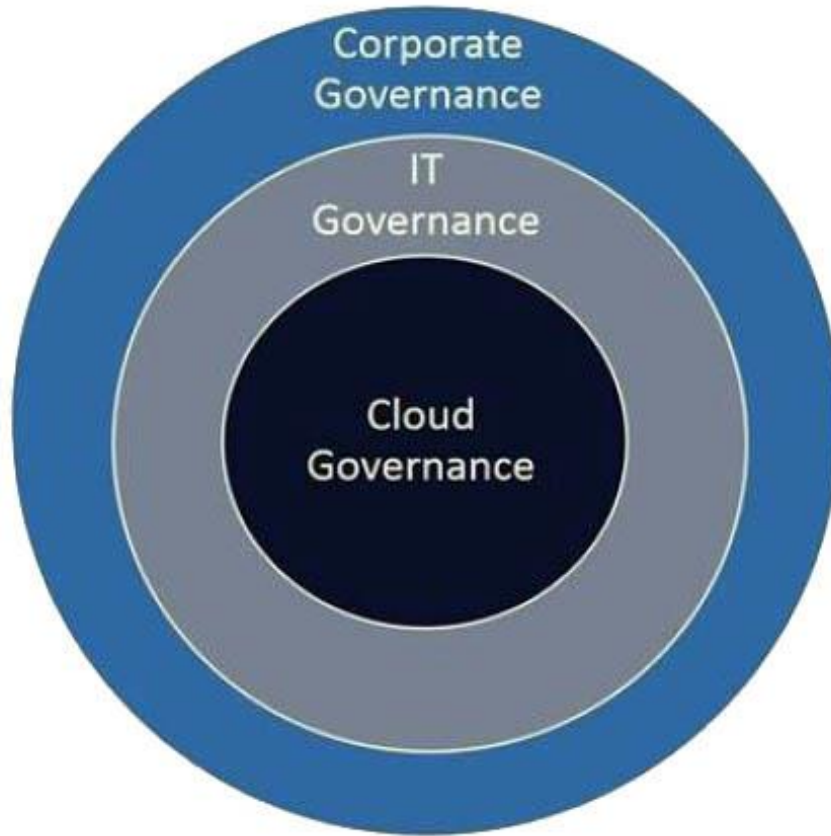


Abbildung 9: Corporate, IT und Cloud Governance [lfu15]

Um Cloud Governance zu definieren, ist es hilfreich, den Kontext zum Verständnis von "Corporate Governance" im Allgemeinen und "IT Governance" im Besonderen zu geben.

Cloud Governance kann als Erweiterung oder Komponente der IT-Governance angesehen werden. In der Abbildung 9 wird gezeigt, wie die Cloud Governance, IT Governance und Corporate Governance aufeinander aufbauen. [lfu15]

5. Motivation für Policy-Driven Governance in Cloud Application Platforms

Corporate Governance ist definiert als "die Gesamtheit der Prozesse, Gebräuche, Richtlinien, Gesetze und Institutionen, die die Art und Weise beeinflussen, wie ein Unternehmen geleitet, verwaltet oder kontrolliert wird" [deLDB09]. Sie befasst sich mit der Notwendigkeit eines Mechanismus, um sicherzustellen, dass die Gesetze, Richtlinien, Standards und Verfahren eingehalten werden, unter denen eine Organisation tätig ist.

Governance beinhaltet ist über:

- Schaffung von Verantwortungsketten, Autorität und Kommunikation zur Befähigung von Menschen (Entscheidungsrecht).
- Festlegung von Mess-, Richtlinien- und Kontrollmechanismen, die es den Menschen ermöglichen, ihre Rollen und Aufgaben wahrzunehmen. [yhe11]

Governance in Cloud-Service-Ökosystemen wird als unterstützender Prozess zur Definition und Durchsetzung von Richtlinien zur Steuerung der Erstellung, Bereitstellung und Nutzung von Cloud-Services durch verschiedene Ökosystempartner definiert. [dko16]

Corporate Governance umfasst alle Aspekte von Unternehmen, von der Personalabteilung bis hin zu Einkauf und Marketing. [yhe11]

IT-Governance schließt die Kultur, Organisation, Richtlinien und Methoden ein, die IT-Management und Kontrolle über fünf Schlüsselbereiche versorgen:

5. Motivation für Policy-Driven Governance in Cloud Application Platforms

Alignment sorgt für die strategische Ausrichtung der IT, sowie für das Alignment von IT und IT Business in Bezug auf Dienstleistungen und Projekte.

Wertlieferung bestätigt, dass die IT / Business-Organisation auf dem maximalen Geschäftswert von IT ausgelegt ist. Überwacht die Wertlieferung von IT an das Geschäft und bewertet ROI²⁶.

Risikomanagement stellt sicher, dass Prozesse vorhanden sind, um diese Risiken zu gewährleisten und angemessen zu verwalten. Sie werden in die Bewertung zu Risikoaspekten der IT-Investition einbezogen.

Ressourcenmanagement: Bereitstellung von Anweisungen für die Beschaffung und die Nutzung von IT/ Ressourcen auf höchster Ebene. Beaufsichtigung der Gesamtfinanzierung von IT auf Unternehmensebene. Stellt sicher, dass es eine angemessene IT-Fähigkeit und Infrastruktur gibt, um die aktuellen und erwarteten zukünftigen Geschäftsanforderungen zu unterstützen.

Leistungsmessung: Überprüft die strategische Compliance, d.h. die Leistung von strategischen IT-Zielen. Überprüft die Messung der IT-Leistung und den Beitrag der IT zum Business (d.h. Lieferung des versprochenen Geschäftswerts). [ISACA12][NCC05]

Die IT Governance untergliedert sich weiter in CEO, CIO, IT Security Governance, System Governance, System & Netzwerk Governance, Datenbank Governance und Application Governance.

²⁶ Return of Investment (deutsch: Kapitalrendite)

5. Motivation für Policy-Driven Governance in Cloud Application Platforms

Die IT-Governance umfasst die Entscheidungsrechte, den Verantwortlichkeitsrahmen und die Prozesse, um ein wünschenswertes Verhalten bei der Nutzung von IT zu fördern.²⁷ [yhe11]

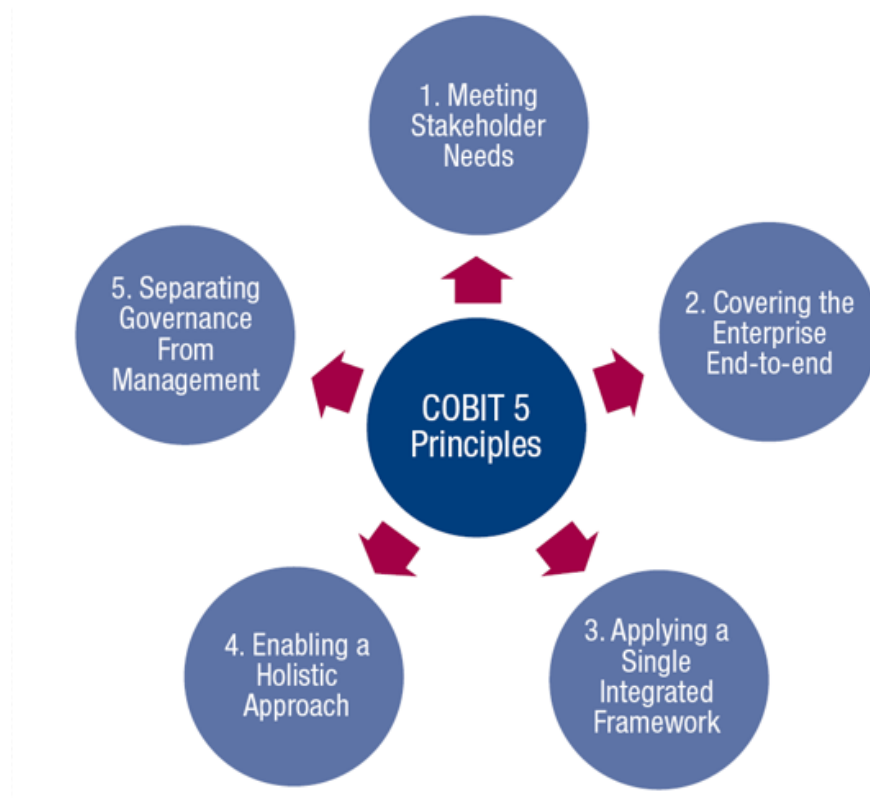


Abbildung 10: Cobit 5 Prinzipien [ISACA12]

Per Definition kann IT-Governance als Teil der Corporate Governance, die sich auf die IT-Prozesse bezieht und das Unternehmensziel unterstützt, behandelt werden. Es betont sowohl die Verwaltung und die Kontrolle von IT-Assets als auch von Personen, Prozessen und Infra-

²⁷COBIT (Control Objectives for Information and Related Technologies), 2005

5. Motivation für Policy-Driven Governance in Cloud Application Platforms

strukturen. Außerdem hebt IT-Governance die Verwaltung und die Beschaffung von Assets hervor. [yhe11]

IT-Governance wird von IBM als eine Facette von Enterprise Governance definiert, die sich auf "die Informationstechnologieprozesse eines Unternehmens und die Art und Weise, wie diese Prozesse die Geschäftsziele unterstützen", konzentriert. [bmt06] Das IT Governance Institute (ITGI) definiert die IT-Governance in ähnlicher Weise: "Führungs- und Organisationsstrukturen und Prozesse, die sicherstellen, dass die IT der Organisation die Strategien und die Ziele der Organisation unterstützt und ausbaut." [ach07].

Für Unternehmen, deren IT-Infrastruktur eine serviceorientierte Architektur (SOA) [kbs05] einsetzt, definiert IBM SOA-Governance eine Erweiterung der IT-Governance. „Eine Erweiterung der IT-Governance speziell konzentriert sich auf den Lebenszyklus von Diensten, Metadaten und Composite Anwendungen in der serviceorientierten Architektur einer Organisation.“[bmt06].

SOA-Governance ist eine Erweiterung der IT-Governance [kab09], die wiederum eine Erweiterung der Corporate Governance darstellt. Die SOA-Governance ändert die IT-Governance, um sicherzustellen, dass die Konzepte und Grundsätze für die Service-Orientierungs-Architektur angemessen verwaltet werden und die Services in der Lage sind, die Geschäftsziele zu erreichen. [yhe11]

5. Motivation für Policy-Driven Governance in Cloud Application Platforms

Mit der schnellen Einführung von Cloud Computing werden die Dienste, auf die moderne Unternehmen angewiesen sind, zunehmend "Cloud-geliefert" anstatt "On-Premise" [lin15]. Dies bringt den Begriff Cloud Service Governance als weitere Erweiterung der IT-Governance hervor. [lin15] definiert die Cloud-Service-Governance als "die Fähigkeit, die Service-Ausführung auf einer beliebigen Anzahl von On-Premise- und Cloud-basierten Plattformen zu definieren, zu verfolgen und zu überwachen". [lin15]

Zu den Kernproblemen der SOA-Governance aus geschäftlichen und IT-Alignment-Perspektiven gehören:

- Es ist schwierig, die Einhaltung von Vorschriften und Gesetzen zu gewährleisten: Es ist offensichtlich, dass ein Audit-Trail-IT-System vorhanden ist, um das Verhalten der Dienste zu überprüfen.
- Es ist schwierig, ein Budget für die Services innerhalb einer Organisation zu erstellen, da die Services übergeordnete Organisationseinheiten sind.
- Schwer zu kontrollierende Konsequenzen der Änderung von Diensten aufgrund verschiedener Verbraucher eines Dienstes und der unklaren Abhängigkeiten verschiedener Dienste.
- Es ist schwer, die Qualität der Dienste zu garantieren, weil sie einerseits sicherstellen müssen, dass sie während der Entwurfszeit den Gesetzen und Vorschriften entsprechen und andererseits, weil die Qualität der Dienste während der Laufzeit eingehalten werden muss, insbesondere die Leistung von Diensten.

5. Motivation für Policy-Driven Governance in Cloud Application Platforms

- Es ist schwer sicherzustellen, dass die erstellten Services den geschäftlichen Wert und die Anforderungen korrekt erfüllen.

[lin09][nad04][sch07]

Governance ist in ihren verschiedenen Ausprägungen grundsätzlich ein disziplinübergreifendes Thema, das sowohl organisatorisch als auch technologisch betrachtet werden kann. [dko16]

5.2 Cloud Governance vs. Cloud Management

Der Begriff "Cloud Governance" wird häufig in einem allgemeinen Sinne verwendet, um sowohl Governance als auch Cloud-Management einzuschließen. Es gibt jedoch eine klare Unterscheidung zwischen Governance und Verwaltung.

Während Cloud Governance die Cloud Computing-Richtung festlegt und ein Freigabesystem in der Organisation erstellt, verwendet Cloud-Management das System zur Ausführung dieser Richtung, die von Governance festgelegt ist.

Abbildung 11 veranschaulicht die Beziehung zwischen Governance und Management. [lfu15]

5. Motivation für Policy-Driven Governance in Cloud Application Platforms

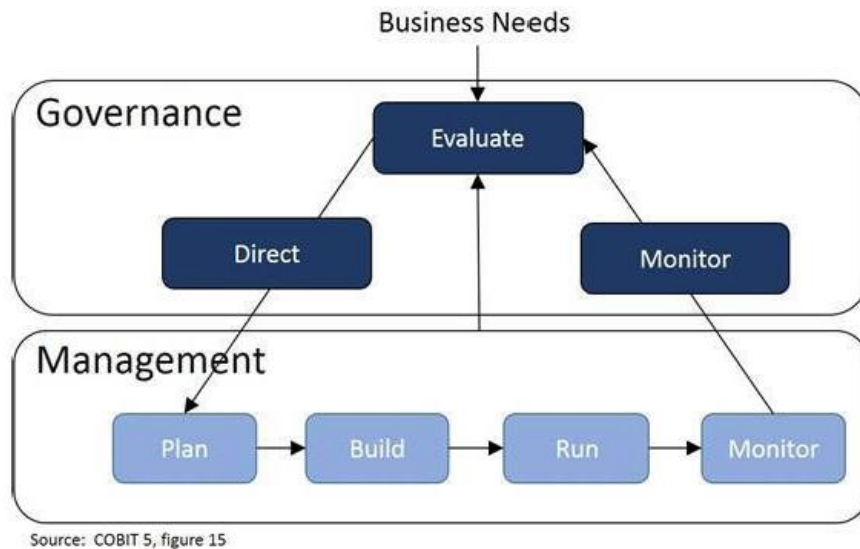


Abbildung 11: Governance versus Management [ISA12]

Obwohl sie getrennt und eindeutig sind, arbeiten Management und Governance zusammen, um sicherzustellen, dass Cloud-Service-Ziele ausgerichtet und realisiert werden. [lfu15]

5.3 Abgrenzung Cloud Governance - SOA Governance

Laut [lin09] sind die meisten Cloud Services nach den SOA Prinzipien konzipiert. Cloud Computing kann als einer der Implementierungs- und Realisierungsansätze für SOA behandelt werden.

Mittlerweile realisieren SOA sowie Virtualisierungstechnologien das Merkmal „Ressourcenpooling“ aus der Cloud. Sowohl SOA-Governance als auch Cloud-Governance erfordern unternehmensbezogene Zusammenarbeit (z.B. Kommunikation zwischen IT und Geschäftszweigen), um den Geschäftswert zu realisieren. Aus diesem

5. Motivation für Policy-Driven Governance in Cloud Application Platforms

Grund ist Governance im Zusammenhang mit SOA-Governance, wie z.B. Service Governance und organisatorische Veränderungen, die am besten geeignete Methode für Cloud Computing. Es ist einfacher, SOA-Governance-Ansätze für Cloud-Services-Governance zu nutzen (Tabelle 4) [lin09]

SOA	Cloud Computing
Der Plattform-Service (serviceorientiert Infrastruktur): liefert die Hard- und Softwaregrundlage wie Server, Netzwerk, Datenbank, Betriebssystem, Clustering / Grid / Virtualisierung etc. auf denen Softwarekomponenten laufen, von denen aber abstrahiert wird.	IaaS und PaaS wurden auf der Basis von SOA-Prinzipien entwickelt.
Die Anwendungs- / Prozess-Serviceebene: bezieht sich auf reine Software-Services.	Viele SaaS Applikationen wurden auch auf der Basis von SOA-Prinzipien entwickelt.

*Tabelle 4: Mapping service level
von Cloud Computing & SOA [ovu10]*

5. Motivation für Policy-Driven Governance in Cloud Application Platforms

Cloud Computing und SOA besitzen auch bestimmte Ähnlichkeiten:

- Organisation-Wise Management [ovu10]
- Der Kern von SOA und Cloud Governance ist Service Governance, zum Beispiel Lifecycle Management of Service, design time, runtime und change time of management [lin09]
- Erfordert ein neues Kostenzuweisungs- / Finanzierungsmodell für den Service innerhalb einer Organisation [ago13]
- Prozess-orientiert: Sowohl Cloud-Governance als auch SOA-Governance sollten sich auf Prozesse stützen, um das Bewusstsein der Stakeholder für die richtige Nutzung zu schärfen, statt sich nur auf Governance-Tools zu verlassen. [One09b]

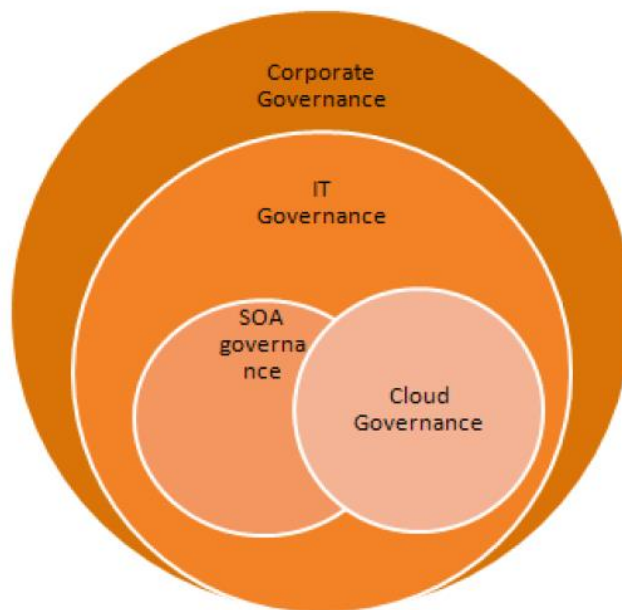


Abbildung 12: Cloud-Governance Position [yhe11]

5.4 Policy-Driven Governance in Cloud Application Platforms

Cloud Computing bietet die Aussicht auf einen zukünftigen Markt, in dem Software von verschiedenen Drittanbietern entwickelt und auf verschiedenen Cloud-Anwendungsplattformen verteilt werden.

Ein Blick auf verschiedene Cloud-Service-Intermediäre, z. B. Cloud-Anwendungsplattform Anbieter, zeigt verschiedene Ansätze und Werkzeuge für die politische Steuerung über Prozesse und Artefakte. Entwicklung und Einsatz von Cloud-Diensten auf dem Intuit Partnerplattform¹⁰²⁸ durchläuft vier Phasen, von denen jede als "eine Linie von Entwicklung" genannt wird. Diese Phasen heißen Entwicklung, Qualitätssicherung, Staging²⁹ und Veröffentlichung. [bko13]

Eine der größten Herausforderungen beim Betrieb einer Cloud-Plattform, die Drittanbieter-Erweiterungen ermöglicht, ist die ordnungsgemäße Regierungsführung durch die Durchsetzung von Richtlinien auf Software, die von verschiedenen Parteien beigetragen wird, zu gewährleisten.

²⁸ <https://developer.intuit.com/>

²⁹ Ein Prozess, der verwendet wird, um eine neue Lösung zu „erzeugen“, zu testen und zu überprüfen, bevor sie in Produktion geht und die bestehende Lösung außer Betrieb genommen wird

5. Motivation für Policy-Driven Governance in Cloud Application Platforms

Die Bewältigung dieser Herausforderung war eines der Hauptziele des kürzlich abgeschlossenen Forschungsprojekts CAST³⁰ [kps12]

Das CAST-Projekt identifizierte fünf zentrale Governance-Funktionalitäten als besonders kritisch:

- Katalogisierung und Speicherung: Solutions, Applikationen und Services müssen katalogisiert werden und ihre Artefakte, die an einem zentralen Ort gespeichert sind.
- Artefakt Validierung: Verwaltete Entitäten (Solutions, Applikationen und Services) und ihre assoziierten Artefakte müssen auf Übereinstimmung mit den Plattform-Richtlinien überprüft werden.
- Lifecycle Management: Die Entwicklung von verwalteten Einheiten muss einem explizit definierten Lebenszyklusmodell folgen, das aus bestimmten Zuständen und Übergängen besteht, wobei Übergänge durch Vorbedingungen geschützt werden.
- Abhängigkeitsverfolgung und Wirkungsanalyse: Die Abhängigkeiten zwischen Lösungen, Applikationen und Diensten müssen verfolgt werden, um eine Auswirkungsanalyse zu ermöglichen.
- Externe Serviceüberwachung: Externe (Web-)Dienste, von denen Applikationen abhängig sein können, müssen überwacht

³⁰ Project CAST war ein von 2009 bis 2012 laufendes Forschungsprojekt zwischen Industrie und Hochschulen und entwickelte Technologien zur Unterstützung der gemeinsamen Entwicklung von Cloud-basierten Business-Softwarelösungen durch Ökosysteme von Softwareunternehmen ([HTTP://WWW.CAST-PROJECT.EU](http://www.cast-project.eu))

5. Motivation für Policy-Driven Governance in Cloud Application Platforms

werden, um Verfügbarkeit und Leistung sicherzustellen.[dko16]

Das Projekt wurde eingerichtet, um eine Cloud-Applikationsplattform zu schaffen, die die Entwicklung und den Einsatz von On-Demand-Geschäftsanwendungen durch Dritte ermöglicht. Die Governance-Werkzeuge in CAST waren vor allem mit zwei Arten von Policies beschäftigt:

- Lifecycle-Governance, d. h. die Kontrolle, wie sich Drittanbieter-Erweiterungen auf der Plattform entwickeln, und
- Artefact-Governance, d. h. die Kontrolle der Struktur und des Inhalts von Software-Artefakten, die mit diesen Erweiterungen verbunden sind. [kps12]

Während des CAST-Projekts haben die Autoren⁴⁰ verschiedene Richtlinien für Lifecycle- und Artefact-Governance definiert und benutzerdefinierte Softwarekomponenten entwickelt, die sie in einem Open-Source-Registry- und Repository-System durchgesetzt haben. Durch diese Übung haben die Autoren einige wertvolle Einblicke in die Einschränkungen der derzeitigen Konzepte des Policymanagements erlangt, die von den heutigen Governance-Tools umgesetzt wurden. [kps12]

5. Motivation für Policy-Driven Governance in Cloud Application Platforms

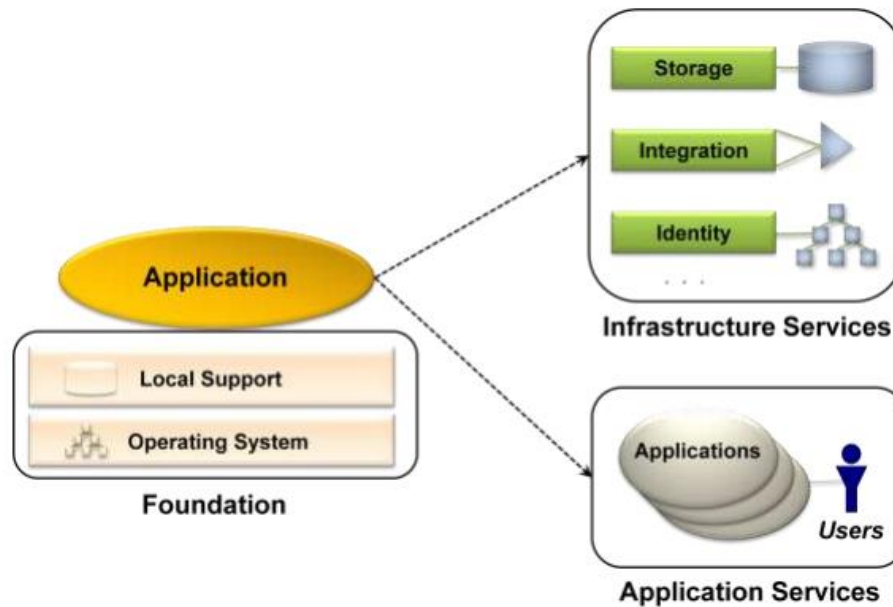


Abbildung 13: Eine moderne Anwendungsplattform kann als aus drei Teilen bestehend angesehen werden [dch08]

Ob lokal oder in der Cloud - eine Anwendungsplattform kann als aus drei Teilen bestehend betrachtet werden:

- Ein Foundation (Grundlage): Fast jede Anwendung verwendet einige Plattform-Software auf der Maschine, auf der sie läuft. [dch08]
Dies umfasst in der Regel verschiedene Unterstützungsfunktionen, z.B. Standardbibliotheken und Speicher, und ein Basisbetriebssystem.

5. Motivation für Policy-Driven Governance in Cloud Application Platforms

- Eine Gruppe von Infrastrukturdiensten: In einer modern verteilten Umgebung verwenden Applikationen häufig grundlegende Dienste, die auf anderen Rechnern bereitgestellt werden. Es ist üblich, Remotespeicher bereitzustellen, z.B. für Integrationsdienste, Identitätsservice und mehr.
- Eine Reihe von Anwendungsservices: Da immer mehr Anwendungen serviceorientiert werden, werden die Funktionen, die sie anbieten, für neue Anwendungen zugänglich.
Diese Anwendungen existieren in erster Linie, um den Endnutzern Dienste zur Verfügung zu stellen und sind damit auch Teil der Anwendungsplattform.

In der oberen Abbildung 13 sind keine Entwicklungstools, die auch eine wichtige Komponente sind, ersichtlich. Moderne Tools helfen den Entwicklern alle drei Komponenten von Applikation-Plattform zu verwenden. [dch08]

Ein wichtiger Trend in der aufkommenden Domäne von Cloud Computing ist die Einführung von Cloud-Applikationsplattformen - eine besondere Unterklasse von PaaS, die die Entwicklung und Bereitstellung von Softwareanwendungen unterstützen.

5. Motivation für Policy-Driven Governance in Cloud Application Platforms

Cloud-Anwendungsplattformen bieten eine Kombination aus verwalteter Computerinfrastruktur, die über das Internet zugänglich gemacht wird, mit einer Reihe von Tools und Services, die es Entwicklern ermöglichen, Anwendungen zu erstellen und sie über diese Infrastruktur zu implementieren und auszuführen. Force.com, Long Jump, Engine Yard und Zoho sind einige der derzeit etablierten Dienstleister in diesem Raum. [kps12]

6. Lifecycle vs. Artefact Governance

In Zukunft wird die Cloud zu einem reichhaltigen Ökosystem von Services, Anbieter und Verbraucher entwickelt, die jeweils auf das Angebot anderer aufbauen. Cloud Service Broker werden eine wichtige Rolle spielen und auch zwischen Anbietern und Verbraucher vermitteln. Neben der vertikalen Integration und Value-added Aggregation von Dienstleistungen, werden Broker eine zunehmende Rolle in der kontinuierlichen Qualitätssicherung und Optimierung spielen.

Die Mechanismen für den Governance stellen Service-Zertifizierungen bereit, um automatische Arbitrage von Kundenpräferenzen zu respektieren. Weiter werden kontinuierliche Optimierung der Servicebereitstellung, Fehler Prävention und Wiederherstellung zur Laufzeit bereitgestellt. [msp13]

6.1 Lifecycle Governance

Lifecycle Governance befasst sich mit der Sicherstellung eines strukturierten und disziplinierten Ansatzes zur Einführung von Drittanbietererweiterungen, der Bereitstellung der Implementierungsumgebung der Plattform, deren Änderung oder deren Beseitigung. [kps12]

Im Mittelpunkt der Lifecycle Governance stehen das Konzept eines Lebenszyklusmodells, das die Phasen definiert, die jede einzelne verwaltete Softwareeinheit durchlaufen muss, sowie die Voraussetzungen für den Übergang von einer Lebenszyklusphase zur nächsten. [kps12]

6. Lifecycle vs. Artefact Governance

Cloud-Service-Brokerage ist eine neue Art von Service und ein aufstrebendes Unternehmensmodell im Bereich Cloud Computing, das Unternehmen helfen soll, diese Herausforderungen zu bewältigen und die Risiken zu mildern, die sich aus der Nutzung großer Cloud-Dienste ergeben können.

Ein Cloud Dienst Broker ist eine Entität, die im Auftrag eines Verbrauchers von Cloud-Diensten intermediär arbeitet, um den konsumierten Diensten einen Mehrwert hinzuzufügen. [msp13] [kps12]

In diesem Zusammenhang wird unter Governance, die Durchsetzung von Policies um den Lebenszyklus eines Cloud-Dienstes aus Sicht des Verbrauchers zu verwalten, sowie die Qualitätskontrolle für den Service und die damit verbundenen Artefakte, verstanden. Diese zwei Bedenken lassen sich auf zwei komplementäre Formen der politischen Steuerung beziehen: Prozess-Governance und Artefakt-Governance [msp13]

6.2 Prozess- & Artefact Governance

- **Prozess-Governance**

Prozess-Governance bezieht sich auf das Definieren und Durchsetzen von Richtlinien, um diese Cloud zu gewährleisten. Die Dienstleistungen werden strukturiert und diszipliniert ausgewählt, getestet, genutzt und ausgezahlt, mit den expliziten Bedingungen für den Übergang von einer Dienstlebenszyklusphase zur nächsten. [msp13]

- **Artefact Governance**

„Artefact-Governance hingegen bezieht sich auf die Definition und Durchsetzung von Richtlinien, um sicherzustellen, dass Artefakte, die mit Cloud-Diensten verbunden sind, bestimmten technischen Anforderungen oder Geschäftsbeschränkungen entsprechen.“ [msp13]

Die Artefakt-Governance befasst sich mit der Sicherstellung, dass alle Artefakte, die mit verwalteten Einheiten verbunden sind, einer Reihe von technischen, geschäftlichen oder rechtlichen Beschränkungen entsprechen, die vom Plattformanbieter definiert werden. [kps12]

Zentral für Artefakt-Governance ist der Begriff der Artefakt-Spezifikationen, die Einschränkungen auf die Struktur und Inhalte, die verschiedenen Arten von Konfiguration, Spezifikation oder Code-Artefakte erlaubt sind.

Eine der für die CAST-Plattform definierten Artefakt-Governance-Richtlinien stellt beispielsweise fest, dass die Schnittstellenspezifikation (WSDL) jedes externen Webdienstes, der von einer oder mehreren Apps verwendet wird, genau zwei nicht identische Endpunkt-URLs enthalten sollte, die auf unterschiedliche Server, auf denen die Dienste bereitgestellt werden, verweisen (primäre und Backup-Endpunkte). Das Grundprinzip besteht darin, eine Failover-Alternative bereitzustellen, falls der primäre Server, der den Service hostet, nicht verfügbar ist. [kps12]

6. Lifecycle vs. Artefact Governance

Der industrielle State of the Art in der Policy-basierten Governance folgt eng der Entwicklung von Tools, die verschiedenen Aspekte der Service-Governance unterstützen, z. B. Artefaktkatalogisierung und Speicherung, Service Lifecycle Management, Abhängigkeitsverfolgung und Richtliniendurchsetzung. Diese Tools sind normalerweise in einer Art von Registry und Repository-System integriert. [msp13]

6.3 Einschränkungen

Software-Tools, die die Governance in offenen Service Delivery-Plattformen unterstützen, sind seit einigen Jahren im Handel erhältlich. Typischerweise kommen solche Tools in Form eines integrierten Registrierungs- und Repository-Systems vor. [kps12]

Das häufigste Einsatzszenario ist die Unterstützung der Verwaltung von serviceorientierten Unternehmensinfrastrukturen.

Ein Feature, das in solchen Governance-Tools zentral ist, bietet Benutzern die Möglichkeit, zu überprüfen, ob die Daten im Registrierungs- / Repository-System den relevanten Richtlinien entsprechen. [kps12]

Ihre Hauptbeschränkungen in Bezug auf die Definition und Durchsetzung von Policies können im Folgenden zusammengefasst werden.

- Mangel an Trennung von Bedenken zwischen Definition und Durchsetzung der Policy,
- Fehlende Abstraktion in der Policy Vertretung und
- Fehlende formale Darstellung von politischen Einschränkungen und Beziehungen

6. Lifecycle vs. Artefact Governance

Die oben genannten Einschränkungen haben negative Implikationen in Bezug auf die Wartbarkeit, Verständlichkeit, Überprüfbarkeit, Rückverfolgbarkeit, Interoperabilität und in Bezug auf die allgemeine Flexibilität der Plattformsteuerung. [kps12] [dko16]

Insgesamt mangelt es an Unterstützung für die dezentrale/verteilte Zusammenarbeit. Modernste Governance-Unterstützungssysteme wurden im Hinblick auf eine zentrale Governance geschaffen.

Ihr Design basiert auf der Vorstellung, dass es eine Einrichtung gibt, die sicherstellen muss, dass bestimmte Richtlinien durchgesetzt werden (zu ihrem eigenen Vorteil, nicht als Teil einer Dienstleistung für andere Einrichtungen in einem Ökosystem). Um dies zu erreichen, wird die zentrale Instanz (typischerweise ein Unternehmen) die Richtlinien erstellen und sie durchsetzen. [dko16]

Um diese Richtlinien zu erstellen und durchzusetzen, erhält oder erstellt diese Entität Beschreibungen der geregelten Ressourcen und speichert sie an einem zentralen Ort (Registrierungs- und Repository-System), der Eigentum der gleichen Entität ist und von ihr gehostet und betrieben wird. [dko16]

6.4 Ontologie-basierter Ansatz, Ziel, Datenschutz

Die laufende Forschungsarbeit von [kps12] zielt auf die oben genannten Einschränkungen ab, durch einen neuen Ansatz bei der Definition und Durchsetzung von Governance-Richtlinien überwunden werden können, wobei die Ontologie basierte Wissensrepräsentation und Diskussion im Mittelpunkt stehen wird. [kps12]

6. Lifecycle vs. Artefact Governance

Die Vorteile der Anwendung von Ontologie und verwandten semantischen Webtechnologien auf Policy Engineering wurden bereits in früheren Arbeiten von [kfj03] und [ubl03] untersucht.

[tbj03] berichtete über reduzierte menschliche Fehler, vereinfachte Policy-Analyse, reduzierte Policy Konflikte und erhöhte Interoperabilität. [ubl03] hat die Vorteile der Wiederverwendbarkeit, Erweiterbarkeit, Überprüfbarkeit, Sicherheit und "Plausibilität" hervorgehoben.

Die bisherige Forschung zu diesem Thema konzentrierte sich hauptsächlich auf Policy in Bezug auf Sicherheit, Datenschutz, Vertrauensmanagement, Dienstqualität oder Geschäftsnormen [abb07].

Es wird hier primär auf Policies von Lifecycle Governance (Regulierung der Entwicklung von Software auf einer Plattform) und Artefact Governance (die Konfiguration der bereitgestellten Software und der zugehörigen Artefakte zu regulieren) eingegangen. [kps12]

6.5 Forschungsstand

Es wurden klar die Grenzen der modernen Governance-Tools in Bezug auf Policy-Engineering gezeigt.

Insbesondere wird auf die fehlende Trennung von Bedenken zwischen der Definition von Richtlinien und der Durchsetzung von Richtlinien hingewiesen. Außerdem wird das Fehlen von Abstraktion auf Domänenebene bei der Kodierung von Richtlinien und das Fehlen einer formellen Darstellung von Richtlinieneinschränkungen und -beziehungen hervorgehoben. [kps12]

6. Lifecycle vs. Artefact Governance

7. SOA

7.1 Problemverständnis

Es ist möglich alle Probleme in zwei große Bereiche zu kategorisieren:

- Unterschied zwischen Business und IT
- Duplizierung von Funktionalität und Prozesssilos

Um diese Probleme lösen zu können, wird eine Fachrichtung, wie die Architekturapplikation, die uns in Unternehmen und in Projekten weiterhelfen kann, benötigt.

In diesem Kapitel werden auch verschiedene Architekturtypen, wie Referenz-, Solutionsarchitektur und gemeinsame Schicht-Konzepte erwähnt. [DvL12]

- **Versicherungsunternehmen – ein Beispiel**

Ein Versicherungsunternehmen kann als Beispiel für die Serviceunternehmen angeführt werden. Auf Abbildung 14 wird dargestellt, dass alle Prozesse in drei Prozesskategorien untergliedert sind: Managementprozesse, Operationale Prozesse und Supporting Prozesse:

7. SOA

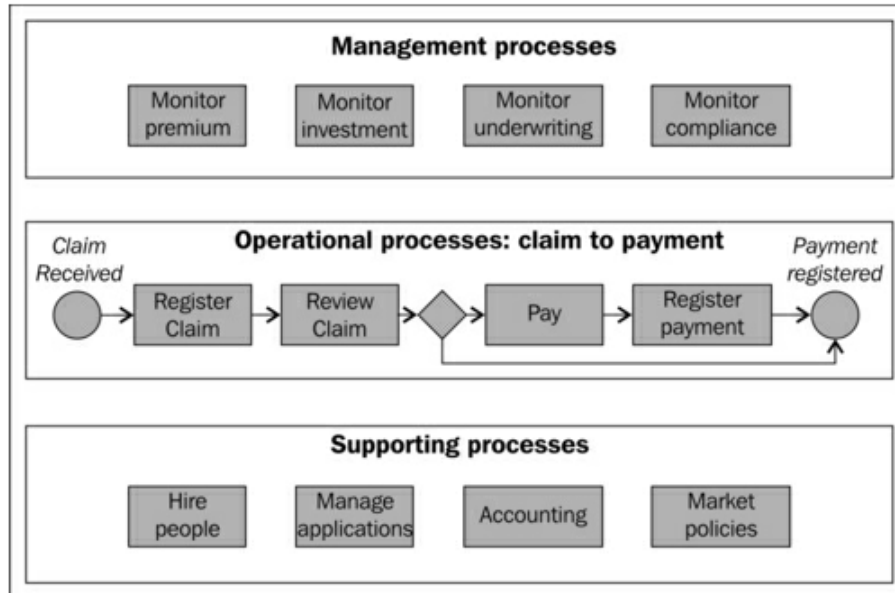


Abbildung 14: Prozesskategorien – Beispiel
Versicherungsunternehmen [DvL12]

Zudem zeigt die Abbildung 14 uns drei Prozesstypen mit ihren Unterprozessen. Diese drei Prozesstypen sind: Managementprozesse, Operationale Prozesse und Supporting Prozesse.

Alle diese Prozesse sind sehr Informationsintensiv. Die Versicherungsunternehmen speichern die Informationen über die verschiedenen Produkte, die gleichzeitig über das Versicherungsunternehmen abgesichert sind. In die Produktliste gehören nicht nur die Informationen über die Produkte, sondern auch über die Kunden, die von dieser Firma versichert sind z.B. die Kombinationen, die Kunden in ihrem Versicherungsvertrag angeboten wurden, wie z.B. die Wünsche und Ansprüche von Kunden, die prozessiert wurden oder wieviel Geld investiert wurde usw.

7. SOA

Diese Informationen wurden dann über alle Prozesse, sowohl in den operativen Prozessen als auch in den Management- und Support-Prozessen, in verschiedenen Szenarien und Kombinationen genutzt. Für ein Versicherungsunternehmen ist die Information die wichtigste Komponente für alle drei Prozesse. [DvL12]

7.2 Wechselwirkung zwischen Business und IT

Ein Unternehmen ist von Informationen abhängig. Aus dem Grund ist es wichtig, dass die Technologie diese Informationen anbieten kann. Diese Informationen werden genutzt um gewährleisten zu können, dass diese Prozesse (Management Prozesse, Operationale Prozesse und Supporting Prozesse) mit den Bedürfnissen der Organisation im Zusammenhang stehen. Dies wird Business- und IT-Alignment genannt. [DvL12]

Als Gründer von Geschäfts- und IT-Alignment werden Henderson und Venkatraman bezeichnet. In dem Artikel³¹, der von Henderson und Venkatrama veröffentlicht wurde, wird aufgezeigt, dass das Ziel von Business- und IT-Alignment ist drei separate Risiken im Zusammenhang mit IT-Projekten zu bewältigen:

- **Technische Risiken:**

Wird das System funktionieren, wie es sein sollte?

³¹ „Strategic Alignment: Leveraging Information Technology for Transforming Organizations. IBM System Journal, vol32, No1.

7. SOA

- **Organisatorische Risiken:**
Werden die Mitarbeiter der Organisation das System nutzen, wie vorgesehen?
- **Business Risiken:**
Wird die Implementierung und Adaptierung des Systems in Business Value konvertieren?

Wenn alle drei Risiken nicht erfolgreich verwaltet werden, ist die Business Value gefährdet. [DvL12]

Von Mitarbeitern verschieden Unternehmen werden oft Beschwerden für die IT-Performance laut ausgesprochen.

Diese Beschwerden können in zwei Gruppen aufgeteilt werden:

- IT ist nicht in der Lage, sich selbst zusammen mit dem Geschäft schnell genug zu ändern
- IT ist nicht in der Lage, die Funktionalität der Geschäftsanforderungen korrekt zu liefern.

Die erste Gruppe wird auf dem heutigen Markt immer wichtiger und ist ein Beispiel, wo SOA jedem weiterhelfen kann, dieses oder diese Probleme zu lösen. Unter einer Voraussetzung: SOA muss korrekt angewendet werden. [DvL12]

Im Allgemeinen müssen sich die Organisationen, die sich in einer der folgenden Situationen befinden, schnell an die Situation am Markt anpassen oder diese ändern können:

7. SOA

- Organisationen, die mit sich ändernden Regeln und Vorschriften umgehen müssen, wie Krankenkassen, Finanzinstitute und der öffentliche Sektor.
- Organisationen, die sich in sich schnell verändernden Märkten befinden, wie die Telekommunikationsindustrie.
- Organisationen, die einen Teil der betrieblichen Prozesse zusammenführen, aufspalten oder auslagern. Diese Organisationen müssen in der Lage sein, ihre IT gemäß den Änderungen in der Organisation und den Prozessen zu ändern. Die genannten Beispiele sind die Finanzdienstleistungsbranche, produktorientierte Unternehmen mit mehreren Lieferanten und Versorgungsunternehmen. [DvL12]

7.3 Die Essenz von SOA-Governance

Dieses Kapitel stellt das Konzept der Governance vor. Es werden die Kernkomponenten von Menschen, Policies und Prozessen vorgestellt und dann veranschaulicht, warum diese für die Annahme von SOA innerhalb eines Unternehmens wichtig sind. [tbi08]

7.3.1 Was ist Governance?

Welcher ist der erste Grundgedanke, wenn das Wort Governance gehört wird? [tbi08]

Für viele, die in der IT-Branche tätig sind, hat es kein positives Image. Die Entwickler z. B. ziehen Parallelen zu Formulare ausfüllen, Präsentationen vorbereiten, Meetings vor der Prüfungskommission abhalten

7. SOA

usw. Auf der anderen Seite ist für die Enterprise Architekten Governance nur positiv behaftet. Enterprise Architekten hören die Präsentationen von Projektteams an und versuchen Anleitungen zu geben, die Bemühungen über die Bedürfnisse des einzelnen Projekts hinausgehen, diese treffen nur Entwickler treffen. Die Entwickler sind mehr daran interessiert, die neuesten Technologien zu testen, nicht aber die Bedürfnisse des Unternehmens zu erfüllen.

Es gibt noch Projekt Manager, der kämpft dafür, dass die Projekte genehmigt werden. Seine Aufgabe ist es nicht, sich tiefgründig mit den Projekten zu beschäftigen, sondern sich um die Genehmigung und Durchsetzung des Projektes zu kümmern. [tbi08]

Wenn die Enterprise Architekten die Entwickler überzeugen wollen, die neuesten Technologien zu verwenden, um die Enterprise Voraussetzungen zu erreichen und zu erfüllen, kann es passieren, dass der Projekt Manager alles abbricht, weil für ihn die Änderungen in Schedule nicht akzeptabel sind. [tbi08]

Viele Organisationen haben sogar einen Ausschuss namens "IT Governance Committee" gegründet, dessen Aufgabe darin besteht, Projektvorschläge zu überprüfen und festzustellen, welche Anstrengungen finanziert werden.

Es ist eine Tatsache, dass Governance ein notwendiger und kritischer Teil jeder Organisation ist. Es ist die Kombination von Menschen, Policies und Prozessen, die zusammengefügt werden, um sicherzustellen, dass die Organisation ein oder mehrere gewünschte Verhaltensweisen erreicht.

7. SOA

Eine richtig angewendete Governance macht den Unterschied zwischen Erfolg und Misserfolg. [tbi08]

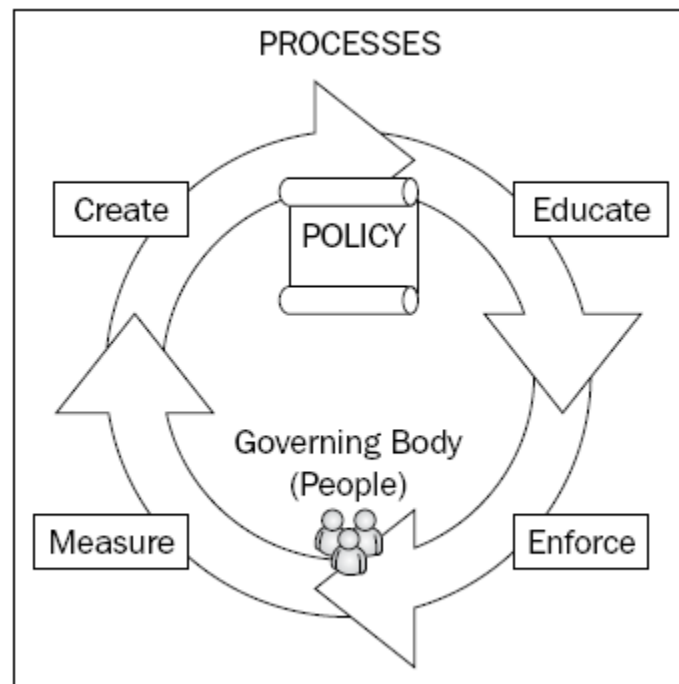


Abbildung 15: Die notwendigen Aspekte für Governance [tbi08]

Auf Abbildung 15 oben zu sehen ist, sind folgende Aspekte notwendig bzw. „Die Essenz von Governance“: gewünschtes Verhalten, Menschen, Policies und Prozesse.

Das gewünschte Verhalten wird durch eine erfolgreiche Kombination von Menschen, Policies und Prozessen erreicht. Menschen sind die Führer, die für die Festlegung des gewünschten Verhaltens des Unternehmens verantwortlich sind, Policies sind die Regeln, die das ge-

7. SOA

wünschte Verhalten ausdrücken, während die Prozesse versichern, dass die Policies verfolgt werden. [tbi08]

Sowohl jede Organisation als auch jedes Unternehmen und jede Regierung werden eigene Leadership Strukturen haben. Das gilt auch für das gewünschte Verhalten, Policies und Prozesse.

Die Governance ist erfolgreich, wenn das gewünschte Verhalten erreicht wird. [tbi08]

7.3.2 Was ist IT Governance?

IT-Governance ist als ein System definiert, das aus Personen, Richtlinien und Prozessen besteht, und die eine Organisation einsetzt, um die angemessenen Verhaltensweisen und Ergebnisse in Bezug auf die Nutzung der Informationstechnologie durch die Organisation sicherzustellen.

In vielen Organisationen ist das IT-Governance-Gremium das Prüfungsgremium, das entscheidet, welche Bemühungen gefördert werden und welche nicht. Viele Organisationen verfügen auch über Portfolio-Management-Organisationen (PMOs), die sicherstellen, dass die einmal finanzierten Maßnahmen ordnungsgemäß priorisiert, besetzt und konsistent ausgeführt werden. [tbi08]

7.4 Was ist SOA?

Was ist serviceorientierte Architektur oder SOA? An dieser Stelle soll zuerst definiert werden, was unter dem Begriff Service verstanden wird.

7. SOA

Laut Merriam-Webster Wörterbuch³² ist Service eine Einrichtung, die einige öffentliche Nachfragen liefern kann. Das Schlüsselwort ist hier die Einrichtung, die eine gewisse Fähigkeit oder Durchführung einer Funktion repräsentiert. Das Wort „liefern“ bedeutet, dass die Funktion zum Kunden bereitgestellt ist, während mit der öffentlichen Nachfrage der eigentliche Wunsch eines oder mehreren Kunden dargestellt wird. Insgesamt gesehen ist SOA einfach die Architektur, die die Kernkonzepte und Dienstleistern nutzt um das System zu definieren. [tbi08]

Serviceorientierte Architektur ist ein technologisches Architekturmodell für serviceorientierte Lösungen mit ausgeprägten Eigenschaften zur Unterstützung der Dienstleistungsorientierung und der strategischen Ziele im Zusammenhang mit serviceorientiertem Computing.

Die vier grundlegenden Merkmale, die in jeder Form von SOA etabliert werden möchten, sind: Business-Driven, Vendor-Neutral, Enterprise-Centric und Composition-Centric. [ebc11]

Es wurde ersichtlich, dass Services ein wichtiger Aspekt jeder SOA sind, und nun exakt festgestellt werden kann, was ein Service ist! Im nächsten Schritt wird herausgefunden, welche Services aufgrund der Anforderungen der Kunden tatsächlich benötigt werden. Dieser Vorgang wird Service-Identifizierung genannt. Sobald festgestellt wurde, welche Dienste die Clients benötigen, kann mit dem Entwurf dieser Dienste begonnen werden, indem deren Operationen, die Eingabe und

³² <http://www.merriam-webster.com/>

7. SOA

Ausgabe dieser entworfen werden. [DvL12]

Laut [Ars04] sollen es Unterschiede zwischen Service Identifizierungsphase, Service Definitionsphase und Service Realisierungsphase geben. [PvD07] verwendet die Termine Analyse und Design statt des Terminus Identifizierung.

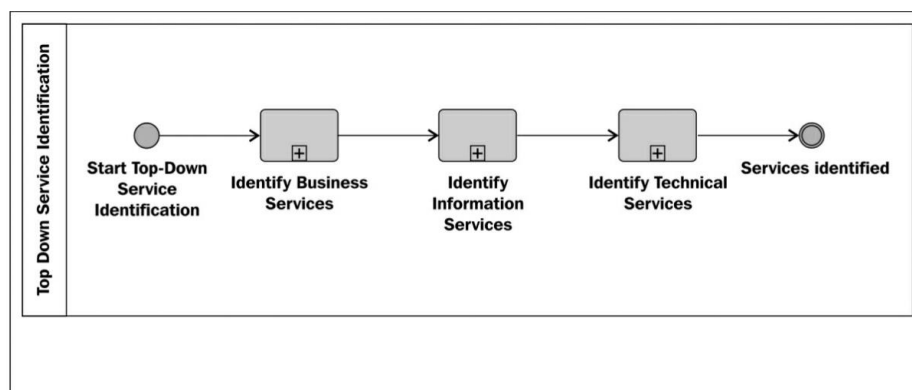


Abbildung 16: Top Down Service Identifizierung [DvL12]

Es gibt zwei Ansätze um die richtige Services zu identifizieren: Top-down und Bottom-up. Auf der Abbildung 16 ist die Reihenfolge ersichtlich, in welcher die Services identifiziert werden, wenn die Top-down Service-Identifizierung basierend auf Unternehmens Strategie angewendet wird.

Folgende Schritte wurden ausgeführt:

- **Identifiziere Business Services:**

Es beginnt mit der Analyse der Geschäftspläne, in der gewünschten Organisation bestimmt welche Geschäftsservices benötigt werden.

7. SOA

- **Identifiziere Information Services:**
Sobald bekannt ist, welche Business Services benötigt werden, kann bestimmt werden, welche Informationsdienste benötigt werden, um diese Business Services zu unterstützen.
- **Identifiziere Technical Service:**
- **Diese technischen Services sind identifiziert.**

Gap analyse (Lückenanalyse)

Das Analysieren der Unterschiede zwischen zwei Szenarien oder Plänen, wie zum Beispiel die Ist- und Soll-Architektur, wird als Lückenanalyse bezeichnet. Mit anderen Worten, es wird analysiert, welche Unterschiede oder Lücken zwischen den beiden Szenarien bestehen.

[DvL12]

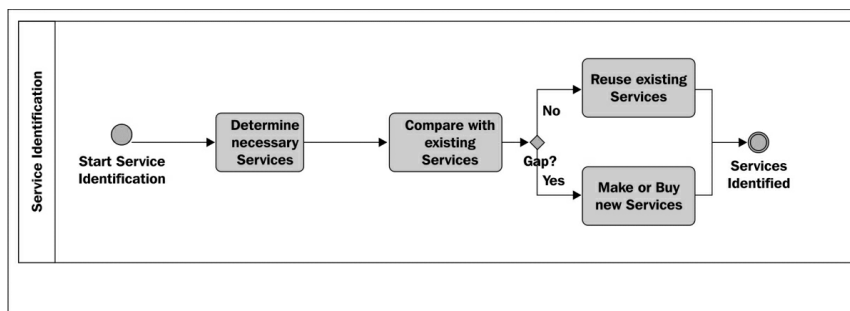


Abbildung 17: Gap analyse oder Lückenanalyse [DvL12]

Die vorangegangene Abbildung 17 zeigt, wie make, buy und reuse in den Service-Identifikationsprozess passen. Dies geschieht auf allen Ebenen der Architektur, also Business, Information und Technik. Die Essenz dessen, worum es bei SOA geht, ist: ein System in eine Sammlung von Konsumenten und Anbietern zu zerlegen. Der Schlüs-

7. SOA

sel zu einer erfolgreichen SOA besteht jedoch darin, sicherzustellen, dass die richtigen Services bereitgestellt werden und dass die Beziehungen zwischen Verbrauchern und Anbietern formell hergestellt und verwaltet werden. [DvL12]

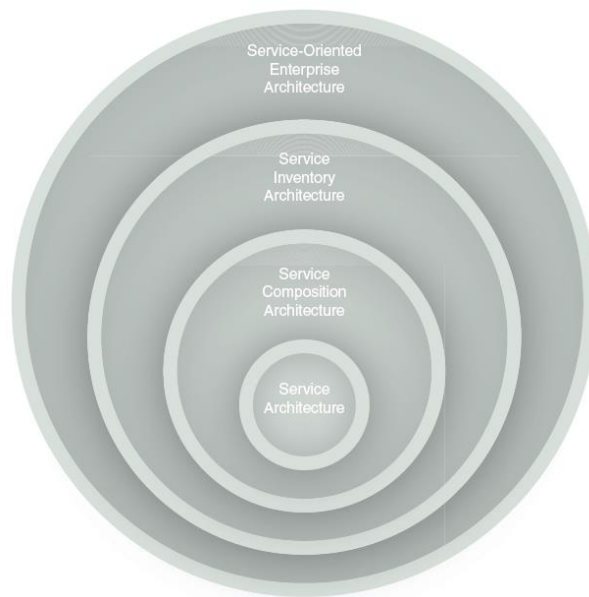


Abbildung 18: Das geschichtete SOA-Modell legt die vier gängigen SOA-Typen fest: Servicearchitektur, Service-Kompositionsarchitektur, Service-Inventararchitektur und Service-orientiert Enterprisearchitektur. [ebc11]

Es existiert eine hohe Anzahl an Applikationen, die mit einem unflexiblen Design, das durch die hohe Kostenänderung eine mögliche Verbesserung des Designs bzw. Applikation untragbar erschwert, entwickelt wurden. Diese unflexiblen Designlösungen sollen als Wachstumskurs gesehen werden und auf keinen Fall als Resultat schlechter Entscheidung, die vor Jahren getroffen wurden.

7. SOA

Die Erwartungen, dass sowohl alle Neuigkeiten, die in den letzten Jahren passierten, von Entwicklern und Eigentümern wahrgenommen werden, als auch die mögliche Implementierung neuester Technologieänderungen, sind sehr unrealistisch. [tbi08]

Im Vergleich eines typischen Corporate-Enterprises mit einer typischen „Community“ wird schnell klar, dass die Hauptunterschiede in den Enterprise-Komponenten liegen. Diese Komponenten sind für alles, wofür Enterprise gelobt wird, verantwortlich.

Wenn sich ein Eigentümer dafür entscheidet eigene App in einer unflexiblen Art zu entwickeln, wird er als einziger von Applikationsinflexibilität betroffen sein. Die „Community“, als ganze, wird davon verschont. Für eine Corporate Enterprise sieht das ganz anders aus. Es geht um die gesamten Kosten. Wenn eine Applikation in Enterprise unflexibel ist, werden die Kosten immer höher und höher sein, solange diese Applikation für Enterprise notwendig ist. Es wird noch teurer sein, die ganze App komplett neu zu entwickeln.

Um kontinuierliche und dauerhafte Inflexibilitätszyklen zu vermeiden, muss heutzutage Enterprise eine andere Richtung einschlagen. [tbi08]

Es muss zuerst ein Enterprise System als eine Kollektion von Möglichkeiten aufgebaut werden. Des Weiteren muss dieses System als eine Servicekollektion angeboten werden. So ein System wird dann dieselben individuellen Applikationen, die Integrationsherausforderungen erfüllen und Inflexibilitätszyklen vermeiden müssen, haben. Der Grund

7. SOA

dafür liegt darin, dass viele Enterprise Systeme bestehende Applikationen einfach übernommen haben. . [tbi08]

Typisches Enterprise hat eine Kollektion von Applikationen, wie auf der Abbildung 19 dargestellt:

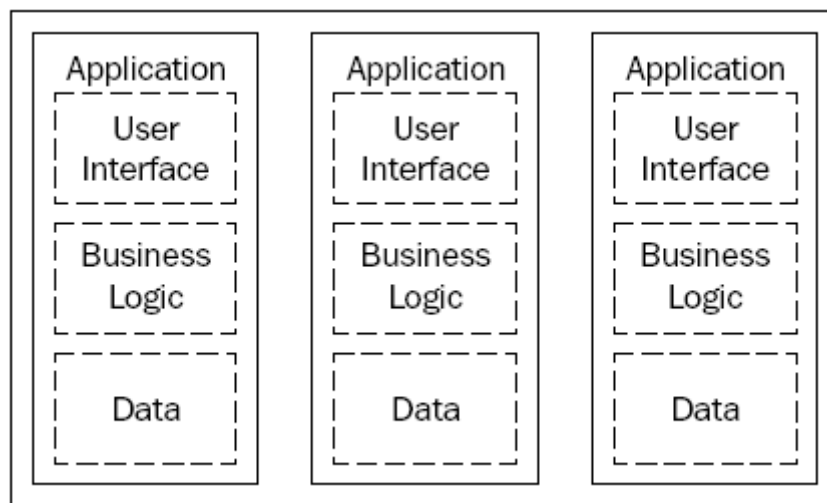


Abbildung 19: Enterprise als eine Kollektion von Applikation[DvL12]

Um die Kommunikation zwischen zwei Applikationen zu ermöglichen, ist die Erstellung eines Adapters allgemein akzeptiert. Dieser Adapter dient sozusagen als Klebstoff zwischen zwei Applikationen. Für die weiteren zwei Applikationen, die integriert werden sollen, wird ein neuer Adapter erstellt, was dazu führt, dass die Kommunikation zwischen den Applikationen immer komplexere ausmaße annimmt.

Um diese Komplexität zu vermeiden, liegt die Lösung darin,

7. SOA

aus diesen unendlichen Kreisen von neuen ständig hinzugefügten Adapters auszusteigen. Enterprise muss von Application Oriented Architecture (AOA) fortziehen. . [tbi08]

Bei AOA wird die Applikation als Kerneinheit genutzt, um das Enterprise als eine Applikation zu beschreiben. Bei SOA schaut die Architektur anders aus. Hier wird Service als Kern gesehen. Als Beispiel wird die Abbildung 19 genommen und die Applikationsgrenzen eliminiert. Die Abbildung 20 würde dann anders aussehen:

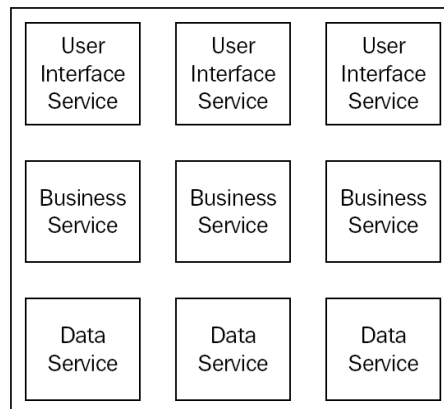


*Abbildung 20: Enterprise als eine Kollektion
von Service Konsumenten und Serviceanbieter[DvL12]*

7.5 Säulen der Serviceorientierung

Service-Orientierung bietet eine eindeutig definierte Methode für Formen von Software-Programmen zu Einheiten von serviceorientierter Logik. Diese Logik können wir als Services (Dienste) bezeichnet werden. Jedes Service, das geliefert wird, bringt uns einen Schritt nä-

7. SOA

her zu dem gewünschten Zielzustand, der durch diese strategischen Ziele und Vorteile repräsentiert wird. [ebc11]

Bewährte Methoden, Muster, Grundsätze und Technologien existieren zur Unterstützung der Serviceorientierung. Es gibt eine Reihe von grundlegenden kritischen Erfolgsfaktoren. Diese kritischen Erfolgsfaktoren werden als Säulen bezeichnet, weil sie, die Grundlage für die Erstellung, Bereitstellung und Steuerung von Services gemeinsam aufbauen.

Diese vier Säulen von Service-Orientierung sind:

- Teamarbeit: Projektübergreifende Teams und Kooperationen sind erforderlich.
- Bildung: Teammitglieder müssen auf der Basis vom gemeinsamen Wissen und Verstehen kommunizieren und kooperieren.
- Disziplin: Teammitglieder müssen ihr gemeinsames Wissen konsequent anwenden. [ebc11]
- Balanced Scope: Das Ausmaß, in dem die erforderlichen Ebenen der Teamarbeit, Bildung, und Disziplin implementiert werden.

Die Festlegung eines Balanced Scope ist eine strategische Planungsentscheidung und daher selbst ein kritischer Erfolgsfaktor. [ebc11]

7. SOA

7.6 SOA Stufen der Organisatorische Reife

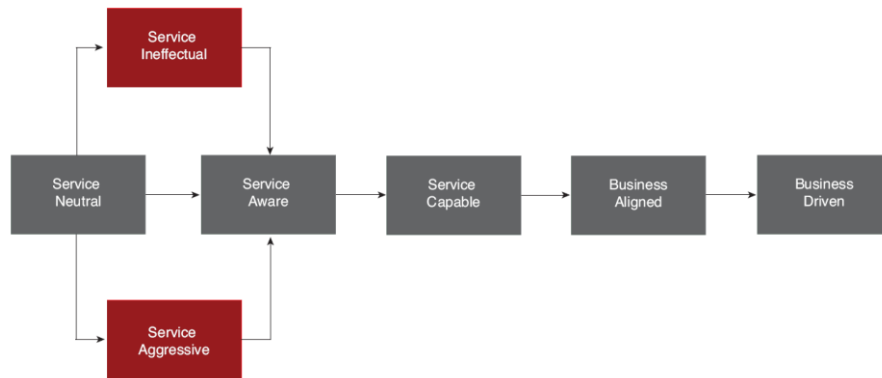


*Abbildung 21: Gemeinsame evolutionäre Ebenen
der organisatorischen Reife.[ebc11]*

Ab dem Zeitpunkt, an dem eine Organisation mit der Planung der Einführung von SOA und Service-Orientierung beginnt bis zu dem Zeitpunkt, an dem er seinen geplanten Zielzustand erreicht, kann sie eine oder mehrere der folgenden gemeinsamen Evolutionsstufen durchlaufen:

- Service Neutral
- Servicebewusst
- Servicefähig
- Geschäft ausgerichtet
- Geschäftsorientiert

7. SOA

Die Levels Service Ineffectual (untauglich) und Service Aggressive gelten als Antipattern und Inhibitoren erfolgreicher SOA-Einführung. [ebc11]

7.7. Key Governance Themen

Das SOA-Governance-Programm ist eine lebendige Einheit, die eine kontinuierliche Wartung erfordert.

7.7.1 Collect the right metrics

Metrics, der vierte Hauptbaustein eines Governance-Systems, stellen ein vitales Element im laufenden Betrieb des SOA-Governance-Programms dar. Die Werkzeuge besitzen ebenso wichtige Prozesse, um key metrics konsistent zu sammeln und zu verbreiten.

7.7.2 Transparenz

Je nach Umfang, kann ein SOA-Governance-Programm eine Vielzahl von Abteilungen, Gruppen und Einzelpersonen betreffen. Die Entwicklung sollte ein offener Prozess sein, der für die Überprüfung und Einbeziehung anderer in der IT-Abteilung zugänglich ist. [ebc11]

7.7.3 Compliance

Ein SOA-Governance-System wird Regeln einführen, die manchmal bestimmte Tasks einschränken, für die die IT-Projektmitarbeiter traditionell frei mit ihrem eigenen Urteil waren. Gleichzeitig helfen Regeln

7. SOA

auch kritische Entscheidungen für IT-Experten zu treffen, die ihre Verantwortlichkeiten entlasten und gleichzeitig Konsistenz über Services und serviceorientierte Lösungen gewährleisten können.

Das Anbieten von formellen Anreizen für das regelmäßige Unterstützen von Regeln kann ein langer Weg zur Förderung der konsequenten Einhaltung sein. [ebc11]

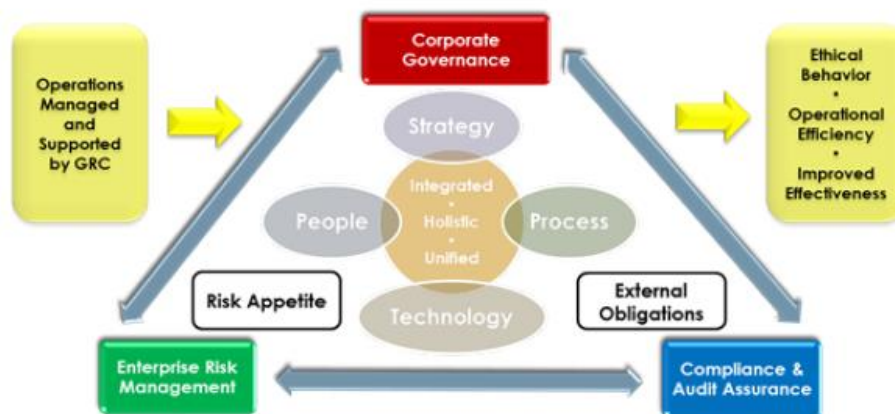


Abbildung 22: GRC Value Ecosystem [csa11]

Compliance kann als das Bewusstsein und die Einhaltung von Verpflichtungen (z.B. soziale Verantwortung von Unternehmen, geltende Gesetze, ethische Richtlinien) definiert werden, einschließlich der Bewertung und Priorisierung von Korrekturmaßnahmen, die als notwendig und angemessen erachtet werden. In einigen Umgebungen, insbesondere solchen, die deutlich reguliert sind, kann der Transparenzaspekt sogar dominieren, wenn die Berichterstattungsanforderungen mehr Aufmerksamkeit erhalten als die Einhaltung selbst. Im besten

7. SOA

Fall ist Compliance kein Hemmnis für die organisatorische Effektivität, sondern eine Ergänzung zu intern festgelegten Richtlinien. [csa11]

Jeder Compliance-Ansatz muss die Beteiligung innerhalb der Organisation, einschließlich der IT, umfassen. Die Rolle externer Anbieter muss sorgfältig geprüft werden, und die Verantwortung für die indirekte oder direkte Einbeziehung in die Governance sollte ausdrücklich in der Kundenorganisation festgelegt werden. [csa11]

7.8 Governance, Risk und Compliance

Governance, Risk and Compliance (GRC) -Management ist ein effektives Mittel für Organisationen, um wichtige Risikodaten zu sammeln, Compliance zu validieren und Ergebnisse dem Management zu melden. [SDS14]

Laut [GYR13] ist GRC ein Managementmodell, das die Vereinheitlichung der Kriterien sowie die Kommunikation und Zusammenarbeit zwischen verschiedenen Stakeholdern bei der Verwaltung und Kontrolle der Organisation fördert.

7. SOA

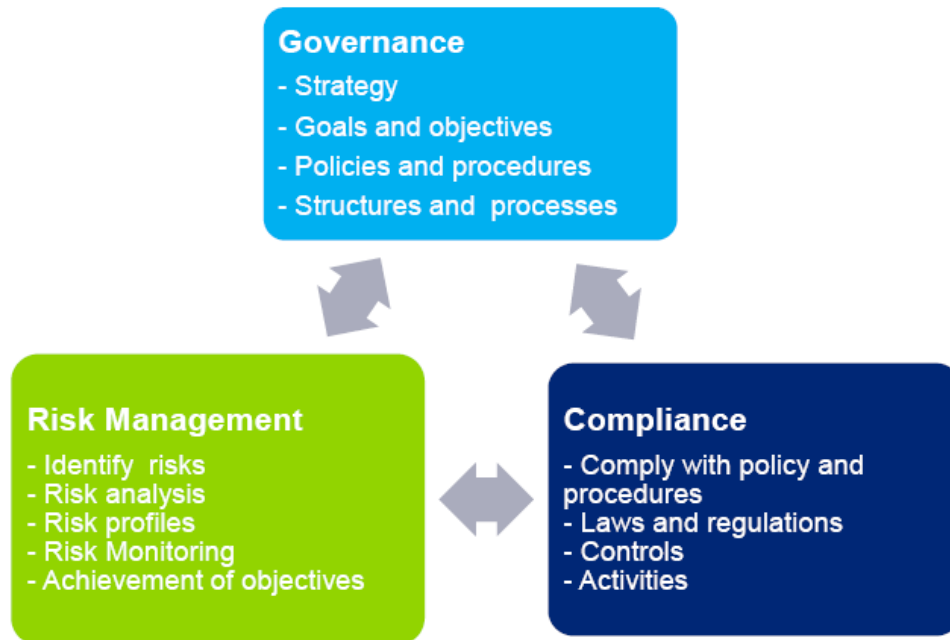


Abbildung 23: Governance, Risk and Compliance (GRC) [GYR13]

Governance steuert die Risiken für die Umsetzung der Unternehmensstrategie sowie die Risiken aus der gewählten Strategie

Risk management bestimmt die Bereiche, die potenziellen Risiken ausgesetzt sind. Compliance ist zuständig für die taktischen Maßnahmen zur Risikominderung. [GYR13]

Compliance bedeutet die Einhaltung der festgelegten Anforderungen, wie sie in Gesetzen, Vorschriften, Standards, Verträgen, Strategien und Richtlinien definiert sind. [SDS14]

Statt separate Lösungen für Compliance, IT und andere Geschäftseinheiten zu erwerben, sind Organisationen zunehmend die Entscheidung für die Nutzung einer einzelnen GRC-Plattform für das Unternehmen

7. SOA

und bei Bedarf die Integration von Lösungen um spezifische GRC-Bedürfnisse zu befriedigen. Data Analytics-Tools ermöglichen Administratoren identifizieren und organisieren die Risikoexposition, ordnen die Einhaltung von Richtlinien externen Vorschriften zu oder verwalten schnell Kundenaudits. [SDS14]

Es ist wichtig auch die GRC Stakeholders zu definieren. Laut [GYR13] können folgende Gruppen, Personen oder Abteilung Stakeholders sein: Board und support committees, management team, legal, Systemabteilungen, für Audit zuständige Personen und Finanzabteilung. GRC fördern die Kriterien Vereinheitlichung, die Aufwandskoordination und die Zusammenarbeit zwischen verschiedenen Charakteren wird in Richtung der Organisation durch involviert:

Die Integration der Verwaltung und Risikomanagement,
interne Kontrolle und Compliance

- Rollen- und Verantwortungszuweisung für Schlüsselpersonal
- Formalisierung der Kommunikationskanäle
- Anwendung eines risikobasierten Ansatzes
- Die Implementierung eines Compliance-Programms [ARR13]

7. SOA



Abbildung 24: The GRC Framework [GYR13]

Compliance Management kann weitere Komponenten beinhalten: Internal Control Matrix Development and Maintenance, Internal Control Evaluation, Internal Control Monitoring, Segregation of Duties (SoD) Analysis, SoD und Super Benutzer Access Monitoring. [SDS14]
Laut [CGO14] ist es möglich die Kosten und Risiken durch strenge Compliance zu reduzieren,

7.9 SOA Governance - Häufigste Fehler

Hier ist eine Menge von häufigen Fehler, die sich direkt auf den Aufbau und den Betrieb einer SOA-Governance beziehen:

- Mangel an anerkannter Autorität
- Fehlausrichtung mit IT-Governance

7. SOA

- Überschätzte und/oder unterschätzte Cloud Computing Faktoren
- Unpraktische oder übermäßig formale Prozesse
- Arme oder keine Dokumentation
- Mehrausgaben auf SOA Governance Tools

Ein Grundrahmen für ein SOA-Governance-Programm besteht aus drei Primärteilelementen, die die Bewertung des aktuellen organisatorischen Zustands, die Planung und den Aufbau des Programms sowie seine Betriebsentwicklung betreffen. [ebc11]

8. Sicherheitsmaßnahmen

Herkömmliche IT-Organisationen müssen sich um die Sicherheit und Kontrolle über diese fünf Stapel (d.h. Netzwerk, Speicher, Server, virtuelle Maschine und Anwendung) kümmern. Die Einführung der Cloud verteilt die Verantwortlichkeiten zwischen Cloud-Service-Konsumenten, Cloud-Service-Providern (CSP) und Broker. Wie Abbildung 28 zeigt, verringert sich das Kontrollniveau von der Konsumentenseite, während das Kontrollniveau von der Anbieterseite zunimmt, wenn von IaaS zu SaaS gewechselt wird. [Guo10]

Zum Beispiel bieten CSPs in IaaS virtuelle Server an und Cloud-Service-Konsumenten erhalten die Fähigkeit, die virtuellen Server zu kontrollieren sowie Betriebssysteme (OS) und Anwendungen darauf zu installieren.

Die Infrastruktur unter dem virtuellen Server unterliegt jedoch der Kontrolle von CSPs. In SaaS können Cloud-Service-Konsumenten nur die Konfigurationsparameter der Services steuern. In PaaS können Verbraucher die gesamten Anwendungen steuern, während CSPs für die Laufzeitumgebung verantwortlich sind und die zugrundeliegende Infrastruktur unterstützen.

Wenn es um das öffentliche (public) Bereitstellungsmodell geht, übertragen Cloud-Service-Konsumenten einen Teil der Verwaltungs- und Kontrollfunktionen an CSPs. Dennoch ist es für die Verbraucherorga-

8. Sicherheitsmaßnahmen

nisationen immer noch Kontingent, einige Mechanismen zur Überwachung der Kontrollmöglichkeiten von CSPs zu übernehmen.

Diese Mechanismen könnten durch die Verwaltung von Service Level Agreements (SLA) oder andere wirksam werden.

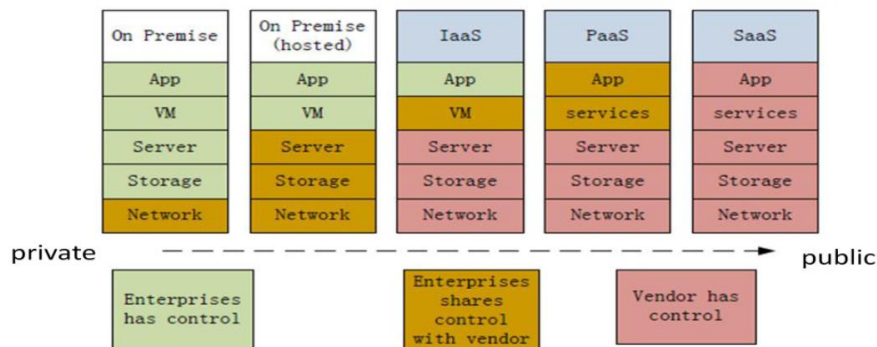
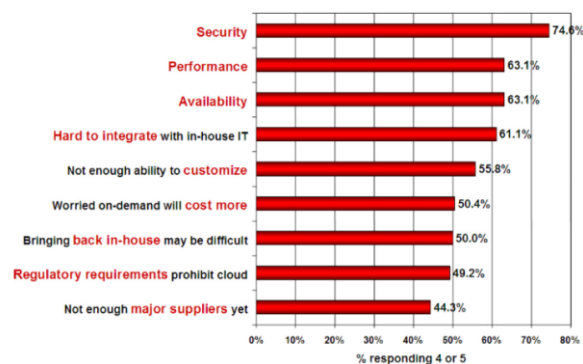


Abbildung 25: Kontrollstufe des Cloud Computing [guo10]

Laut der Umfrage von [idc08] fassen die größten Herausforderungen bei der Einführung von Cloud Computing Sicherheit, Leistung, Verfügbarkeit, Kosteneffizienz und die Einhaltung gesetzlicher Vorschriften um (siehe Abbildung 24). [idc08]



8. Sicherheitsmaßnahmen

Abbildung 26: Herausforderung der Annahme von Cloud Computing
[idc08]

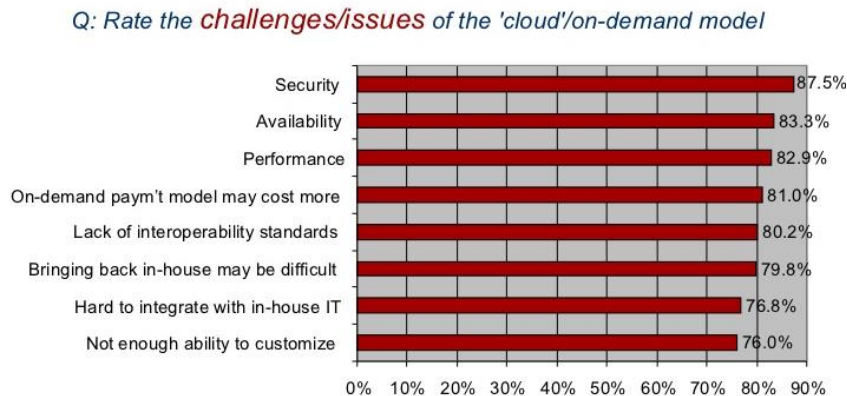


Abbildung 27: Herausforderung der Annahme von Cloud Computing
[idc09]

Sicherheit ist in nur einem Jahr zu einer noch größeren Herausforderung geworden und um 13.1% gewachsen.. Availability und Performance folgen danach. Die neuen Herausforderungen sind „On-demand payment model may cost more“ und „Lack of interoperability standards“.

Sieben Jahre später ist Sicherheit nicht mehr die wichtigste Herausforderung, sondern „Lack of resources/expertise“. Danach folgen Sicherheit und Compliance. Unter den Top 8 haben noch die Verwaltung von „multiple cloud services“ und die Kostenverwaltung Platz gefunden. Es ist interessant, dass die Performance immer noch aktuell ist und Availability nicht mehr auf der Liste zu finden ist. Neu sind Governance/Control und zwar sowohl in 2016 als auch ein Jahr

8. Sicherheitsmaßnahmen

später, wenn Governance/Control als noch wichtiger betrachtet wird.

[idc09]

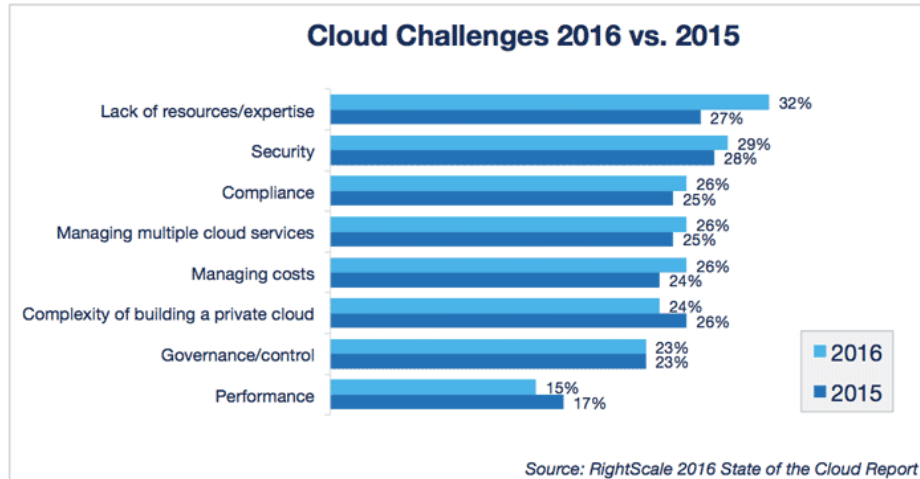


Abbildung 28: Herausforderung der Annahme von Cloud Computing

[rs16]

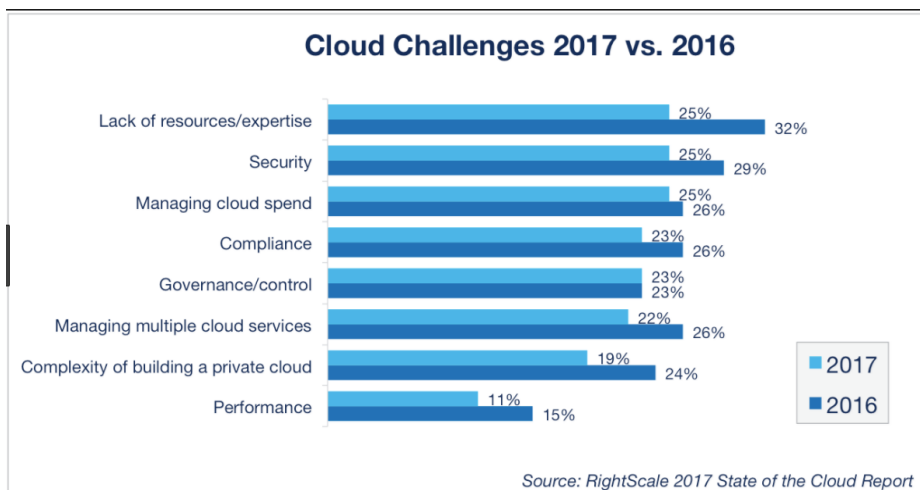


Abbildung 29: Herausforderung der Annahme von Cloud Computing

[rs16]

8.1 Vulnerabilities

Sicherheitsbedrohungen können sowohl außerhalb als auch innerhalb von Organisationen auftreten. Laut der CyberSecurity Watch-Umfrage 2011, die an 607 Unternehmen, Regierungsvertretern, Fachleuten und Beratern durchgeführt wurde, wurden 21 % der Cyberangriffe von Insidern verursacht. 33 % der Befragten hielten die Insider-Angriffe für kostspieliger und für Organisationen schädlich. [cws11]

Die häufigsten internen Angriffe waren unbefugte Zugriffe auf und Nutzung von Unternehmensinformationen (63 %), unbeabsichtigte Offenlegung privater oder sensibler Daten (57 %), Viren, Würmer oder andere bösartige Schadsoftware (37 %) sowie Diebstahl des geistigen Eigentums (32 %).

Die Schwachstellen von Cloud Computing gegenüber böswilligen Insidern sind: unklare Rollen und Verantwortlichkeiten, mangelhafte Durchsetzung von Rollendefinitionen, Nichtanwendbarkeitsprinzip, AAA-Schwachstellen, System- oder Betriebssystemschwachstellen, unzureichende physische Sicherheitsverfahren, Unmöglichkeit der Datenverarbeitung in verschlüsselter Form, Anwendungsschwachstellen oder schlechtes Patch-Management. [cho09]

8.2 Missbrauchsgefahren

Es gibt drei Arten von Cloud-bezogenen Insider-Bedrohungen:

- Den Rogue-Administrator,
- Insider, die Cloud-Schwachstellen ausnutzen,
- und Insider, die die Cloud für ruchlose Aktivitäten nutzen.

Der Rogue-Administrator hat das Recht, ungeschützte Dateien zu stehlen, Brute-Force-Angriffe über Passwörter durchzuführen und Kundendaten von der Opferorganisation herunterzuladen. Insider, die Cloud-Schwachstellen ausnutzen, versuchen, unberechtigten Zugriff auf vertrauliche Daten in einer Organisation zu erlangen. Sie könnten ein Vermögen verdienen, indem sie die sensiblen Informationen verkaufen oder die Informationen für ihre zukünftigen Geschäfte verwenden. Insider, die die Cloud für ruchlose Aktivitäten nutzen, führen Angriffe gegen die IT-Infrastruktur ihres eigenen Arbeitgebers durch. Da die Insider den IT-Betrieb ihrer eigenen Unternehmen kennen, sind die Angriffe in der Regel mit forensischen Analysen schwer zu verfolgen. [cer12]

Die Daten der Endbenutzer, die in der Cloud gespeichert sind, sind vertraulich und privat. Zugriffssteuerungsmechanismen könnten angewendet werden, um sicherzustellen, dass nur autorisierte Benutzer Zugriff auf ihre Daten haben können. Nicht nur, dass die physikalischen Computersysteme (wo Daten gespeichert werden) kontinuierlich

8. Sicherheitsmaßnahmen

überwacht werden müssen, sondern auch der Datenzugriff auf die Daten sollte durch Sicherheitstechniken eingeschränkt werden.

Beim Erstellen von Software, die kryptografische Algorithmen implementieren müssen, gibt es eine Reihe wichtiger Überlegungen. Für benutzerorientierte Software ist eines der Hauptanliegen, wie der Schlüssel gespeichert oder eingegeben wird. [kss17]

8.3 Empfehlungen für die Policies

8.3.1 Access Management:

Firewalls und Intrusion Detektion-Systeme sind gängige Tools, die von nichtvertrauenswürdigen Zugriff auf Ressourcen einschränken und bösartige Aktivitäten überwachen. Darüber hinaus können Authentifizierungsstandards, SAML (Security Assertion Markup Language) und XACML (eXtensible Access Control Markup Language) zur Steuerung des Zugriffs auf Cloud-Anwendungen und -Daten verwendet werden. SAML konzentriert sich auf die Mittel zur Übertragung von Authentifizierungs- und Autorisierungsentscheidungen zwischen kooperierenden Entitäten, während XACML sich auf den Mechanismus zum Erreichen von Autorisierungsentscheidungen konzentriert. [jag11]

8.3.2 Data Loss Prevention

Data Loss Prevention (DLP) ist als Produkt definiert, das basierend auf zentralen Richtlinien Daten im Ruhezustand, in Bewegung und im Gebrauch identifiziert, überwacht und schützt. Dies erfolgt durch eine umfassende Inhaltsanalyse.

8. Sicherheitsmaßnahmen

DLP wird in der Regel für die Inhaltssuche und zur Überwachung von Daten in Bewegung mit den folgenden Optionen verwendet:

- Dedizierte Appliance / Server. Standardhardware, die an einem Netzwerkdrosselpunkt zwischen der Cloud-Umgebung und dem Rest des Netzwerks / Internets oder innerhalb verschiedener Cloud-Segmente platziert wird.
- Virtuelle Appliance
- Endpunkt-Agent
- Hypervisor-Agent. Der DLP-Agent wird auf der Hypervisor-Ebene eingebettet oder auf diese zugegriffen, anstatt auf die Instanz zuzugreifen.
- DLP-SaaS. DLP ist in einen Cloud-Dienst (z. B. gehostete E-Mail) integriert oder wird als eigenständiger Dienst (in der Regel Content-Discovery) angeboten. [csa11]

Datenschutzverletzungen durch Insider können entweder unbeabsichtigt oder vorsätzlich sein. Da es schwierig ist, das Verhalten der Insider zu identifizieren, ist es besser, geeignete Sicherheitswerkzeuge anzuwenden, um mit Insider-Bedrohungen zu umgehen. Zu den Tools gehören: Systeme zur Verhinderung von Datenverlusten, Tools zur Erkennung von Verhaltensmustern, Tools zur Formatspeicherung und -verschlüsselung, Profilierung von Benutzerverhalten, Kryptotechnologie sowie Authentifizierungs- und Autorisierungstechnologien. [csr10] [ssk12]

8. Sicherheitsmaßnahmen

Diese Tools bieten Funktionen wie die Echtzeiterkennung bei der Überwachung des Datenverkehrs, die Protokollierung von Prüfpfaden für zukünftige Forensik und das Einfangen von bössartigen Aktivitäten in Lock-Dokumenten. [tsc13]

8.3.3 Data Leak Protection (DLP)

Vorher ist es notwendig die Data Leak Prevention (DLP) zu definieren. Die meisten DLP-Lösungen umfassen eine Reihe von Technologien, die drei Hauptziele unterstützen:

- Lokalisieren und Katalogisieren sensibler Informationen, die im gesamten Unternehmen gespeichert sind
- Überwachung und Kontrolle der Übertragung vertraulicher Informationen in Unternehmensnetzwerken
- Überwachung und Kontrolle der Übertragung sensibler Informationen auf Endbenutzersystemen

Diese Ziele sind mit drei primären "Informationszuständen" verbunden: Daten im Ruhezustand, Daten in Bewegung und Daten in Verwendung. [ISA10]

8.3.4 Data at rest

Eine grundlegende Funktion von DLP-Lösungen ist die Fähigkeit bestimmte Arten von Informationen, die im gesamten Unternehmen gespeichert sind, zu identifizieren und zu protokollieren.

Dies bedeutet, dass die DLP-Lösung die Fähigkeit innehaben muss, bestimmte Dateitypen zu suchen und zu identifizieren.

8. Sicherheitsmaßnahmen

Wenn die Dateitypen gefunden sind, muss die DLP-Lösung in der Lage sein, diese Dateien zu öffnen und ihren Inhalt zu scannen, um festzustellen, ob bestimmte Informationen vorhanden sind, z.B. Kreditkarten oder Sozialversicherungsnummer.

Um diese Aufgaben zu erfüllen, verwenden die meisten DLP-Systeme Crawler. Das sind die Applikationen, die remote bereitgestellt sind und DLP Systemen erlauben, sich bei jedem Endsystem anzumelden und durch Datenspeicher zu "crawlen". Infolgedessen kann der Speicherort bestimmter Informationsgruppen, die auf einer Reihe von Regeln, die in die DLP-Verwaltungskonsole eingegeben wurden, basieren, gefunden werden.

Das Sammeln dieser Informationen ist ein wertvoller Schritt, um dem Unternehmen zu ermöglichen bzw. zu bestimmen wo seine Schlüsselinformationen liegen sowie diese Informationen auch korrekt zu lokalisieren. Des Weiteren soll bestimmt werden, ob seine Position in vorhandenen Richtlinien erlaubt ist und welche Pfade diese Daten, die gegen die Richtlinien verstoßen, möglicherweise durchlaufen würden.
[ISA10]

8.3.5 Daten in Bewegung (Data in motion (network))

Um die, über das Netzwerk gesendete Information zu prüfen, muss die DLP-Lösung in der Lage sein den Netzwerkverkehr passiv zu überwachen, die richtigen Datenströme zu erfassen und die gesammelten Datenpakete zusammenzustellen. Außerdem muss es imstande sein, die im Datenstrom enthaltenen Dateien zu rekonstruieren und anschließend die gleiche Analyse mit den Daten im Ruhezustand durch-

8. Sicherheitsmaßnahmen

zuführen, um zu bestimmen, ob irgendein Teil des Dateiinhalts durch seinen Regelsatz eingeschränkt ist. Der Kern dieser Fähigkeit ist ein Prozess, der als Deep Packet Inspection (DPI) bekannt ist und die DLP-Daten-in-Bewegung-Komponente dazu befähigt, diese Aufgaben zu erfüllen. DPI geht über die grundlegende Kopfinformation eines Pakets hinaus, um den Inhalt innerhalb der Nutzlast des Pakets zu lesen.

Eine wichtige Überlegung für Netzwerk-DLP ist, dass die Daten entschlüsselt werden müssen, bevor die DLP-Lösung die Daten überprüfen kann. Entweder muss die DLP-Lösung selbst dazu in der Lage sein, oder es muss ein Gerät vorhanden sein, das den Datenverkehr vor seiner Überprüfung durch das DLP-Modul entschlüsselt und danach erneut verschlüsselt, sobald die Daten überprüft und übergeben wurden. [ISA10]

8.3.6 Data in use (end-point)

Daten in Verwendung ist vielleicht der schwierigste Aspekt von DLP. Die verwendeten Daten beziehen sich hauptsächlich auf die Überwachung der Datenbewegungen, die von den Aktionen der Endbenutzer auf ihren Workstations stammen. Dabei verfügen sie über die Informationen, ob das Kopieren von Daten auf einen USB-Stick, das Senden von Informationen an einen Drucker oder das Ausschneiden und Einfügen zwischen Anwendungen erforderlich ist. [ISA10]

9. Compliances Challenges

9.1 Audit

Zu einer ordnungsgemäßen organisatorischen Steuerung gehören natürlich auch das Audit und die Überwachung. Das Audit muss unabhängig durchgeführt werden und sollte robust ausgelegt sein, um bewährte Verfahren, angemessene Ressourcen und getestete Protokolle und Standards widerzuspiegeln.

Sowohl interne als auch externe Audits und Kontrollen haben eine legitime Rolle für die Cloud, und zwar nicht nur für den Kunden, sondern auch für den Anbieter. Größere Transparenz könnte in den Anfangsphasen der Einführung der Cloud am besten geeignet sein, um den Komfort der Stakeholder zu erhöhen. Ein Audit stellt eine Methode dar, mit der sichergestellt werden kann, dass die Aktivitäten des operativen Risikomanagements gründlich getestet und überprüft werden.

Es ist zu empfehlen, dass die externen Prüfer entweder im Voraus oder gemeinsam von Anbieter und Kunde ausgewählt werden. [csa11]

9.2 Digital Rights Management (DRM)

Es gibt zwei große Kategorien von Digital Rights Management:

- Consumer DRM schützt weit verbreitete Inhalte wie Audio-, Video- und elektronische Bücher, die für ein Massenpublikum bestimmt sind. Es gibt eine Vielzahl verschiedener Technolo-

10. Entwicklung eines Governance Modells

gien und Standards, und der Schwerpunkt liegt auf der einseitigen Verteilung.

- Enterprise DRM wird verwendet, um den Inhalt einer Organisation intern und mit Geschäftspartnern zu schützen. Der Schwerpunkt liegt auf komplexeren Rechten, Richtlinien und Integration in Geschäftsumgebungen insbesondere mit dem Unternehmensverzeichnisdienst.

Enterprise DRM kann Inhalte, die in der Cloud gespeichert sind, gut absichern, erfordert jedoch eine umfassende Infrastrukturintegration. Es ist am nützlichsten für die dokumentenbasierte Verwaltung und Verteilung von Inhalten. Consumer DRM bietet einen guten Schutz für die Verteilung von Inhalten an Kunden, hat jedoch keine gute Erfolgsbilanz, da die meisten Technologien irgendwann geknackt werden. [csa11]

10. Entwicklung eines Governance Modells

10.1 Bestehende Governance Modelle

Die Position der Cloud-Governance, wie in der Abbildung 12 nahegelegt wurde, zeigt, dass SOA-Governance-Lösungsmodell auch für die Cloud geeignet ist. Ein weiterer nützlicher Input für die Strukturierung des Lösungsmodells sind bestehende Cloud-Governance-Frameworks oder -Modelle. [yhe11]

10. Entwicklung eines Governance Modells

In diesem Teil des Kapitels werden die relevante Governance Modelle beschrieben und der Begriff Modell und Modellentwicklung definiert. Es wird auch eine Auflistung von möglichen Modellvorschlägen gegeben. Es werden auch relevante und bestehende Modelle eingeführt. Der Zweck für die Präsentation dieser Modelle ist doppelt. Auf der einen Seite können diese Modelle als sehr wichtige Inputs dienen, um den Lösungsvorschlag zu definieren. Auf der anderen Seite kann eine geeignete Referenz für die Prozessmodellierung gefunden werden.

Hier sind 4 Modelle, die kurz umrissen werden:

- Schepers' Lifecycle SOA Governance Modell
- AUS SOA Governance Framework
- GUO's Cloud Governance Modell
- Microsoft's Cloud Governance Modell [Sch07]

10. Entwicklung eines Governance Modells

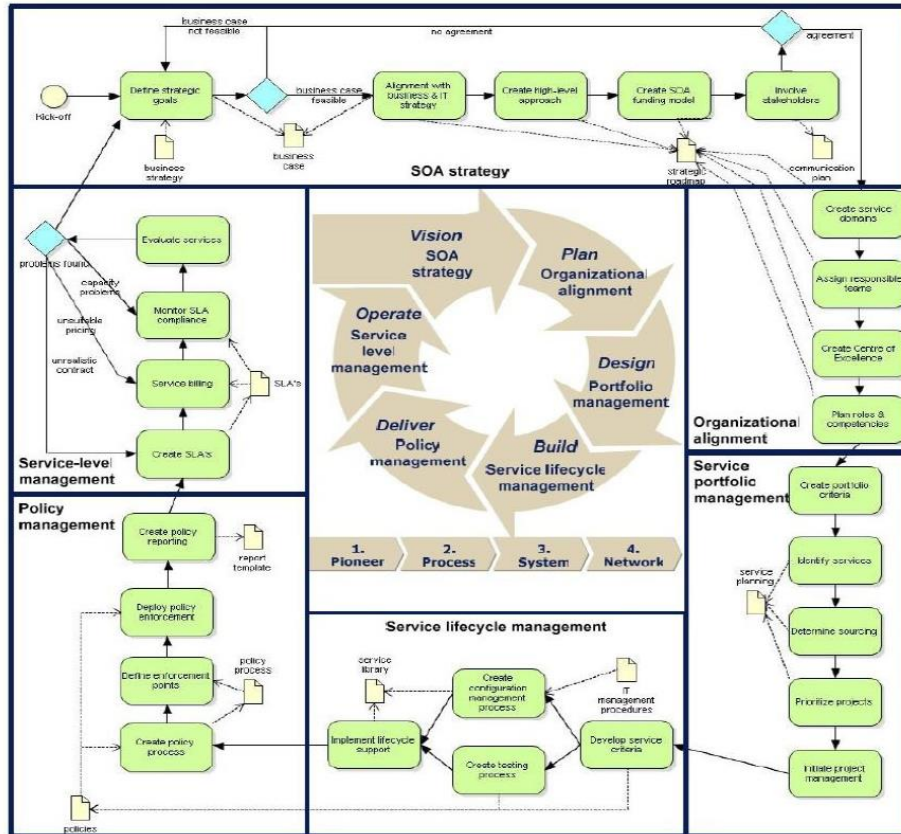


Abbildung 30: Lifecycle Methode für SOA Governance [Sch07]

[Sch07] hat einen Lifecycle-Ansatz für die SOA-Governance entwickelt. Zu den Governance-Bereichen seines Modells gehören Portfolio-Governance, Technologie-Governance, Projekt-Governance und Service-Level-Governance. Das Modell auf der Abbildung 28 besteht aus 6 Phasen um SOA innerhalb einer Organisation zu überwachen.

Der Lifecycle zeigt die Reihenfolge an, in der die Phasen initiiert werden sollen. Diese Reihenfolge ist gleichzeitig keine chronologische

10. Entwicklung eines Governance Modells

Reihenfolge zwischen den Phasen. Für jeden Prozess wird eine entsprechende Herangehensweise diskutiert und analysiert. Diese sechs Bereiche sind nach dem [Sch07]:

- SOA Strategie oder Vision: enthält langzeitige SOA-Planung, wie die Modellfinanzierung und Einbeziehung von Stakeholders
- Organisatorische Alignment auf SOA (Plan): konzentriert sich auf organisatorische Änderungen und die Rollen / verantwortliche Anpassung für besseres Business/IT Alignment.
- Portfolio Management (Design): Prozesse einzurichten, um zu bestimmen, welcher Dienst erstellt werden soll und wann ein Service dem Portfolio hinzugefügt werden soll.
- Service Lifecycle Management (Build): Sicherstellung der qualitativen Service-Entwicklung und Einführung des Change-Management
- Policy Management (Delivery): wie kann Service Qualitätsgarantie auf einem bestimmten Niveau gehalten werden.
- Service level management (operate): operational SOA Services Qualität [Sch07]

10. Entwicklung eines Governance Modells

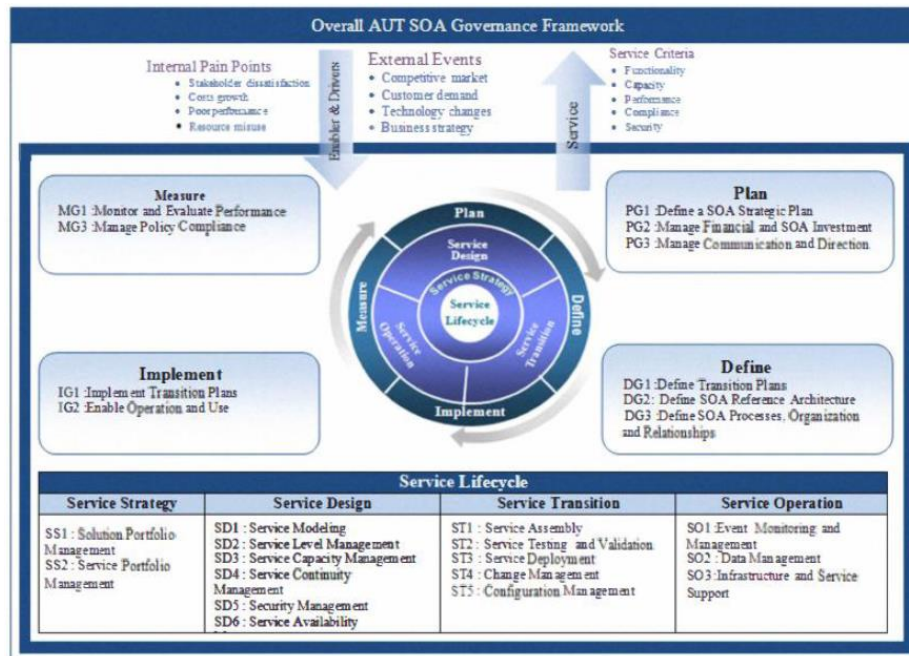


Abbildung 31: AUT SOA Governance Framework [HoS10]

Das Framework wird durch die Durchsetzung von Governance-Strukturen von COBIT und gründliche Analyse von sechs bestehenden populären SOA-Governance-Modellen erreicht. Es wendet Service-Management-Aktivitäten auf einem Lifecycle-Ansatz an. Das Framework bietet gut definierte und strukturierte Prozessmengen an.

[HoS10] Das Modell kann nicht nur zu dem Modell von Scheppers komplementär sein, sondern auch andere Lösungsvorschläge für Cloud-Governance anbieten, wenn es notwendig ist.

10. Entwicklung eines Governance Modells

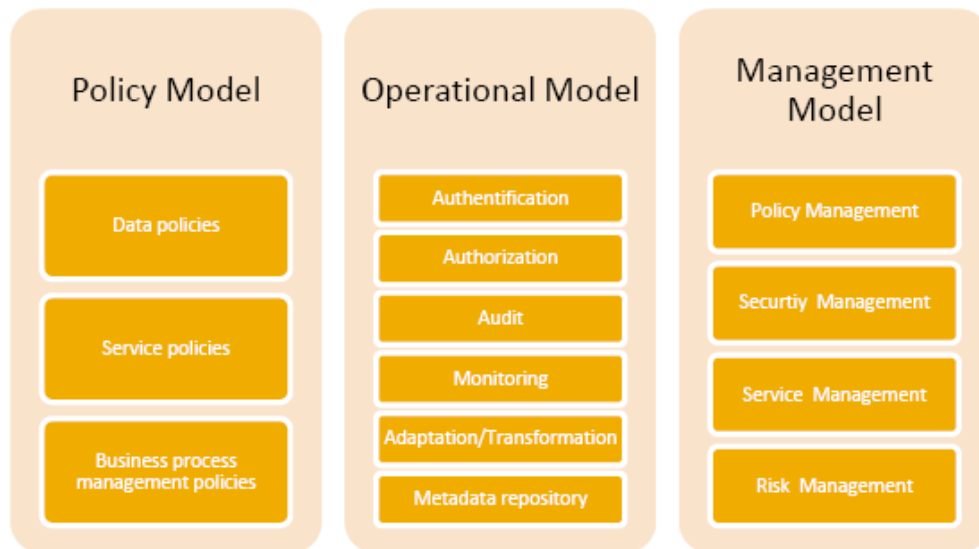


Abbildung 32: Cloud Governance Modell from Guo et al. [guo10]

Das ist ein Governance Modell für Cloud Computing. Dieses Modell ist das einzige im akademischen Bereich, das Aspekte der Cloud-Governance im Allgemeinen diskutiert. Dieses Modell skizziert notwendige Komponenten für Cloud-Governance und konzentriert sich auf Policy Modellierung, operationelles Modell und andere Managementaktivitäten wie z.B. Service Management, Risiko Management, Security Management und Policy Management. [guo10] [yhe11]

10. Entwicklung eines Governance Modells

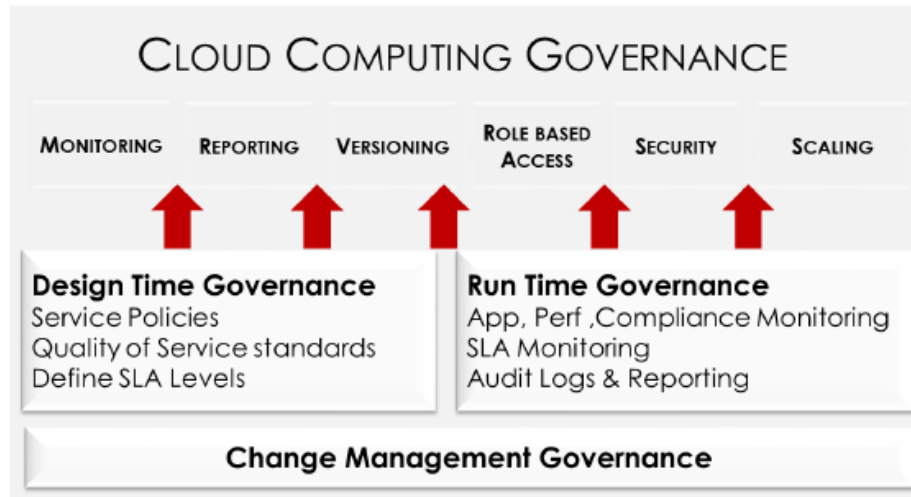


Abbildung 33: Microsoft's Cloud Governance Modell [Microsoft, 2010]

Im Jahr 2010 hat Microsoft ein eigenes Cloud Governance Modell für eigene Azure Cloud Plattform veröffentlicht. Microsoft hat Schwerpunkt auf Policy Management gesetzt. Das Modell besitzt drei Hauptkomponenten: Design Time, Run Time Governance und change Management Governance.

Während der Design Time müssen Service-Policies, die Qualität der Standards und die SLA-Ebenen festgelegt werden.

Während der Run Time werden Richtlinien durchgesetzt und die Anwendungs- / Serviceleistung sowie die Compliance sorgfältig überwacht. Auf der anderen Seite fokussiert sich

Change Management Governance auf Aktivitätsänderungen und Asset. [yhe11]

Es ist erforderlich gleichzeitig Berichte, Warnungen und Protokolle bereitzustellen und zu verwalten. Die drei Komponenten arbeiten zu-

10. Entwicklung eines Governance Modells

sammen, um eine korrekte Version und Skalierung zu gewährleisten und die Einhaltung von Sicherheitsrichtlinien sicherzustellen. [yhe11]

10.2 Anforderungen für ein wirksames Governance Modell

Jede Organisation muss eigene Kriterien für eine effektive Cloud-Governance definieren. Die Fördermengen einer Organisation von eigenem Cloud-Governance-System sind den Bedürfnissen der Organisation angepasst. Da es keine zwei vollkommen gleichen Businesses im wahren Leben gibt, variieren auch die Kriterien zwischen den Organisationen/Unternehmen. Für die meisten Cloud-Governance-Systeme sollen die gleichen Cloud-Governance-System-Kernkriterien existieren und angewendet werden:

1. Es garantiert Alignment von Cloud-Services mit Business-Vorgaben und Zielsetzungen, IT-Vorgaben und Zielsetzungen und Stakeholder Bedürfnissen.
2. Es garantiert entsprechende Cloud Service-bezogene Kommunikation und Berichterstattung.
3. Es stellt sicher, dass Cloud-Service-Akquisitionen ordnungsgemäß erstellt werden, um die Cloud Service- und Geschäftsanforderungen zu erfüllen
4. Es stellt sicher, dass Cloud-Service-Ziele erreicht werden.
5. Es gewährleistet Agilität in Prozessen und Praktiken, um die Möglichkeiten von Cloud-Services vollständig zu nutzen.
6. Es stellt sicher, dass erwartete Cloud-Service-Vorteile realisiert werden.

10. Entwicklung eines Governance Modells

7. Es stellt sicher, dass organisatorische Risiken im Zusammenhang mit Cloud-Diensten, einschließlich Sicherheitsrisiken, identifiziert, verfolgt und entsprechend verwaltet werden.

8. Es stellt sicher, dass Cloud-Service-bezogene Aktivitäten mit gesetzlicher, regulatorischen, vertraglichen Anforderungen und internen Verfahren und Leistungsziele konform sind.

9. Es stellt sicher, dass die Interessengruppen angemessen beteiligt sind.

10. Es stellt sicher, dass in der Cloud gespeicherte Daten und Informationen sicher sind.

11. Es stellt sicher, dass Teams richtig trainiert werden; Einzelpersonen haben die angemessene Kompetenz, und jeder ist sich seiner Führungsrolle und Verantwortungsbereiche bewusst.

Sie sollten die Listenkriterien für die Anforderungen Ihrer Organisation hinzufügen. [lfu15]

10. Entwicklung eines Governance Modells

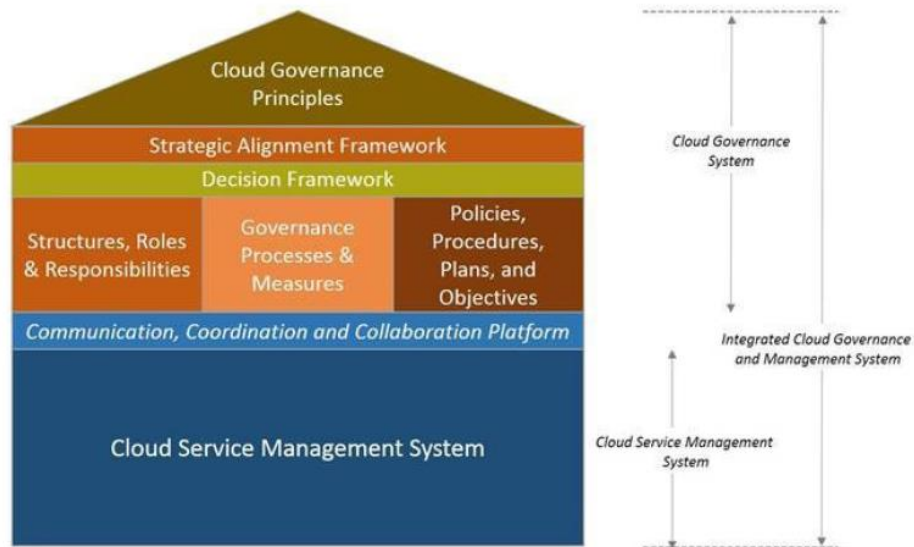


Abbildung 34: Good Cloud Governance [Ifu15]

Abb. 32 zeigt die Bausteine für eine gute Cloud-Governance. Wie jeder Block entworfen und implementiert wird, hängt von den Bedürfnissen und Einschränkungen eines Unternehmens ab.

Good Cloud Governance bietet Kontext für das Cloud Governance System in Bezug auf ein Cloud Service Management System und ein integriertes Cloud Governance und Management System. Das Integriertes Cloud Governance- und Managementsystem ist die Summe der einzelnen Governance- und Managementsysteme. [Ifu15]

10.2.1 GDPR

Die EU - Datenschutzgrundverordnung (DSGVO) oder General Data Protection Regulation (GDPR) ist „die wichtigste Änderung in Datenschutzregelung in den letzten 20 Jahren“. [EUGD18]

10. Entwicklung eines Governance Modells

Die DSGVO schützt die personenbezogenen Daten von Einzelpersonen, einschließlich Personen, die sich in der EU aufhalten, auch wenn sie keine EU-Bürger sind.

- Durch die Festlegung des Geltungsbereichs der DSGVO, einschließlich der Überwachung des Verhaltens von Einzelpersonen, ist die Anwendbarkeit umfassend. Praktisch jede Website und App verfolgt die digitalen Aktivitäten ihrer Besucher in gewisser Weise.
- Die DSGVO erstreckt sich nun auf Sorgfaltspflichten und eine mögliche Haftung gegenüber Daten-Verarbeitern und nicht nur Daten-Kontrolleuren.
- Die DSGVO definiert personenbezogene Daten ziemlich weit gefasst. Zum Beispiel sind geschäftliche Kontaktinformationen wie die geschäftliche E-Mail-Adresse einer Person in der Regel von der DSGVO abgedeckt. [TR18]

10.2.2 GDPR-Schlüsseländerungen

Ziel der Datenschutz-Grundverordnung ist es, alle EU-Bürger in einer zunehmend datengetriebenen Welt vor Datenverletzungen zu schützen, die sich erheblich von der Zeit unterscheiden, in der die Richtlinie von 1995 aufgestellt wurde.

10. Entwicklung eines Governance Modells

Die Schlüsseländerungen betreffen folgendes: Größerer territorialer Umfang, härtere Strafen, klare Strafmaßnahmen. Unter Datensubjekt-Rechte sind folgende Punkte verpflichtend: Verstoßmeldung, das Zugangsrecht für Datensubjekte, das Recht vergessen zu werden, Daten Portabilität, Datenschutz durch Design und Datenschutzbeauftragte. [<https://www.eugdpr.org/>]

10.2.3 Individuelle Rechte und Rechtsmittel

Eine Schlüsseländerung im Rahmen der Datenschutz-Grundverordnung besteht in der Ausweitung der individuellen Rechte auf beispielsweise das Recht auf Information, das Recht auf Zugang, das Recht auf Berichtigung, das Recht auf Einschränkung der Verarbeitung, das Recht auf Widerspruch, das Recht auf Löschung und das Recht auf Datenübertragbarkeit.

Aufgrund dieser Erweiterung müssen die bestehenden Richtlinien, Prozesse und Verfahren der Unternehmen überprüft werden. In einigen Fällen müssen technologische Veränderungen vorgenommen werden. [TR18]

10. Entwicklung eines Governance Modells

Risk Level vs. Level of Effort				
		Level of Effort		
		HIGH	MODERATE	LOW
Risk Level	HIGH	Data Lifecycle Management Process Privacy Audit Program	Vendor Review Framework Employee Training Privacy Team Data Flow Monitoring Privacy Breach Preparedness	Contract Language for Vendors Privacy Ownership across Organization Data Governance Committee
	LOW			Privacy Team Training

Tabelle 5: Level of Effort (LOE) [TR18]

Die Tabelle 5 zeigt den Beispielwert von Schätzungsaufwand (LOE) - Niedrig, Mittel und Hoch, die zur Visualisierung die Prioritäten Ihres Plans beitragen.

10.2.4 ISO/IEC 27000 family

- Information security management systems (ISMS)

ISO/IEC 27001:2013 (ISO 27001) ist der internationale Standard, der Best Practice für ein ISMS (Information Security Management System) beschreibt. Das Erreichen einer akkreditierten Zertifizierung nach ISO 27001 zeigt, dass Ihr Unternehmen die Best Practices für Informationssicherheit befolgt und eine unabhängige, fachkundige Überprüfung durchführt, dass die Informationssicherheit im Einklang mit internationalen Best Practice- und Geschäftszielen verwaltet wird. ISO 27001

10. Entwicklung eines Governance Modells

wird durch seinen Verhaltenskodex für das Management der Informationssicherheit, ISO / IEC 27002: 2013, unterstützt. [itg18]

Was ist ein ISMS?

„Ein ISMS ist ein systematischer Ansatz, um sensible Unternehmensinformationen so zu verwalten, dass sie sicher bleiben. Es umfasst Personen, Prozesse und IT-Systeme unter Anwendung eines Risikomanagementprozesses.“³³

Ein ISMS ist ein System von Prozessen, Dokumenten, Technologien und Personen, das hilft, die Informationssicherheit Ihres Unternehmens zu verwalten, zu überwachen, zu prüfen und zu verbessern. Es hilft Ihnen, alle Ihre Sicherheitsmaßnahmen einheitlich und kosteneffizient an einem Ort zu verwalten. [itg18]

³³ <https://www.iso.org/isoiec-27001-information-security.html>

11. Privacy-Driven Governance Modell

Bei der Erstellung des Privacy-driven Governance Modells wurden folgenden Aspekte berücksichtigt: Requirements, Policies, Operationale Komponente und Threads und Vulnerabilities.

Die Komponenten wie zum Beispiel Decision Rights und Information Quality oder Testing Lifecycle werden in dieser Arbeit nicht weiter betrachtet.

11.1 Konstruktion eines Governance Modells

Zuerst wird es notwendig strategische Ziele zu setzen, die das privacy-driven Governance Modell erfüllen muss.

Wenn diese Ziele realisierbar sind, kann zur parallelen Überprüfung der Voraussetzungen und Policies weitergegangen werden.

Am Anfang galt die Voraussetzungen für das Governance Modell und anschließend, ob das Modell GDPR-konform ist. Dazu ist es notwendig zu erwähnen, dass in der Zukunft auch mit einem GDPR Nachfolger zu rechnen ist und dieser Schritt privacy legislation Compliance Komponente genannt wird. Es ist auch äußerst wichtig, dass das Governance Modell auch die ISMS Voraussetzungen und ISO/IEC 27001:2013 (ISO 27001) völlig erfüllt.

Bei der Erstellung des SOA Modells, müssen alle diese Schritte erfüllt werden.

11. Privacy-Driven Governance Modell



Abbildung 35: SOA strategy Snap aus Lifecycle Method for SOA governance [sch07]

Um das komplette Modellkonzept darzustellen, wurde noch die CSA Cloud Control Matrix berücksichtigt und wie in der Abbildung 40 zu sehen ist, im Modell angepasst.



Abbildung 36: CSA Star Certification³⁴

³⁴ <https://www.bsigroup.com/en-GB/CSA-STAR-Certification/Benefits-CSASTAR-Certification/>

11. Privacy-Driven Governance Modell

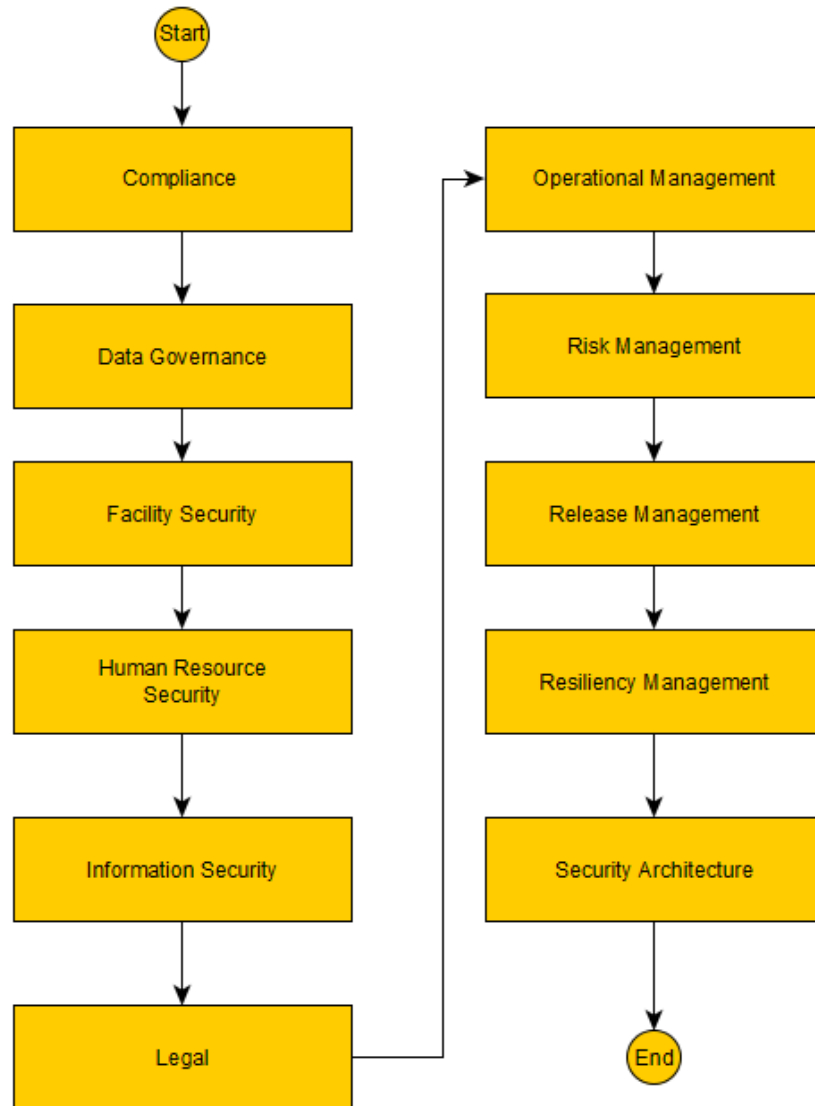


Abbildung 37: Basierend auf Abb.34 CSA Cloud Control Matrix Flow

11. Privacy-Driven Governance Modell

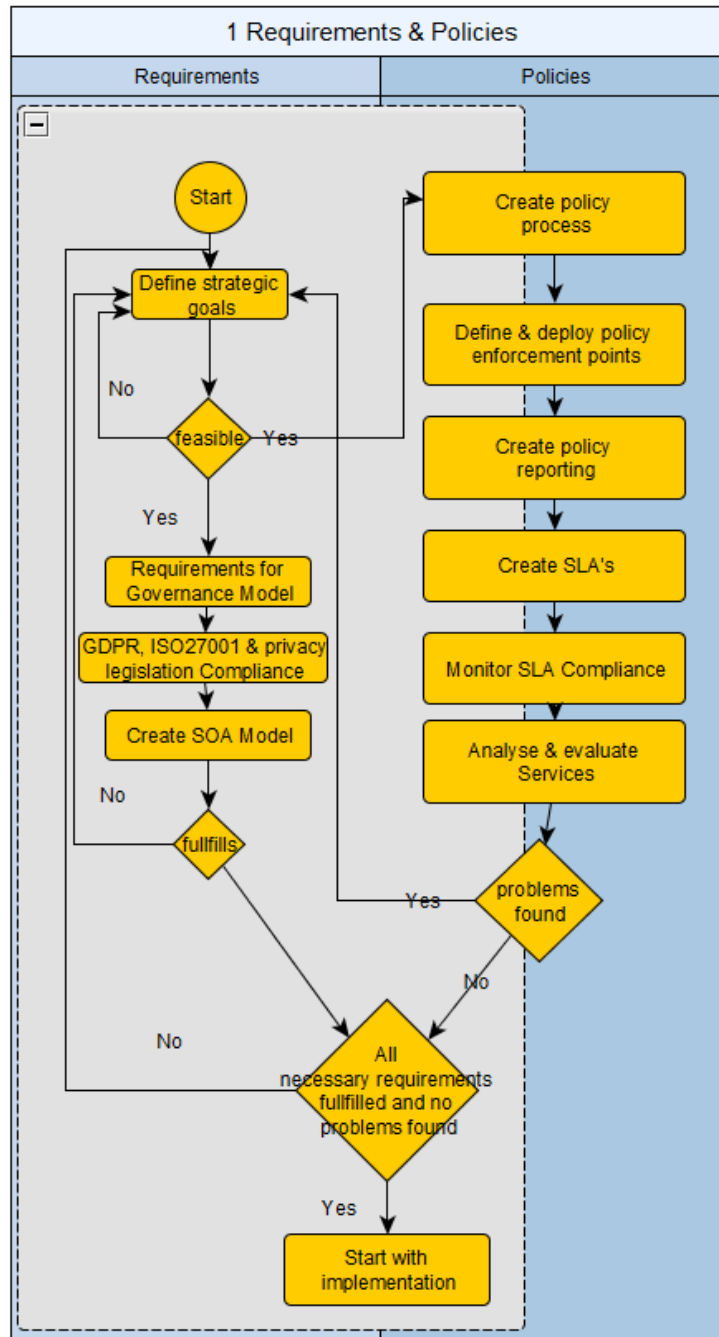


Abbildung 38: Modell Requirements & Policies

11. Privacy-Driven Governance Modell

Ein funktionsfähiges und realitätsnahes Modell aufzusetzen, stellt jederzeit eine Herausforderung dar. Die zentrale Aufgabe eines Modells ist, eine Liste von Voraussetzungen und Richtlinien zu erfüllen. Am Anfang ist es notwendig, diese zu definieren.

Die wesentlichen Schritte eines Modells, zu sehen Abbildung nn, sind die strategischen Ziele zu definieren und zu überprüfen, ob diese anwendbar sind. Danach besteht die Notwendigkeit, die Voraussetzungen für Governance Modell zu überprüfen und somit auch, ob das Modell mit aktuellen GDPR-Richtlinien konform ist. Dazu wird das Modell auf den ISO 27001 Standard überprüft.

Es ist äußerst wichtig, dass das Modell ebenso auf die aktuellen Datenschutzgesetze geprüft wird.

In der nächsten Phase wird SOA Modell erstellt. Die Voraussetzungen dafür werden noch einmal kontrolliert und überprüft. Sind diese Voraussetzungen nicht gegeben, muss der ganze Prozess von oben wiederholt werden.

Parallel zu diesem Prozess, nach dem die strategischen Ziele gesetzt sind und auch auf Machbarkeit überprüft wurden, wird mit der Erstellung des Policyprozesses gestartet.

Darüber hinaus werden die Richtlinienerzwingungspunkte definiert und implementiert. Es erfolgt die Erstellung zu den Richtlinien für die Bereiche.

11. Privacy-Driven Governance Modell

In der rechten Spalte der Policies besteht die Notwendigkeit, die SLA³⁵ zu erstellen und anschließend zu überwachen, in wie weit diese Service Level Agreements eingehalten sind. Die Services werden die komplette Zeit analysiert, evaluiert und im Fall, dass irgendwelche Probleme gefunden werden, die strategischen Ziele wiederholt überprüft.

Im Fall, dass die Voraussetzungen und Policies erfüllt sind, kann mit der Implementierung gestartet werden.

³⁵ Service-level Agreement

11. Privacy-Driven Governance Modell

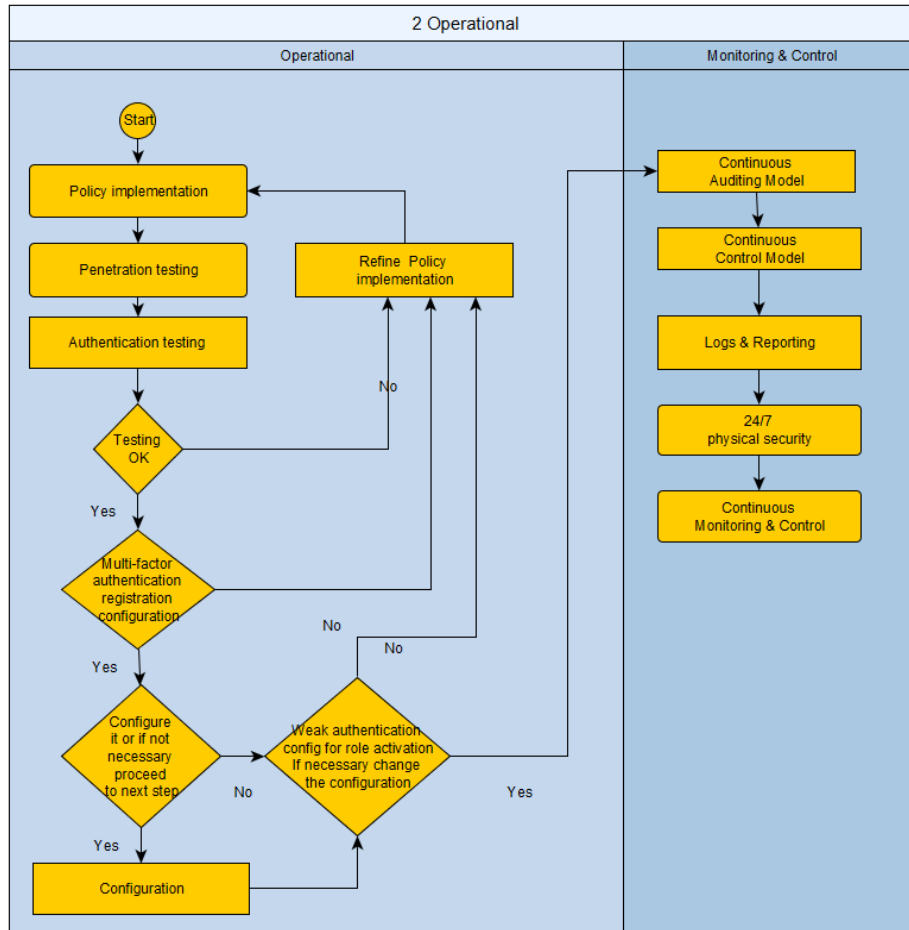


Abbildung 39: Modell Operationale Komponente

Im operationelem Teil wird mit der Policyimplementierung und den dazu benötigten unterschiedlichen Tests gestartet. Beginnend mit dem Penetrationstests und gefolgt von den Authentifizierungstests werden die Untersuchungen durchlaufen. Wenn beide Tests positiv abgeschlossen sind, kann mit dem nächsten Schritten fortgeführt werden.

11. Privacy-Driven Governance Modell

Hier wird überprüft, ob die Registrierung von Multi-Faktor-Authentifizierung konfiguriert ist, für den Fall, dass keine Konfiguration stattgefunden hatte, wird die Policyimplementierung redefiniert und der gesamte Prozess wird wiederholt. Im anderen Fall wird die Registrierung von Multi-Faktor-Authentifizierung konfiguriert oder falls keine Notwendigkeit besteht, dieser Konfigurationsschritt übersprungen.

Im nächsten Schritt gilt es zu überprüfen, ob die Authentifizierungskonfiguration für die Rollenaktivierung ausreichend ist. Wenn es Bedarf gibt, wird die Konfiguration entsprechend angepasst.

Nach dem die Authentifizierungskonfiguration überprüft wird, geht es weiter zum kontinuierlichen Auditing-Modell und kontinuierlichem Steuerungsmodell.

Ein privacy-driven Governance Modell für Cloud Computing muss ein kontinuierliches Auditing- und Steuerungsmodell besitzen.

Dazu gehören die regelmäßigen Speicherprozeduren für die Logdateien und verschiedenen Berichtarten.

Es ist äußerst wichtig, auch nach dem ISO 27001 Standard eine 24/7 physische Sicherheit zu gewährleisten. Die Server, die Räume sowie die Gebäude müssen nach den entsprechenden Standards, inkl. ISO27001, gesichert werden.

Kontinuierliche Monitoring und Systemsteuerung sind eine Voraussetzung, die in allen Arbeitsphasen durchgeführt werden müssen.

11. Privacy-Driven Governance Modell

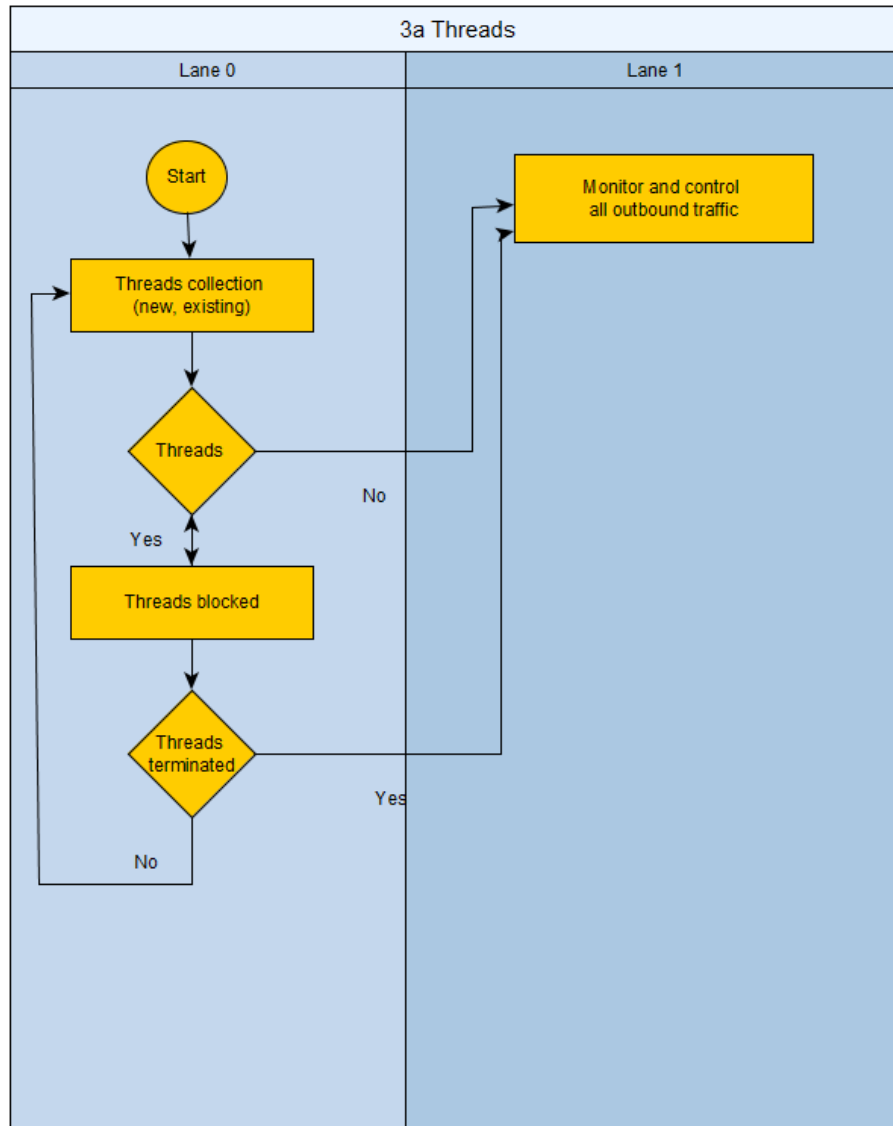


Abbildung 40: Model Threads

Wie in einem Betriebssystem besteht auch hier die Notwendigkeit, mit einem privacy-driven Governance-Modell zu versichern, dass die Threads rechtzeitig entdeckt werden. Wenn es nicht frühzeitig möglich

11. Privacy-Driven Governance Modell

ist diese zu entfernen, müssen die Threads zumindestens blockiert werden, bis die Lösung gefunden wird. Im Anschluss werden die blockierten Threads fehlerfrei aus dem System entfernt.

Es findet über den gesamten Zeitraum eine Überwachung und Steuerung des ein- und ausgehenden Datenverkehrs statt.

11. Privacy-Driven Governance Modell

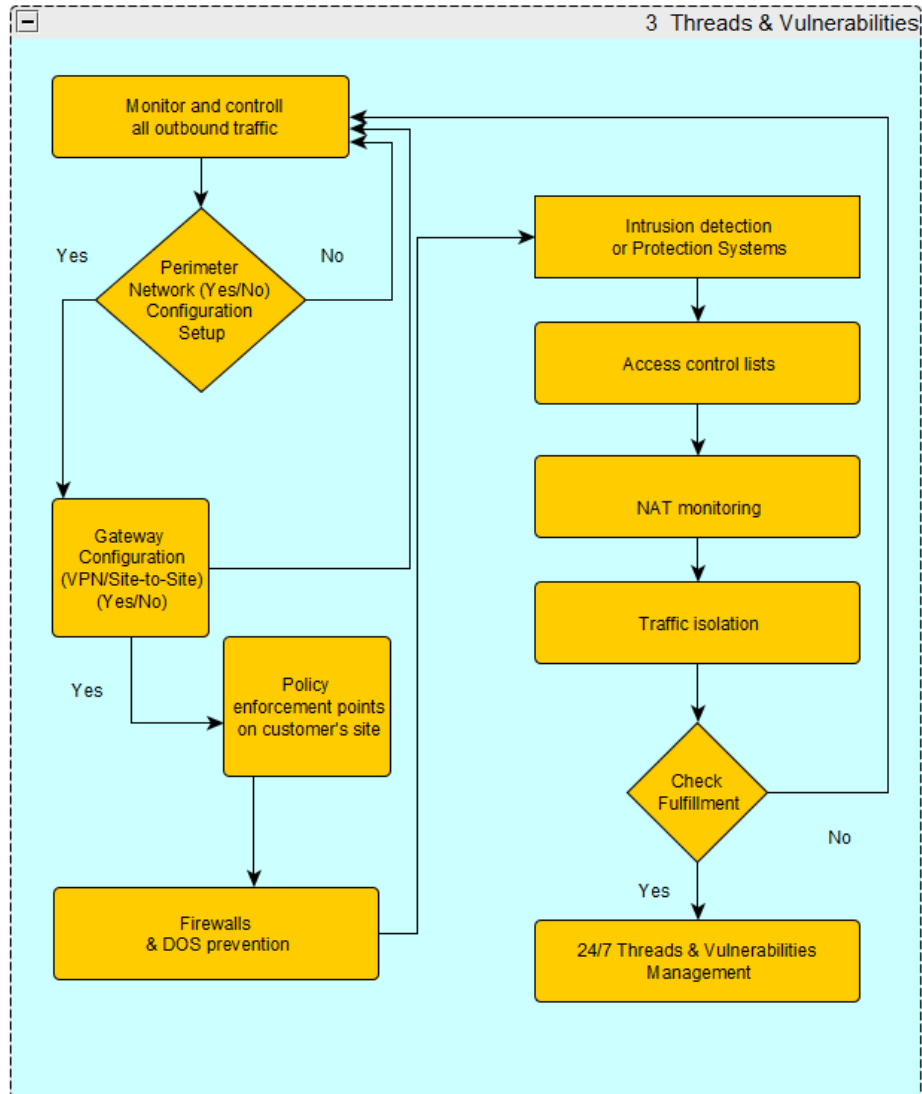


Abbildung 41: Modell Vulnerabilities

Wie bei den Threads, muss das System, wenn es um die Vulnerabilities geht, auch konstant überwacht und gesteuert werden.

Als erster Schritt wird abgefragt, ob die Konfiguration für die Perimeter-

11. Privacy-Driven Governance Modell

Netzwerk abgeschlossen ist. Sollte dies nicht geschehen sein, wird der Prozess auf die obere Ebene zurückgewiesen. Wenn das Perimeter-Netzwerk gesamtheitlich konfiguriert wurde, wird überprüft, ob die Gateway-Konfiguration zu 100 % abgeschlossen ist. I.d.R. ist hier die Rede von VPN oder Site-to-site. Wenn die Gatewaykonfiguration abgeschlossen ist, kann es zum nächsten Schritt weitergehen. Es besteht nicht nur auf der Serverseite die Notwendigkeit bestimmte Richtlinien und Standards zu implementieren, sondern auch auf der Clientseite müssen bestimmte Richtliniendurchsetzungspunkte durchgeführt werden, damit die Schwachstellen und denkbare unsichere Schnittstellen vorzeitig gesichert werden können.

In einem weiteren Schritt ist es notwendig, dass System präventiv mit einer Firewall gegen DOS³⁶ und gegen weitere Datenangriffe zu schützen.

Eine Reihe von präventiven Maßnahmen muss zusätzlich angewendet werden: Intrusion detection oder Protection Systems, anschliessend eine Zugangssteuerungsliste, in der exakt definiert wurde, welchen Personen welche Rollen zugewiesen wurden.

Die Zugriffssteuerungsrichtlinie ist Bestandteil der allgemeinen Richtlinien und wird einem formellen Überprüfungs- und Aktualisierungsprozess unterzogen.

NAT³⁷ wird konstant überwacht und der Datenverkehr muss von dem anderen Verkehr im Netz isoliert werden. Ob das Feature bzw. die

³⁶ Denial of Service

11. Privacy-Driven Governance Modell

Protokolle wie z. B. (Perfect) Forward Secrecy oder andere angewendet werden, ist für diese Arbeit nicht entscheidend.

11.2 Was ist Perfect Forward Secrecy?

Perfect Forward Secrecy schützt zusätzlich die Vertraulichkeit und Integrität der Daten, welche innerhalb einer bestehenden und verschlüsselten TLS-Verbindung von oder zu einer Website bzw. Dienst ausgetauscht werden. [sch14]

Zum Ende des Prozesses Fulfillment wird überprüft, ob keine Beanstandungen oder Voraussetzungen vernachlässigt wurden bzw. die notwendigen Entscheidungsfragen erfüllt wurden, so dass die Phase „24/7 Threads und Vulnerabilities Management“ anschließen kann.

³⁷ Network address translation

11.3 Reality Check / Praxis Test

– Anwendungsbeispiel für MS Windows Azure

Das privacy-driven Governance Modell wird mit dem aktuellen bestehenden MS Windows Azure und allen notwendigen Schritten verglichen als auch überprüft.

Windows Azure ist ein Cloud Services-Betriebssystem, welches als Entwicklungs-, Service-Hosting- und Service-Management-Umgebung für die Windows Azure-Plattform dient.

Die Windows-Azure-Kerndienste (Compute, Storage und Virtual Network) sind nach ISO / IEC 27001: 2005 (aka ISO 27001) zertifiziert.

Darüber hinaus ist die physische Infrastruktur von GFS, welche in der Windows Azure mit Ausnahme für CDN ausgeführt wird, nach ISO 27001 zertifiziert.

Die GFS-Infrastruktur unterliegt einer jährlichen Auditierung nach (SAS) Nr. 70 des AICPA³⁸, welche jedoch durch eine AICPA-Stellungnahme zu SSAE³⁹ Nr. 16 und einer International Audits Standards für Assurance Engagements (ISAE) Nr. 3402 Audit ersetzt wurde. Die finale Planung für eine SSAE 16-Prüfung von Windows Azure wird derzeit angestrebt. [ms18]

Die Überprüfung der 11 Schritte aus CSA Cloud Control Matrix ergibt:

³⁸ American Institute of Certified Public Accountants

³⁹ Standards for Attestation Engagements

11. Privacy-Driven Governance Modell

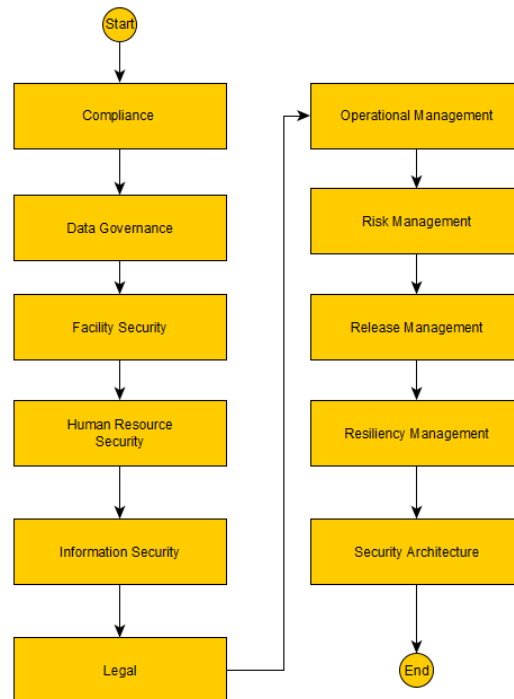


Abbildung 42: Basierend auf Abb.34 CSA Cloud Control Matrix Flow

MS Azure Compliance fokussiert auf die Datenduplizierungen, den Zugriff und die Begrenzungen von Daten mit Ziel, dass Risiko von Geschäftsprozessstörungen zu minimieren.

In Data Governance wird eindeutig definiert, dass alle Daten durch die verantwortliche Personen definiert, dokumentiert und kommuniziert werden müssen. Die Richtlinien und Verfahren müssen festgelegt und umgesetzt werden, um das geistige Eigentum zu schützen. [ms18]
Weiter ist es notwendig, auf die Verwendung von proprietärer Software innerhalb der vorgegebenen Formen, wie gesetzliche Zuständigkeit oder vertragliche Beschränkungen zu achten und diese zu schützen.

11. Privacy-Driven Governance Modell

Data Governance und Security Policy werden zusammen mit Handling von den ISO 27001-Normen abgedeckt. Die Datenaufbewahrung wird in Übereinstimmung mit gesetzlichen, vertraglichen oder geschäftlichen Anforderungen implementiert. Das Windows Azure-Sicherungs- und Redundanzprogramm wird jährlich überprüft und validiert. [ms18]

Auf Information Security Ebene werden die Grundanforderungen sowie Policy Enforcement und Benutzerzugangspolicies- und Beschränkungen überprüft.

Microsoft besitzt Richtlinien, Verfahren und Mechanismen, welche für eine effektive Schlüsselverwaltung eingerichtet wurden, um die Verschlüsselung von Datenspeichern als auch bei der Datenübertragung für die Schlüsselkomponenten des Windows Azure-Dienstes zu unterstützen. [ms18]

Der „Windows Azure Inzident Response-Prozess“ folgt den folgenden Phasen: Identifizierungen, Containment, Eradication und Recovery. Jeder Sicherheitsvorfall wird analysiert, um sicherzustellen, dass geeignete Gegenmaßnahmen ergriffen werden, um ihn vor einem erneuten Auftreten zu schützen.

Windows Azure erfüllt auch weitere notwendige Schritte, so sind z. B. Windows Azure-Quellcode-Bibliotheken auf autorisiertes Personal beschränkt. Change Management ist auch unter dem ISO 27001 Standard berücksichtigt.

System- und Netzwerkumgebungen sind durch Firewalls getrennt, um sicherzustellen, dass die folgenden Anforderungen erfüllt werden:

11. Privacy-Driven Governance Modell

Business- und Kundenanforderungen, Sicherheitsanforderungen, Compliance mit gesetzlichen, regulatorischen und vertraglichen Anforderungen, Trennung von Produktions- und Nichtproduktionsumgebungen sowie Schutz und die Isolierung sensibler Daten.

11.4 Zukünftige Anwendung des Modells

Es stellt sich die Frage, wie dieses Modell in der Zukunft angewendet werden kann und welche Voraussetzungen erfüllt werden müssen. Es gilt herauszufinden, welche konkreten Richtlinien und weitere Forschungsgebiete, und welche alternativen Ansätze die Wissenschaftler in der Zukunft in einem weiteren Forschungsprojektentwickeln sollen. Gegebenenfalls besteht die Möglichkeit einen wiederverwendbaren Software-Rahmen zu entwickeln, auf dem andere zukünftige Modelle aufbauen könnten.

Cloud-Service-Ökosysteme wurden als eine Unterklasse von Software-Ökosystemen identifiziert. Es stellt sich die Frage, ob andere Klassen von Software-Ökosystemen ähnliche Anforderungen in Bezug auf Governance ausüben.

Einige Prozesse sollten ebenfalls adaptiv gestaltet werden. Die Steuerungsebene ist bspw. bei verschiedenen Cloud-Service-Modellen inhomogen. Aus diesem Grund sollten die Konfigurationselemente bezüglich des unterschiedlichen Servicemodells auch unterschiedlich aufgebaut werden.

11. Privacy-Driven Governance Modell

Aufgrund der vorliegenden Unreife der Cloud-Governance-Tools und des Marktes, unterstützen die meisten Tools die gesamten Prozesse nicht vollständig.

Die Verbraucherorganisationen müssen darüber nachdenken, ob sie Organisationen wie Governance outsourcen sollten, unabhängig davon, wie sie die internen und externen Kontrollmechanismen kohärent gestalten können.

Tatsächlich benötigt nicht jede Organisation die gleiche Governance-Ebene.

Eine Erweiterung dieser Arbeit könnte mehr zukünftige privacy-driven Governance Modelle umfassen, die im Vergleich zu diesem Modell weiter evaluiert werden könnten. Die zukünftigen privacy-driven Governance Modelle sollen auf die Governance-Anforderungen des Cloud-Computing-Ökosystems achten.

Ein interessantes weiteres Forschungsprojekt wäre die Untersuchung der relativen Vor- und Nachteile des nur kurz, im Kapitel 6.4⁴⁰ vorgestellten alternativen Ansatzes.

Forscher können auch die Perspektive des Auditors einnehmen, um die Inhalte aus einem anderen Blickwinkel zu untersuchen.

⁴⁰ 6.4 Ontologische Methode, Ziel, Datenschutz

11. Privacy-Driven Governance Modell

Die folgenden fünf Punkte:

- Strategische Planung,
- Organisatorische Alignment,
- Service Lifecycle Management
- Policy Management und
- SLA Management

sollen detailliert analysiert und erforscht werden.

12. Conclusio

12.1 Diskussion der Ergebnisse

Privacy-driven Governance für Cloud Computing fällt immer häufiger in den Fokus von Softwarefirmen und Softwareentwicklern. Dieses Modell wird zukünftig immer achtsamer verwendet und weiter entwickelt.

Das Hauptziel des Forschungsprojekts ist es, ein allgemeines Prozessmodell für die privacy-driven Cloud Governance zu entwickeln, welches für alle Arten von Clouds eine Anwendung findet. Das Modell in dieser Arbeit kann als Grundlage oder als Leitfaden angesehen werden.

Das Modell kann von einzelnen Personen, kleinen Unternehmen, o.ä. als Grundlage verwendet werden, um weitere wissenschaftliche Analysen, Diskussionen und möglichen Implementierungen oder Entwicklungen Stand zu halten. Des Weiteren könnte dieses Modell zur Überprüfung bestehender Modelle verwendet werden. Eines der Forschungsergebnisse war das Modell, das mit einem Anwendungsbeispiel von Microsoft Azure bestätigt wurde.

Es kann auch als ein Überblick über alle aktuellen Richtlinien und Policies, welche notwendig sind um eine erfolgreiche Modell-Implementierung anzuwenden, gesehen werden.

12. Conclusio

Artefact-Governance⁴¹ konnte zukünftigen Entwicklern die wissenschaftliche Forschung erleichtern und mit der Kontrollstruktur als auch Inhaltsabgleich von Software-Artefakten, welche mit diesen Erweiterungen verbunden sind, helfen.

12.2 Lessons learned

Nach einer aktuellen EU Richtlinie entsteht eine neue Version der ISO/IEC 27001:2017 und anschließend noch eine GDPR Richtlinie, die als eine weitere Erweiterung gesehen werden kann.

Unternehmen werden in Zukunft wesentlich mehr Zeit und Geld in die privacy-driven Governance investieren müssen, damit Ihre Daten sicher aufbewahrt werden können.

Die Welt ist inzwischen tief vernetzt, die Sicherheitsaspekte und die Compliance, Data Governance, Facility Security, Information Security sowie Legalaspekte und verschiedene Arten von Management, wie Operational, Risk, Release, Resiliency, werden immer eine stärkere Rolle spielen.

Vermutlich besteht die Notwendigkeit, die bestehende Kenntnisse mit Technologien wie Blockchain Management zu kombinieren. Als Folge darauf öffnen sich in einem so verteilten System weitere potenzielle Fragen bzgl. Security und gemeinsamen Sicherheitsaspekten.

⁴¹ 6.2 Prozess- & Artefact Governance

12. Conclusio

Die finale Hauptfrage bleibt bestehen und gilt zu lösen: Wie kann privacy-driven Governance ein Verhältnis zwischen kostengünstig und sicher erreichen?

13. Abbildungsverzeichnis

- Abbildung 1: NIST Ein visuelles Modell von Cloud Computing Definition [csa09]
- Abbildung 2: Enterprise Architecture Stack und erweitertes Cloud Service Modell [rup16]
- Abbildung 3: Fünf Ebenen der Abstraktion [rup16]
- Abbildung 4: Hybrid Cloud sorten [rup16]
- Abbildung 5: Nutzung von Cloud-Computing-Diensten, 2014 und 2016 [Eur17]
- Abbildung 6: Cloud Computing Aktionsprogramm [tcl17]
- Abbildung 7: Gründe für Unternehmen in Deutschland, keine Cloud-Dienste zu nutzen [tcl17]
- Abbildung 8: Support während des gesamten Lebenszyklus der Cloud Service-Nutzung [tcl17]
- Abbildung 9 Corporate, IT und Cloud Governance [lfu15]
- Abbildung 10: Cobit 5 Prinzipien [ISACA12]
- Abbildung 11: Governance versus Management [ISA12]
- Abbildung 12: Cloud-Governance Position [yhe11]
- Abbildung 13: Eine moderne Anwendungsplattform kann als aus drei Teilen bestehend angesehen werden [dch08]
- Abbildung 14: Prozesskategorien – Beispiel Versicherungsunternehmen [DvL12]
- Abbildung 15: Die notwendigen Aspekte für Governance [tbi08] [ebc11]
- Abbildung 16: Top-Down Service Identifizierung [DvL12]
- Abbildung 17: Gap analyse oder Lückenanalyse [DvL12]

13. Abbildungsverzeichnis

- Abbildung 18: Das geschichtete SOA-Modell legt die vier gängigen SOA-Typen fest: Servicearchitektur, Service-Kompositionsarchitektur, Service-Inventararchitektur und Service-orientiert Enterprisearchitektur[ebc11]
- Abbildung 19: Enterprise als eine Kollektion von Applikation[DvL12]
- Abbildung 20: Enterprise als eine Kollektion von Service Konsumenten und Serviceanbieter[DvL12]
- Abbildung 21: Gemeinsame evolutionäre Ebenen der organisatorischen Reife.[ebc11]
- Abbildung 22: GRC Value Ecosystem [csa11]
- Abbildung 23: Governance, Risk and Compliance (GRC) [ARR13]
- Abbildung 24: The GRC Framework [GYR13]
- Abbildung 25: Kontrollstufe des Cloud Computing [guo10]
- Abbildung 26: Herausforderung der Annahme von Cloud Computing [idc08]
- Abbildung 27: Herausforderung der Annahme von Cloud Computing [idc09]
- Abbildung 28: Herausforderung der Annahme von Cloud Computing [rs16]
- Abbildung 29: Herausforderung der Annahme von Cloud Computing [rs16]
- Abbildung 30: Lifecycle Methode für SOA Governance [Sch07]
- Abbildung 31: AT SOA Governance Framework [HoS10]
- Abbildung 32: Cloud Governance Modell von Guo et al. [guo10]
- Abbildung 33: Microsoft's Cloud Governance Modell [Microsoft, 2010] [lfu15]
- Abbildung 34: Good Cloud Governance [lfu15]
- Abbildung 35: SOA strategy Snap aus Lifecycle Method for SOA governance [sch07]

Abbildung 36: CSA Star Certification⁴²

Abbildung 37: Basierend auf Abb.34 CSA Cloud Control Matrix Flow

Abbildung 38: Modell Requirements & Policies

Abbildung 39: Modell Operationale Komponente

Abbildung 40: Modell Threads

Abbildung 41: Modell Vulnerabilities

Abbildung 42: Basierend auf Abb.34 CSA Cloud Control Matrix Flow

⁴² <https://www.bsigroup.com/en-GB/CSA-STAR-Certification/Benefits-CSASTAR-Certification/>

14. Tabellenverzeichnis

Tabelle 1: Fünf Charakteristiken des Cloud Computings [rup16]

Tabelle 2: Cloud-Service/Modelle und die Zuständigkeit [lfu15]

Tabelle 3: Service- und Bereitstellungsmodelle bilden eine Matrix [dro12]

Tabelle 4: Mapping service level von Cloud Computing & SOA [ovu10]

Tabelle 5: Level of Effort (LOE) [TR18]

15. Literaturverzeichnis

- [abb07] Antoniou G.; Baldoni M., Bonatti P. A.; Nejdl W. and Olmedilla D. : *Rule-based Policy Specification, in Secure Data Management in Decentralized Systems*. Vol. 33, part III, Springer, 2007, pp. 169–216.
- [ach07] Afshar M.; Cincinatus M.; Hynes D.; K. Clugage K. and V. Patwardhan: *SOA governance: Framework and best practices*. An Oracle White Paper, Oracle Corporation, 2007
- [ago13] Australian_Government, Department of Finance and De-regulation: *Cloud computing strategic direction paper: Opportunities and applicability for use by the Australian Government*. April 2013 URL
http://www.finance.gov.au/e-government/strategy-and-governance/docs/draft_cloud_computing_strategy.pdf
abgerufen am 2018-06-30
- [ail11] Syed A.Ahson; Mohammad Ilyas: *Cloud Computing and Software Services, Theory and Techniques*. CRC Press, USA; 2011
- [ars04] Arsanjani: *Service Oriented Modeling and Architecture: How to identify, specify, and realize services for your SOA*. IBM 2004
- [bko13] Bratanis Konstantinos; Kourtesis Dimitrios: *Introducing Policy-Driven Governance and Service Level Failure Miti-*

15. Literaturverzeichnis

- gation in Cloud Service Brokers: Challenges Ahead*,
ICSOC 2013
- [bsi10] Bundesamt für Sicherheit in der Informationstechnik: *BSI Mindestsicherheitsanforderungen an Cloud Computing Anbieter* Stand 2010 Sep 27
- [bmt06] Brown W. A.; Moore G. and Tegan W.: *SOA governance—IBM's approach, Effective governance through the IBM SOA Governance Management Method approach*, White Paper, 2006.
- [car61] McCarthy, J.: *MIT's Centennial Keynote Address*: Massachusetts Institute of Technology (MIT), USA, 1961
- [ail11] Syed A.Ahson, Mohammad Ilyas: *Cloud Computing and Software Services, Theory and Techniques*. CRC Press, USA; 2011
- [cer12] *Insider Threats Related to Cloud Computing*, CERT, Stand July 2012. URL: <http://www.cert.org/>
- [CGO14] IBM: Compliance. Governance and Oversight Council: *Information Lifecycle Governance Leader Reference Guide*, IBM 2010-2014
- [cho09] Catteddu D.; Hogben G.: *Cloud Computing Benefits, Risks and Recommendations for Information Security*. The European Network and Information Security Agency (ENISA), November 2009.
- [csa09] Cloud Security Alliance: *Security Guidance for Critical Areas of Focus in Cloud Computing V2.1* Dec 2009

15. Literaturverzeichnis

- [csa11] Cloud Security Alliance: Security Guidance for Critical Areas of Focus in Cloud Computing V3.0 2011
- [cws11] CERT Coordination Center at Carnegie Mellon University: *CyberSecurity Watch Survey*., Software Engineering Institute: Carnegie Mellon University 2011
- [dch08] David Chappel: A short introduction to Cloud Platforms: An Enterprise-oriented view. August 2008
- [deLDB09] de Leusse, P., Dimitrakos, T., & Brossard, D.: *A Governance Model for SOA*. Presented at the 2009 IEEE International Conference on Web Services. 6-10 July
- [DvL12] Dikmans Lonneke and van Luttikhuizen Ronald: *SOA Made Simple*. Packt Publishing Ltd. December 2012
- [dko16] Dimitrios Kourtesis: *Policy-Driven Governance in Cloud Service Ecosystems*. The University of Sheffield, Faculty of Engineering, Dep. of Computer Science, 28 Sep 2016
- [ebc11] Erl Thomas, Bennett Stephen G., Carlyle Benjamin und Gee Clive: *SOA Governance: Governing Shared Services On-Premise and in the Cloud*. Prentice Hall April 2011
- [ego13] Eugene Gorelik: *Cloud Computing Models*. Composite Information Systems Laboratory (CISL), MIT Sloan School of Management, January 2013
- [eugd18] GDPR Portal, URL: <https://www.eugdpr.org/>, [Stand am 22.7.2018]
- [gfq14] Göllner, Fenz & Quirchmayr: *Cloud-Sicherheit*, Austria, Wien, 2014

15. Literaturverzeichnis

- [guo10] Guo, Z., Song, M., & Song, J.: *A Governance Model for Cloud Computing*. Paper presented at the Management and Service Science (MASS). 2010
- [GYR13] Galaz, Yamazaki, Ruiz Urquiza, S.C.: *Governance, Risk and Compliance*, ISACA Monterrey, May 2013
- [Han10] Hansen, Markus: *Cloud Computing*. URL <https://www.datenschutzzentrum.de/vorlesungen/cau/CAU-20100630-hansen-cloud-computing.pdf>, [Stand am Juni 2010]
- [HoS10] Hojaji Fazilat & Shiraz Mohammad Reza Ayatollahzadeh: *AUT SOA Governance: A New SOA Governance Framework Based on COBIT*. 3rd IC on Computer Science & Information Technology 2010
- [ISA12] COBIT 5 *A Business Framework for the Governance and Management of Enterprise IT*. Rolling Meadows, IL ISACA. (2012).
- [itg18] URL <https://www.itgovernance.co.uk/iso27001>, [Letzter Stand 30.6.2018]
- [jag11] Jansen W. and Grance T.: *Guidelines on Security and Privacy in Public Cloud Computing*. Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Special Publication 800-144, December 2011.
- [kab09] Keen, M., Adamski, D., Basu, I., Chilcott, P., Eames, M., Endrei, M., et al.: *Implementing Technology to Support SOA Governance and Management* IBM/Redbooks. 2007

15. Literaturverzeichnis

- [kav14] Kavis Michael: *Architecting the Cloud: Design decisions for cloud computing service models (SaaS, PaaS, IaaS)*, Wiley, USA, 2014
- [kbs05] Krafzig D.; Banke K. and Slama D.: *Enterprise SOA: Service-oriented architecture; best practices*. Prentice Hall Professional, 2005.
- [kdv10] Krutz Ronald L. und Dean Vines Russel: *Cloud Security - A comprehensive Guide to Secure Cloud Computing*, Wiley Publishing Inc. 2010
- [kfss13] Kiran Mariam, Friesen Andreas, Simons Anthony J.H. und Schwach Wolfgang K.R. , *Model-Based Testing in Cloud Brokerage Scenarios*, Springer Verlag, Berlin, pp. 192-208. ISBN 978-3-319-06858-9
- [kfj03] Kagal L.; Finin T. und Johshi A.: *A Policy Language for a Pervasive Computing Environment*,” in Proc. of the 2003 IEEE Workshop on Policies for Distributed Systems and Networks, IEEE Computer Society, 2003, pp. 63–74
- [kps12] Kourtesis Dimitrious; Paraskakis Iraklis und Simons Anthonz J.H.: *Policy-driven governance in cloud application platforms: an ontology-based approach*.
The 7th International Conference on Formal Ontology in Information Systems, FOIS 2012, Graz, Austria, July 24-27, 2012

15. Literaturverzeichnis

- [kss17] Khajuria Samant, Sørensen Lene Tolstrup, Skouby Knud Erik: *Cybersecurity and Privacy – Bridging the Gap*. CMI/Aalborg University, Denmark, River Publishers, 2017
- [lin09] Linthicum, D. S.: *Cloud Computing and SOA Convergence in Your Enterprise*, Addison-Wesley Professional, 2009
- [lin15] D. S. Linthicum: *The Evolution of Cloud Service Governance*. *IEEE Cloud Computing*, vol. 2, no. 6, pp. 86–89, Nov. 2015.
- [lfu15] Lita Fulton: *Cloud Governance and Management Made Simple*, Right Solutions, Inc. 2015
- [mb12] M. Bevir, *Governance: A Very Short Introduction*. Oxford University Press, 2012.
- [MS18] URL: <https://docs.microsoft.com/en-gb/azure/security/azure-security>, [Stand am 1.Juli 2018]
- [mgt09] Mell Peter und Grance Timothy: *Cloud Computing*. GTSI NIST Oktober 2009
- [msp13] Gregoris Mentzas¹, Anthony J.H. Simons², and Iraklis Paraskakis³: *Cloud Service Brokerage: Methods and Mechanisms*. White Rose, University Consortium, Uni of Leeds, Sheffield & York 2013
- [nad04] Nadhan, E.: *Service-Oriented Architecture: Implementation Challenges*. Microsoft Architecture Journal. 2004
- [ncc05] The National Computing Centre: *IT Governance, Developing-a-Successful-Governance-Strategy, A Best Practice Guide for decision makers in IT*, , Oxford House, Ox-

15. Literaturverzeichnis

- ford Road Manchester M1 7ED, 2005
- [nis09] NIST: Mell Peter & Grance Timothy: *The NIST Definition of Cloud Computing*. URL:
<https://www.nist.gov/sites/default/files/documents/itl/cloud/cloud-def-v15.pdf>, [Stand am 22.7.2018]
- [nis11] NIST: Mell Peter & Grance Timothy: *The NIST Definition of Cloud Computing*, Special Publication 800-145, 2011, September
- [One09b] O'Neill, M: *Connecting to the Cloud, Part 3: Cloud governance and security*. URL
<http://www.ibm.com/developerworks/xml/library/x-cloudpt3/> 2009
- [ovu10] Ovum: *Cloud governance: an overview*. 2010
- [pet10] Peterson, G.: Don't Trust. And Verify: *A Security Architecture Stack for the Cloud*. *Security & Privacy*, IEEE, 8(5), 83-86. 2010
- [pvH06] Papazoglou and Van Den Heuvel,: *Service Oriented Design and Development Methodology*, *IJWET Vol.2. No.4* 2006
- [rup16] Ruparelia Nayan B. und Dixon Walter: *Cloud Computing. The MIT Press Essential Knowledge Series*, USA, LLC Gildan Media 2016
- [pvH06] Papazoglou and Van Den Heuvel,: *Service Oriented Design and Development Methodology*, *IJWET Vol.2. No.4* 2006
- [rsa15] Rana Salman Anwar & Ali Salman: *Economies of scale*.

15. Literaturverzeichnis

- The Islamia University of Bahawalput, Pakistan, Vol.1
No.1, 2015 page 51
- [sch07] Schepers, T.: A Lifecycle Method for Service Oriented Architecture Governance. University of Twente, Enschede. 2007
- [sch14] Schum Chris: *Correctly Implementing Forward Secrecy*. SANS Institute, March 2014
- [SDS14] Governance, Risk, and Compliance (GRc) White Paper, Secure Digital Solutions, April 2014
- [ssk12] Stolfo S. J., Salem M. B., and Keromytis A. D.: *Fog computing: Mitigating Insider Data Theft Attacks* in the Cloud. IEEE Symposium on Security and Privacy Workshops, pp. 125-128, San Francisco, CA, 2012.
- [tbi08] Todd Biske: *SOA Governance – The key to successful SOA adoption in your organisation*, Packt Publishing Ltd. Oct 2008
- [tbj03] Tonti G., Bradshaw J., Jeffers R., Montanari R., Suri N. and Uszok A.: *Semantic Web Languages for Policy Representation and Reasoning: A Comparison of KAoS, Rei and Ponder*. in *International Semantic Web Conference 2003*, LNCS vol. 2870, Springer, 2003, pp. 419–437
- [tr18] URL: <https://www.trustarc.com/>, [Stand am 22.7.2018]
- [tsc13] Te-Shun Chou: *Security threats on cloud computing vulnerabilities*. in *International Journal of Computer Science & Information Technology (IJCSIT)* Vol 5, No 3, June

15. Literaturverzeichnis

- 2013 DOI : 10.5121/ijcsit.2013.5306 79
- [ubl03] A. Uszok, J. Bradshaw, J. Lott, M. Breedy, L. Bunch, P. Feltovich, M. Johnson and H. Jung: *New Developments in Ontology-Based Policy Management. in Proc. of the 2008 IEEE Workshop on Policies for Distributed Systems and Networks*, IEEE Computer Society, 2008, pp. 145–152.
- [yhe11] Yu He: *The Lifecycle Model for Cloud Governance*, University of Twente, 2011
- [WPCC09] *White Paper Cloud Computing*. T-Systems Enterprise Services GmbH

16. Abkürzungsverzeichnis

AICPA	American Institute of Certified Public Accountants
Amazon S3	Amazon Simple Storage Service
AOA	Application oriented architecture
API	Application programming interface
BaaS	Backend as a service
BMWi	Bundesministerium für Wirtschaft und Technologie in Deutschland
BP	Business Process
BPaaS	Business Process as a service
CEO	Chief executive officer
CIO	Chief information officer
CPU	Central processing unit
CRM	Customer Relationship
CSA	Cloud Security Alliance
CSP	Cloud Service Provider
DICaaS	High Performance Computing as a service
DLoSSP	Data Loss Prevention
DLP	Data Leak Protection
DPI	Deep Packet Inspection
DRM	Digital rights management
SSgVO	EZ-Datenschutzgrundverordnung
EC2	Elastic Computer Cloud
ENISA	European Network und Information Security Agency

16. Abkürzungsverzeichnis

ERP	Enterprise Ressource Planung
FZI	Forschungszentrum des Informatik
GDPR	General data protection regulation
IaaS	Infrastructure as a Service
INaaS	Information as a service
IoT	Internet of Things
ISACA	Information Systems Audit and Control
ISAE	International Audits Standards for Assurance Engage- ment
ISMS	Information Security Management System
ISO	International standard organisation
ISV	International software vendor
ITGI	IT Governance Institute
LAN	Local area network
MIT	Massachusetts Institute of Technology
NaaS	Network as a service
NIST	National Institute of Standards and Technology
PaaS	Platform as a service
PDA	Personal digital assistant
PMO	Portfolio Management Organisation
REST	Representational State Transfer
ROI	Return of investment
SaaS	Software as a service
SAP	Systeme, Anwendungen und Produkte in der Datenver- arbeitung
SAML	Security Asssertion Markup Language

16. Abkürzungsverzeichnis

SLA	Service level agreement
SSAE	Standards for Attestation Engagements
SOA	Service oriented architecture
USA	United States of America
XaaS	Anything as a service
XACML	eXtensible Access Control Markup Language
WAN	Wide area network
WSDL	Web Services Description Language