Berner Fachhochschule
Wirtschaft

Einsatz von Community Cloud in den Schweizer Behörden

Bachelor-Thesis

Eingereicht im Studiengang: Bachelor in Wirtschaftsinformatik
Datum der Einreichung: Bern, 11.05.2012
Verfasst von: Olivier Brian, 10-586-246

Auftraggeber: Willy Müller, Informatiksteuerungsorgan des Bundes ISB
Erstgutachter: Prof. Dr. phil.-nat. Andreas Spichiger
Zweitgutachter: Dr. rer. oec. Konrad Walser

Management Summary

Ziel dieser Arbeit ist zu beschreiben, in welcher Form die Behörden Cloud Computing verwenden können. Die Behörden wollen die Vorteile von Cloud Computing ausnutzen und damit sowohl die Cloud Strategie als auch eGovernment Ziele verfolgen. Das Deploymentmodell Community Cloud soll gemäss dem aktuellen Entwurf Cloud Strategie den Anforderungen der Schweizer Behörden gerecht werden. Diese Ausgangslage ergibt die Frage, welche Ausprägungen eine Community Cloud für die Behörden haben soll. Als Grundlagen für Arbeit dient die Cloud Definition des National Institute of Standards and Technology (NIST) sowie der Entwurf der Cloud-Strategie der Schweizer Behörden.

Als Ergebnisse der Arbeit können folgende Punkte zusammengefasst werden:

Beim Einsatz von Cloud Computing stellen sich zusätzliche Behörden-spezifische Anforderungen. So muss der Staat seine nationale Unabhängigkeit auch in Ausnahmesituationen bewahren können und untersteht anderen gesetzlichen Regulationen als die Wirtschaft. Anstelle einer Geschäftsleitung oder eines CEO entscheidet die Politik über Strategien und Vorhaben der Behörden. Auch die Budgetierung und damit die Finanzierung unterscheiden sich wesentlich von der Privatwirtschaft.

Um eine Zusammenarbeit über Organisationsgrenzen hinweg zu ermöglichen, bedingt es eine Steigerung des IT-Reifegrades von allen betroffenen Behörden. Durch Cloud Computing können auch für kleinere Organisationseinheiten interoperable IT-Anwendungen effizient und effektiv betrieben werden.

Durch den Einsatz von mehreren Behörden-Clouds (Government Cloud) können die Services anhand ihrer unterschiedlichen Anforderungen entsprechend betrieben werden. Das Konzept beinhaltet eine Highest-Secure Cloud für besonders schützenswerte Daten, eine Secure Cloud für die meisten Behördenanwendungen sowie der Einsatz von Public Clouds für Services, welche keine spezifischen Anforderungen aufweisen. Zusätzlich wird es innerhalb der Behörden auch Services und Daten geben, welche nicht in einer Cloud betrieben werden dürfen.

Die Government Cloud (GovCloud) kann teilweise auch für private Organisationen geöffnet werden. Die Eigenschaften Swissness mit den Attributen wie Zuverlässigkeit, politische Stabilität, Exklusivität, Tradition und Qualität wird auch auf dem internationalen Markt nachgefragt.

„Wenn man Cloud Computing nutzt, dann nutzt man schlussendlich auch nur einen IT-Service und die IT ist und bleibt fehleranfällig.“

Lew Moorman, Chief Strategy Officer von Rackspace

Inhaltsverzeichnis

1. Einleitung

Cloud Computing ist das aktuelle Modewort in der IT-Branche. Alles wird als Cloud Computing bezeichnet und sämtliche Daten werden nur noch in der Wolke abgelegt. Doch die Realität sieht, zumindest in der Schweiz, noch etwas anders aus. Risiken wie Verlust der Datenhoheit, Sicherheit und Provider-Unabhängigkeit lassen den einen oder andern zögern, seine sensitiven Daten in die Cloud auszulagern. Trotz unterschiedlichen Definitionen von Cloud Computing scheint klar zu sein, dass eine Cloudlösung mehr ist als ein Webservice oder ein traditionelles Outsourcing. Nach der Definition von NIST muss eine Cloudlösung auf Abruf via Netzwerk verfügbar sein, bündeln von Ressourcen (Ressourcen-Pooling) erlauben, sich elastisch an den Anforderungen anpassen können, als messbarer Service angeboten und entsprechend nach Verwendung verrechnet werden. Die Ziele von Cloud Computing entsprechen den aktuellen Anforderungen des Business. Es sollen Kosten eingespart werden, die IT ist gezwungen sich schnell an den stetig ändernden Business Zielen angleichen können, immer verfügbar und dabei möglichst effizient sein.

1.1 Ausgangslage

„Im Intensiv-Workshop zur Erarbeitung der Cloud-Computing-Strategie waren sich die rund dreissig Experten aus Behörden, Wirtschaft, Bildung und Forschung einig: Cloud-Computing kann einen signifikanten Beitrag zur Umsetzung der E-Government-Strategie Schweiz leisten." – Entwurf Cloud-Computing-Strategie Schweizer Behörden.[1]

Im Entwurf der Cloud Strategie der Schweizer Behörden wird das Nutzungsmodell Community Cloud für erhöhte Anforderungen als mögliche Variante vorgeschlagen. Eine Community Cloud soll den Anforderungen gerecht werden, welche weder eine Public noch eine Private Cloud abdecken können.

Das Community Cloud Nutzungsmodell bietet, soweit beschrieben, interessante Eigenschaften, Rahmenbedingungen und eine Balance zwischen Vor- und Nachteilen für eine Cloud-Strategie des Bundes. Jedoch ist dieses Konzept noch wenig definiert und lässt noch viele Fragen offen.

1.2 Problemstellung

Das Thema Cloud Computing ist in aller Munde und wird von der Wirtschaft rasant vorangetrieben. Gartner beispielsweise prognostizierte für 2011 ein Wachstum im SaaS Bereich von 21 Prozent[2].

Die Probleme der IT sind längst erkannt: Die IT ist zu wenig agil und kann die stetig ändernden Business Anforderungen nicht rechtzeitig erfüllen. Der Einsatz von Cloud geschieht nicht erst in der Zukunft sondern bereits in der Gegenwart, selbst wenn es der Endbenutzer unter Umständen gar nicht mitbekommt. Beim Einsatz von Cloud Computing

[1] (Müller, Dischl, & Widmer, 2011)

[2] (Gartner, 2011)

dürfen nicht nur die Risiken der noch neuen Technologie betrachtet werden, es muss eine Abwägung zwischen Chancen und Risiken sowie Nutzen und Aufwand getroffen werden.

Michael Binder von Symantec[3] vergleicht den heutigen Einsatz von IT mit einer Stadt im Mittelalter, welche von einer starken Burgmauer (Firewall) umgeben ist und gegen aussen abgeschottet ist. Die IT der Zukunft muss, wie unsere moderne Gesellschaft, auf einem starken Vertrauenssystem basieren, welches Burgmauern überflüssig macht.

Im Rahmen dieser Arbeit wird davon ausgegangen, dass Schweizer Behörden die Lösungsbezüger sind. Diese Organisationseinheiten können auf den unterschiedlichen föderalen Ebenen wie Bund, Kanton oder Gemeinde angesiedelt sein.

Somit folgt als Fragestellung der Arbeit:

Wie kann für die Behörden basierend auf ihren Anforderungen ein Cloud Dienst mit einer Community Organisation betrieben werden?

Aus dieser Fragestellung beantwortet diese Arbeit folgendes:

- Was sind die Besonderheiten einer Community Cloud?
- Wie kann (eine) Community Cloud die Schweizer Behörden unterstützen?
- Welche Referenzmodelle bieten sich für die Organisation und das Betreiben einer Community Cloud an?

1.3 Zielsetzung

Mit der Bachelor Thesis soll die Idee und das Konzept einer Community Cloud mit ihren Eigenschaften aufgezeigt und mit anderen Cloud Definitionen verglichen werden. Untersucht wird, wie diese spezielle Community Organisationsform in Referenzmodellen (z.B. COBIT) einzuordnen ist. Weiter wird beschrieben, welche Governance Anforderungen die Behörden an eine Community Cloud haben.

Eine weitere Frage der Bachelor Thesis ist, wie sich verschiedene Cloud Provider innerhalb einer Community Cloud organisieren. Wie wird die Zusammenarbeit zwischen Behörden und Privaten (Public Private Partnership) organisiert? Wer ist für den externen Leistungsbezüger die Ansprechperson innerhalb der Community? Wie werden zum Beispiel Changes aufgenommen und umgesetzt?

Aus abgeschlossenen (Community) Cloud Projekten sollen nach Möglichkeit Erkenntnisse gewonnen und Projektentscheidungen verstanden werden. Besonders interessant sind Cloud Projekte im Government Bereich; allenfalls auch, wie ausländische Staaten mit dem Thema Goverment-Cloud umgehen. Mögliche Fragen könnten sein: Wieso wurde der Anbieter gewählt? Welche SLA wurden erarbeitet? Welche AGB's wurden ausgehandelt?

[3] Präsentation und Referat (ISSS Information Security Society Switzerland, 2011)

Als Folgerung wird aufgezeigt, welche Aspekte es bei der Umsetzung einer Government Community Cloud zu beachten gilt.

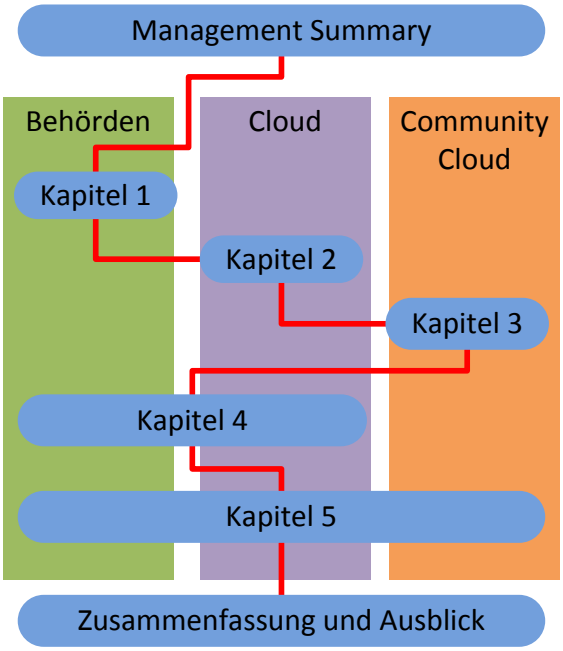
Dies kann in drei Ziele zusammengefasst werden:

1. Einleitung ins Thema Cloud Computing
2. Aufzeigen der Besonderheit Community Cloud
3. Einsatz von Community Cloud am Beispiel der Schweizer Behörden

1.4 Methodik und Aufbau der Arbeit

Die Arbeit ist in fünf Hauptteile gegliedert welche sich auf die Bereiche Behörden, Cloud und Community Cloud verteilen. Die Abbildung 1 – Aufbau der Arbeit stellt diese Aufteilung grafisch dar. Das erste Kapitel beschreibt in der Einleitung die Problemstellung rund um die Behörden. Das Kapitel Grundlagen Cloud Computing beschreibt grob die verschiedenen Cloud Konzepte und die verwendeten Referenzmodelle. Das dritte Kapitel beschreibt das Konzept der Community Cloud und dessen Eigenschaften. Im vierten Kapitel werden die Verwendung, die Verbreitung, das Umfeld und der Einsatz von Cloud Computing für Behörden beschrieben. Der fünfte und letzte Hauptteil umfasst, wie eine Community Cloud innerhalb der Behörden eingesetzt werden kann. Die Arbeit wird mit einer Zusammenfassung und einem Ausblick abgeschlossen.

Abbildung 1 – Aufbau der Arbeit



Quelle: Eigene Darstellung

Für die Bachelorarbeit werden Frameworks aus der Vertiefungsrichtung IT-Governance verwendet. Neben Fachliteratur zum Thema werden nach Möglichkeit auch Webartikel, Interviews und Studien als Quellen verwendet. Referate und Tagungen rund um das Thema Cloud bringen aktuelle Inhalte und Meinungen von Experten in die Arbeit ein. Um das komplexe Thema verständlich zu machen, wird mit Alltagsanalogien wie beispielsweise der Stromproduktion[4] ein Bezug zur Realität geschaffen.

1.5 Abgrenzung

Nicht Inhalt der Arbeit ist die Einführung von Organisationen und Prozessen innerhalb der Behörden. Eine detaillierte Beschreibung des Kompetenzzentrums Cloud Computer und einer allfälligen Zertifizierungsstelle, wie es in der Strategie beschrieben wird, wird nicht abgedeckt.

Auf die verschiedenen Cloud-Konzepte wird nicht tiefer eingegangen; sie werden im Kapitel Grundlagen Cloud Computing nur grob beschrieben. Das Servicemodell Infrastructure as a Service (Iaas) wird primär als Referenz verwendet. Platform as a Service (PaaS) wird aufgrund der unterschiedlichen Plattformen innerhalb des Bundes und der fehlenden Standardisierung im Rahmen dieser Arbeit nicht detaillierter betrachtet.

[4] Vgl. Beispiel aus The Big Switch: Rewiring the World, from Edison to Google (Carr, 2008)

2. Grundlagen Cloud Computing

2.1 Definition

Für Cloud Computing existieren unterschiedliche pragmatische Definitionen. In der Industrie wird nicht zuletzt aus aktuellen Marketingüberlegungen oft jeder Webservice bereits als Cloud definiert. Doch eine „richtige" Cloud hat Eigenschaften, welche über das Bereitstellen eines Webservices hinausgehen.

Forrester Research[5] definiert Cloud Computing wie folgt:

„Cloud Computing" steht für einen Pool aus abstrahierter, hochskalierbarer und verwalteter IT-Infrastruktur, die Kundenanwendungen vorhält und falls erforderlich nach Gebrauch abgerechnet werden kann.

Die Definition von Saugatuck Technology[6] lautet:

„Cloud Computing" umfasst On-Demand-Infrastruktur (Rechner, Speicher, Netze) und On-Demand-Software (Betriebssysteme, Anwendungen, Middleware, Management- und Entwicklungs-Tools), die jeweils dynamisch an die Erfordernisse von Geschäftsprozessen angepasst werden. Dazu gehört auch die Fähigkeit, komplette Prozesse zu betreiben und zu managen.

Die aktuellste und umfassendste Definition von Cloud Computing wurde vom NIST[7] erstellt:

The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

Die NIST Definition trifft das in dieser Arbeit verwendete Cloud Computing Konzept am konkretesten und wird auch in der Literatur sowie in der Praxis häufig verwendet.

[5] (Forester Reserch, 2008)

[6] (Saugatuck Technology, 2008)

[7] (NIST, National Institute of Standards and Technology, 2011)

2.2 Charakteristiken

Cloud Computing ist eine Art des Outsourcings, hat jedoch spezifische Eigenheiten und Ausprägungen, welche Vor- und Nachteile mit sich bringen. Durch zunehmende Aktualität und Verbreitung der ‚Cloud' wird dieser Begriff oftmals missbraucht. Nur wenn ein Service alle die in Tabelle 1 aufgeführten Charakteristiken besitzt, kann nach NIST von einem ganzheitlichen Cloud Angebot gesprochen werden.

Tabelle 1 – Charakteristik von Cloud Computing

Charakteristik	Beschreibung
On-demand self-service	IT wird als Service genutzt und steht auf einfache Weise, ohne manuelle Interaktion, auf Abruf zur Verfügung.
Broad network access	Der Service wird unabhängig vom Endgerät über ein Netzwerk bereitgestellt. Die Verbindung muss entsprechend des Service performant und verfügbar sein.
Resource pooling	Die benötigten Ressourcen werden vom Provider für unterschiedliche Kunden zur Verfügung gestellt. Dies wird durch Technologien wie Virtualisierung und Mandantenfähigkeit (Multitenancy) ermöglicht.
Rapid elasticity	Die benötigten Ressourcen werden bei Bedarf spontan bereitgestellt und bei Nichtgebrauch ohne manuellen Eingriff wieder freigegeben.
Measured Service	Der bezogene Service muss mit den dafür benötigten Ressourcen messbar sein. Dadurch wird eine verbrauchsorientierte Abrechnung[8] ermöglicht.

Quelle: Eigene Darstellung in Anlehnung an (NIST, National Institute of Standards and Technology, 2011)

[8] Auch mit "pay as you go" oder "pay-per use" beschrieben

2.3 Allgemeine Erwartungen an die Cloud

Die allgemeinen Business Erwartungen[9] an die Cloud können wie folgt zusammenfassend beschrieben werden. Je nach Organisation werden die Erwartungen unterschiedlich gewichtet und ergänzt.

Kostenbegrenzung – Durch den Einsatz von Cloud und der Möglichkeit der Skalierbarkeit sind keine Investitionen in Infrastrukturanschaffungen und Wartungen mehr notwendig. Der Service und die gewünschten Kapazitäten sind auf Abruf verfügbar und werden nach Verwendung verrechnet (pay-per-use). Durch das Einsparen von ungenutzten internen Ressourcen kann das Business in Innovation des Kerngeschäfts investieren, anstatt das Kapital in ungenutzter Infrastruktur zu binden. Vor der Einführung einer Cloud-basierten Lösung vergleicht das Business die aktuellen Kosten mit den potentiellen Cloud Kosten. Dabei werden immer die Gesamtkosten (TCO) verglichen.

Innovationsgeschwindigkeit – Cloud Services lassen sich im Gegensatz zu herkömmlichen IT-Projekten statt in Wochen oder Monaten innerhalb eines Tages bereitstellen. Dies ermöglicht es dem Business, schnell auf Veränderungen zu reagieren und die Markteinführungszeit (Time-to-market) möglichst kurz zu halten.

Verfügbarkeit – Dank dem Skaleneffekt können grössere Cloudprovider eine hohe Verfügbarkeit bieten. Durch redundante Anbindung und Lastenausgleich (load balancing) können die hohen Verfügbarkeitsanforderungen des Business befriedigt werden. Die versprochene Verfügbarkeit sollte unabhängig vom Provider gemessen werden. Für den Fall des Nichteinhaltens des SLAs sind entsprechende Möglichkeiten zur Eskalation beim Lösungsanbieter oder Auflösungsbedingungen des Vertrages (Exit-Klausel) definiert.

Skalierbarkeit – Durch die Flexibilität und Skalierbarkeit des Cloud Services kann sich die IT schnelle an dem sich ändernden Business anpassen und es besser unterstützen. Da die Leistung auf Abruf zu Verfügung steht, wird auf Lastspitzen sehr schnell oder sogar automatisch reagiert. Die benötigten Ressourcen werden nach Bedarf entsprechend alloziert.

Effizienz – Das Business kann sich dank effizienter IT auf ihr Kerngeschäft konzentrieren und innovativ in Forschung und Entwicklung investieren. Dieser Vorteil kann zum Wachstum und Wettbewerbsvorteil der Organisation wesentlich beitragen und übertrifft vielleicht sogar die finanziellen Vorteile einer Cloudlösung.

Elastizität – Die Cloudprovider verfügen über gespiegelte Systeme, welche sowohl für Notfallszenarien (Disaster Recovery), wie auch für Lastenausgleich (Load Balancing), verwendet werden können. Durch geographische Trennung der Serverräume kann die Cloudlösung auch gegen grosse Naturkatastrophen abgesichert werden.

[9] (ISACA, 2009)

Durch den Einsatz von Cloudlösungen kann sich das Business und die interne IT auf ihre unternehmensspezifischen Kernaufgaben beschränken. Cloudanbieter können die operative IT besser, schneller und kosteneffizienter betreiben.

2.4 Servicemodelle

Die Servicemodelle beschreiben, welche Art von Services aus der Cloud bezogen werden (vgl. Abbildung 2). Je nach gewähltem Modell stellt der Anbieter unterschiedliche Layer zu Verfügung, welche auch durch den Anbieter betrieben werden. Diese Layer werden als ‚Blackbox' angeboten und es bleibt dem Anbieter überlassen, wie der Service innerhalb der vereinbarten SLA erbracht wird.

Es wird zwischen folgenden Layer unterschieden:

Applications: Die Fachanwendung welche von dem Business verwendet wird.

Runtime: Ausführungsumgebung in welcher die entsprechende Applikation ausgeführt wird. Diese Umgebung enthält für die Applikation benötigten Funktionen (runtime library).

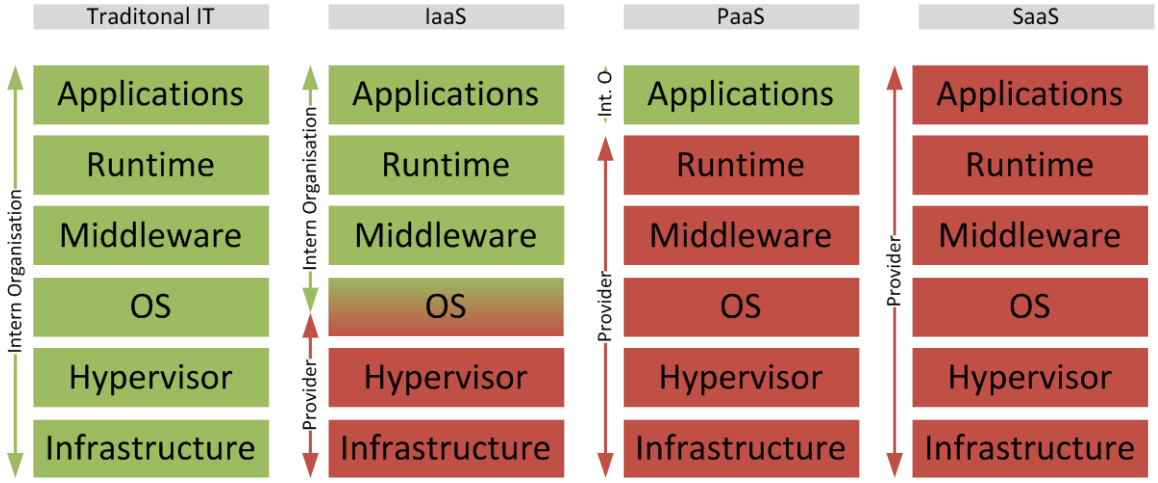
Middleware: Diese Zwischenschicht oder Vermittlungssoftware wird für die Kommunikation mit anderen Anwendungen, Datenbanken oder dem Betriebssystem benötigt.

OS: Das Betriebssystem (Operation System) stellt der Anwendung die Systemressourcen der Hardware, respektive des Hypervisors, zur Verfügung und verwaltet diese.

Hypervisor: Diese Virtualisierungsschicht stellt dem Betriebssystem die virtualisierten Ressourcen der Infrastruktur bereit.

Infrastructure: Die Infrastruktur besteht aus den physikalischen Einheiten wie Server, Speicher oder Netzwerk.

Abbildung 2 – Servicemodelle



Quelle: Eigene Darstellung in Anlehnung an (NIST, National Institute of Standards and Technology, 2011)

Die nächsten Kapitel beschreiben grob die verschieden Cloud Servicemodelle mit ihren jeweiligen Vor- und Nachteilen. Dies soll die unterschiedlichen Eigenschaften aufzeigen und bei der Auswahl des richtigen Servicemodelles unterstützen.

2.4.1 Infrastructure as a Service (IaaS)

Dem Kunden werden Rechen-, Speicher und Netzwerkkapazitäten angeboten. Auf dieser Infrastruktur betreibt der Kunde seine eigene Plattform, Software und Betriebssysteme. Die Tabelle 2 beschreibt in einer Argumentenbilanz die Vor- und Nachteile von IaaS gegenüber einem Eigenbetrieb.

Tabelle 2 – Vor- und Nachteile von IaaS

Vorteile	Nachteile
• Hohe Skalierbarkeit der benötigten Systeme, je nach benötigtem Bedarf • Redundante Datenspeicherung • Physisch getrennte Aufbewahrung und Nutzung von Daten • Keine Maintenance für Einrichtung und Betrieb der Infrastruktur • OPEX statt CAPEX[10] • Pay-as-you-Go	• Standort der Daten bei Public- wie auch bei Private Clouds nicht immer erkennbar • Stark abhängig von der Verfügbarkeit der Infrastruktur und Netzwerke • Fehlende oder mangelnde Abgrenzung / Isolierung der Datenbearbeitungen • Unberechtigter Datenzugriff auf Grund einer Fehlkonfiguration[11] • Gewährleistung und Haftung bei Verletzung der der Vertraulichkeit, Sicherheit und Integrität der Daten

Quelle: Eigene Darstellung in Anlehnung an (EuroCloud Swiss, 2012)

2.4.2 Platform as a Service (PaaS)

Im PaaS Modell beinhaltet der Service eine vollständige Plattform inklusive Entwicklungswerkzeuge. Solche Lösungen werden für Eigenentwicklungen oder für eine spezielle Software, welche auf der Plattform läuft, genutzt. Die unterliegende Infrastruktur wird vom Anbieter bereitgestellt und verwaltet.

[10] OPEX (OPerational Expenditure) Ausgaben für den operative Geschäftsbetrieb.
CAPEX (CAPital Expenditure) Investitionsausgaben für längerfristige Anlagegüter.

[11] In der Annahme, dass Rechenzentren oder Netzwerke geteilt werden, ist dieses Risiko anders einzuschätzen als im Eigenbetrieb.

Tabelle 3 – Vor- und Nachteile von PaaS gegenüber Eigenbetrieb

Vorteile	Nachteile
• Weniger Administrationsaufwand, da die notwendige Infrastruktur nicht selbst implementiert und bereitgestellt werden muss • Entwicklung im Team (auch geographisch verteilt) • Eine einzige Plattform mit minimalen Kosten (Standardisierung) • Keine Maintenance für Einrichtung und Betrieb der Plattform und deren Tools • OPEX statt CAPEX • Pay-as-you-Go	• Vendor Lock-in o Fehlende Portabilität o Fehlende Interoperabilität o Keine standardisierten Technologien • Mangelnde Flexibilität • Anforderungen von proprietären Anwendungen oder Entwicklungsumgebungen

Quelle: Eigene Darstellung in Anlehnung an (EuroCloud Swiss, 2012)

2.4.3 Software as a Service (SaaS)

Im SaaS Modell werden vollständige Applikationen, meistens über ein Webinterface, zur Verfügung gestellt. Auf die Plattform und die darunterliegenden Infrastruktur hat der Kunde keinen Einfluss.

Tabelle 4 – Vor- und Nachteile von SaaS gegenüber Eigenbetrieb

Vorteile	Nachteile
• Trennbarkeit / Mandantenfähigkeit der Applikationen • Schnell einsatzfähig / Schnellere Projekteinführung (time to market) • Keine Maintenance für den Betrieb der Business-Funktionalitäten • OPEX statt CAPEX • Pay-as-you-Go • Niedrigere Gesamtkosten (TCO) • Mobilität / Standortunabhängigkeit	• Auswahl des richtigen Providers • Fehlende Portabilität • Geringere Integrierbarkeit in bestehende Applikationslandschaften • Geringere Anpassungsmöglichkeiten, da vorgegebene Standardisierung • Evtl. höhere Antwortzeiten • Auswirkung von Sicherheitslücken beim Einsatz gemeinsamer SaaS Lösungen • Keine Nutzung ohne Internetzugang

Quelle: Eigene Darstellung in Anlehnung an (EuroCloud Swiss, 2012)

2.4.4 Weitere XaaS Formen

Weitere Cloud Service sind derzeit am Entstehen. Wobei das ‚X' für Everything stehen kann, also alles aus der Cloud, oder aber auch für weitere Service wie zum Beispiel Business Process as a Service (BPaaS) oder Communitcation as a service (CaaS).

2.5 Deploymentmodelle

Cloud Computing kann in verschiedenen Organisationsformen betrieben werden. Ausschlaggebend dafür, welches Deploymentmodell eingesetzt wird, sind die Anforderungen des Lösungsbenutzers und die am Markt verfügbaren Angebote.

2.5.1 Private Cloud

Der Lösungsbenutzer ist explizit eine Organisation oder eine Organisationseinheit. Eine private Cloud kann sowohl intern wie auch bei einem externen Anbieter betrieben werden. Die Vorteile von Cloud können nur teilweise ausgenutzt werden, dafür ist aber ein weitgehendes Customizing möglich.

2.5.2 Community Cloud

Im Gegenteil zur Private Cloud Architektur wird der Service von mehreren, aber definierten Gruppen verwendet. Der Dienst kann aber auch von einer Community, also von mehreren Lösungsanbietern, angeboten werden. Auf dieses Deployment Modell wird im Kapitel 3 näher eingegangen.

2.5.3 Public Cloud

Der angebotene Service steht der Öffentlichkeit zur Verfügung und wird meistens nur von einem Anbieter angeboten. Die Vorteile der Skalierbarkeit und des Ressourcen Poolings können am besten ausgenutzt werden.

2.5.4 Hybride Cloud

Hybride Cloud bieten eine Kombination aus den verschiedenen Organisationsformen und kombiniert dabei deren Vor- und Nachteile. So können beispielsweise die Daten intern in einer Private Cloud gehalten werden während die Applikation in einer Public Cloud läuft.

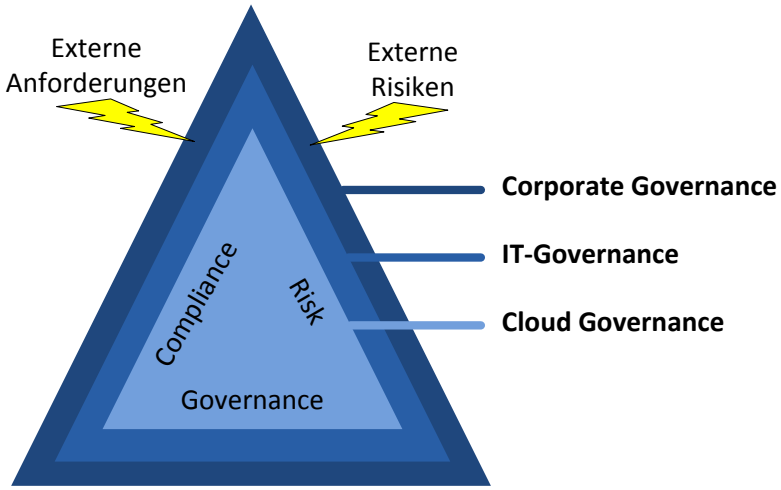
2.6 Cloud Governance

Die IT-Governance verändert sich mit der Einführung von Cloud Diensten, abhängig vom gewählten Service- und Deploymentmodell, in ihrem Umfang und Komplexität wesentlich.

Im Unterschied zu einem Outsourcing kann ein Cloud Anbieter, besonders wenn er sich im Ausland befindet, weniger eng kontrolliert werden.

Obwohl die Anforderungen des Business an die IT gleich bleiben oder wachsen, hat die Veränderung der Sourcing-Strategie einen massiven Einfluss auf die Steuerung der IT. Es muss sichergestellt sein, dass die Services das Business effektiv unterstützen, die Systeme sicher sind und die Risiken gemanged werden. Die drei Disziplinen Governance, Risk und Compliance (GRC) müssen auch mit dem Einsatz von Cloud Providern sichergestellt sein. Um dies zu ermöglichen, wird der Cloud Provider soweit wie möglich in das Governance Modell integriert. Nach der Ableitung von der Corporate in die IT-Governance kann weiter auf eine Cloud Governance herunter gebrochen werden.

Abbildung 3 – Von der Corporate Governance zur Cloud Governance



Quelle: In Anlehnung an (Johannsen & Goeken, 2011)

Von ausserhalb der Organisation wirken externe Anforderungen und Risiken auf die Corporate Governance. Diese sind nicht nur Business relevant, sondern können auch Auswirkungen bis zur Cloud Governance haben. Durch diese Abhängigkeit der Cloud Governance hat das Business einen indirekten Einfluss auf die Steuerung des Clouds-Betriebs.

2.6.1 Risiken aus Governance Perspektive

Aus Governance Sichtweise müssen folgende Chancen und Risiken beim Verwenden von Cloud Computing betrachtet werden:[12]

Generelle Risiken

Die generellen (IT)-Risiken unterscheiden sich durch den Einsatz von Cloud Computing nur teilweise im Vergleich mit bestehenden IT Lösungen.

- Verfügbarkeit: Ist die Lösung nicht verfügbar, kann der geforderte Geschäftsbetrieb des Unternehmens oder der Behörde nicht mehr sichergestellt werden. Hohe finanzielle Aufwände oder Reputationsschäden können die Folge sein.
- Vertraulichkeit: Die Vertraulichkeit, Integrität und Sicherheit der Daten muss gewährleistet sein.
- Haftungsfragen bei Versagen des Services: Wenn nicht ausdrücklich definiert, ist die Haftungsfrage beim bei einem Ausfall des Services oder Verlust von Daten unklar.
- Revisionssichere Nachvollziehbarkeit: Die Anforderungen einer Revisionsstelle oder die geforderte Einsicht in Daten durch ein Gericht müssen auch beim Einsatz von Cloudlösungen sichergestellt sein.

Risiken durch den Einsatz von Cloud Computing

- Eigentum der Daten: Wer ist Datenowner und verantwortlich für die Daten? Durch den Einsatz von verteilten Rechenzentren kann der Standort der Daten nicht mehr

[12] (ISACA, 2009)

sicher festgelegt werden. Je nach Land, in welchem die Daten sich befinden, können die entsprechenden Behörden oder Gerichte mittels Gesetzen auch auf die Daten von ausländischen Firmen zugreifen.

- Abgrenzung: Durch die Zusammenfassung von Daten und Services werden unterschiedliche Kunden in gleichen Rechenzentren betrieben. Eine effektive Kapselung (Multi-Tenancy) ist zwingend erforderlich. Bei einem Ausfall oder Fehler können auch andere Benutzer in Mitleidenschaft gezogen werden.
- Lock in: Durch proprietäre Schnittstellen oder komplexe Verträge ist der Lösungsbezüger vom Provider stark abhängig. Entsprechende Migrationskosten können bei einem Wechsel so gross sein, dass trotz hohen Laufzeitkosten eine Migration zu einem günstigeren Anbieter wirtschaftlich nicht mehr sinnvoll ist.

Rechtliche Anforderungen

Die datenschutzrechtlichen Anforderungen müssen auch beim Einsatz von Cloudlösungen eingehalten werden. Relevant sind Aspekte beim Umgang mit personenbezogenen oder besonders schützenswerten Daten. Für Vertraulichkeit, Verfügbarkeit und Integrität der Daten nach aktueller und gültiger Gesetzgebung muss gesorgt sein. Besonders wenn Daten bei ausländischen Providern gespeichert werden, müssen die jeweiligen rechtlich geltenden Bestimmungen betrachtet werden. Etliche Länder, besonders ausserhalb Europa, verfügen über ein tieferes Datenschutzniveau als die Schweiz oder haben andere Datengesetze (vgl. PatriotAct). Im Anhang 7.1 sind die relevanten datenschutzrechtlichen Anforderungen bei der Nutzung von Cloud-Computing-Diensten aufgeführt.

Service Modell

Je nach gewähltem Service Modell sind andere Chancen und Risiken in der Governance Sichtweise zu beachten.

Infrastructure as a Service (IaaS):	Mögliche alternative Optionen bei einem Teil- oder Totalausfall des Lösungserbringer.
Platform as a Service (PaaS):	Zusätzlich zu IaaS: welche Rahmenbedingungen sind durch die Plattform vorgegeben?
Software as a Service (SaaS):	Wer ist Eigentümer der Applikation und wo, respektive wie wird sie betrieben?

Deployment Modell

Massgebend für die Cloud Governance ist auch, welches Deployment Modell eingesetzt wird:

Private Cloud:	Cloud Service mit minimalen Risiken. Bietet dafür auch nicht die vollen Vorteile von Cloud (Scalability, Pooling)
Community Cloud:	Ähnlich der Private Cloud, jedoch verteilt über mehrere Anbieter und gemeinsame Verwendung mit anderen Lösungsbenutzern.
Public Cloud:	Der Speicherort der Daten ist nicht mehr zwingend bekannt und nachvollziehbar.

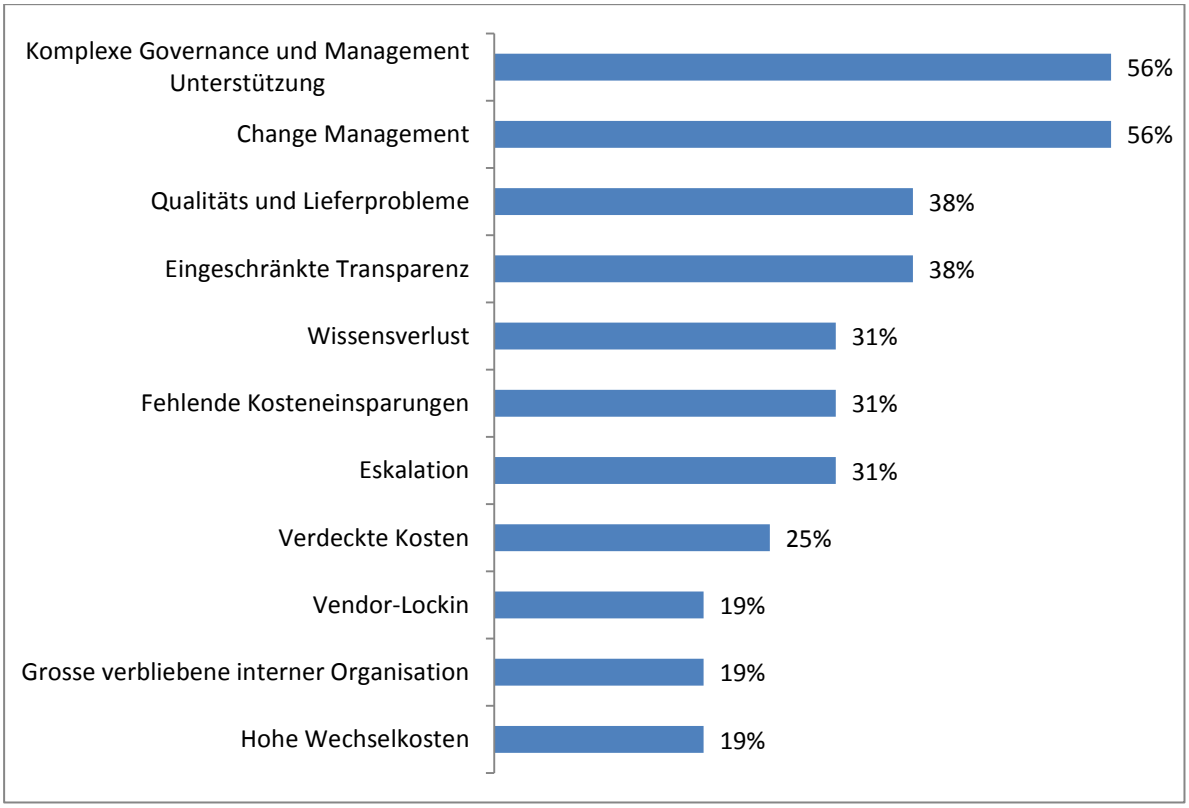
Hybrid Cloud: Mögliche Kombination aus den Risiken von Private und Public Cloud. Daten und Services müssen klassifiziert werden und es muss sichergestellt sein, dass sie im entsprechenden Teil der Hybrid Cloud gespeichert respektive ausgeführt werden.

2.6.2 Erfolgsfaktoren im Cloud-Outsourcing

Wie beim klassischen Outsourcing ist die Governance ein wichtiger Erfolgsfaktor für ein erfolgreiches Betreiben einer Cloud Architektur. Die Beziehung zum Outsourcing- respektive dem Cloud-Partner ist keine einfache Angelegenheit und ist gemäss einer Studie von Deloitte[13] oft der Grund für das Scheitern von Outsourcing Verhältnissen.

Um ein Scheitern von Cloud Vorhaben zu verhindern, ist auch ein erfolgreiches Change Management wichtig, welches die Migration eines Services von on-premise in die Cloud begleitet.

Abbildung 4 – Gründe für das Scheitern von Outsourcing Beziehungen



Quelle: Eigene Darstellung in Anlehnung an (Deloitte, 2005)

[13] (Deloitte, 2005)

2.6.3 Betrachtungsfelder

In Anlehnung an die IT Governance Focus Area von Cobit[14] ergeben sich für die Cloud Governance folgende Betrachtungsfelder, welche betrachtet werden müssen.

Strategischer Abgleich (IT-Alignment): Der Abgleich erfolgt zusätzlich zwischen der Geschäftsstrategie und IT-Strategie auch mit der Strategie der Cloud Anbieter. Um das Alignment zu erleichtern, ist der Zeithorizont der verschiedenen Strategien von Vorteil identisch.

Wertbeitrag: Die Services liefern der Organisation einen Mehrwert.

IT-Compliance: Die Compliance Anforderungen an die IT bleiben vorhanden. Die Einhaltung von regulatorischen und gesetzlichen Bestimmungen ist auch in der Cloud sicher zu stellen. Für Durchführung von IT-Audits müssen entsprechende Regeln definiert werden, da ein direkter Zugriff auf die Cloud Umgebung unter Umständen nicht möglich ist.

Performance: Die gewünschte Leistung muss messbar erbracht werden können. Die Ressourcen des Cloud-Providers sowie die eignen eingesetzten Ressourcen müssen effizient und effektiv zusammen arbeiten können. Sämtliche Ressourcen müssen überwachen und verbessert werden.

Sicherheit: Die IT-Sicherheit kann nicht vollständig an den Cloud Anbieter übertragen werden. Einige Dienste werden immer noch intern betrieben. Netzwerk und Endgeräte bleiben meistens in der Verantwortung des Kunden.

Risikomanagement: Durch den Cloud Einsatz müssen neue Risiken ins Risikomanagement aufgenommen und die Relevanz von bestehenden überprüft werden. Das Risikomanagement wird erschwert, da die Dienste des Cloudproviders für den Bezüger intransparent ablaufen.

Mechanismen: Das Einhalten der Governance in der Cloud kann durch verbindliche Rahmen- oder Leistungsverträge (SLA) geregelt werden. Entsprechende Strukturen der Cloud Partnerschaft und ein entsprechendes gegenseitiges Vertrauen helfen bei der Umsetzung der Governance.

2.7 Referenzmodelle

Referenzmodelle helfen, eine Cloud Architektur erfolgreich aufzubauen und zu betreiben. Wie der Name besagt, handelt es sich um Referenzmodelle, welche situativ auf die Organisation angepasst werden. Der Aufwand, um ein komplettes Referenzmodell in einer Unternehmung einzuführen, darf daher nicht unterschätzt werden. Im Kapitel 0 wird beschrieben, wie Referenzmodelle und welche Bestandteile (Prozesse) davon für eine Community Cloud verwendet werden können.

Die nächsten Abschnitte beschreiben grob die Referenzmodelle welche beim Einsatz von Cloud Computing verwendet werden.

[14] (IT Governance Institute, 2007)

2.7.1 IT Infrastructure Library (ITIL)

Herausgeber: United Kingdom's HM Goverment, bis 2010 Office of Government Commerce (OGC) - http://www.itil-officialsite.com

Aktuelle Version: ITIL 2011 Edition (29. Juli 2011)

Kurzbeschreibung: ITIL ist ein de-facto Standard basierend auf Good/Best Practices für IT-Servicemanagement. Die umfangreiche Sammlung von Publikationen beschreibt die für den Betrieb einer IT-Infrastruktur notwendigen Prozesse, Funktionen und die Aufbauorganisation. Es wird beschrieben, *wie* IT-Servicemanagement umzusetzen ist.

ITIL besteht aus den fünf Prozessgruppen Service Strategy, Service Design, Service Transition, Service Operation und Continual Service Improvement.

2.7.2 European Interoperability Framework (EIF)

Herausgeber: Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens (IDABC)

Aktuelle Version: EIF Version 1.0 (November 2014)

EIF Version 2.0 als Anhang II (16. Dezember 2011)

Kurzbeschreibung: Das EIF Framework beinhaltet ein Set von Empfehlungen für die Kommunikation zwischen Verwaltung, Wirtschaft und Bürger innerhalb der EU und über dessen Grenzen.

2.7.3 Control Objectives for Information and Related Technology (COBIT)

Herausgeber: ISACA - http://www.isaca.org

Aktuelle Version: COBIT 4.1 (2007)

COBIT 5 (10.04.2012)

Kurzbeschreibung: COBIT ist ein Referenzmodell für die IT-Goverance und beinhaltet Prozessbeschreibungen und Kontrollziele (Control Objectives).

COBIT 5 beschreibt 37 Prozesse in den fünf Prozessareas:

- Evaluate, Direct and Monitor
- Align, Plan and Organise
- Build, Acquire and Implement
- Deliver, Service and Support
- Monitor, Evaluate and Assess

Die Prozesse von COBIT 4.1 und COBIT 5 sind im Anhang 7.2 zu finden.

3. Community Cloud Ansatz

Dieses Kapitel beschreibt den theoretischen Ansatz einer Community Cloud. Die Definition wird anhand einer Analogie beschrieben. Diese Sonderform der Cloud bringt zusätzliche Problemstellungen und Fragen mit sich, welche zu klären sind. Für die Organisation werden mögliche Formen mit ihren Vor- und Nachteilen aufgearbeitet. Die Erbringung des Service innerhalb einer Community ist sehr abhängig von der Art des Servicemodells (IaaS, PaaS, SaaS).

3.1 Definition von Community Cloud

In der Cloud Literatur wird zwischen Public Cloud und Private Cloud unterschieden. Dazwischen gibt es verschiedene Mischformen (Hybrid), welche die Vorteile und auch die Nachteile von Public und Private Cloud kombinieren.

Von einer Community Cloud wird gesprochen, wenn mehrere Anbieter eine oder mehrere Lösungen für ein oder mehrere Leistungsbezüger anbieten. Der Community Cloud Ansatz lässt sich mit der Stromproduktion vergleichen. Verschiedene Kraftwerke, von grossen Kern- und Speicherkraftwerken bis zu kleinsten Solar-, Wind- oder Flusskraftwerken, produzieren für den Verbraucher Strom. Die Eigentümer sind so unterschiedlich wie die Kraftwerke selber: von grossen Unternehmen bis zu Einzelpersonen, welche für ihr Einfamilienhaus ein Kleinkraftwerk betreiben. Die Gemeinsamkeit ist das Produkt, welches hergestellt, beziehungsweise konsumiert wird. Als Endkonsument kann es egal sein, aus welchem Kraftwerk der Strom kommt – es kann, rein physikalisch gesehen, auch nicht ausgesucht werden, was für Strom aus der Steckdose kommt. Zusatzverträge mit dem Stromlieferanten zum ausschliesslichen Bezug von Solarstrom sind zwar möglich, jedoch ändert sich am Strom, der bezogen wird, nichts.

Der Strommarkt verhält sich ähnlich einer Community. Eine Community Cloud Organisation kann eine vergleichbare Struktur haben. In einer Community-Cloud liefern viele unterschiedliche Produzenten Rechenleistung. Allerdings sind, anders als beim Strom, unterschiedliche Anforderungen vorhanden. Während beim Strom alle mit der gleichen Stromart (230V, 60Hz) zurechtkommen, sind die Anforderungen bei Computer-Power differenzierter. Fast jeder Kunde hat verschiedene Anforderungen betreffend Sicherheit, Stabilität, Verfügbarkeit, Plattformen, Software, Prozesse, etc. Nur dank dem Aufkommen der Virtualisierungs-Technologie in den letzten Jahren, nimmt die Bedeutung der Hardware (Infrastructure) ab.

Eine Community Cloud setzt voraus[15]:

- Eine definierte Anzahl, grösser als zwei, von Leistungsbezüger oder Leistungserbringer,
- eine gemeinsame Vision und Strategie,
- rechtliche Grundlage,
- abgeglichene Prozesse und Organisation,
- semantische Übereinstimmung für die Zusammenarbeit und
- kompatible Technologie.

Als Alternative zur Strom-Analogie könnten auch die Entwicklergruppen rund um Open-Source Projekte genommen werden. Diese sind oftmals als Community organisiert. Die aufgezählten Voraussetzungen treffen mehrheitlich auch zu, jedoch ist in den meisten Fällen keine rechtliche Körperschaft vorhanden, was einen Vertragsabschluss verunmöglicht. Die geplante Leistung der Community ist somit auch nicht verpflichtend oder garantiert.

3.2 Herausforderungen

Die Verschiebung von Services in eine Community Cloud ist eine Art des Outsourcings mit speziellen Herausforderungen. Durch die Beteiligung von mehreren Akteuren mit unterschiedlichen Interessen wird die Organisation erschwert.

Auch technisch besteht eine Abhängigkeit zwischen den Providern. So ist ein SaaS Provider von der Plattform und der Infrastruktur abhängig, obwohl er diese isoliert als Service beziehen kann. Wird der Service an geografisch verschiedenen Orten erbracht, ist eine entsprechend performante Netzwerkverbindung zwischen den Rechenzentren und dem Leistungsbenutzer erforderlich, damit die Verfügbarkeit der Daten und gewünschte Performance des Services gewährleistete werden kann.

Der Vorteil beim Einsatz von mehreren Providern ist eine höhere Verfügbarkeit des gesamten Systems, wobei der einzelne Provider keine höchste Verfügbarkeiten bieten muss. Jeder Provider trägt zur hohen Gesamtverfügbarkeit bei. Zudem kann der Pooling Effekt besser ausgenutzt werden, was bei den Providern wiederum Kosten einsparen kann.

Den Service auf mehrere Provider zu verteilen bringt aber auch einige Schwierigkeiten mit sich. So müssen die Aufgaben, Kompetenzen und Verantwortungen klar geregelt werden, da in den meisten Fällen kein einzelner Ansprechpartner mehr vorhanden ist. Damit die Community entsteht und auch erhalten bleibt, müssen gewisse Spielregeln für die Zusammenarbeit und Ziele definiert werden. Richtlinien innerhalb der Community verhindern, dass ein Lösungsanbieter den gesamten Service übernehmen kann und damit eine Monopol Stellung erhält. Andererseits sind die Anforderungen der Community an die Lösungserbringer zu hoch oder zu wenig lukrativ sind, gibt es keine Anbieter mehr welche in der Community mit machen.

[15] In Anlehnung an das European Interoperability Framework (IDABC, 2004)

3.3 Rollen

Damit eine Organisation, sei es eine Unternehmung oder eine Behörde, erfolgreich operieren kann, ist es unerlässlich, Rollen mit entsprechenden Aufgaben, Kompetenzen und Verantwortungen zu definieren. Besonders im Cloud Umfeld, wo die Transparenz durch die Wolke verschleiert wird, ist ein entsprechendes Rollenkonzept unerlässlich.

Neben dem Lösungsbezüger, welcher die vom Lösungserbringer geliefertem Service nutzt, werden noch zwei weiter Rollen beschrieben. Ein Broker kann eine vermittelnde Rolle innerhalb einer Community übernehmen und steht als intermediär zwischen Bezüger und Erbringer. Ein Konsortium besteht aus Vertretern von den Lösungsbezüger und Lösungserbringer. Dieses Gremium bietet eine Plattform für den Austausch von Informationen und Entscheidungsfindungen welche innerhalb der gesamten Community getroffen werden müssen.

Um eine Organisation erfolgreich auszugestalten braucht es von allen Beteiligten[16]:

- Partnerschaftliches Verhalten – Interesse an einer langfristigen Geschäftsbeziehung und die Bereitschaft, in diese über den Vertrag hinaus zu investieren.
- Gegenseitiges Vertrauen – Die Erwartung, dass der Geschäftspartner in guter Absicht handelt und die getroffenen Vereinbarungen erfüllen wird, soweit es ihm möglich ist.
- Flexibilität – die Bereitschaft, die getroffenen Vereinbarungen anzupassen, wenn sich die Rahmenbedingungen ändern.
- Offene und ehrliche Kommunikation – den Geschäftspartner proaktiv, korrekt und zeitnah zu informieren.

Die nächsten Unterkapitel beschreiben die einzelnen Rollen. Eine Tabelle mit den detaillierten Aufgaben, Kompetenzen und Verantwortungen ist im Anhang 7.3 zu finden.

3.3.1 Leistungsbezüger

Der Leistungsbezüger bezieht die Leistung im gewünschten Umfang und entsprechender Qualität vom Leistungserbringer. In den meisten Fällen bezahlt der Leistungsbezüger den Leistungserbringer für die konsumierte Leistung. Der Leistungsbezüger kann gegenüber dritten mit den bezogenen Leistungen selber wieder als Leistungserbringer auftreten.

3.3.2 Leistungserbringer

Der Leistungserbringer produziert die gewünschte Leistung und kann diese im Markt für einen oder mehrere Leistungsbezüger erbringen. Wie er die Leistung erbringt und welchen Service der Leistungserbringer generiert, hängt von seinem Produktportfolio und seiner Strategie ab. Der Leistungserbringer kann auch Leistungen von dritten beziehen, um seinen eigenen Service zu erbringen. Damit sich der Leistungserbringer innerhalb einer Community engagiert, muss für ihn ein Anreiz bestehen, welcher für ihn auch zu einem Mehrwert führt. Synonyme zu Leistungserbringer sind Provider oder Anbieter.

[16] In Anlehnung an IT-Governance in der Praxis, Seite 175 (Rüter, Schröder, Göldner, & Niebuhr, 2010)

3.3.3 Broker

Der Broker vermittelt die Leistungen zu bestimmten Qualitäten zwischen Leistungserbringer und Leistungsprovider. Je nach Ausprägung handelt es sich um einen organisatorischen oder auch technischen Vermittler.

3.3.4 Konsortium

Das Konsortium kann aus Vertretern der Leistungsbezüger sowie Leistungserbringer bestehen. Es kann notwendige Standards und Richtlinien erarbeiten und vorgeben.

3.4 Organisationsformen

Für die Organisation einer Community Cloud können verschiedene Modelle mit unterschiedlichen Ablauf- und Aufbauorganisation angewendet werden. Die Möglichkeiten werden anhand Ideal-Modelle mit Vor- und Nachteilen aufgezeigt und beschrieben. Je nach Szenarien kann auch eine Kombination von den Organisationsformen gewählt werden.

Entscheidend für die richtige Organisationsform ist die erfolgreiche Kontrolle, Kommunikation und Koordination zwischen den Stakeholdern. Je nach verwendetem Modell fallen diese Tätigkeiten unterschiedlich aus. Beispielsweise ist bei einer offenen Community die Kommunikation mit den unterschiedlichen Partnern erschwert. Durch die lose Organisation einer offenen Community, können im Gegenzug die Transaktionskosten tief gehalten werden, da die Organisation (Verträge, SLA, Abhängigkeiten) sehr einfach ist.

Aus einer Analyse wird die Ausprägung des IT-Service Providings wie folgt beschrieben:

„Die Ausprägung des IT Service Providings: Hier geht es darum zu analysieren, ob die Auslagerung von Teilen der IT zu einem bestehenden Strategieszenario in einer Verwaltung gehört. Hier kann wie folgt gefragt werden: Wird die IT vollständig oder in Teilen ausgelagert? Ja oder Nein? Die Untersuchung der Institutionsform des Service Providers, an welchen die IT ausgelagert wurde: Hier geht es im Wesentlichen um die Klärung der institutionellen Form, d.h. darum abzuklären, ob der Service Provider als verwaltungsintern, -übergreifend oder -extern institutionalisiert wurde und welche möglichen aktuellen oder künftigen Entwicklungen gegeben sind.“ – (Walser & Breidung, 2010)

Die IT Infrastructure Library (ITIL) unterscheidet, als Best Practice Ansatz, in der Phase Service Strategy drei verschiedene Outsourcing-Strukturen:

Tabelle 5 – Outsourcing Strukturen

Outsourcing Strukturen	Beschreibung
Internes Outsourcing	Internes Bereitstellen und Liefern von Services (Internal Service Provider - Type I) oder Zusammenarbeit mit internen Geschäftseinheiten (Shared Service Unit - Typ II)
Traditionelles Outsourcing	Vollständiges Outsourcen eines Services an einen Service Provider (External Service Provider - Type III)
Outsourcing mit mehreren Anbietern	Dieses Mulitsourcing bezieht den Service von mehreren unterschiedlichen Anbietern. Dies entspricht in der Definition einer Community Cloud.

Quelle: Eigene Darstellung in Anlehnung an ITIL[17]

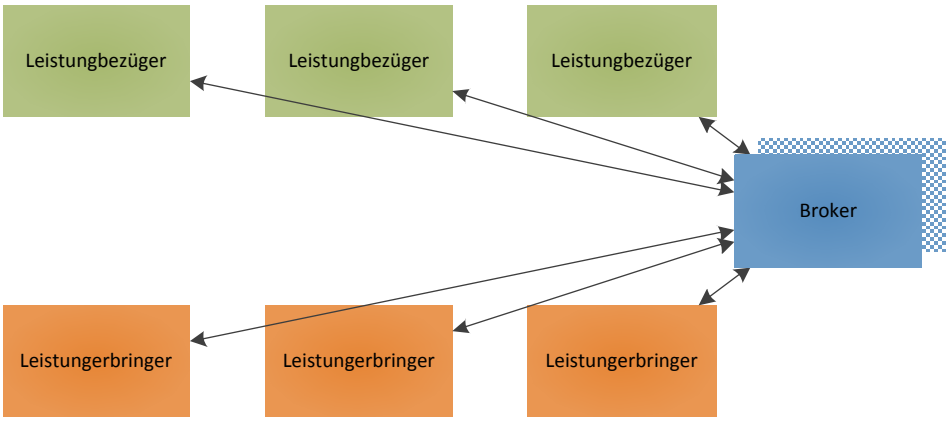
Ausgehend von diesen drei verschiedenen Strukturen wird in den nächsten Abschnitten mögliche Organisationsformen für eine Community Cloud beschrieben. Dabei handelt es sich um Ideallösungen welche nur das Verhältnis zwischen dem Lösungserbringer und Lösungsbezüger aufzeigen. Eine Kombination der verschiedenen Organisationsformen ist Möglich und teilweise sogar notwendig.

[17] (Bon, 2009) Seite 51

3.4.1 Zentrale Stelle (Broker)

Die Leistungsbezüger beziehen die Services über einen zentralen Broker, welcher die Koordination mit den Leistungserbringern übernimmt. Denkbar wären auch mehrere Broker, welche unterschiedliche Services anbieten. Diese Form der Organisation wird in der Energieversorgung oder von Generalunternehmen angewendet.

Abbildung 5 – Zentrale Stelle (Broker)



Quelle: Eigene Darstellung

Vorteile

- Der Broker bietet eine zentrale Anlaufstelle, was die Kommunikation erleichtert.
- Sämtliche Koordination läuft über den Broker.
- Marktübersicht durch begrenzte Anzahl an Anbietern (Brokern).

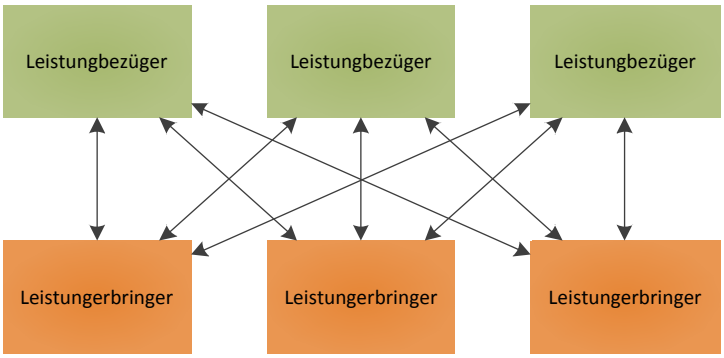
Nachteile

- Der Leistungsbezüger ist vom Broker direkt abhängig.
- Die Neutralität des Brokers muss sichergestellt sein.
- Klärung der Haftbarkeit des Brokers.
- Der Broker fungiert als Intermediär, was ein Mehraufwand bedeuten kann.
- Begrenztes Angebot des Brokers.
- Kleinerer Wettbewerb innerhalb der Community.

3.4.2 Offene Community

In einer offenen Community kann jeder, der sich an die von der Community aufgesetzten Spielregeln hält, mitmachen. Diese Spielregeln werden meistens durch ein Konsortium erstellt und können durch die Mitglieder beeinflusst werden. Beispiele sind unter anderem in der Entwicklung von Open Source zu finden.

Abbildung 6 – Offene Community



Quelle: Eigene Darstellung

Vorteile

- Verschiedene Anbieter können sich einfach an der Community beteiligen.
- Anbieter können die Community durch ihre Kernkompetenzen ergänzen.
- Lösungen stehen der ganzen Community zur Verfügung.

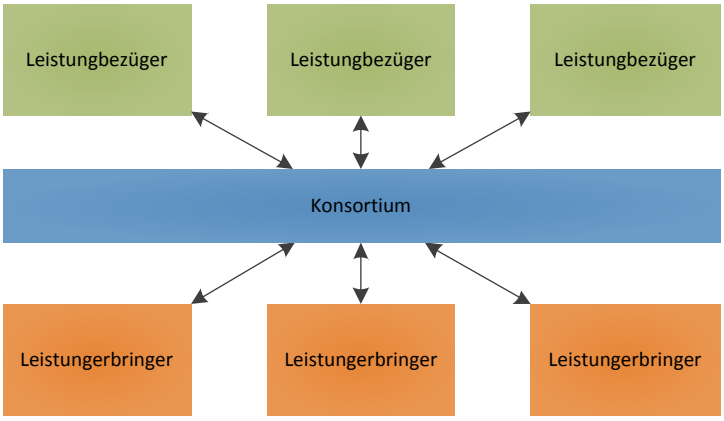
Nachteile

- Die Kommunikation und die Koordination sind durch die lose Organisation erschwert.
- Der einzelne Lösungsbenutzer hat einen geringen Einfluss auf die Community.
- Kontinuität der Community ist von den Mitgliedern abhängig.
- Einfluss von innovativen Ideen kann durch die Community Regeln erschwert werden.
- Die Community kann aus Sicht eines Mitgliedes eine ungewohnte Eigendynamik entwickeln.
- Rechtsform der Community ist nicht geklärt.

3.4.3 Konsortium bildet Cloud

Ein Konsortium von Anbietern und oder Nutzern stellt eine Community Cloud zu Verfügung. Dadurch können Synergien (z.B. redundante Rechenzentren) genutzt werden. Der angebotene Service wird vom Konsortium definiert und angeboten. Solche Konsortien mit namhaften Beteiligungen sind z.B. Standardisierungsorganisation wie W3C, ISACA oder eCH.

Abbildung 7 – Konsortium bildet Cloud



Quelle: Eigene Darstellung

Vorteile

- Die Beteiligungen am Konsortium sind klar definiert.
- Eine breite Abstützung wird durch verschiedene Beteiligte ermöglicht.
- Das Konsortium organisiert die Kommunikation und Koordination.

Nachteile

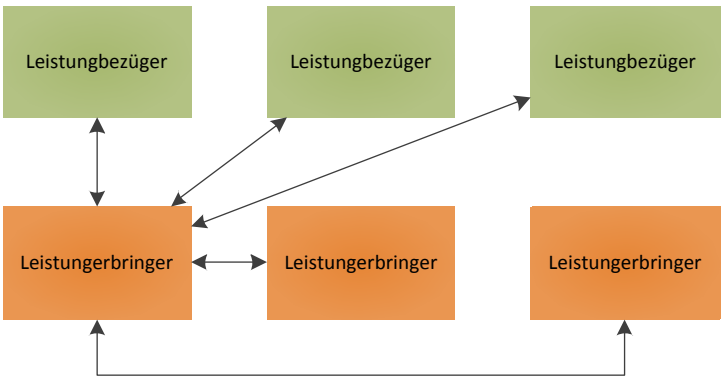
- Sämtliche Entscheide und Vorstösse müssen über das Konsortium erfolgen oder im Rahmen der in der Community vereinbarten Regeln.
- Benachteiligte Anbieter, welche nicht dem Konsortium angehören.
- Möglichkeit zu Preisabsprachen innerhalb des Konsortiums.
- Die Beteiligten vertreten das Anliegen ihrer Organisation und sind allenfalls wenig objektiv.

3.4.4 Master Anbieter Cloud

Diese Form besteht aus einem Hauptanbieter, welcher von anderen Unteranbietern (Subcontractors) unterstützt wird. Dies ermöglicht eine breite Abstützung und Berücksichtigung von anderen Anbietern. Im Gegensatz zu einem Broker kann der Hauptanbieter auch selber noch gewisse Funktionalitäten zum Service beitragen.

Eine solche Organisationsform ist beispielsweise im öffentlichen Verkehr zu finden. Die SBB tritt als Hauptanbieter auf und wird teilweise durch Privatbahnen unterstützt. So sind SBB Billette auch bei der BLS gültig. Die Leistung wird von der BLS erbracht ist aber für den Fahrgast nicht relevant.

Abbildung 8 – Master Anbieter Cloud



Quelle: Eigene Darstellung

Vorteile

- Klare Ansprechperson für Kommunikation, Koordination und die Kontrolle.
- Der Hauptanbieter kann sein Risiko auf die Subcontractors abwälzen.
- Ergänzende Angebote durch die Subconotractors welche der Hauptanbieter nicht anbieten kann.

Nachteile

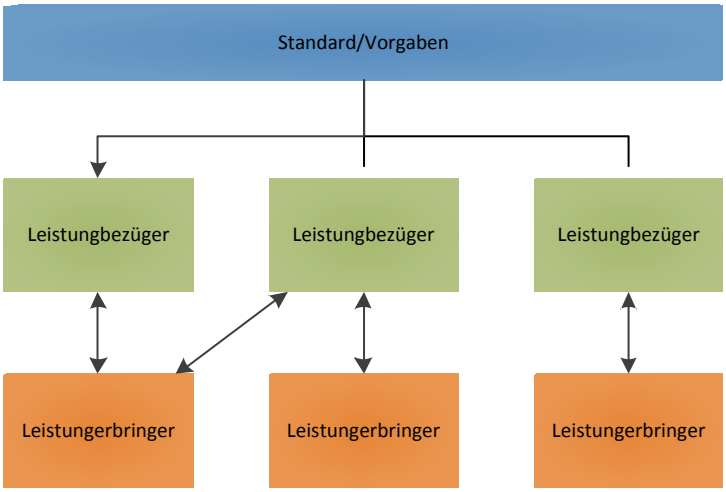
- Starke Abhängigkeit vom Hauptanbieter.
- Klärung der Haftbarkeit des Hauptanbieters für die Subcontractors.
- Der Hauptanbieter hat ein Quasi-Monopol und kann die Subcontrators stark beeinflussen.

3.4.5 Cloud mit Standards und Vorgaben

Die Lösungsbezüger bilden ein Konsortium, welches die Standards, Vorgaben und Anforderungen an eine Community Cloud definieren. Die Anbieter sind definiert und müssen die Vorgaben einhalten und werden durch Vergabe von Lose geregelt.

Eine Analogie ist bei den Stromproduzenten mit einem liberalisierten Markt zu finden. Die Regulationen sind vom Bund klar und können von der Wirtschaft umgesetzt werden. Ein anderes Beispiel sind die Internet Provider, welche nach gewissen Normen ein kongruentes Produkt (Anbindung an einen Internet Backbone) anbieten. Obwohl dies über unterschiedliche Kanäle wie Telefonnetzwerk, TV Netz oder auch Satellit erfolgt, ist die gelieferte Leistung ein Internetzugang.

Abbildung 9 – Government Cloud mit Standards und Vorgaben



Quelle: Eigene Darstellung

Vorteile

- Der Lösungsbezüger kann innerhalb des Angebotes frei auswählen.
- Die gelieferte Leistung ist vergleichbar.
- Es wird dem Lösungsanbieter überlassen, wie er seinen Service aufbaut. Das Produkt wird gemessen und entschädigt.
- Direkte Kontrolle und Kommunikation des Lösungsbezügers mit dem Leistungserbringer.

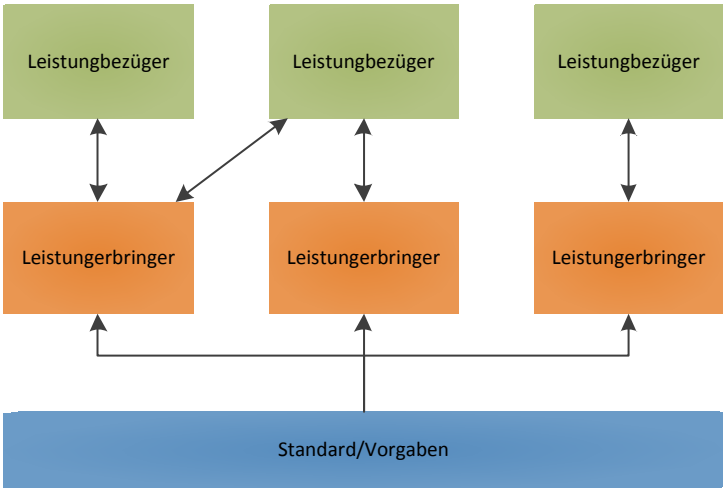
Nachteile

- Kommunikation und Koordination erfolgt redundant über den jeweiligen Leistungserbringer.
- Die Vorgaben an die Leistungserbringer sind komplex zu definieren und aufwändig zu überwachen.

3.4.6 Standard Compliant Cloud

Analog zur Organisation im Kapitel 0 setzen die Behörden einen Standard fest. Es sind jedoch alle Anbieter, welche sich an den Standard halten, berechtigt, sich einzubringen und ihre Leistung zu verkaufen. Solche Organisationsformen sind im Grid Computing zu finden. Das SETI Forschungsprojekt[18] nutzt zum Beispiel mit Einwilligung der Benutzer mehr als 3 Millionen fremde Computer, um sich Rechenzeit zu verschaffen.

Abbildung 10 – Standard Compliant Cloud



Quelle: Eigene Darstellung

Vorteile

- Einfache Selektion des Lösungserbringers durch Zertifikate oder Labels.
- Enormes Potential an Rechenleistung in der Community vorhanden.
- Die offene Struktur ermöglicht es vielen Anbietern teilzunehmen.
- Keine direkte Abhängigkeit von einem Provider.

Nachteile

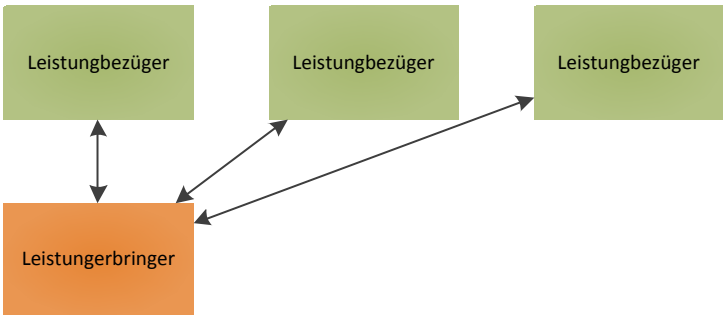
- Keine eigentliche Organisationsform möglich. Fast eher anarchistisch organisiert.
- Nachvollziehbarkeit nur sehr aufwändig zu gewährleisten.

[18] (University of California, 2012)

3.4.7 Keine Community Cloud

Eine Cloud für die Behörden wird durch einen einzelnen Anbieter angeboten. Falls Cloud genutzt werden will, muss dieser Anbieter vorgezogen werden.

Abbildung 11 – Keine Community Cloud



Quelle: Eigene Darstellung

Vorteile

- Es ist ein definierter Ansprechpartner für alle Belange vorhanden.
- Bei Störungen ist ein Ansprechpartner vorhanden und Changes müssen nicht über eine Community erfolgen.
- Zentrale Kompetenz: Das Know-How kann bei einem Anbieter gesammelt werden.
- Interne Prozesse des Anbieters können schnell und effizient aufgestellt werden.

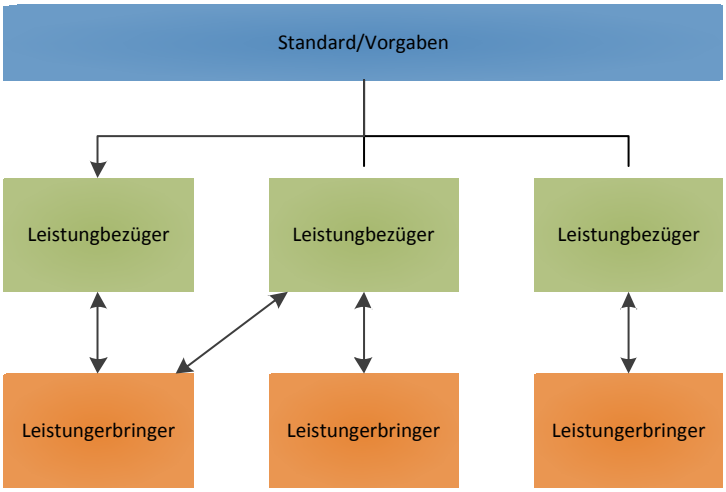
Nachteile

- Monopolistische Stellung; Eine Substituierung des Angebotes ist nicht möglich. Preisgestaltung, Innovation und Marktbestimmung liegen ganz in der Hoheit des Anbieters.
- Pooling Effekte; Die Charakteristik des Pooling Effektes kann nur begrenzt ausgenutzt werden.
- To big to fail Problematik: Der Anbieter muss von den Behörden getragen werden. Ein Konkurs oder nicht Erbringung des Services, hat massive Folgen für die Behörden und ist nicht akzeptierbar.
- Vendor Lock-in: Die Abhängigkeit vom Anbieter ist sehr gross. Die eingesetzte Technologie kann vom Anbieter bestimmt werden. Ein Wechsel zu einem anderen Anbieter ist nur mit sehr viel Aufwand möglich.

3.4.8 Minimale Regulationen

Es werden von einer übergeordneten Stelle[19] nur minimale Regulationen vorgeben, welche einzuhalten sind. Dies kann das Auswahlverfahren oder auch die Kategorisierung von Daten beinhalten. Jeder Leistungsbezüger entscheidet anschliessend innerhalb diesen minimalen Regulationen, wie und wo sie Cloud einsetzen will. Die Verantwortung bleibt voll bei dem einzelnen Lösungsbezüger.

Abbildung 12 – Minimale Regulationen



Quelle: Eigene Darstellung – entspricht der Abbildung 9

Vorteile

- Schnelle Adaption des Angebotes am Markt.
- Geringe Einschränkung der Autonomie der Lösungsbezüger.
- Klare Richtlinien und Vorgaben.

Nachteile

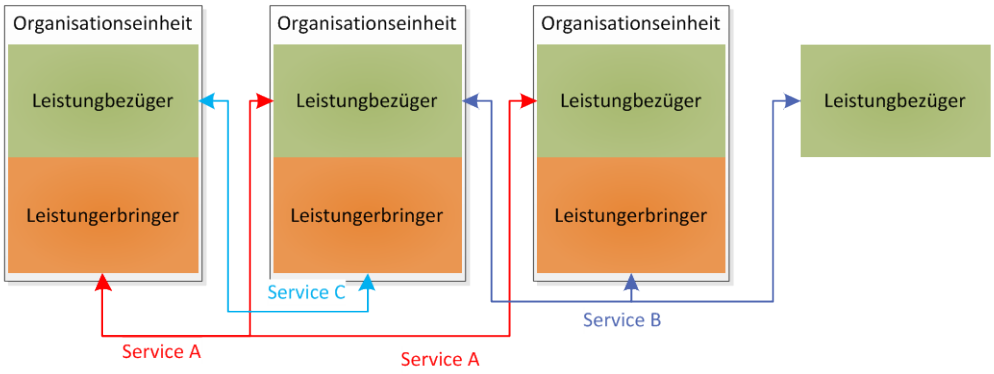
- Wenig Synergienutzen in der Cloud.
- Jedes Auswahlverfahren und Marktanalysen wird von jedem Lösungsbezüger eigenständig und redundant durchgeführt.
- Die Leistungsbezüger können die kritische Masse nicht erreichen und fungieren als kleine Abnehmer am Markt.

[19] Beim Bund könnten dies das beispielsweise durch das Informatiksteuerungsorgan des Bundes (ISB) oder vom Informatikrat verkörpert sein

3.4.9 Shared Service

Die Lösungsbezüger treten mittels Shared Service gleichzeitig als Lösungsanbieter am offenen Markt oder innerhalb einer Organisation auf. Dieser angebotene Shared Service kann wiederum von mehreren Lösungsbezügern bezogen werden. Ihre Kernkompetenz kann die Organisationseinheit anderen zur Verfügung stellen.

Abbildung 13 – Shared Service



Quelle: Eigene Darstellung

Vorteile

- Die Organisationeinheiten können sich auf eigene (Kern-)Kompetenzen konzentrieren.
- Klare Verantwortung des Leistungserbringers.
- Direkte Leistungsverrechnung zwischen den Organisationseinheiten.
- Bestehende Kompetenzen können erhalten bleiben.

Nachteile

- Rollentrennung zwischen Lösungserbringer und Bezüger in der Organisationseinheit.
- Rollenkonflikt innerhalb der Organisationseinheit.
- Angebotsübersicht über die verschieden Organisationeinheiten sind schwierig zu behalten.
- Leistungsbezüger und Leistungserbringer sind beim Bund per Definition zu trennen.[20]

[20] Eine Behörde darf nur ihren gesetzlichen Zweck verfolgen und dabei ihren hoheitlichen Auftrag erfüllen und die Wirtschaft nicht konkurrenzieren. Verordnung über die Informatik und Telekommunikation in der Bundesverwaltung (Die Bundesbehörden der Schweizerischen Eidgenossenschaft, 2011)

3.5 Referenzmodelle für die Community

Die Muster-Organisationsformen, welche im Kapitel 3.4 beschrieben werden, können abhängig vom Szenario unterschiedlich oder auch in Kombination eingesetzt werden. Nach der Definition der Organisationsstruktur, können mithilfe von Referenzmodellen die Rollen innerhalb der Organisation verteilt werden.

Referenzmodelle bieten Hilfestellung beim Betreiben von IT-Services (ITIL) oder beim Sicherstellen der Governance (COBIT). Die Herausforderung innerhalb einer Community besteht darin, die Prozesse auf die verschiedenen Organisationen zu verteilen. Dabei müssen Leistungsanbieter und Leistungsbezüger klären, wer welche Rolle übernimmt und welche Rollen gemeinsam getragen werden. Diese Kombination, wie sie beispielsweise bei der Definition der Service Strategie vorkommen kann, bringt einen erhöhten Aufwand in der Kommunikation und Kooperation, weil die verschiedenen Parteien unterschiedliche Ziele verfolgen. Um den Einsatz von Referenzmodellen zu auditieren, stehen entsprechende Standards, nach welchen sich Organisationen zertifizieren können, zur Verfügung. Mit der Hilfe von Referenzmodellen lässt sich auch bei verteilten Services den Überblick behalten.

Im Anhang 7.4 ist ein Beispiel zu finden, wie die Prozesse aus ITIL und COBIT auf die Rollen innerhalb der Community aufgeteilt werden könnten.

3.6 Standards

Akzeptierte Standards können helfen, innerhalb der Community-Organisation Mindestanforderungen zu definieren und ein gemeinsames Vokabular aufzubauen. Aktuell gibt es noch keinen eigentlichen Cloud Standard; vielmehr ist ein ‚Wildwuchs' von Standards und Definitionen am entstehen. Die Anbieter von Cloudlösungen verwenden IT und andere Standards um ihre Produkte am Markt zu etablieren und entsprechend anzupreisen. Durch die Einhaltung der Standards kann der Provider an Vertrauen gewinnen und sich einen Marktvorteil erarbeiten.

Die Tabelle 6 – Verwendete Standards beschreibt eine Auswahl der am häufigsten verwendeten Standards der Cloudanbieter. Eine erweiterte Auflistung der Standards ist im Anhang 7.5 beschrieben.

Tabelle 6 – Verwendete Standards

Norm	Beschreibung
ISO/IEC 9001	Internationaler Standard fürs Qualitätsmanagement Sicherstellung des Einsatzes von breit akzeptieren Qualitätsrichtlinien.
ISO/IEC 20000	Internationaler Standard fürs IT-Service-Management Zertifizierung des Einsatzes von Best-Practises Ansätze referenzierend auf ITILv2.0
ISO/IEC 27001	Internationaler Standard für ein Informationssicherheits-Managementsystem Definiert den Aufbau und Betrieb eines dokumentierten ISMS (Informationssicherheits-Managementsystem)
SSAE 16 SAS 70	Standard des American Institute of Certified Public Accountants (AICPA). Durch diese Sets von Standards kann ein Serviceprovider das Einhalten von definierten Service Prozessen gegenüber Dritten bestätigen. Dadurch muss der Revisor des Lösungsbenutzers den Provider nicht noch zusätzlich zu auditieren, wenn beispielsweise Daten ausgelagert wurden. Für den Provider entfallen somit unzählige Audits von allen seinen Kunden.
Eurocloud Star Audit[21]	Europäisches Zertifikat für SaaS Lösungen

Quelle: Eigene Darstellung

[21] (EuroCloud, 2010)

3.7 Technische Tools

Ausgehend von den im Kapitel 3.4 beschrieben Organisationsformen, welche sowohl geografisch als auch über verschiedene Provider verteilt sind, werden entsprechende technische Werkzeuge benötigt, welche eine Community Cloud verwalten können.

Für die Administration einer Community Cloud muss es möglich sein, verschiedene Clouds über entsprechende application programming interface (API) zu steuern. Wenn sich die Provider an offene Standards halten, ist auch eine Integration von unterschiedlichen Systemen in ein gemeinsames konsolidiertes Administrationssystem möglich. Die Administratoren, Revisoren und anderen Stakeholder können anschliessend auf einem System die gesamte Cloud überwachen, steuern und auswerten. Unterschieden wird zwischen einem rein administrativen Interface und einem technischen Broker.

3.7.1 Anforderungen an ein technisches Tool

In der folgenden Tabelle sind die Anforderungen an ein Cloud Tool aufgeführt.

Tabelle 7 – Anforderungen an technische Tools

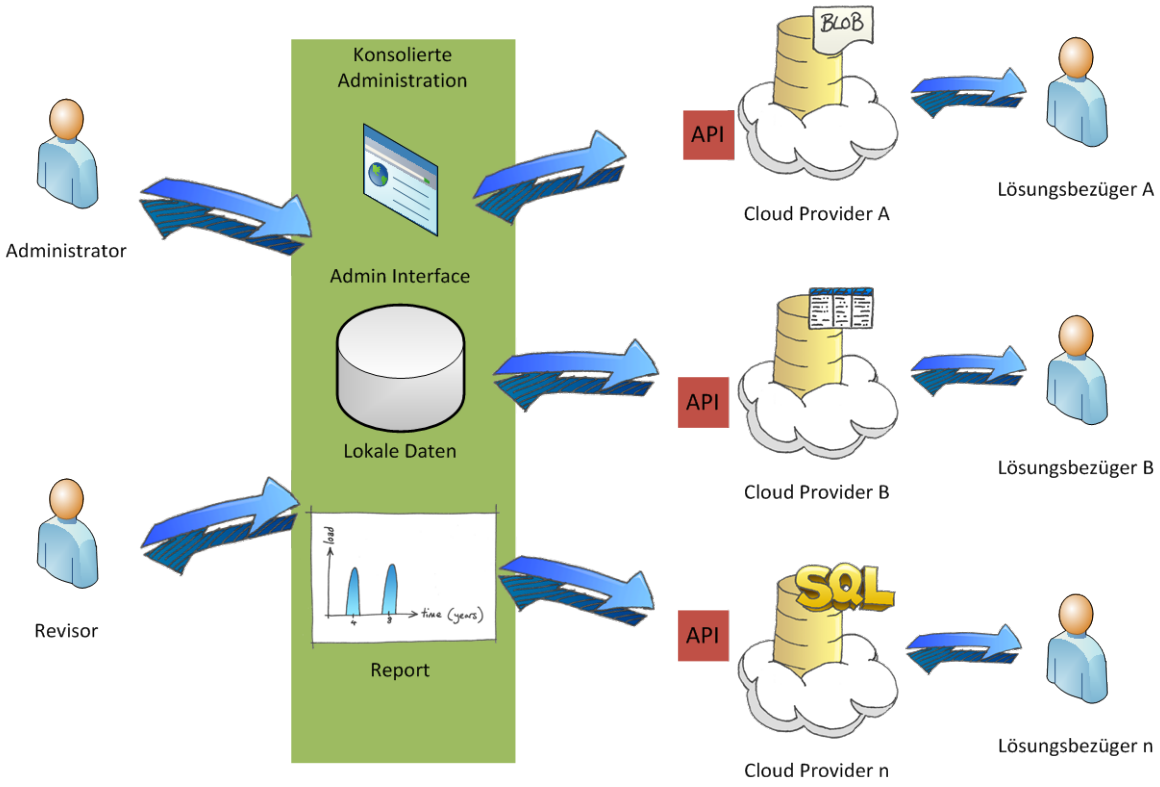
Anforderung	Beschreibung
Mandantenfähigkeit	Das gleiche System wird von mehreren Mandaten (Kunden) gleichzeitig verwendet, ohne das Mandanten auf die Daten der anderen Mandaten Zugriff zu haben.
Abrechnung	Das Tool ermöglicht Abrechnungen nach Verbrauch oder Auswertungen pro Mandat.
Controlling	Durch eine Definition von Warnungen, Metriken und Schwellenwerten kann das System überwacht werden und beim Überschreiten entsprechend reagieren.
Reporting	Der aktuelle Status des Systems sowie ein Reporting über einen vergangen Zeitraum kann erstellt werden.
Identitäts- und Rechtemanagement	Nur identifizierte und berechtigte Subjekte dürfen auf das System zugreifen. Entsprechende Berechtigungsregulationen im System können umgesetzt werden. Funktionstrennung (segregation of duties (SoD)) kann über das gesamte System gewährleistet werden.
Sicherstellen der Governance	Das Einhalten von gesetzten Governance Anforderungen wird durch das System sichergestellt und ist nachvollziehbar.
Interoperabilität	Durch Einhalten von offenen Standards wird die Interoperabilität gewährleistet.

Quelle: Eigene Darstellung

3.7.2 Administratives Interface

Um die verschiedenen Cloudanbieter zu kontrollieren und zu koordinieren wird ein administratives Interface verwendet, welches die verteilten Ressourcen steuert. Über die eingesetzten APIs werden Daten wie Auslastung, Verfügbarkeit oder Performance bezogen. Vom Admin-Interface können zentral Steuerinformationen wie Starten oder Stoppen von virtuellen Maschinen (IaaS) oder die Parametrisierung von Applikationen (SaaS) über die API an die verschiedenen Cloud gesendet werden. Die eigentliche Leistung wird jedoch direkt vom Provider bezogen, ohne über eine zentrale Stelle verteilt zu werden.

Abbildung 14 – Schematische Darstellung Administratives Interface

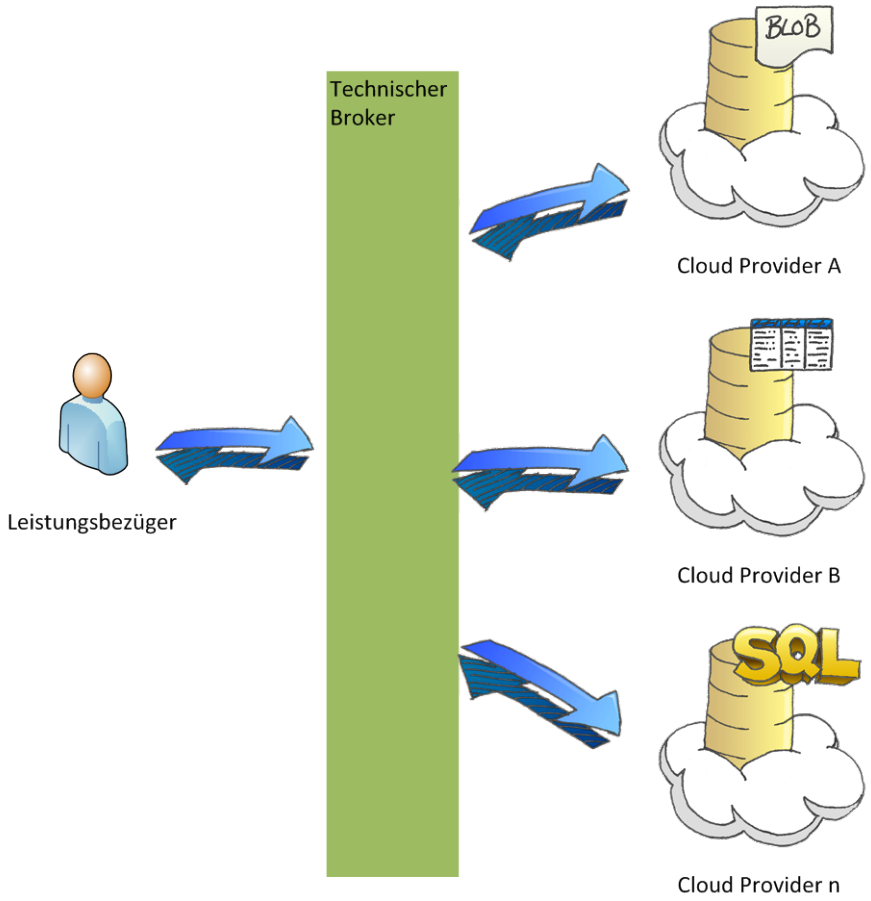


Quelle: Eigene Darstellung

3.7.3 Technischer Broker

Durch den Einsatz eines technischen Brokers kann ein zusätzlicher Abstraktionslayer eingeführt werden. Dadurch erscheinen die Community Cloud respektive die Cloudanbieter für den Leistungsbezüger als Blackbox. Alle Cloud Provider kommunizieren über einen gemeinsamen definierten Standard mit dem Broker. Dadurch wird die Kommunikation und Koordination vereinfacht und der Cloudanbieter austauschbar, sofern die gleiche Leistung von einem andern Anbieter übernommen werden kann. Durch diesen Vermittler kann auch ein Vendor Lock-in vermieden werden, sofern die Cloudanbieter bereit sind, mit dem Broker zusammenzuarbeiten. Die Services werden über den Broker erbracht, was die Relevanz des Anbieters aus der Sicht des Lösungsbenutzers verringert.

Abbildung 15 – Technischer Broker



Quelle: Eigene Darstellung

4. Erbringung IT-Dienstleistungen für Behörden aus der Cloud

Als Ausblick wird in diesem Kapitel beschrieben, welchen Nutzen die Behörden vom Einsatz von Cloud Computing erwarten können und wo und wie bereits Cloud Computing in den Behörden genutzt wird. Ein kurzer Blick über die Grenze zeigt auf, wie andere Länder mit dem Thema Cloud Computing umgehen und welche Strategien verfolgt werden.

4.1 Nutzen von Cloud

Eine Behörde muss wie eine Unternehmung wirtschaftlich denken und handeln. Die Anforderungen an die IT selbst sind ähnlich wenn nicht sogar grösser. Der Kostendruck ist gross und somit das Interesse an Cloud Computing mit seinen Vorteilen berechtigt. Anstelle der IT Abteilung oder des Managements ist es in den Behörden die Politik, welche über die IT Strategie und somit über das Sourcing entscheidet.

Viele Behörden betreiben bereits heute eine verteilte Infrastruktur und Anwendungen. Beispielsweise betreiben viele Gemeinden selber ein Einwohnerkontrollsystem, was gesamtschweizerisch durch die grossen Redundanzen viel Synergiepotential mit sich bringt. Demgegenüber stehen proprietäre Anwendungen welche für spezielle Aufträge, welche die Behörden haben, entwickelt und betrieben werden.

Durch den Einsatz von Cloud Computing wird die Maturität der IT gesteigert und die Zusammenarbeit vereinfacht werden. Cloud Computing bietet in seinem Konzept eine ideale Lösung für Behörden und behördenübergreifende IT Anwendungen.

4.1.1 Zusammenarbeit

Um eine erfolgreiche Zusammenarbeit zu ermöglichen sind interoperable Systeme notwendig. Nach dem Europen Interoperability Framework (EIF)[22] müssen folgende Eigenschaften gegeben sein:

- eine gemeinsame Vision und Strategie
    - Wird durch eine gemeinsame IT Strategie unterstützt. Der Wille zur Zusammenarbeit muss aber zusätzlich in den entsprechenden Entscheidungsträgern vorhanden sein.
- rechtliche Grundlage
    - Wo noch nicht vorhanden, muss eine rechtliche Grundlage für einen Datenaustausch und allenfalls für Cloud Computing geschaffen werden.
- abgeglichene Prozesse und Organisation
    - Durch den Einsatz von Standards, beispielsweise GEVER[23], können Prozesse auch über Organisationsgrenzen hinweg laufen.

[22] In Anlehnung an das European Interoperability Framework (IDABC, 2004)

[23] Standard eCH-0037: GEVER Vorgaben Bund (eCH, 2005)

- semantische Übereinstimmung für die Zusammenarbeit
    - Eine einheitliche Schnittstellte, beispielsweise GEVER Schnittstelle Bund, ermöglicht auch die Zusammenarbeit von unterschiedlichen Systemen.
- kompatible Technologie
    - Mit standardisierten Cloud Lösungen kann eine kompatible Technologie erreicht werden.

4.1.2 SWOT–Analyse

Mithilfe einer SWOT Analyse werden die Chancen, Risiken, Stärken und Schwächen einer Cloudlösung für die Behörden beschrieben. Durch die Kombination der Eigenschaften entstehen potentielle Strategien für den Umgang mit Cloud Computing.

Tabelle 8 – SWOT–Analyse Vor- und Nachteile Cloudlösung

Chancen	**Stärken**
• Kosteneinsparung und Transparenz • Nutzen von Systemen mit hohem Reifegrad[24] • Verlagerung der Kosten; weg von den Investitionen (CAPEX <-> OPEX) • Kurze Time to Market • Economies of Scale • Steigerung der Standortattraktivität Schweiz • Behördenübergreifendes Zusammenarbeiten	• Verfügbarkeit • Stabilität • Performance • Reaktionszeiten • Skalierbarkeit • Unterstützen von strategischen eGovernment-Zielen
Risiken	**Schwächen**
• Datensicherheit • Datenschutz • Datenmissbrauch • Abhängigkeit vom Lösungsanbieter • Anpassung der Budgetierung an den Verwendungsansatz • Fehlendes behördenübergreifendes Denken	• Keine eigene oder Verlust von IT-Kompetenz • Fehlende Standardisierung • Kontrollverlust über Service und Angebot (Wildwuchs) • Staatliche Regulationen verhindern Cloud Computing

Quelle: Eigene Darstellung in Anlehnung an (ISACA, 2009)

[24] Besonders Interessant für kleine Organisationseinheiten

Aus den Kombinationen dieser Eigenschaften lassen sich folgende Strategien bilden:

Stärken-Chancen: Durch den Einsatz von Cloud Computing können strategische Ziele der Behörden wie effizientes Zusammenarbeiten erreicht werden.

Stärken-Risiken: Der Umgang mit Daten kann durch kontrolliertes Einsetzen von Cloudlösungen verbessert werden. Standardisierte Prozesse vermindern die Abhängigkeit von Lösungsanbietern.

Schwächen-Chancen: Die Behörden können sich auf ihren Auftrag fokussieren und die IT als Standardleistung (Commodity) einkaufen. Fehlendes IT Know-How innerhalb der Behörden kann durch den Cloudprovider kompensiert werden.

Schwächen-Gefahren: Wo Cloud Computing nicht sinnvoll ist oder Gefährdung der Daten oder des Auftrages der Behörden darstellt, greifen entsprechende staatliche Regulationen oder Richtlinien. Falls notwendig müssen Gesetze auf die neue Technologie angepasst werden.

4.2 Anwendung und Stand im internationalen Vergleich

Dieses Kapitel vergleicht den Einsatz von Cloud Computing in der Schweiz mit den USA und der Europäischen Union. Die USA hat eine Vorreiterrolle übernommen und setzt schon in zahlreichen Behörden auf Cloud Computing.

4.2.1 Schweiz

Die Cloud Strategie der Schweiz ist erst als Entwurf[25] verfügbar.

Trotzdem wird in den Schweizer Behörden bereits Cloud Computing verwendet. Teilweise wird eine Cloud Lösung eingesetzt, ohne dass es den Benutzern überhaupt bewusst ist. Auch die Vorteile, welche die Cloud Lösung bietet, werden nicht voll ausgenutzt.

Eine viel zitierte Cloud Lösung ist das digitale Kartenportal des Bundes Geoportal[26]. Verantwortlich für dieses Portal ist die Swisstopo. Betrieben wird es in einer Cloud bei Amazon. Die Anforderungen wie Zeit (time-to-market), Kosten, Verfügbarkeit und Skalierbarkeit sind für diese Lösung entscheidend. Bei der Einführung des Dienstes wurde die Webseite mit rund 35‘000 gleichzeitigen Besuchern stark benutzt. Dank der Skalierbarkeit und der leistungsabhängigen Abrechnung des Cloud Dienstes kann auf Schwankungen sehr flexibel reagiert werden. Da es sich um öffentliche und nicht speziell kritische Daten handelt, ist ein Einsatz in einer Public Cloud sehr sinnvoll.[27] [28]

[25] (Müller, Dischl, & Widmer, 2011)

[26] Link: http://map.geo.admin.ch/

[27] Case Studie von Amazon (Amazon Web Service, 2012)

[28] Vorstellung des Geoportal an der OpenExpo (openexpo, 2010)

4.2.2 United States of America

Die „Federal Cloud Computing Strategy“[29] des U.S. Chef Information Officer beschreibt, wie sich die Vereinigten Staaten mit dem Thema Cloud Computing auseinandersetzen. Die Strategie beinhaltet eine Beschreibung von Cloud Computing, ein Migrationsframework für die Entscheidungsfindung sowie die Einführung von Cloud-Diensten. Die Strategie wird vom Präsidenten Barack Obama unterstützt und er fordert sogar eine „cloud first“ Richtlinie, welche alle Behörden verpflichtet, Cloud Lösungen zu nutzten, wenn diese sicher, vertrauenswürdig und kosteneffektiv sind. Durch den Einsatz von Cloud soll per 2015 mindestens 40% der Datencenter eingespart werden können.

Weitere Angebote wie apps.gov helfen den US Behörden bei der Wahl des richtigen Cloud Angebots und vermeiden redundante Verhandlungen und aufwändige Marktanalysen der verschiedenen Behörden. Das NIST liefert neben Definitionen zu Cloud Computing auch Sicherheits-Guidelines und bietet Unterstützung bei der Einführung von Cloudlösungen.

Betreffend Standardisierung und Regulierungen sind die US-Behörden sehr ausführlich. So beschreibt beispielsweise der FIBS 200[30] die minimalen Sicherheitsanforderungen an Bundesinformationen und Informationssysteme analog des ISO 27001 Standards. Wie dieser Standard umzusetzen ist, wird ebenfalls vom NIST in der Publikation SP800-53[31] ausführlich beschrieben.

Neben Amazon bietet auch salesforce.com für verschiedene US-Behörden ihre Cloud Dienste an. Wenn der Service die oben erwähnten Richtlinien einhält, dürfen die US-Behörden den Dienst nutzen. Teilweise werden spezielle Government Clouds gebildet, um den Regularien gerecht zu werden. Die Anbieter haben den Government Markt für sich entdeckt und sind bereit den spezifischen Anforderungen gerecht zu werden.

[29] (Kundra, 2011)

[30] (NIST, National Institute of Standards and Technology, 2006)

[31] (NIST, National Institute of Standards and Technology, 2009)

4.2.3 Europäische Union

Die EU beschreibt in ihrer Digitalen Agenda für Europa, wie die Weiterentwicklung der IT im digitalen Binnenmarkt voranzutreiben ist. Die im Jahr 2010 definierte Strategie soll Europa bis 2020 auf die neuen Herausforderungen vorbereiten und die Wirtschaft stärken.

Durch den Ausbau des „schnellen und ultraschnellen Internetzugangs“ (Kapitel 2.4 des Aktionsplans) wird auch eine Voraussetzung für den Einsatz von Cloud Computing erfüllt (Cloud Charakteristik „Broad network access“). Zudem wird in der Digitalen Agenda eine Strategie für Cloud Computing, insbesondere für den staatlichen und wirtschaftlichen Bereich, gefordert.

Innerhalb Europa definiert und vergibt EuroCloud[32] Standards und Qualitätsnormen im Cloud Umfeld. Für SaaS Anwendungen ist zudem ein Gütesiegel erhältlich, welches die Grundvoraussetzungen wie SLA, Vertragsgestaltung, Handhabung der Nutzerdaten und Wechselmöglichkeiten garantiert.

Das Bundesamt für Sicherheit und Informationstechnik (BSI) hat ein Eckpunktpapier zum Thema „Sicherheitsempfehlungen für Cloud Computing Anbieter“[33] herausgegeben, welches die minimalen Anforderungen an die Informationssicherheit aufzeigt.

[32] (EuroCloud Deutschland_eco)

[33] (Bundesamt für Sicherheit und Informationstechnik (BSI), 2012)

5. Einsatz von Community Cloud in den Schweizer Behörden

Das Kapitel beschreibt, wie eine Community Cloud für die Schweizer Behörden eingesetzt werden kann. Die nächsten Seiten liefern Antwort auf eine kritische Frage:[34]:

„Dürfen Behörden überhaupt in die Cloud?“

Diese Frage ist nicht so einfach mit Ja oder Nein zu beantworten. Welche Vision und Strategie die Schweiz verfolgt, welche Problemstellung es beim Einsatz einer Government Cloud und was die Schweizer Behörden für spezifische Anforderungen haben, helfen beim Beantworten dieser Frage.

5.1 Vision und Strategie

Als Vision für den Einsatz von Cloud Computing in den Schweizer Behörden wurden folgende Grundsätze[35] definiert:

- Die Behörden nutzen Cloud-Angebote
- Die Behörden bieten Cloud-Dienste an
- Government-Cloud für erhöhten Sicherheitsbedarf

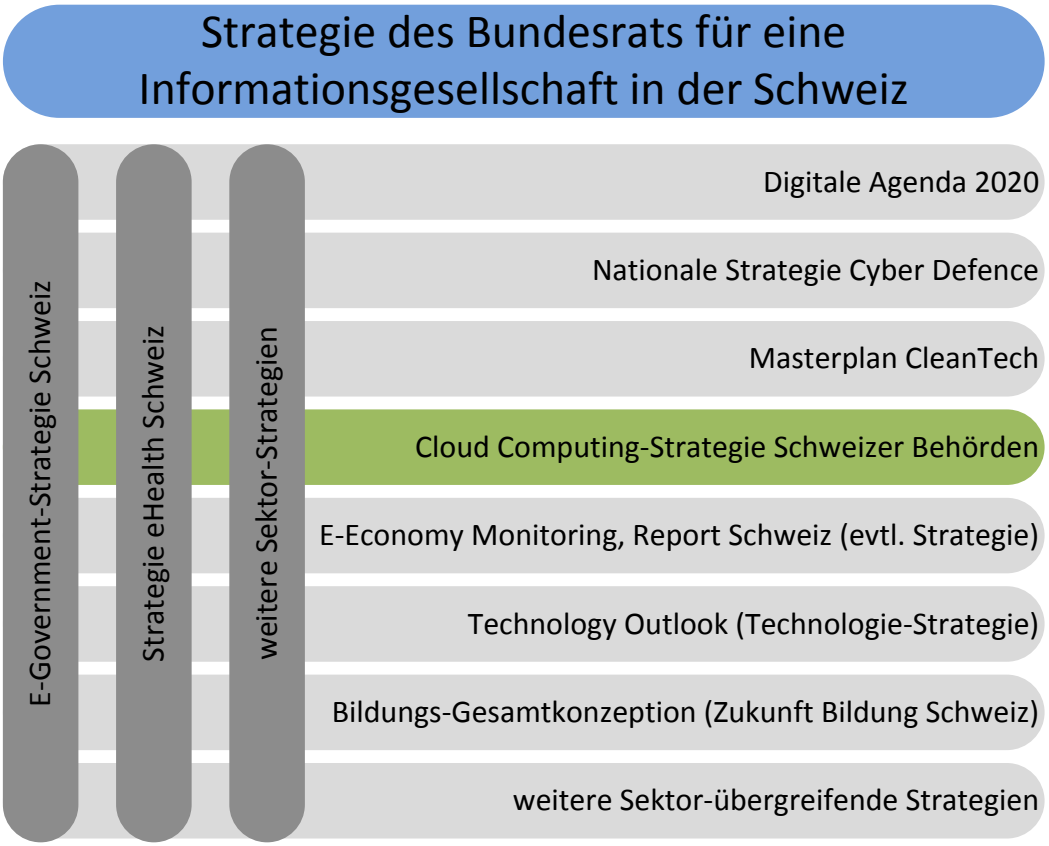
Unter der Leitung des ISB wurde ein Entwurf für eine Cloud-Strategie der Schweizer Behörden erstellt. Als Grundlage für deren Ausarbeitung wurde eine Vorstudie ausgearbeitet, welche Potentiale, Risiken und Rahmenbedingungen für den Einsatz von Cloud Computing in den Schweizer Behörden untersucht. Die Cloud-Strategie steht als Entwurf zur Verfügung. Bis Sommer 2012 werden die Rückmeldungen der Experten von Bund, Kantonen, Gemeinden, Wirtschaft sowie Lehre und Forschung verarbeitet und eine entschlussfähige Fassung vorhanden sein.

Die Abbildung 16 beschreibt, wo sich die Cloud Computing-Strategie positioniert und welche Strategien einen Einfluss auf die Cloud Strategie haben.

[34] Willy Müller am ISSS Forum 2011

[35] Aus der Cloud-Computing-Strategie der Schweizer Behörden (Müller, Dischl, & Widmer, 2011)

Abbildung 16 – Positionierung der Cloud Computing Strategie



Quelle: Eigene Darstellung in Anlehnung an (Fischer, 2012)

5.1.1 Die Behörden nutzen Cloud-Angebote

„Die Schweizer Behörden und ihre IKT-Leistungserbringer nutzen im Rahmen der gesetzlichen Grundlagen für die IKT-Unterstützung ihres Geschäfts Cloud-Dienste, wenn diese betriebswirtschaftlich vorteilhaft und angemessen sicher sind. Sie tun dies, um

- ihre Kosten zu senken,
- ihre Effizienz zu steigern,
- die Flexibilität ihres IKT-Einsatzes zu erhöhen,
- mehr Ressourcen für das Kerngeschäft freizumachen,
- Synergien zwischen den Behörden zu nutzen,
- die Modernisierung der Verwaltung flächendeckend auf allen föderalen Stufen voranzutreiben und
- den Adressaten ihrer Leistungen — Privaten, Wirtschaft wie anderen Behörden — ein zeitgemässes und kostengünstiges Leistungsangebot anzubieten.“ [36]

[36] Auszug Cloud-Computing-Strategie der Schweizer Behörden (Müller, Dischl, & Widmer, 2011)

5.1.2 Community Cloud für die Schweizer Behörden

Durch den Einsatz einer Community Cloud können die Schweizer Behörden dem Bundesgesetz über das öffentliche Beschaffungswesen[37] gerecht werden und trotzdem eine Government Cloud (GovCloud) beschaffen. Die vier Grundsätze des Beschaffungswesens sind:

- Transparenz
- Wirtschaftlichkeit
- Wettbewerb
- Gleichbehandlung

Durch den Einbezug von mehreren Anbietern entsteht kein Vorteil für einen einzelnen Anbieter und aus der Community können die Stärken kombiniert werden. Die von den Behörden geforderte Verfügbarkeit wird durch die Community sichergestellt, ohne dass jeder einzelne für sich eine sehr hohe Verfügbarkeit anbieten muss.

Der weitere Vorteil einer Community ist die Austauschbarkeit des Anbieters. Durch die Standards oder die Vorgaben innerhalb der Community kann ein neuer Anbieter einsteigen oder ein bisheriger die Community verlassen, ohne die Gesamtleistung zu gefährden. Dies erfordert aber geringe Einstiegshürden und das Vermeiden von zu grosser Abhängigkeit von einem einzelnen Anbieter.

Die GovCloud soll nicht nur den Behörden sondern kann auch behördennahen Betrieben oder der Privatwirtschaft zur Verfügung gestellt werden, welche analoge Anforderung hat. Durch die ‚Swissness' könnte sich eine GovCloud sogar als attraktives Angebot im internationalen Markt entwickeln. Diese Swissness wird mit den Attributen Zuverlässigkeit, politische Stabilität, Exklusivität, Tradition und Qualität verbunden, was auch Eigenschaften einer GovCloud sein könnten.

Auch Anbieter von Government Lösungen können von einer GovCloud profitieren. Möglich wäre es, dass sie ihre Produkte den Behörden in der GovCloud anbieten und keine eigene Infrastruktur aufbauen müssen.

5.2 Problemstellung

Das Konzept der Community Cloud passt sehr gut mit der Vision der Behörden zusammen. Jedoch bringt die Organisationform Community einige Herausforderungen, speziell für die Behörden, mit sich.

5.2.1 Transparenz

Die Transparenz, zum Beispiel für Revision, wird allgemein durch den Einsatz von Cloud Computer erschwert. In Public Cloud ist es nicht mehr in jedem Fall klar nachvollziehbar, wo sich die Daten physikalisch befinden. Werden Leistungen von verschiedenen Anbietern in einer Community Cloud zusammengefasst, wird die Nachvollziehbarkeit nochmals erschwert. Um nicht jedes Community Mitglied einzeln zu prüfen, helfen Standards wie

[37] (Die Bundesbehörden der Schweizerischen Eidgenossenschaft, 2012)

SAS70 Provider-übergreifend, um die Governance sicherzustellen und eine einfache Revision durchzuführen.

Nicht nur die Transparenz sondern auch die gewünschten Anforderungen müssen sichergestellt werden. Diese in SLAs formulierten Anforderungen müssen über die gesamte Community gemessen und überwacht werden können.

Fragwürdig ist, ob es innerhalb des Marktes Anbieter gibt, welche in einer Community mitmachen würden. Die geforderte offene Transparenz innerhalb einer Community kann Anbieter abschrecken, weil sie sich nicht mehr von ihren Mitbewerbern differenzieren.

5.2.2 Anbieter einer Goverment Cloud

Damit eine Community entstehen kann, muss für die Anbieter ein Anreiz existieren. Falls kein Interesse an einer Community vorhanden ist, und die Anbieter die ganze Leistung erbringen wollen und können, kann die Community auch mittels Losbildung erzwungen werden. Somit hat jeder Anbieter die Wahl, in der Community mitzuarbeiten oder ganz auf das entsprechende Geschäft zu verzichten.

5.3 Anforderungen und Voraussetzung

Die Behörden haben, ergänzend zu den allgemeinen Erwartungen an eine Cloudlösung, einige spezielle Anforderungen, welche erfüllt werden müssen. Hervorgehoben wird die Sicherstellung der nationalen Unabhängigkeit, der regulative Einfluss durch den Bund sowie die politische Machbarkeit.

5.3.1 Nationale Unabhängigkeit

Die nationale Unabhängigkeit ist dann gewährleistet, wenn die Behörden nicht von einer anderen Nation oder Organisation abhängig oder beeinflusst werden können. Dies kann erreicht werden, wenn der Anbieter entweder:

- Behörden intern angesiedelt,
- ein von den Behörden kontrolliertes Unternehmen mit Aktienmehrheit,
- oder durch Private mit entsprechenden Verträgen geregelt ist.

Je nach Daten und Service müssen die Behörden jederzeit sicherstellen, dass die Unabhängigkeit gewährleistet werden kann. Durch unternehmerische Übernahmen oder politische Veränderungen, können sich innerhalb kürzester Zeit die Eigentümer von Cloud Anbietern ändern.

In der Cloud Strategie des Bundes[38] wird im Strategischen Grundsatz „G4 - Nationale Souveränität“ auf diese Herausforderung verwiesen.

[38] Strategische Grundsätze S. 6 (Müller, Dischl, & Widmer, 2011)

5.3.2 Gesetzliche Rahmenbedingungen

Im Gegensatz zur Privatwirtschaft unterstehen die Behörden zusätzlichen regulativen Einflüssen. Die gesetzlichen Anforderungen unterscheiden sich zusätzlich zwischen Bund und Kantonen. So kann beispielsweise gegen grössere Beschaffungen Einsprache erhoben werden, was ein IT-Projekt zu massiven Verspätungen oder sogar zum Scheitern bringen kann.

5.3.3 Politische Machbarkeit

Das Interesse und die Einflussmöglichkeiten in eGovernment Vorhaben werden durch die Politik, Organisationen und Bürgern wahrgenommen und entsprechend beeinflusst. So ist eine einzige Government Cloud Lösung von nur einem Anbieter rein politisch sehr unwahrscheinlich.

5.3.4 Finanzierung

Die Privatwirtschaft erlangt ihre Einnahmen anders als die Behörden, was auch eine andere Finanzierung erforderlich macht. Die Finanzierung einer Government Cloud muss mit Steuergeldern erfolgen, welche der Staat sparsam und effektiv einsetzen muss.

Staatliche Aufgaben müssen bedarfsgerecht und wirtschaftlich erfüllt werden.[39]

Für die Finanzierung einer Government Cloud stellen sich einige Fragen:

Wie teuer wird eine GovCloud? Übersteigt der Nutzen die Aufwände? Wie teuer darf die GovCloud werden?

Auch eine GovCloud muss im Markt bestehen. Ansonsten werden auch die Behörden, falls erlaubt, sich eine andere Cloud Lösungen suchen. Die Qualität „swissness“ darf sicher ihren Preis haben, jedoch ist dieser sehr schwierig zu quantifizieren.

Darf, um die Kosten besser zu verteilen (Skaleneffekt), auch die Privatwirtschaft die Government Cloud nutzen?

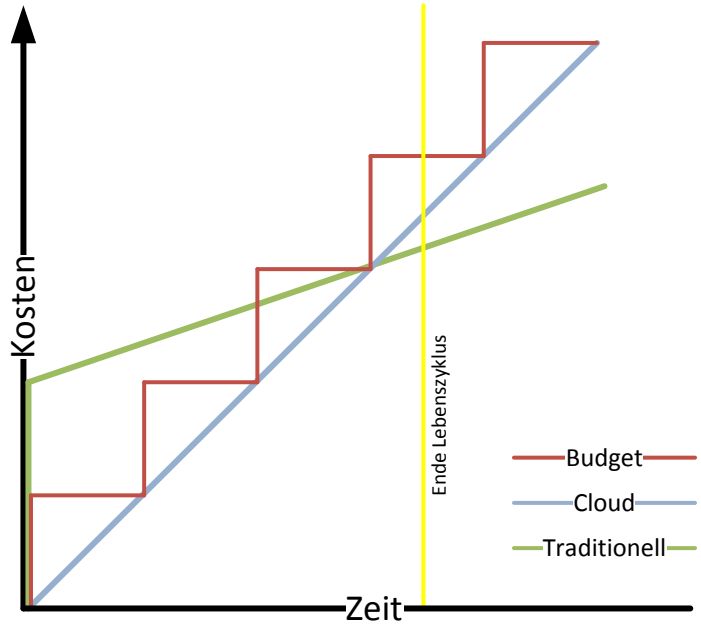
Das Bedürfnis nach einer Cloud Lösung, welche zu 100% schweizerisch ist und damit auch nur dem Schweizer Recht untersteht, ist sicher auch ausserhalb des Behördenumfelds vorhanden. Jedoch gibt es gerade im Hochsicherheitsbereich gewisse Applikationen, welche sehr hohe Anforderungen haben und nicht in einer Government Cloud betrieben werden dürfen. Es ist vorstellbar, dass gewisse dedizierte Dienste auch von der Privatwirtschaft genutzt werden.

[39] Bundesverfassung der Schweizerischen Eidgenossenschaft Art43a Abs 5 (Die Bundesbehörden der Schweizerischen Eidgenossenschaft, 2011)

Kann auch eine kleine Gemeinde nach Abwägung der Kosten und Nutzen von einer GovCloud profitieren?

Durch tiefe Investitionskosten sind auch kleinere Organisationseinheiten, wie beispielsweise kleinere Gemeinden, fähig, innerhalb ihres Budgets eine Cloud Anwendung zu nutzen. Durch das pay as you go Nutzungsmodell sind sogar sehr grosse und komplexe Anwendungen für kleine Organisationseinheiten potentiell erschwinglich, welche ohne diese Cloud Charakteristik viel zu teuer wären.

Abbildung 17 – Modell einer IT-Investition



Quelle: Eigene Darstellung

Die Abbildung zeigt auf den Dimensionen Zeit und Kosten, wie sich eine Modell-IT-Investition verhalten kann. Eine traditionelle Lösung (grün) hat in den meisten Fällen eine Anfangsinvestition zur Folge, welche kleinere Budgets (rot) in der Startphase übersteigt. Eine ‚pay per use' Cloud Lösung (blau) hat keine bis nur sehr geringe Anfangsinvestitionskosten. Obwohl der TCO (Total Cost of Ownership) der Cloudlösung bis zum Erreichen des Endes des Lebenszyklus, wie in diesem Beispiel dargestellt, grösser sein kann, kann bei diesem Budget nur die Cloud Lösung beschafft werden. Die traditionelle Lösung ist infolge hohen Investitionskosten (CAPEX) nicht möglich.

Die Steilheit und Position der jeweiligen Kurven ist ein Muster und kann sich je nach zu beschaffener Lösung verändern. Daher werden vor jeder Investition der Aufwand und die Nutzen spezifisch betrachtet.

5.3.5 Steigerung des Reifegrades der Behörden IT

Durch den Einsatz von Cloudlösungen soll das Ziel von interoperablen IT-Lösungen weiter verfolgt werden. Ohne grosse Initialkosten sollen auch kleinere Organisationeinheiten, beispielsweise kleine Gemeinden, Zugang zu Systemen mit einem hohen Reifegrad erhalten. Dies ist für eine erfolgreiche Zusammenarbeit über die Organisationsgrenze hinweg notwendig. Erst wenn sich eGovernment Lösungen verbreitet haben, kann ein barrierefreier Datenaustausch stattfinden.

5.3.6 Gewährleistung der Verfügbarkeit in Ausnahmesituationen

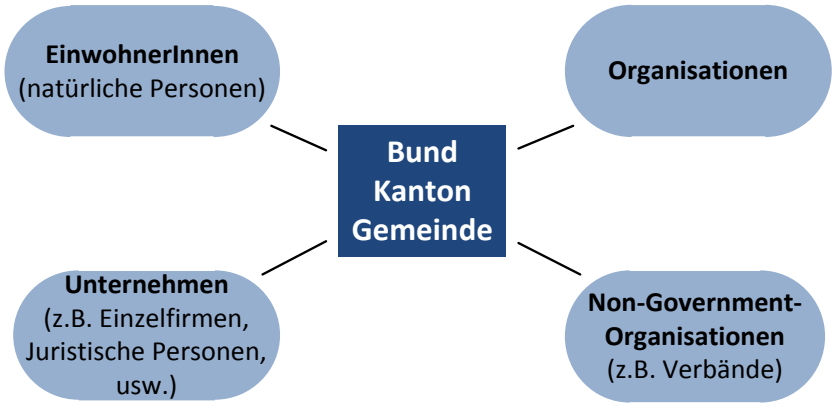
Zusätzlich zu der Verfügbarkeit, welche standardmässig in den SLAs definiert ist, erfordern gewisse Services der Behörden besonders in Notfällen ein einwandfreies Funktionieren. Im Falle einer grossen nationalen Katastrophe, wenn die Verfügbarkeit von der privatwirtschaftlichen IT nicht mehr relevant ist, müssen IT-Systeme wie Kommunikation und Alarmsysteme der Behörden verfügbar sein. Dies kann durch geographisch verteilte, redundante Systeme in entsprechenden Schutzräumen gewährleistet werden.

Auch wenn die Eintrittswahrscheinlichkeit eines solchen Ereignisses sehr klein ist, müssen entsprechende Massnahmen getroffen werden.

5.4 Organisation

Die drei Föderalen Ebenen Bund, Kanton und Gemeinde haben die gleichen Partner, mit welchen sie zusammenarbeiten müssen. Dies sind natürliche Personen, wie Einwohnerinnen und Einwohner, grosse internationale Organisationen, Kleinstunternehmen, weltweit tätige Konzerne und auch Non-Goverment-Organisationen sein. Um den unterschiedlichen Ansprüchen der verschiedenen Partner zu entsprechen, ist eine effektive und effiziente Organisation notwendig.

Abbildung 18 – Partner der Behörden



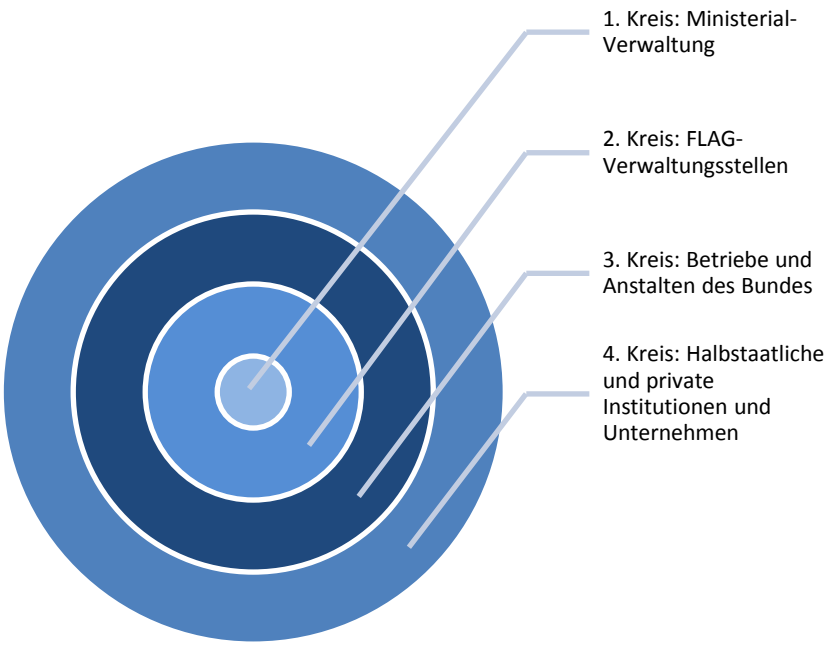
Quelle: Eigene Darstellung in Anlehnung an E-Government-Architektur Schweiz (Müller W. , 2009) Folie Nr. 8

Beim Anwenden der im Kapitel 3.4 Organisationsformen vorgestellten Modelle müssen die Vor- und Nachteile abgeschätzt und besonders auf ihre Eignung für die Behörden geachtet werden. Eine Kombination aus verschiedenen Organisationsformen ist zudem denkbar, wenn nicht sogar notwendig, um den Anforderungen der Behörden gerecht zu werden. So werden sowohl auf Seiten der Lösungsanbieter wie auch -bezüger entsprechende Richtlinien notwendig sein.

5.4.1 Der Staat als Holding

Innerhalb des Staates kann eine Cloud in vier unterschiedlichen Kreisen betrieben werden. Je nach Kreis hat der Staat mehr oder weniger direkten Einfluss auf den Betrieb.

Abbildung 19 – Der Staat als Holding



Quelle: Eigene Darstellung in Anlehnung an (Ritz, Rieder, & Jenzer, 1999)

Beschreibung der Kreise:[40]

1. Kreis: Verwaltungsstellen, die im wesentlichen politische Koordinations- und Steuerungsleistungen erbringen. Sie können nach wirkungs- und leistungsorientierten Prinzipien und mit Leistungsauftrag geführt werden, verfügen aber über keinen erweiterten Handlungsspielraum und kein Globalbudget.

2. Kreis: Verwaltungsstellen, die mit Leistungsauftrag und Globalbudget geführt werden. Sie verfügen über einen erweiterten Handlungsspielraum, nicht aber über eine eigene Rechtspersönlichkeit und haben keine eigene Rechnung.

3. Kreis: Betriebe und Anstalten im öffentlichen Recht, die zu 100 Prozent im Besitz des Bundes sind und mit Leistungsauftrag geführt werden. Sie haben eine eigene Rechtspersönlichkeit und verfügen über eine eigene Rechnung.

4. Kreis: Gemischtwirtschaftliche und private Unternehmungen, die mit dem Vollzug von Bundesaufgaben betraut sind (eigene Rechtspersönlichkeit und Rechnung).

[40] Quelle (Ritz, Rieder, & Jenzer, 1999)

5.4.2 Ausprägungen Government Cloud

Ausgehend von den Problemstellungen und unterschiedlichen Bedürfnisse innerhalb der Behörden wird es nicht möglich sein, eine einzige GovCloud zu betreiben. Vielmehr geht es darum, die Services und Daten zu kategorisieren und in einer entsprechenden Cloud zu betreiben, welche nur diese Anforderungen erfüllt. Ausgegangen wird davon, dass je höher die Anforderungen sind, umso teurer wird auch das Betreiben der jeweiligen Cloud. Wird jedoch eine Cloud zu wenig verwendet, kann kein Skaleneffekt erreicht werden, was die entsprechende Lösung auch wieder teurer macht. Dies könnte dazu führen, dass selbst eine Highest-Secure-Lösung in der Verwendung (Beispielsweise CPU/Zeit) günstiger kommt, weil ein grösserer Skaleneffekt erreicht wird. Trotzdem kann aber von einer Differenzierung des Cloudangebots ausgegangen werden.

Als Möglichkeit werden drei verschiedene Clouds vorgeschlagen, welche sich durch Vor- Nachteile unterscheiden und unterschiedliche Anforderungen abdecken.

Tabelle 9 – Vor- und Nachteile von verschiedenen GovClouds

	Beschreibung	Vorteile	Nachteile
Highest Secure	Bietet den bestmöglichen Schutz der Daten und höchste Verfügbarkeit.	• Marktlücke auf dem freiem Markt • Notwendigkeit für gewisse Behördenlösungen	• Sehr aufwändig und daher kostenintensiv. • Angebot ev. nicht als Cloud Lösung umsetzbar • Technische und organisatorische Machbarkeit ist nicht sichergestellt
Secure	Unter wirtschaftlichen Bedingungen ausreichenden Schutz und entsprechende Verfügbarkeit.	• Ideallösung für die meisten Behördenanwendungen • State of the art • Konkurrenzfähig	• Nichterfüllen der Anforderungen • Konkurrenzierung der Privatwirtschaft durch den Staat mittels Steuergelder
Public	Diese Cloudlösung kann auch als Public Cloud bezogen werden, welche die entsprechenden Anforderungen erfüllen.	• Effiziente Lösung mit gutem Preis-Leistungsverhältnis • Offener Markt • Der Markt spielt • Zahlreiche Angebote • Ideal für Lösungen oder Daten, welche die Behörden der Öffentlichkeit zur Verfügung stellen wollen (OpenData)	• Wenig Einfluss auf dem Public Anbieter • Evaluation des Anbieters und Vertragsverhandlungen sind individuell und aufwändig

Quelle: Eigene Darstellung

5.5 Entscheidungsfindung

Die entsprechende Cloud Lösung wird abhängig vom Verwendungszweck und dessen Umfang bestimmt. Aufgrund der identifizierten Anforderungen und Voraussetzungen aus dem Kapitel 5.3, müssen folgende Fragestellungen jeweils beachtet werden:

Lassen die gesetzlichen Rahmenbedingungen eine Cloud Lösung zu? Falls nein, ist es sinnvoll und möglich die gesetzlichen Bestimmungen anzupassen?

Um was für eine Art der Cloud Lösung handelt es sich?

- IaaS
- PaaS
- SaaS

Welche Sicherheitsanforderungen sind mindestens notwendig?

- Public
- Secure
- Highest secure

Wer verwendet die Lösung

- Einzellösung
- Innerhalb einer Behörde (Behördenweit)
- Über Organisationsgrenzen hinweg. Unter Umständen zwischen Behörden und Unternehmen/Organisationen (Behördenübergreifend)

Muss von einer Gefährdung der nationalen Unabhängigkeit durch das Verlagern von Service oder Daten in die Cloud ausgegangen werden?

- Nein
- Zwingend

Da es sich bei der Wahl der Cloud Lösung um eine strategische Entscheidung handelt, ist zu definieren, wer mit der Entscheidungsfindung beauftragt wird. Die Tabelle 10 beschreibt in den Entscheidungsdomänen, wer für welche Entscheidungen zuständig ist und wer eine empfehlende Rolle hat.

Beteiligte Rollen im Entscheidungsfindungsprozess sind:

Vorstand: Entspricht im Behördenumfeld der Regierung, welche über die Gesamtstrategie entscheidet.

Sourcing – strategisches Komitee: Verantwortlicher der Business/IT-Strategie innerhalb der Behörde.

Sourcing – operatives Komitee: Verantwortlicher Architektur, Operations, Projekte oder Projektportfolio

Interne Organisation: Verantwortlicher Finanzen, Benutzervertreter, …

Entscheidungsdomänen für einen Einsatz von Cloud Computing sind:

Strategie: Definieren und vertreten der Cloud-Gesamtstrategie (Strategische Grundsätze)

Vertrag: Ausarbeitung und Genehmigung des Cloud Vertrags.

Dienstleistung: Definition, welche Dienstleistungen aus welcher Cloud bezogen werden.

Finanzen: Definition der Lösungsfinanzierung und der -budgetierung. (Nutzen/Aufwand-Rechnung)

Kommunikation: Definition der Kommunikation

Tabelle 10 – Entscheidungsdomänen

		Entscheidungsdomänen				
		Strategie	Vertrag	Dienstleistung	Finanzen	Kommunikation
Beteiligte	Vorstand	E			I	
	Sourcing – strategisches Komitee	M	M		E	E
	Sourcing – operatives Komitee	I	E	M	M	M
	Interne Organisation	I	M	E	M	M

E = entscheidet; M = empfiehlt; I = wird informiert

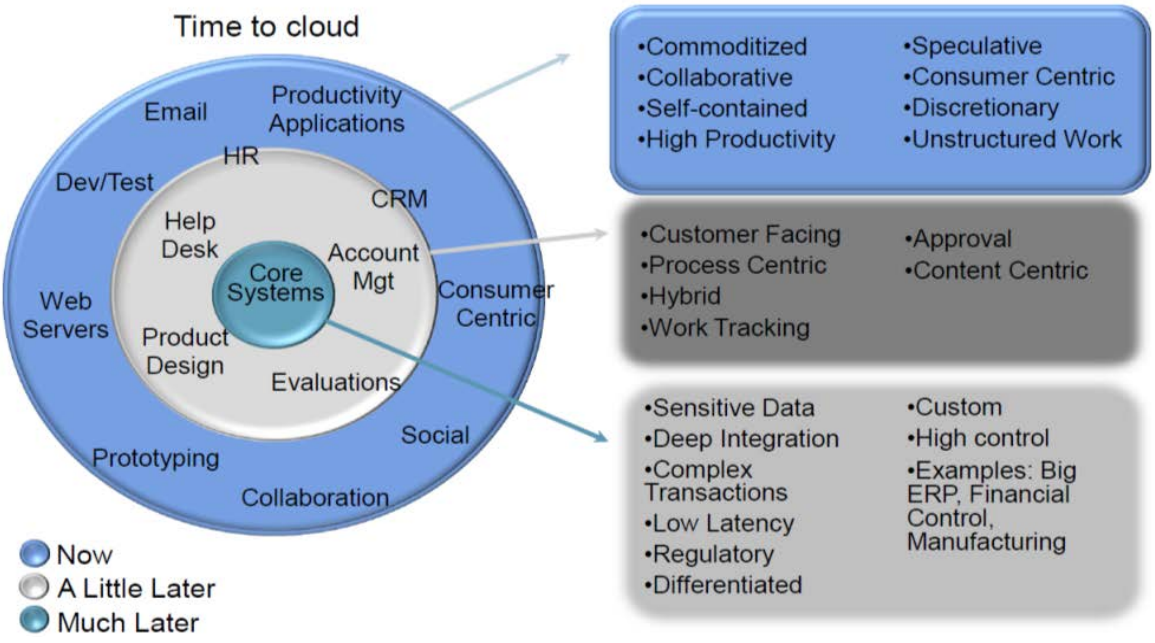
Quelle: Eigene Darstellung in Anlehnung an (Rüter, Schröder, Göldner, & Niebuhr, 2010)

6. Zusammenfassung und Ausblick

Die Vorteile, welche Cloud Computing verspricht, treffen sehr gut die aktuellen Anforderungen des Business an die IT. Die Erwartungen an die IT sind: Kosten zu sparen, effizienter zu sein und gleichzeitig noch agil auf die stetig ändernden Anforderungen reagieren können. Diese sich fast konkurrenzierenden Ziele sind mit der heutigen IT-Landschaft fast nicht erfüllbar - Cloud Computing wird allerdings exakt mit diesen Vorteilen beworben. Doch wie jede neue Lösung bringt Cloud Computing auch Risiken und Unbekanntes mit sich, welche es zu beherrschen gilt. Die neuen Risiken dürfen jedoch nicht isoliert betrachtet werden, sondern müssen zusammen mit den Vorteilen gegenüber der bestehenden Situation verglichen werden. So kann eine Datensicherung in der Cloud, trotz berechtigten Sicherheitsbedenken, um einiges sicherer sein, als die bestehende Lösung im eigenen Keller. Einige Herausforderungen, wie beispielsweise die Wahrung der Datenhoheit, bekommen eine andere Ausprägung durch den Einsatz von Cloud Lösungen. Andere Risiken wie die Sicherheit der sensitiven Daten sind nicht neu, sondern bestehen schon seit der systematischen Erhebung von Daten. Durch die Verbreitung von Cloud Computing und den damit errungenen Erfahrungen können die Risiken zusätzlich minimiert werden.

Gartner zeigt mit der Abbildung 20 – „What Moves to the Cloud First?“ auf, wann sich welche Services in die Cloud verlagern lassen. Somit lassen sich bereits heute hochautomatisierte und in sich geschlossene Prozesse wie Email oder Webservice, in die Cloud auslagern. Bis jedoch hochkritische und komplexe Services mit sensiblen Daten aus der Cloud bezogen werden können, braucht es noch einige Zeit.

Abbildung 20 – „What Moves to the Cloud First?“



Quelle: Garnter, Adriatic (Maglić, 2012)

Auf die Frage, ob Behörden überhaupt in die Cloud dürfen, gibt es keine klare Antwort. Vielmehr ist es ein „ja, aber“. Cloud Computing wird in Zukunft in der Breite eingesetzt werden, wenn auch zu Beginn nur gewisse Services in die Cloud ausgelagert werden. Längerfristig werden sich die Charakteristiken von Cloud auch für interne Services etablieren und so eine breite Verwendung in der IT erlangen. Diesen Paradigma-Wechsel werden oder wollen auch die Behörden nicht umgehen können.

Zusammenfassend sind drei Punkte für die Etablierung von Cloud Computing für die Schweizer Behörden zu beachten:

- Um unterschiedliche Anforderungen zu erfüllen, braucht es auch unterschiedliche Clouds.
- Daten und Services müssen differenziert betrachtet werden. Es wird für jede Anwendung separat entschieden, was, wie in welche Cloud ausgelagert werden kann.
- Es braucht Zeit, bis sich eine Sourcing-Strategie durchgesetzt hat.

Als Ausblick, wie mit der Cloud für die Schweizer Behörden gestartet werden kann, bieten sich folgende nächste Schritte an:

- Partner identifizieren: Wer würde sich bei einer Community Organisation für eine Behörden Lösung (GovCloud) beteiligen?
- Organisationsform wählen und Rollen klären
- Aufsetzen eines konkreten Pilotes mit einer konkreten Leistung. Um ein relevanter Pilot zu sein, muss dieser auch mit kritischen Daten aufgesetzt werden.
- Durch fehlende Standardisierung auf der Plattformebene würde sich eine IaaS Lösung zum Starten anbieten.

Der Abschluss der Arbeit bildet ein Zitat[41] von Peter Kummer, CIO der SBB, welches die aktuelle Lage um das Business-IT-Alignment und Cloud Computing sehr gut trifft.

„Um wirklich innovativ zu sein,
muss die IT das Geschäft genauso gut kennen
wie die neusten IT-Entwicklungen“

Peter Kummer, CIO Schweizerische Bundesbahnen

[41] (Computerworld, 2012)

7. Anhang

7.1 Datenschutzrechtliche Anforderungen bei der Nutzung von Cloud-Computing-Diensten

1. Werden bei der Nutzung von Cloud Computing personenbezogene Daten bearbeitet, so liegt aus datenschutzrechtlicher Sicht normalerweise eine Datenbearbeitung durch Dritte im Sinne von Art. 10a DSG vor. Demnach kann das Bearbeiten von Personendaten durch Vereinbarung oder Gesetz Dritten (hier: Cloud-Service-Anbieter) übertragen werden, wenn die Daten nur so bearbeitet werden, wie der Auftraggeber (hier: Cloud-Nutzer) selbst es tun dürfte, und wenn keine gesetzliche oder vertragliche Geheimhaltungspflicht es verbietet. Der Auftraggeber muss sich insbesondere vergewissern, dass der Dritte die Datensicherheit gewährleistet. Der Cloud-Service-Anbieter muss also verpflichtet werden, sich vollumfänglich an die in der Schweiz geltenden Datenschutzbestimmungen zu halten. Dies gilt in gleichem Masse für allfällige Subunternehmer, die vom Anbieter beigezogen werden. Die Umsetzung dieses Erfordernisses bereitet in der Praxis jedoch Schwierigkeiten, da bei den Cloud-Computing-Anwendungen die Unterauftragsverhältnisse des Cloud-Service-Anbieters für den Cloud-Nutzer oft nicht transparent sind.

2. Weiter muss sich der Cloud-Nutzer vergewissern, dass der Cloud-Service-Anbieter als Dritter die Datensicherheit im Sinne von Art. 7 DSG und Art. 8 ff. bzw. 20 ff. VDSG gewährleistet. Das heisst, die Personendaten müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden. Es muss für Vertraulichkeit, Verfügbarkeit und Integrität der Daten gesorgt sein. Der Cloud-Service-Anbieter muss die Daten gegen folgende Risiken schützen: unbefugte oder zufällige Vernichtung oder zufälligen Verlust; technische Fehler; Fälschung; Diebstahl oder widerrechtliche Verwendung; unbefugtes Ändern, Kopieren, Zugreifen oder andere unbefugte Bearbeitungen. Diese Massnahmen sind periodisch vor Ort zu überprüfen. Wie die Datenschutzanforderungen im Einzelnen umzusetzen sind, hängt vom Unternehmen bzw. der Behörde, von der Art der Daten, aber auch von der Organisation und des Zuschnitts der Cloud-Lösung (bspw. Private oder Public; IaaS, PaaS oder SaaS) ab. Als Grundregel gilt: Je vertraulicher, geheimer, wichtiger (weil geschäftskritisch) oder sensitiver (weil besonders schützenswert) die Daten sind, umso eher ist von einer Auslagerung der Daten in die Cloud, insbesondere eine ausländische Cloud, abzusehen, und desto strikter und umfassender müssen die (Datenschutz-) Sicherheitsvorkehrungen und deren Kontrolle sein.

3. Die Nutzung von Cloud Computing bedingt in vielen Fällen eine Datenbekanntgabe ins Ausland, da die Verarbeitung oftmals auf weltweit verstreuten Servern stattfindet. Häufig werden dazu auch Subunternehmer beigezogen. Sehr oft geht es dabei um Länder, die ein tieferes Datenschutzniveau als die Schweiz aufweisen, so dass mit der Übermittlung dorthin die Gefahr einhergeht, dass mit diesen Daten Bearbeitungen durchgeführt werden, die in der Schweiz nicht erlaubt wären. Aus diesen Gründen dürfen Personendaten nicht ins Ausland bekannt gegeben werden, wenn dadurch die

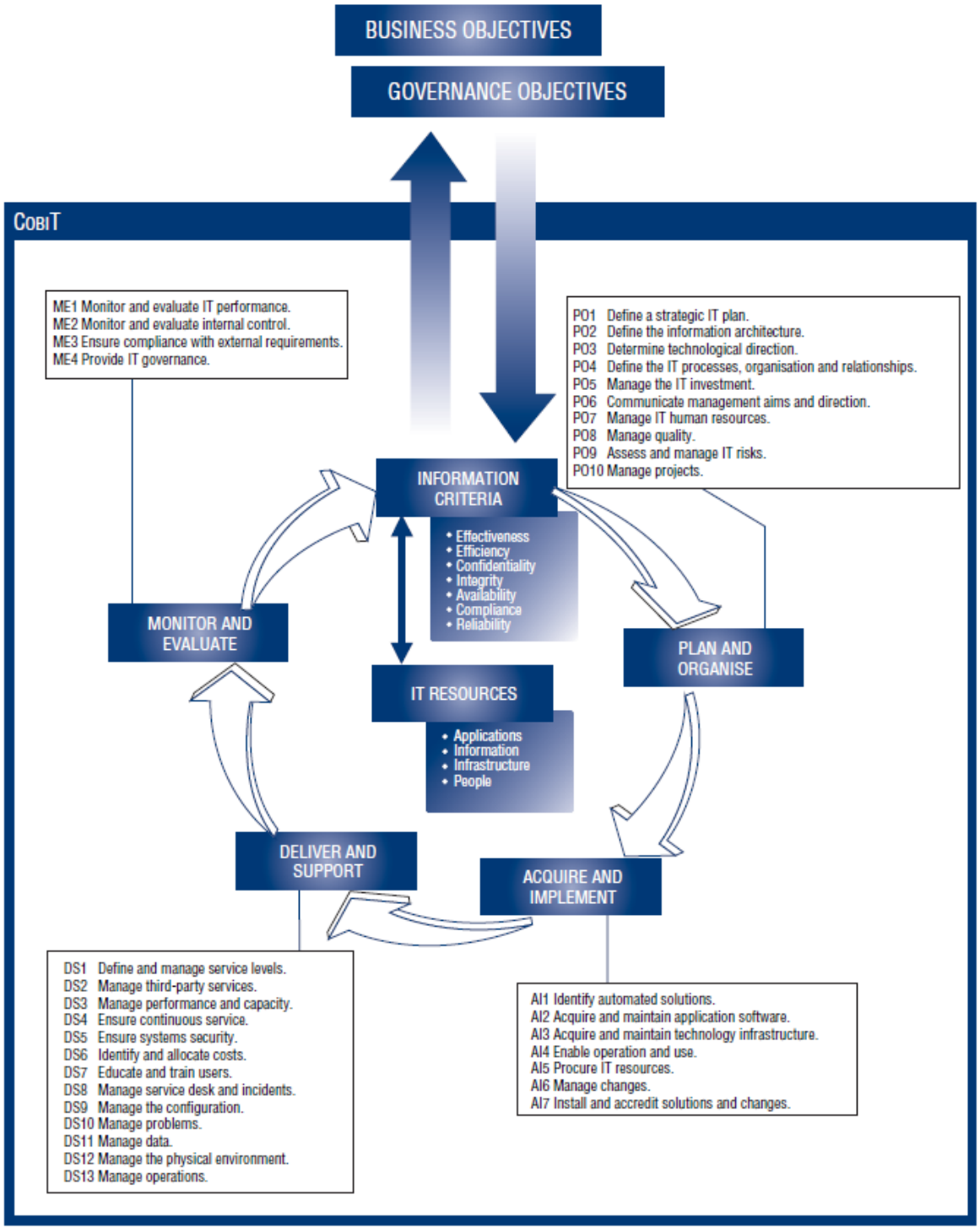
Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde, namentlich weil eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet (Art. 6 Abs. 1 DSG). Unter diesen Umständen können Personendaten nur ins Ausland bekannt gegeben werden, wenn eine der in Art. 6 Abs. 2 DSG aufgeführten Bedingungen erfüllt ist. In vielen Fällen wird der Cloud-Nutzer daher nicht umhin kommen, mit dem Cloud-Service-Anbieter (unter Einbezug allfälliger Subunternehmer) vertragliche Datenschutzgarantien abzuschliessen. Dabei besteht die praktische Schwierigkeit, dass alle Teilnehmer in der Cloud, auf deren Rechner personenbezogene Daten bearbeitet werden, vertraglich eingebunden werden müssen. Es ist zu bedenken, dass grundsätzlich derjenige, welcher Personendaten ins Ausland übermittelt, nachweisen muss, dass er alle erforderlichen Massnahmen getroffen hat, um ein angemessenes Schutzniveau zu gewährleisten.

4. Schliesslich ist der Cloud-Nutzer auch dafür verantwortlich, dass das Auskunftsrecht nach Art. 8 DSG und das Recht auf Löschung und Berichtigung nach Art. 5 DSG jederzeit gewährleistet sind und entsprechend den datenschutzrechtlichen Vorgaben umgesetzt werden. Die Einhaltung dieser Erfordernisse kann mit erheblichen Schwierigkeiten verbunden sein, da mit der Nutzung von Cloud-Anwendungen wie erwähnt oftmals ein Kontrollverlust über die Daten einhergeht und der Cloud-Nutzer nicht (mehr) weiss, wo welche Daten bearbeitet werden. Er kann sich von diesen gesetzlichen Pflichten jedoch nicht befreien.

Quelle: (Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB), 2011)

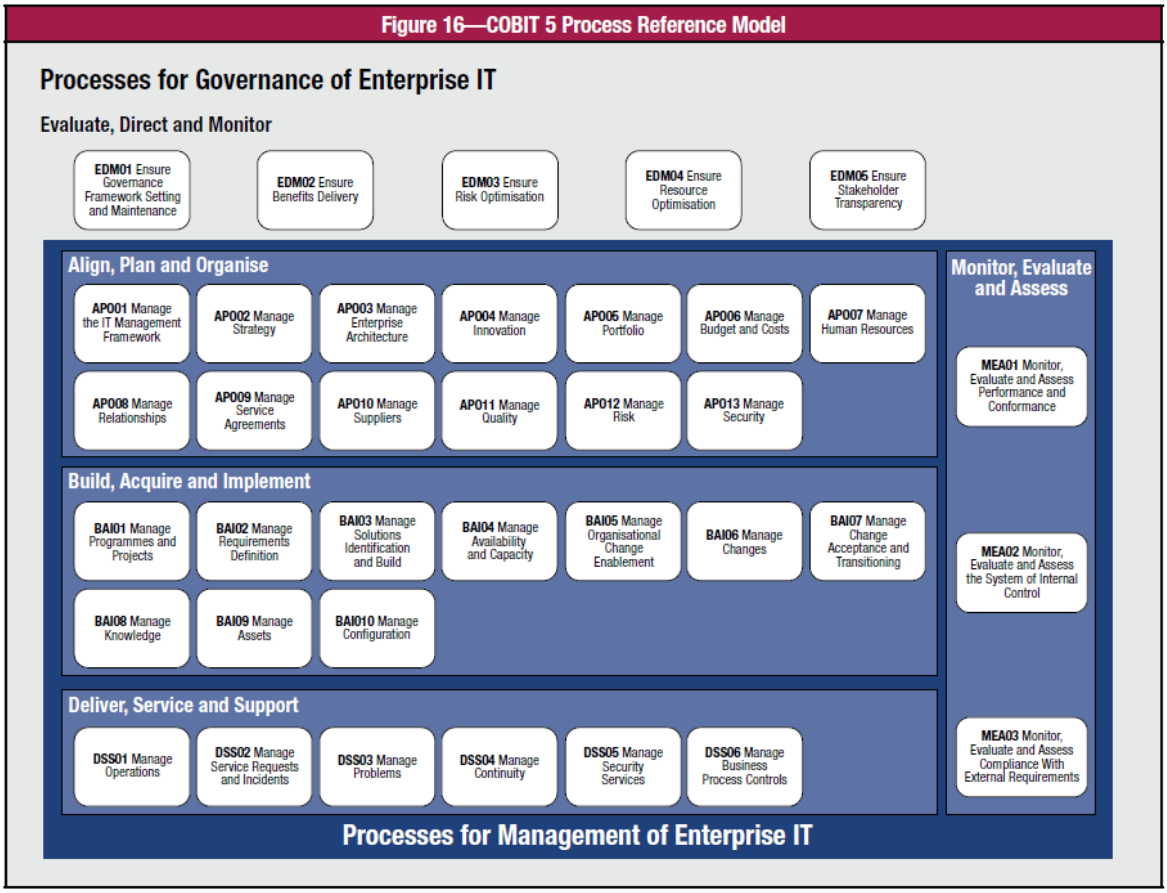
7.2 COBIT Prozess Modelle

Abbildung 21 – COBIT 4.1 Prozesse



Quelle: (IT Governance Institute, 2007) Figure 24

Abbildung 22 – COBIT 5 Process Reference Model



Quelle: (ISACA, 2012) Figure 16

7.3 Aufgaben, Kompetenzen und Verantwortung der Rollen

Tabelle 11 – Aufgaben, Kompetenzen und Verantwortung der Rollen in einer Community Cloud

Rolle	Aufgabe	Kompetenz	Verantwortung
Leistungsbezüger	Kann den Service innerhalb der vorgegeben Richtlinien beziehen Entschädigt den Leistungserbringer	Kennt seine Anforderungen und Regulationen	Misst und überwacht die Leistung
Leistungserbringer	Erbringt die Leistung innerhalb der definierten Richtlinien	Hat das entsprechende Know-How und Mittel, um die Leistung sicherzustellen.	Gewährleistung der Erfüllung des SLA, besonders der Vertraulichkeit
Broker	Berät den Leistungsbezüger	Kennt die Angebote auf dem Markt	Tritt als unabhängiger Berater auf.
Konsortium	Erstellt Richtlinien, welche die Anforderungen der Leistungsbezüger berücksichtigen und die Möglichkeiten des Leistungserbringers berücksichtigen. Vertritt die Leistungsbezüger und Leistungserbringer Vertreter.	Kennt die Anforderungen der Leistungsbezüger	Vertritt die Anforderungen des Konsortiums und keine eigenen Interessen.

Quelle: Eigene Darstellung

7.4 COBIT und ITIL in der Community Cloud

Tabelle 12 – COBIT und ITIL in der Community Cloud

COBIT 4.1

Area	Prozesse	LB	LE	Community
Plan and Organise	PO1 Define a Strategic IT Plan			A;R
Plan and Organise	PO2 Define the Information Architecture	A	R	
Plan and Organise	PO3 Determine Technological Direction		A;R	
Plan and Organise	PO4 Define the IT Processes, Organisation and Relationships			A;R
Plan and Organise	PO5 Manage the IT Investment		A;R	
Plan and Organise	PO6 Communicate Management Aims and Direction			A;R
Plan and Organise	PO7 Manage IT Human Resources		A;R	
Plan and Organise	PO8 Manage Quality			A;R
Plan and Organise	PO9 Assess and Manage IT Risks			A;R
Plan and Organise	PO10 Manage Projects		A;R	
Acquire and Implement	AI1 Identify Automated Solutions		A;R	
Acquire and Implement	AI2 Acquire and Maintain Application Software		A;R	
Acquire and Implement	AI3 Acquire and Maintain Technology Infrastructure		A;R	
Acquire and Implement	AI4 Enable Operation and Use		A;R	
Acquire and Implement	AI5 Procure IT Resources		A;R	
Acquire and Implement	AI6 Manage Changes	I	A;R	
Acquire and Implement	AI7 Install and Accredit Solutions and Changes	I	A;R	
Deliver and Support	DS1 Define and Manage Service Levels		R	A
Deliver and Support	DS2 Manage Third-party Services	I	R	A
Deliver and Support	DS3 Manage Performance and Capacity		A;R	
Deliver and Support	DS4 Ensure Continuous Service		A;R	
Deliver and Support	DS5 Ensure Systems Security		A;R	
Deliver and Support	DS6 Identify and Allocate Costs		A;R	
Deliver and Support	DS7 Educate and Train Users			A;R
Deliver and Support	DS8 Manage Service Desk and Incidents		A;R	
Deliver and Support	DS9 Manage the Configuration		A;R	
Deliver and Support	DS10 Manage Problems		A;R	
Deliver and Support	DS11 Manage Data		A;R	
Deliver and Support	DS12 Manage the Physical Environment		A;R	
Deliver and Support	DS13 Manage Operations		A;R	
Monitor and Evaluate	ME1 Monitor and Evaluate IT Performance		A;R	
Monitor and Evaluate	ME2 Monitor and Evaluate Internal Control		A;R	
Monitor and Evaluate	ME3 Ensure Compliance With External Requirements			A;R
Monitor and Evaluate	ME4 Provide IT Governance			A;R

ITIL v3

Area	Prozesse	LB	LE	Community
Service Strategy	Strategy Generation	R	R	A
Service Strategy	Financial Management		R	A
Service Strategy	Service Portfolio Management			A
Service Strategy	Demand Management	R		A
Service Design	Service Level Management	I	A	
Service Design	Service Catalogue Management	R	R	A
Service Design	Information Security Management	I	R	A
Service Design	Supplier Management	I	R	A
Service Design	IT Service Continuity Management		A	
Service Design	Availability Management		A	
Service Design	Capacity Management		A	
Service Transition	Knowledge Management		A, R	
Service Transition	Change Management	C, I	A, R	
Service Transition	Service Asset and Configuration Management		A, R	
Service Transition	Transition Planning and Support		A, R	
Service Transition	Release and Deployment Management		A, R	
Service Transition	Service Validation and Testing	R	A, R	
Service Transition	Evaluation		A, R	
Service Operation	Funktion: Service Desk		A, R	
Service Operation	Funktion: Technical Management		A, R	
Service Operation	Funktion: IT Operations Management		A, R	
Service Operation	Funktion: Application Management		A, R	
Service Operation	Incident Management		A, R	
Service Operation	Request Fulfillment		A, R	
Service Operation	Event Management		A, R	
Service Operation	Access Management		A, R	
Service Operation	Problem Management		A, R	
Continual Service Improvement	The 7-Step Improvement Process			A
Continual Service Improvement	Service Reporting		A, R	
Continual Service Improvement	Measurement		A, R	
Continual Service Improvement	Business Questions for CSI			A
Continual Service Improvement	Return on Investment for CSI			A

LB: Leistungsbezüger
LE: Leistungserbringer
Community: beinhaltet die gesamte Community
Responsible – verantwortlich (Durchführungsverantwortung), zuständig für die eigentliche Durchführung. Die Person, die die Initiative für die Durchführung (durch Andere) gibt oder die die Aktivität selbst durchführt. Wird auch als Verantwortung im disziplinarischen Sinne interpretiert.
Accountable – rechenschaftspflichtig (Kostenverantwortung), verantwortlich im Sinne von „genehmigen", „billigen" oder „unterschreiben". Die Person, die im rechtlichen oder kaufmännischen Sinne die Verantwortung trägt. Wird auch als Verantwortung aus Kostenstellensicht interpretiert.
Consulted – konsultiert (Fachverantwortung). Eine Person, deren Rat eingeholt wird. Wird auch als Verantwortung aus fachlicher Sicht interpretiert.
Informed – zu informieren (Informationsrecht). Eine Person, die Informationen über den Verlauf bzw. das Ergebnis der Tätigkeit erhält, oder die Berechtigung besitzt, Auskunft zu erhalten.

Quelle: Eigene Darstellung

7.5 Übersicht Cloud-Standards

Abbildung 23 – Übersicht der 20 "Cloud-Standards"

Fokus		Standards, Zertifizierungen, Vorgaben und Vorarbeiten	Ähnliche	Initiator
Technik	CC	CCRA (Cloud Computing Reference Architecture): Referenzarchitektur für Cloud Service Angebote	Referenzarchitekturen der NIST oder des BSI	TOG
	CC	CDMI (Cloud Data Management Interface): API zum Zugriff auf Daten in IaaS, DaaS Szenarios	XAM, iSCSI, NFS, WebDAV	SNIA
	CC	Cloud Audit (Automated Audit, Assertion, Assessment, and Assurance API): API zum Zugriff auf Auditinformationen	SCAP	CSA
	CC	CTP (Cloud Trust Protocol): Einheitliche Techniken und Nomenklatur zur Erhöhung der Transparenz	SCAP, OCRL	CSA
	CC	OCCI (Open Cloud Computing Interface): API zum Management von Clouds (insb. IaaS)	DeltaCloud, Libcloud, APIs von EC2, Rackspace, Eucalyptus, vCloud u.w.	OGF
	CC	OpenStack (OpenStack Cloud Software): Rahmenwerk zum Aufbau von Cloud-Infrastrukturen	OpenNebula, Nimbus (Schnittstellen: CMDI, OCCI, OVF)	(Diverse)
	IKT	CIMSVM (CIM System Virtualization Model): Objektmodel und Schnittstellen für Virtuelle Systeme & Komponenten	–	DMTF
	IKT	Hive (Apache Hive): Programmiermodell für Datenabfragen	JAQL, PIG	Apache
	IKT	OAuth (Web Authorization Protocol): Protokoll und Schnittstelle zum Identitätsmanagement	OpenID, WS-Federation, SAML	IETF
	IKT	OVF (Open Virtualization Format): Dateiformat für Virtuelle Maschinen	AMI, EMI	DMTF, ANSI, ISO
	IKT	SCAP (Security Content Automation Protocol): Protokoll und Schnittstelle zum Abruf von Sicherheitsinformationen	CloudAudit	NIST
	IKT	USDL (Unified Service Description Language): Beschreibungssprache für virtuelle Dienstleistungen	WSDL, UDDI, WADL, OWL-S, SNN, WSMO, e3Value, PAS1018 u.w.	W3C
	IKT	WS-* (Web Service Standards): Spezifikationen, Standards und Normen für Web Services	WSDL, WS-Policy, WS-Agreement, WS-Security, WS-I u.w.	OASIS, OGF, W3C
Management	CC	BSI-ESCC (Eckpunktepapier Sicherheitsempfehlungen für Cloud Computing Anbieter): Leitfaden	Andere Anforderungsdokumente	BSI
	CC	EuroCloud-SA (EuroCloud Star Audit): Zertifikat für Anbieter von Cloud-Diensten	EuroPriSe, TiC	EuroCloud
	CC	GRC-Stack (Governance, Risk Management and Compliance Stack): Rahmenwerk zu Bewertungdes Risikos von Cloud Anbietern	CloudAudit, CCM, CAIQ, CTP	CSA
	CC	NIST-UC (Cloud Computing Use Cases): Leitfaden für Anwendungsfälle im Cloud Computing mit Fokus auf US-Behörden	Use Cases von OGF oder DMTF	NIST
	Allg.	SSAE-16 (Statement on Standards for Attestation Engagements No. 16): Zertifikat für Anbieter von Cloud-Diensten	CobiT, BSI-100, ISAE 3402, ITIL, SAS 70, IDW PS 330/951/FAIT1	AICPA
Recht	CC	OCM (Open Cloud Manifesto): Selbstverpflichtung zu Offenheit für Cloud-Anbieter	–	(Diverse)
	Allg.	95/46/EG (EU-Richtlinie 95/46/EG „Datenschutzrichtlinie"): Datenschutzvorgaben der EU	BDSG, Datenschutzgesetze der Länder, Safe Harbor	EU

Quelle: (Bundesministerium für Wirtschaft und Technologie (BMWi), 2012), Abbildung 8, Seite 10

7.6 Abbildungsverzeichnis

7.7 Tabellenverzeichnis

7.8 Quellenverzeichnis

Amazon Web Service. (2012). *AWS Case Study: swisstopo*. Abgerufen am 26. März 2012 von Amazon: http://aws.amazon.com/de/solutions/case-studies/swisstopo/

Bon, J. v. (2009). *Foundations in IT Service Management basierend auf ITIL V3.* Zaltbommel: Van Haren Publishing.

Bundesamt für Sicherheit und Informationstechnik (BSI). (Februar 2012). *Sicherheitsempfehlungen für Cloud Computing Anbieter.* Abgerufen am 25. April 2012 von Bundesamt für Sicherheit und Informationstechnik (BSI): https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindestanforderungen/Eckpunktepapier-Sicherheitsempfehlungen-CloudComputing-Anbieter.pdf?__blob=publicationFile

Bundesministerium für Wirtschaft und Technologie (BMWi). (2012). *Das Normungs- und Standardisierungsumfeld von Cloud Computing.* Berlin: BMWi.

Carr, N. (2008). *The Big Switch: Rewiring the World, from Edison to Google.* New York: W. W. Norton & Company Inc.

Computerworld. (20. April 2012). Swiss IT, Die CIO-Agenda 2012. *Computerworld*, S. 29.

Deloitte. (2005). *Calling a Change in the Outsourcing Market.* Abgerufen am 08. März 2012 von Deloittle: http://www.deloitte.com/assets/Dcom-Luxembourg/Local%20Assets/Documents/Global_brochures/us_outsourcing_callingachange.pdf

Die Bundesbehörden der Schweizerischen Eidgenossenschaft. (1. Januar 2011). *Bundesverfassung der Schweizerischen Eidgenossenschaft.* Abgerufen am 29. April 2012 von http://www.admin.ch/ch/d/sr/101/a43a.html

Die Bundesbehörden der Schweizerischen Eidgenossenschaft. (09. Dezember 2011). *Verordnung über die Informatik und Telekommunikation in der Bundesverwaltung.* Abgerufen am 2012. Mai 02 von http://www.admin.ch/ch/d/sr/172_010_58/index.html

Die Bundesbehörden der Schweizerischen Eidgenossenschaft. (01. Januar 2012). Bundesgesetz über das öffentliche Beschaffungswesen.

eCH. (24. Februar 2005). *eCH-0037: GEVER Vorgaben Bund.* Abgerufen am 26. April 2012 von Verein eCH E-Government Standards: http://www.ech.ch/vechweb/page?p=dossier&documentNumber=eCH-0037&documentVersion=1.00

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB). (Oktober 2011). *Erläuterungen zu Cloud Computing.* Abgerufen am 2012. April 28 von Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB): http://www.edoeb.admin.ch/themen/00794/01124/01768/index.html?lang=de&download=NHzLpZeg7t,lnp6I0NTU042l2Z6ln1acy4Zn4Z2qZpnO2Yuq2Z6gpJCDdYR_gmym162epYbg2c_JjKbNoKSn6A--Z6gpJCDdYR_gmym162epYbg2c_JjK

EuroCloud. (Dezember 2010). *Saas Star Audit.* Abgerufen am 02. April 2012 von EuroCloud Star Audit – SaaS: http://www.saas-audit.de/files/2011/03/quick-reference_de.pdf

EuroCloud Deutschland_eco. (kein Datum). *Über uns*. Abgerufen am 25. April 2012 von EuroCloud Deutschland_eco: http://www.eurocloud.de/ueber-uns/

EuroCloud Swiss. (März 2012). *Leitfaden Cloud Computing Risk & Compliance.* Abgerufen am 28. April 2012 von EuroCloud Swiss: http://www.eurocloudswiss.ch/images/stories/brochures/2012_EuroCloud_Leitfaden_CH_final_b.pdf

Fischer, M. (2012). Gap analysis & recommendations. *Cloud Computing Workshop 2012* (S. Folie 4). Rüschlikon: SATW.

Forester Reserch. (12. Dezember 2008). *Definitionen für Cloud Computing.* Abgerufen am 2012. November 15 von Computerwoche: http://www.computerwoche.de/management/cloud-computing/1881561/index7.html

Gartner. (07. Juli 2011). *Gartner Newsroom*. Abgerufen am 15. November 2011 von Gartner: http://www.gartner.com/it/page.jsp?id=1739214

IDABC. (2004). *EUROPEAN INTEROPERABILITY FRAMEWORK*. Abgerufen am 02. April 2012 von Europäische Kommission: http://ec.europa.eu/idabc/servlets/Docd552.pdf?id=19529

ISACA. (10 2009). *Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives.* Abgerufen am 10. April 2012 von ISACA:

http://www.isaca.org/Knowledge-Center/Research/Documents/Cloud-Computing-28Oct09-Research.pdf?id=c6508bea-eb36-4a4f-92f4-9512cfa0004e

ISACA. (2012). *COBIT 5 - A Business Framework for the Governance and Management of Enterprise IT.* Rolling Meadows: ISACA.

ISSS Information Security Society Switzerland. (24. November 2011). *14. ISSS Berner Tagung für Informationssicherheit*. Abgerufen am 17. Februar 2012 von Information Security Society Switzerland: https://www.isss.ch/veranstaltungen/2011/14-berner-tagung/

IT Governance Institute. (2007). *COBIT 4.1, Framework, Control Objectives, Management Guidelines, Maturity Models.* IT Governance Institute.

Johannsen, W., & Goeken, M. (2011). *Referenzmodelle für die IT-Governance.* Heidelberg: dpunkt.

Kundra, V. (08. Februar 2011). *Federal Cloud Computing Strategy*. Abgerufen am 26. März 2012 von cio.gov: http://www.cio.gov/documents/federal-cloud-computing-strategy.pdf

Maglić, I. (19. April 2012). *Präsentation Cloud & Mobility.* Abgerufen am 02. Mai 2012 von CIO's View on IT Industry's Reshaping Trends: http://www.qss.ba/doc/eday2012/?id=595

Müller, W. (16. November 2009). *B1.06 -E-Government-Architektur Schweiz 2. ffO-Meeting.* Abgerufen am 29. April 2012 von E-Government Schweiz: http://www.egovernment.ch/dokumente/veranstaltungen/ffo-2009-2/ffO-Meeting_B1_06.pdf

Müller, W., Dischl, J., & Widmer, U. (2011). *Cloud-Computing-Strategie Schweizer Behörden - Entwurf.*

NIST, National Institute of Standards and Technology. (März 2006). *Minimum Security Requirements for Federal Information and Information Systems*. Abgerufen am 26. März 2012 von NIST: http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

NIST, National Institute of Standards and Technology. (August 2009). *Recommended Security Controls for Federal Information Systems and Organizations*. Abgerufen am 26. März 2012 von NIST: http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

NIST, National Institute of Standards and Technology. (2011). *The NIST Definition of Cloud Computing.* Gaithersburg: U.S Department of Commerce.

openexpo. (2010). *Hanspeter Christ und Dr. David Oesch: OSS & CloudComputing: der Motor für das Geoportal Bund*. Abgerufen am 26. März 2012 von http://www.youtube.com/watch?v=33O3TrWyFO8

Ritz, Rieder, & Jenzer. (1999). Die Evaluation des Projektes „Führen mit Leistungsauftrag und Globalbudget FLAG“. *Verwaltungsreform in der Schweiz – eine Zwischenbilanz*, S. 203-244.

Rüter, A., Schröder, J., Göldner, A., & Niebuhr, J. (2010). *IT-Governance in der Praxis.* Berlin: Springer.

Saugatuck Technology. (12. Dezember 2008). *Definitionen für Cloud Computing.* Abgerufen am 2011. November 15 von Definitionen für Cloud Computing: http://www.computerwoche.de/management/cloud-computing/1881561/index7.html

University of California. (2012). *SETI@home*. Abgerufen am 17. März 2012 von SETI@home: http://setiathome.berkeley.edu/

Walser, K., & Breidung, M. (2010). *Vergleichende Analyse des IT-Service-Providing in der Öffentlichen Verwaltung in Deutschland und der Schweiz.* Bern: Berner Fachhochschule.

7.9 Selbständigkeitserklärung

Ich bestätige, die vorliegende Arbeit selbständig verfasst zu haben.

Sämtliche Textstellen, die nicht von mir stammen, sind als Zitate gekennzeichnet und mit dem genauen Hinweis auf ihre Herkunft versehen.

Die verwendeten Quellen (gilt auch für Abbildungen, Grafiken u.ä.) sind im Literatur- bzw. Quellenverzeichnis aufgeführt.

Unterschrift:

Olivier Brian