



Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD  
**Informatiksteuerungsorgan des Bundes ISB**  
IKT -Planung und -Steuerung

Willy Müller, 28. Oktober 2013

---

# Studie „Cloud Labeling“

Erstellt im Auftrag des Informatiksteuerungsorgans des Bundes durch die  
CBusiness Services GmbH und die Fachhochschule Nordwestschweiz  
Oktober 2013

---

## Inhaltsverzeichnis

<b>1</b>	<b>Ausgangslage .....</b>	<b>3</b>
<b>2</b>	<b>Projektgegenstand .....</b>	<b>4</b>
2.1	Die Gov–Cloud Strategie .....	4
2.2	Datensicherheit .....	4
2.2.1	Allgemein.....	4
2.2.2	Datenschutz Schweizer Behörden .....	5
<b>3</b>	<b>Methodik.....</b>	<b>6</b>
<b>4</b>	<b>Definition Labeling und Zertifizierung .....</b>	<b>6</b>
4.1	Label / Labeling.....	7
4.2	Zertifizierung / Zertifikat .....	8
4.3	Bestehende Labels .....	9
4.4	Bestehende Zertifizierungen .....	10
4.5	Vor- und Nachteile von Labels .....	11
4.6	Vor- und Nachteile von Zertifizierungen.....	12
<b>5</b>	<b>Cloud Service Qualität (CSQ) .....</b>	<b>12</b>
5.1	Kunden Hemmnisse.....	12
5.2	Kriterien für Cloud Service Anbieter.....	14
5.3	Kriterien der Klassifikation.....	14
<b>6</b>	<b>Gegenüberstellung der definierten Kriterien und vorhandener Ansätze</b>	<b>15</b>
6.1	Labels .....	16
6.2	Zertifizierungen .....	16
<b>7</b>	<b>Mapping und Bewertung der erhobenen Varianten.....</b>	<b>18</b>
<b>8</b>	<b>Potenzialabschätzung .....</b>	<b>19</b>
<b>9</b>	<b>Empfehlungen.....</b>	<b>20</b>
9.1	Labels .....	20
9.2	Zertifizierung .....	20
9.3	Datenschutz und weitere Massnahmen.....	20

# 1 Ausgangslage

Die Entwicklung der globalen Wirtschaft und neue Technologien führen dazu, dass die Anforderungen an IT-Lösungen und deren Rahmenbedingungen immer umfangreicher und komplexer werden. Gleichzeitig sind Unternehmen, Institutionen und Organisationen einerseits gefordert effizienter, flexibler und innovativ zu sein, andererseits wettbewerbsfähig zu bleiben und immer schneller neue Produkte und Dienstleistungen zu entwickeln und auf den Markt zu bringen.

Auf Grund dieser Entwicklung sind die IT-Unternehmen gefordert neue Lösungen und neue Produkte zu entwickeln. Für die Entstehung von Cloud Computing waren Virtualisierungs- und Automatisierungstechnologien, sowie enorme Steigerungen in Rechner-, und Speicherleistungen, neue Softwareprodukte und eine flächendeckende Verfügbarkeit von höheren Bandbreiten erforderlich. Als Synthese dieser neuen IT- und Telekommunikations-Umgebungen sind mit Cloud Computing Service auf drei verschiedenen Ebenen, IaaS (Infrastructure as a Service), PaaS (Platform as a Service) und SaaS (Software as a Service) entstanden.

Der Begriff Cloud Computing steht aber auch für einen Evolutionsschritt der ICT in die vierte industrielle Revolution, die bereits begonnen hat. Diese wird beschrieben als die Zeit in welcher „Autonome Produkte und Entscheidungsprozesse, Wertschöpfungsnetzwerke in nahezu Echtzeit gesteuert werden“. In diesem Zeitalter werden Waren, Dienstleistungen und Menschen miteinander über das Internet verbunden. Aus dieser Definitionen ist erkennbar, dass das Internet sowohl für Privatpersonen wie Unternehmen immer mehr im Zentrum steht.

Die Evolution der ICT hat nicht nur Einfluss auf die Technologie sondern betrifft auch andere Bereiche, wie z.B. das soziale Verhalten der Menschheit, die Gesetzgebungen, den Datenschutz, Cyberkriminalität etc. und somit verändert sich auch der Einsatz und die Nutzung der IT in Unternehmen.

Um dieser Entwicklung zu begegnen wurden deshalb digitale Agenden (z.B. von der EU und von CH) entwickelt. Auf Basis der digitalen Agenda der EU hat die Europäische Kommission eine Cloud-Strategie entwickelt mit folgenden Zielen (siehe auch Anhang):

- Cloud-Standards zu entwickeln
- Gewissheit für Nutzer zu schaffen, dass Daten zwischen Rechnerwolken übertragen oder ganz abgezogen werden können
- EU-weite Zertifizierung vertrauenswürdiger Cloud-Anbieter
- Musterverträge für das Cloud Computing zu erstellen, die rechtliche Verpflichtung klar darstellen
- Eine europäische Cloud-Partnerschaft zwischen dem öffentlichen Sektor und der Industrie, um Bedarf zu ermitteln und zu gewährleisten, dass der europäische IT-Sektor diesen decken kann. Dies soll die europäischen Unternehmen im Wettbewerb mit ausländischen (v.a. US-amerikanischen) Firmen stärken.

Parallel dazu wurde in der Schweiz die Gov-Cloud Strategie entwickelt. Mit der Umsetzung dieser Strategie wurde die Firma CBusiness Services GmbH in Kooperation mit der Fachhochschule Nordwestschweiz (FHNW) beauftragt die Studie „Labeling“ zu erstellen.

## 2 Projektgegenstand

### 2.1 Die Gov-Cloud Strategie

Die Cloud-Strategie ergänzt die E-Government-Strategie der Schweiz im Hinblick auf den Einsatz von Cloud-Computing. Sie beschreibt, wie die Schweizer Behörden mit den neu entstehenden Möglichkeiten umgehen wollen und welche Massnahmen zu treffen sind, damit die mit dem Cloud-Einsatz einhergehenden Risiken minimiert und die sich damit eröffnenden Chancen insbesondere auch zur Unterstützung von E-Government genutzt werden können. Ergänzt wird sie durch einen Katalog der Umsetzungsmassnahmen.

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. Gemäss Vision der Strategie tun sie 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.

Die Ziele der Gov-Cloud Strategie sind:

- Die Behörden von Bund, Kantonen und Gemeinden können Cloud-Angebote einfach und ohne grossen Aufwand evaluieren.
- Die Behörden sind sensibilisiert für die Risiken des Cloud-Einsatzes und können beurteilen, ob ein Angebot ihre Sicherheitsanforderungen erfüllt.
- Sie nutzen schrittweise die Möglichkeiten, um ihre Effizienz und Effektivität zu steigern und die Kosten zu minimieren.
- Die IKT-Leistungserbringer verfügen über das nötige Know-how, um selbst Cloud-Dienste zu nutzen, bereitzustellen und ihre Kunden bei der Auswahl von Cloud-Diensten zu beraten.

Zur Unterstützung der Strategieziele soll der Einsatz und Nutzen eines Labels oder einer Zertifizierung geprüft werden.

### 2.2 Datensicherheit

#### 2.2.1 Allgemein

Die Datensicherheit ist mit dem Einsatz und der Nutzung von Cloud Services auf allen Ebenen geprägt durch physische, logische und organisatorische Massnahmen. Vor allem sind es aber Technologische, wie auch Management und Rechtliche Aspekte, welche den Datenschutz ausmachen. Auf Grund der vielfachen

Herausforderungen bei Cloud Services sind auch Standards gefragt. Die folgende Abbildung (Studie Booz & Company 2013), gibt einen Überblick über die Herausforderungen und vorhandenen Standards.

Field	Type of Challenges	Examples
<b>Technology</b>	File & exchange format	OVF, EC2, USDL, CIM SVM...
	Programming models	MapReduce, JAQL, PIG, HIVE
	Protocols & interfaces	OCCI, CDMI, CloudAudit, Google DLF, ..
	Standard components & reference architectures	OpenStack, OSGI, NIST RM, IBM RM, DMTF, CTP, ...
	Benchmarks & tests	Benchmarking Suites, Security Assessment, .
<b>Management</b>	Business models	IaaS, PaaS, SaaS operating models, ...
	Service Level Agreements	WS-Agreement, Business SLAs, ...
	Condition of contracts	EVB-IT, EU SVK, components for AGB, EULA
	Management models & processes	ISO 27001/27002, ITIL, COBIT, ...
	Controlling models & processes	SSAE, SAS 70, ....
	Guidelines	BSI requirements, NIST UC, EuroCloud LRD&C
<b>Legal</b>	Legal requirements	EU data protection directive, BDSG, Safe Harbor
	Voluntary commitments	Open Cloud Manifesto, ...
	Company policies	Internal policies, ...

Quelle: Booz & Company und FZI (2012)

Auf technischer Ebene sind es dabei vor allem Standards, welche in den Bereichen Austauschformate, Protokolle etc. als Herausforderung gelten. Im Management sind es Prozessanforderungen, Controlling und Richtlinien und im rechtlichen Bereich sind es unterschiedliche Vorgaben. So gibt es hier einerseits staatliche Vorgaben, aber auch beispielsweise branchenspezifische Richtlinien und schlussendlich Firmeninterne Regelungen, welchen Beachtung bezüglich Sicherheit und Datenschutz verdienen.

### 2.2.2 Datenschutz Schweizer Behörden

Das schweizerische Datenschutzgesetz umfasst den Schutz der Daten sowohl für Bundesbehörden als auch für Privatpersonen. Für kantonale Behörden gilt das individuelle kantonale Datenschutzgesetz. Die Durchführung und Einhaltung dieser kantonalen Gesetze wird nicht durch den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten kontrolliert. Dafür sind die jeweiligen Kantone selbst zuständig. Auch auf Gemeindeebene können individuelle Ausprägungen zum Datenschutz festgelegt werden.

Dies führt dazu, dass im öffentlichen Bereich viele verschiedene Auslegungen des Datenschutzes bestehen und dessen Einhaltung nur mit enormem Aufwand gewährleistet werden kann.

### 3 Methodik

Das angestrebte Lösungskonzept für die Studie „Labeling“ umfasst drei verschiedene Phasen. Aufbauend auf den ersten beiden Phasen, werden in der dritten Phase Empfehlungen für die Behörden und den Schweizer Markt abgegeben. Die einzelnen Phasen werden wie folgt erarbeitet:

#### 1. *Phase: Datenanalyse und Kriterienkatalog*

Diese erste Phase umfasst das Sichten und Sammeln von Information über:

- die Begriffe Label und Zertifizierung
- bestehende Cloud-Labeling- und Zertifizierungskonzepte. Ebenso werden dahingehende Vorhaben, welche in der Planung sind berücksichtigt.
- Studien und Informationen zusammengetragen, aus welchen die Herausforderungen an Cloud Services hervorgehen.

Mit den Informationen über die Herausforderungen bei Cloud Services wird ein Kriterienkatalog erstellt, durch welchen die nachfolgende Evaluation der gefundenen Labels/Zertifizierungen bewertet wird.

#### 2. *Phase: Akzeptanz von Labels/Zertifizierungen und Marktpotenziale*

Durch die Bewertung von Vor- und Nachteilen solcher Labels/Zertifizierungen aus Sicht des Kunden, sowie durch die Vorarbeiten in ähnlichen Projekten werden Einschätzungen über die Akzeptanz einer solchen Zertifizierung für potenzielle Nutzer und Anbieter auf dem Schweizer Markt gemacht.

Auf Grund diverser bestehender aktueller Studien und der vorhergehend Akzeptanzeinschätzung wird eine Einschätzung der Potenziale für Schweizer Cloud Services abgeleitet. So können beispielsweise Prognosen über den Schweizer Cloud Computing Markt sowie Ämterverzeichnisse als Grundlage für eine Entwicklungsabschätzung von zukünftigen Labels/ Zertifizierungslösungen herangezogen werden.

#### 3. *Phase: Empfehlungen*

Abgeleitet von den vorhergängig gesammelten Informationen und Bewertungen werden Empfehlungen für das weitere Vorgehen von Cloud-Label/Zertifizierung bei den Behörden und in der Schweiz gemacht.

### 4 Definition Labeling und Zertifizierung

Die Begrifflichkeiten Label/Labeling und Zertifizierung/Zertifikat werde oftmals unterschiedlich verstanden oder sogar verwechselt. Dieses Kapitel soll eine Grundlage schaffen, welche das weitere Verständnis der Begriffe auf einen Nenner bringt. Dadurch wird ein gemeinsames Verständnis der Problematik sichergestellt.

## 4.1 Label / Labeling

Verschiedene Definitionen eines Labels weisen darauf hin, dass ein solches für verschiedene Ausprägungen ausgelegt werden kann. So beschreibt beispielsweise [www.label-online.de](http://www.label-online.de) dass:

- **Eigenmarken sind firmeneigene Labels.** Sie werden von den Herstellern selbst entwickelt und kennzeichnen mindestens eine Produktlinie.
- Gütezeichen sind Zeichen, die nach einem besonderen Prüfverfahren als Gütezeichen anerkannt worden sind und somit den „Grundsätzen für Gütezeichen“ entsprechen. Der Begriff ist wettbewerbsrechtlich geschützt.
- **Als Prüfzeichen werden die Labels bezeichnet, die von wissenschaftlich-technischen Instituten vergeben werden.** Es wird hierbei geprüft, ob das Produkt die sicherheitstechnischen Anforderungen erfüllt und gebrauchstauglich ist (z.B. VDE-Zeichen, GS-Zeichen, TÜV-Prüfzeichen u.a.). Bei den Prüfungen kann es sich sowohl um aufwendige Laboruntersuchungen als auch um stichprobenhafte Kontrollen der Produkte handeln.
- **Regionalzeichen oder Herkunftszeichen sind Labels,** die für Produkte vergeben, die in einer bestimmten Region hergestellt sind.
- **Umweltzeichen oder Öko-Labels sind produktbezogene Kennzeichen,** die sich auf die Umwelteigenschaften eines Produkts oder dessen Produktion beziehen. Sie finden sich auf Produkten, die z.B. umweltschonend hergestellt werden (z.B. Bio-Lebensmittel), sich durch geringe Schadstoffbelastungen auszeichnen oder besonders umweltfreundlich entsorgt werden können.

Das Eidgenössische Büro für Konsumentenfragen (BFK) legt in ihrer Definition den Schwerpunkt auf die freiwillige Beschriftung eines Produktes, welches den Kunden zur Information über einen bestimmten Mehrwert dienen soll:

Labels enthalten Angaben hinsichtlich eines oder mehrerer Merkmale, welche ein Produkt betreffen. Das Vorliegen dieser Merkmale dient jedoch nicht als Voraussetzung für das in Verkehr bringen. Somit sind Labels im Gegensatz zu Kennzeichnungsvorschriften freiwillige Beschriftungen eines Produktes oder einer Dienstleistung. Einerseits dienen sie als Hilfe zur Information des Konsumenten, der ein Produkt oder eine Dienstleistung in besserer Kenntnis auswählen kann. Andererseits sind sie marktwirtschaftliche Instrumente, die es erlauben, den Wert von gewissen Merkmalen eines Produktes oder einer Dienstleistung hervorzuheben.

Labels bieten den Konsumentinnen und Konsumenten die Möglichkeit, bewusst Produkte oder Dienstleistungen mit Mehrwert zu kaufen resp. in Anspruch zu nehmen. Für das weitere Verständnis dieser Studie wird der Begriff Label wie folgt festgelegt.

### **Definition Label**

Ein Label wird grundsätzlich lediglich einmal vergeben. Die Einhaltung der Anforderungen wird nicht wiederholend bewertet. Ein Label kann über verschiedene Aspekte, wie Herkunft, Zusammensetzung, Qualität, Produktionsbedingungen eines Produktes oder Dienstleistung vergeben werden. Die Erteilung eines Labels erfolgt über eine Organisation und nicht über eine eigentliche Prüfungsstelle. Im Vergleich zu einer Zertifizierung ist ein Label eine stark abgeschwächte Form und besonders auf Marketingzwecke ausgerichtet.

## 4.2 Zertifizierung / Zertifikat

Ein Blick auf das Verständnis über Zertifizierungen zeigt unisono, dass es sich dabei um eine Art Überprüfung von unterschiedlichen, themenbezogenen Anforderungen handeln muss. So beschreibt Wikipedia die Zertifizierung wie folgt:

- Zertifizierung ist ein Teilprozess der Konformitätsbewertung. Zertifizierungen werden oft zeitlich befristet von unabhängigen Zertifizierungsstellen wie z. B. DQS, TÜV oder DEKRA vergeben und hinsichtlich der Standards unabhängig oder proprietär kontrolliert.

Durch ein ausgestelltes Zertifikat soll dabei bescheinigt werden, dass die Qualität eines Produktes oder einer Dienstleistung den gegebenen Anforderungen entspricht:

- Als Zertifikate oft auch Gütesiegel genannt, werden grafische oder schriftliche Produktkennzeichnungen bezeichnet, die eine Aussage über die Qualität, über eingehaltene Sicherheitsanforderungen oder Umwelteigenschaften machen sollen. **Als Zertifizierung wird ein Verfahren bezeichnet, mit welchem die Einhaltung solch bestimmter Anforderungen nachgewiesen wird.**
- Der Zweck dieser meist privatwirtschaftlich getragenen „Siegel“ bzw. „Zeichen“ soll sein, einerseits dem Verbraucher positive Hinweise über die Qualität oder Beschaffenheitsmerkmale eines Produktes zu liefern und andererseits den Hersteller eines Produktes als besonders vertrauenswürdigen Anbieter herauszustellen.

Das schweizerische Bauwesen kann beispielsweise das Minergie-Zertifikat, dieses wird wie folgt definiert: *Das Zertifikat ist der Qualitätsausweis für ein Produkt, das genau umschrieben und definiert ist. Es liefert klare Kenndaten als Sicherheit für Bauherren und Käufer und verschafft dem Eigentümer handfeste Vorteile*

Der Branchenverband schweizerischer Krankenversicherer, Santesuisse, sieht in einer Zertifizierung eine Konformitätsbestätigung, einen Qualitätsnachweis, welche über Anforderungen vordefiniert sein müssen. Sind diese Anforderungen ungenügend definiert, ist die Zertifizierung sinnlos. Eine Zertifizierung taugt nur dann, wenn sie auch der Verringerung oder Beherrschung von Risiken dient. In diesem Sinne soll das Zertifikat für Prozessqualität oder Outcome-Qualität. Dabei können Produkte, Dienstleistungen, Personal und Systeme zertifiziert werden.

Grundsätzlich können Zertifikate von einem Brand, durch eine Organisation oder einer Unternehmung festgelegt und ausgestellt werden. Werden dabei staatliche Anforderungen, wie beispielsweise zum Datenschutz berücksichtigt, so kann eine staatliche Anerkennung des Zertifikats erfolgen, was in der Schweiz eine Akkreditierung erfordert.

Für das weitere Verständnis dieser Studie wird der Begriff Zertifikat wie folgt festgelegt.



**Definition Zertifikat:**

Ein Zertifikat wird von einer unabhängigen Stelle geprüft und vergeben. Es legt grundsätzlich die Qualitätsstandards für ein Produkt, System oder eine Dienstleistung fest und ist zeitlich beschränkt. Eine Überprüfung der Einhaltung dieser Standards findet regelmäßig statt, wodurch die Erneuerung des Zertifikats gewährleistet werden kann. Die Zertifizierung ist dabei der Prozess, welcher durchlaufen werden muss, um an die Bescheinigung (das Zertifikat) zu gelangen.

Die folgende Tabelle gibt einen kurzen Überblick über die wesentlichen Unterschiede zwischen Label und Zertifikat:

	<b>Label:</b>	<b>Zertifikat:</b>
<b>Gültigkeit</b>	<ul style="list-style-type: none"> <li>- Regional</li> <li>- Umweltverträglichkeit</li> <li>- Qualität bestimmter Produkteigenschaften</li> <li>- Sozialverträglichkeit</li> </ul>	<ul style="list-style-type: none"> <li>- National und International</li> <li>- Produkt, Service – Eigenschaften</li> <li>- Einhaltung von Standards (offene und proprietäre)</li> <li>- Überprüfung von Erfüllung vorgeschriebener Anforderungen</li> </ul>
<b>Zeithorizont</b>	<ul style="list-style-type: none"> <li>- Wird meist einmalig geprüft, daher oft langfristig</li> </ul>	<ul style="list-style-type: none"> <li>- Befristet</li> <li>- Meist 2 – 4 Jahre</li> </ul>
<b>Auszeichnung</b>	<ul style="list-style-type: none"> <li>- Einmalige Überprüfung</li> </ul>	<ul style="list-style-type: none"> <li>- Wiederkehrende Überprüfung durch unabhängige Zertifizierungsstelle</li> </ul>

**4.3 Bestehende Labels**

- **Fujitsu Green IT:** Dieses Label macht auf den ersten Blick erkennbar, dass Produkte entsprechend den weitreichenden Unternehmensrichtlinien zu Energieeffizienz und Nachhaltigkeit entwickelt wurden. Dadurch können sich die Kunden einfach für umweltverträgliche Produkte entscheiden. Das Label verwendet ein einfaches dreistufiges System von einem Stern bis hin zu drei Sternen, um die Umweltverträglichkeit jedes Produktes darzustellen. Um ein Green IT Label zu bekommen, muss das Produkt eine umfassende Liste verschiedener Kriterien in den Kategorien Material, Recyclingfähigkeit und Energieverbrauch erfüllen. Die höchste Green-IT Auszeichnung – drei Sterne – erhalten nur Produkte, die über die geltenden Gesetze und Bestimmungen zur Green IT hinausgehen. Es wird unter anderem für die Prüfung von IaaS-Bestandteilen, wie Server und Speichersysteme eingesetzt. Link: (<http://www.fujitsu.com/ch/de/about/fts/environment-care/green-label/>).
- **Experton Group „Cloud Leader“:** durch einen mehrstufigen Prozess analysiert und bewertet die Experton Group jährlich den deutschen Cloud-Markt.

Der „Cloud Vendor Benchmark 2013“ soll dabei IT-Entscheidern unterstützen bei:

- Einheitlichen Marktüberblick zu Cloud Services, Technologien sowie Beratung und Integration
- Stärken und Schwächen der Anbieter werden transparent und vergleichbar
- Differenzierte Positionierung der Anbieter nach Segmenten und Deployment-Modellen
- Klare Kriterien für das Erstellen von Shortlists und die Investitionsplanung, bieten.

Um dies zu erreichen, werden jeweils den Siegern dieser Analyse und Bewertung, das Label „Cloud Leader“ vergeben, welches wiederum das Fundament für erfolgreiches Marketing auf Anbieterseite eingesetzt werden kann (<http://www.cloudvendorbenchmark.de/>):

- **Swiss made Software:** Das Label "swiss made software" steht für Schweizer Werte in der Softwareentwicklung. Seit 2007 haben sich dem Label über 200 Mitglieder angeschlossen, die ihre Produkte mit "swiss made software" auszeichnen. Es gibt zwei Bedingungen, die erfüllt sein müssen, damit bei einem Produkt die Schweizer Herkunft angegeben werden darf:
  - Der Schweizer Wertanteil an den Herstellungskosten muss mindestens 60 Prozent betragen.
  - Der wichtigste Fabrikationsprozess muss in der Schweiz stattgefunden haben.
- **Cloud Security Alliance STAR:** Die Cloud Security Alliance (CSA) ist eine Non-Profit Organisation mit dem Ziel, den Einsatz von Best Practices bzgl. der Sicherheit im Cloud Computing zu fördern, um Aufklärung über die Verwendung von Cloud Computing zu bieten sowie alle anderen Formen der IT Services abzusichern. Die Cloud Security Alliance wird von einer breiten Koalition von Praktikern aus der Industrie, Unternehmen, Verbänden und anderen wichtigen Interessengruppen geführt.

#### 4.4 Bestehende Zertifizierungen

- **ISO:** die Internationale Organisation für Normung stellt verschiedene Standards zur Verfügung, welche durch eine Zertifizierung überprüft werden können. ISO 20000 legt dabei Anforderungen für die Erstellung, Durchführung, Überwachung und Überprüfung, Wartung und Verbesserung eines Management-Systems fest, d.h. eine allgemeine Verwaltung und ein Kontrollraster um Sicherheitsrisiken eines Unternehmens zu überblicken und zu handhaben. Es schreibt keine spezifischen Informationen über Sicherheitskontrollen vor und bleibt auf dem Niveau des Management-Systems
- **TÜV Rheinland:** Certified Cloud Service ist die Zertifizierung von TÜV Rheinland für die Cloud. Vertrauenswürdigkeit, Transparenz und Qualität sind die wichtigsten Kriterien bei der Auswahl des passenden Cloud Services. Ob Infrastructure as a Service, Platform as a Service oder Software as a Service - für potenzielle Kunden ist dabei auch die Sicherheit ihrer Unternehmensdaten entscheidend.

Der TÜV Rheinland hat auf der Grundlage der wichtigsten Standards wie beispielsweise ISO 27001, BSI-Grundschutz und ITIL das Zertifikat „Certified Cloud Service“ entwickelt.

- **EuroCloud:** ist eine europäische Organisation mit 30 Landesorganisationen. EuroCloud arbeitet eng mit nationalen und internationalen Organisationen im Bereich Technologie, Forschung, öffentliche Verwaltung, Sicherheit, Datenschutz und rechtlichen Themen zusammen. Diese vernetzte Kompetenz wird genutzt, um Wissen aufzubereiten, spezielle Qualitätskriterien zu erstellen und Cloud Service-Provider dabei zu unterstützen eine differenzierende Qualität zu erreichen und den Reifegrad der Dienstleistungen durch die Euro-Cloud Star Audit-Zertifizierung nachzuweisen.  
Link: [www.saas-staraudit.de](http://www.saas-staraudit.de)
- **FedRamp:** Das bundesweite "Federal Risk and Authorization Management Program" (FedRAMP) der US-Regierung ist ein Programm, das einen standardisierten Ansatz zur Sicherheitsbewertung, zur Zulassung für die Nutzung bei Behörden und zur ständigen Überwachung der Cloud Services und Dienstleistungen bietet.
- **Trust in Cloud:** Anbieter von SaaS und Cloud-Lösungen können sich freiwillig der Trust-in-Cloud-Zertifizierung unterziehen und nach erfolgreichem Abschluss die Qualität der Lösung dokumentieren. Hierzu beantworten die Anbieter den Fragenbogen zur Checkliste und schaffen somit Transparenz für den Auswahlprozess.  
Als neutrale Instanz prüft das Cloud-EcoSystem die Angaben der Anbieter nach verschiedenen Kriterien und veröffentlicht die Fragebögen. Anwender können die Lösungen anhand dessen besser vergleichen und erhalten so Unterstützung bei der Auswahl der passenden SaaS und Cloud-Lösung für ihre Anforderungen.
- **EuroPriSe:** hat zum Ziel durch Informations-Technologie für Privatsphäre durch integrierte Technologien zu sorgen(Privacy by Design).Das Zertifizierungsprogramm wurde entwickelt, um die Sichtbarkeit für die Privatsphäre und die Verbesserung konformer IT-Produkte und Dienstleistungen zu fördern.  
Durch die Einführung eines transparenten und überprüfbaren Verfahrens von unabhängigen Behörden, überwacht EuroPriSe Ziele für den Wettbewerb in der Privatsphäre zu mobilisieren und das Vertrauen der Nutzer zu fördern. Das Siegel bietet einen positiven Anreiz durch Markt-und Marketing-Vorteile zu implementieren und zu beobachten Privatsphäre.  
Link: <https://www.european-privacy-seal.eu/>

#### 4.5 Vor- und Nachteile von Labels

Labels bieten verschiedene Vorteile gegenüber Zertifizierungen. So ist der Initialaufwand für die Erstellung eines Labels wesentlich geringer. Kontrollprozesse beispielsweise müssen weit weniger spezifisch aufgebaut werden, da diese lediglich einige Aspekte berücksichtigen müssen. Im Gegensatz wird bei einer Zertifizierung ein ganzheitlicher Ansatz angesprochen, damit ein Produkt / Dienstleistung vollumfänglich auf Herz und Nieren geprüft werden kann. Da Labels oftmals nur sehr selten (nicht alle 2-4 Jahre) nachgeprüft werden,

kann auch hier mit einem geringeren Aufwand gerechnet werden.

Dies sind aber gerade auch die Nachteile eines Labels. Es werden keine tiefer gehende Abklärungen, kein Audit durchgeführt. Dadurch kann dem Kunden beispielsweise keine eigentliche Garantie über die Qualität des Produktes / der Dienstleistung gewährleistet werden.

#### **4.6 Vor- und Nachteile von Zertifizierungen**

Durch eine Zertifizierung werden Standards auf die zu untersuchenden Kriterien definiert. Dadurch entstehen klare Qualitätsmerkmale, welche es einzuhalten gilt und zu berücksichtigen sind. Durch dessen Erstellung können spezifische Anforderungen (z. B. behördliche Datenschutz-Ansprüche) berücksichtigt werden und in den Standard mit einfließen.

Ein wesentlicher Nachteil einer Zertifizierungslösung besteht im Aufbau einer unabhängigen Zertifizierungsstelle. Dabei müssen Rollen, Regeln und vor allem klare Prozesse, auch rund um den Zertifizierungsprozess definiert und aufgebaut werden. Eine wiederkehrende Prüfung der einzuhaltenden Standards muss durch geschultes Personal (Auditoren) erfolgen, d.h. intensive Schulungsangebote müssen ebenfalls erstellt und angeboten werden. Somit ermöglichen Zertifikate eine langfristige Sicherstellung der Produkte und Service-Qualität.

Für den Anwender bedeutet dies, dass eine Gewährleistung für die einzelnen Service-Qualitätskriterien gegeben ist und er sich darauf verlassen kann, dass diese auch eingehalten werden.

Auf der anderen Seite ist die Zertifizierung für einen Provider auch eine Möglichkeit, sich gegenüber der Konkurrenz abzuheben und zu behaupten. Durch das Zertifikat kann somit der oftmals mühsame Vertrauensbildungsprozess erheblich vereinfacht werden.

## **5 Cloud Service Qualität (CSQ)**

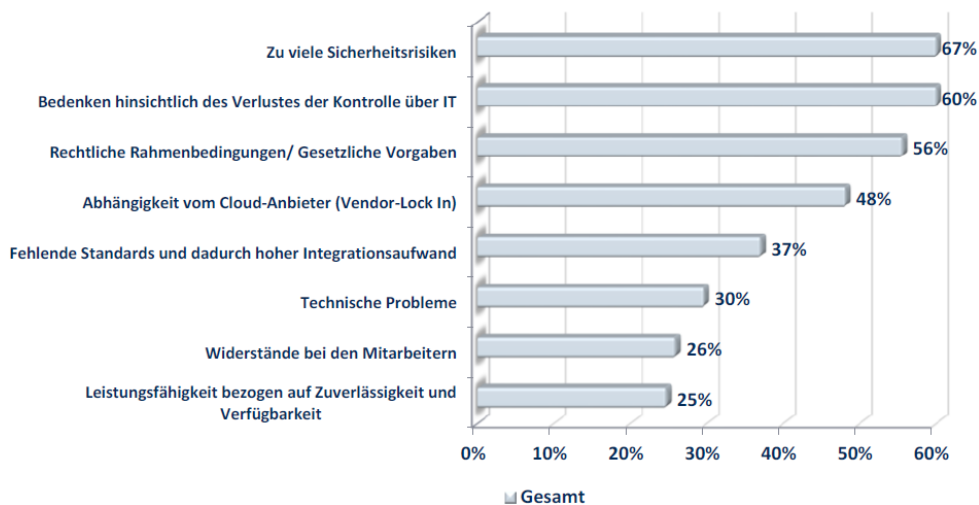
Cloud Services bringen viele Aspekte mit sich, egal welches Deployment oder Service Modell, die es für die Definition der Qualität zu berücksichtigen gilt. Für eine ganzheitliche Betrachtung wurden diverse Markstudien gemacht bezüglich:

- Kunden Hemmnisse
- Auswahl für Cloud Services
- Kriterien und Herausforderungen

### **5.1 Kunden Hemmnisse**

Der aktuelle Quartals-Bericht (Q2 2013) der techConsult GmbH zeigt das Unternehmen vor allem Hemmnisse bei der Sicherheit und den Kontrollverlust der IT für einen Einstieg in die Cloud Nutzung haben

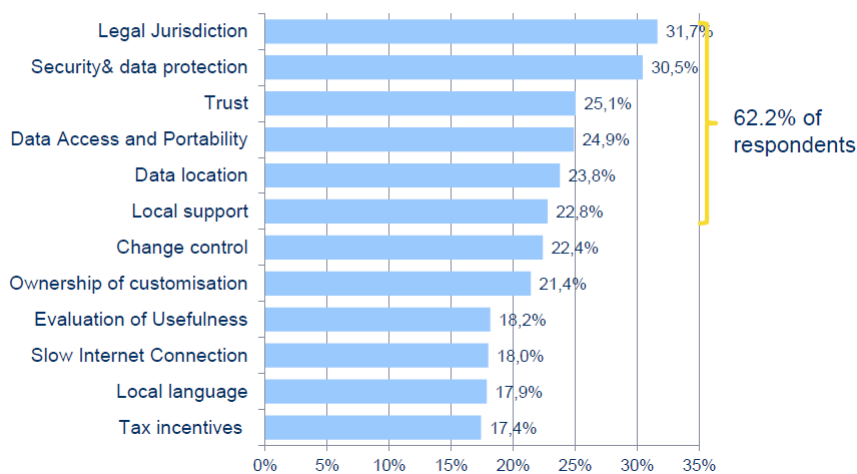
### Wo sehen Sie die größten Hemmnisse für die Einführung von Cloud Services?



Quelle 2013 techconsult GmbH

Eine weitere Untersuchung der Booz & Company aus dem Jahre 2012 identifiziert zusätzlich Barrieren zum Cloud Computing aus Nutzersicht:

### % of respondents stating barrier is restricting (very/completely) cloud adoption



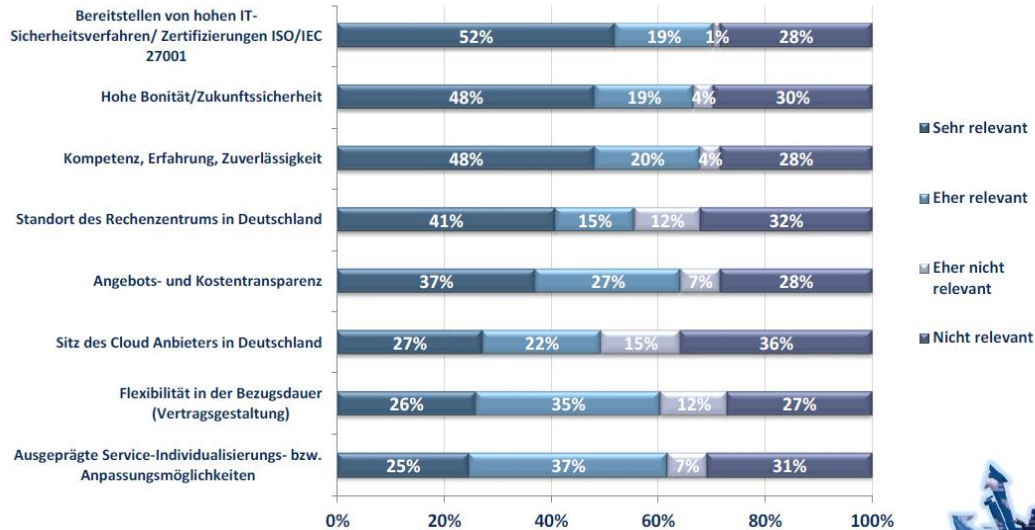
Quelle: Booz & Company und FZI (2012)

So sind es vor allem rechtliche und Sicherheitsfragen, aber auch der Vertrauensaufbau zum Provider, welche als grosse Herausforderungen gesehen werden.

## 5.2 Kriterien für die Auswahl von Cloud Services

Für die Auswahl eines geeigneten Cloud Partners, dem sogenannten Cloud Service Provider sind nach den Unternehmen vor allem Zertifizierungen des Providers und dessen Zukunftssicherheit sehr wichtig.

Welche der Kriterien sind für Sie entscheidend für die Auswahl eines Cloud Services Anbieters und seiner Cloud Lösungen?



Basis: 200 Unternehmen  
Mehrfachnennung möglich

© 2013 techconsult GmbH | Tel.: +49 (0) 561/8109-0 | www.techconsult.de

Quelle 2013 techconsult GmbH



## 5.3 Kriterien und Herausforderungen

Ausgehend von den identifizierten Barrieren stellen Booz & Company neun verschiedene Herausforderungen zusammen, welche es anzugehen gilt.

<b>1 Effektivität der Dienstleistung</b> a Skalierbare Architektur c Management von Ressourcen & Flexibilität d Verfügbarkeit von verschiedenen Diensten	<b>5 Datenschutz</b>
<b>2 Effektivität des Dienstes für den Anwender</b> a Verträge inkl. Fragen der Haftung b Kontrolle des Dienstes durch den Anwender c Steuerungs- und Eskalationsmechanismen	<b>6 Kompatibilität</b> a Migration in die Cloud und aus der Cloud b Möglichkeit der Integration in eine on-premise IT c Cloud-Verband
<b>3 Transparenz über Service-Erbringung und Kosten</b> a Kosten inkl. Lizenz-Management b Qualitätssicherung und Kontrolle der Supportvereinbarungen c Art und Ort der Datenvereinbarungen	<b>7 Übertragbarkeit zwischen verschiedenen Providern</b> a Übertragbarkeit der Services b Übertragbarkeit der Daten
<b>4 Information s-Sicherheit</b> a Identitäts- & Rechtemanagement b Datenschutz & Integrität c Zugangskontrolle, Logging, Abwehr von Angriffen d Gewährleistung & Zertifizierung	<b>8 Sicherung des fairen Wettbewerbes im Markt</b>
	<b>9 Einhaltung rechtlicher Anforderungen</b>

Quelle: Booz & Company und FZI (2012)

Aus diesen Herausforderungen lassen sich so aus Kundensicht folgende Bereiche und Ausprägungen/ Kriterien ableiten, die für die Sicherstellung einer Cloud Service Qualität berücksichtigt werden müssen. Dunkel eingefärbte Kriterien sollen dabei höher priorisiert werden:

	Bereich	Thema
	Vertrag	Geschäftsbedingungen, SLA, ...
	Gesetzliche Regulierung	Gesetzliche Anforderungen, Ort der Datenhaltung, Datenschutzbestimmungen, Export Kontrolle,..
	Daten Sicherheit	ISMS, Zugriffskontrolle, Archivierung ...
	Datenschutz	Datentrennung, Datenlöschung, Zugriffskontrolle, Datenlöschung..
	Rechenzentrum	Technik und Infrastruktur
	Betriebsprozesse	Service Management
	Anwendung und Schnittstellen	Daten-Export Funktionalität und Vollständigkeit, allgemeine Benutzerfreundlichkeit, Transparenz, ...

Dabei stellt sich die Frage, welche Hilfsmittel sind heute verfügbar, die den Kriterien der Anwender genügen und Hemmnisse, Schranken abbauen? Dabei sollen Kriterien bestimmt werden, welche die Anforderungen einer solchen „Qualitätssicherung“ gestellt werden, wonach die identifizierten Zertifikate und Labels klassifiziert werden können, dies insbesondere mit Hinblick auf Cloud Services für die öffentliche Verwaltung.

Unter der weiteren Berücksichtigung, dass bei Cloud Services die Partnerstabilität und die Nutzbarkeit wichtig sind, kommen noch die Elemente Service-Provider, Implementierbarkeit und Schulung dazu. Somit setzen sich die Bewertungskriterien wie folgt zusammen:

- Service Provider
- Vertrag und Service Level Vereinbarungen
- Gesetze und Regulatoren
- Sicherheit und Datenschutz
- Anwendung bezogene Services (SaaS, PaaS und IaaS), und Schnittstellen (Interoperabilität)
- Betriebsprozesse
- Infrastruktur Rechenzentrum
- Implementierung und Schulung

## 6 Gegenüberstellung der definierten Kriterien und vorhandener Ansätze

Im Folgenden werden per Definition (Label, Zertifizierung) die aufgeführten Labels und Zertifizierungen ausgewählt und hinsichtlich der aufgestellten Kriterien einander gegenübergestellt und analysiert.

## 6.1 Labels

**Fujitsu Green IT:** das Label der Fujitsu untersucht Produkte hinsichtlich ihrer Energieeffizienz und Nachhaltigkeit. Im Cloud-Bereich gilt dies vor allem für Infrastruktur Angebote, wie Server und Speicherlösungen. Dabei werden Rechtliche oder auch vertragliche Aspekte nicht berücksichtigt. Ebenso sind Datenschutz und –sicherheit, Betriebsprozesse und Software und Interoperabilität für das Erhalten des Labels keine Kriterien.

Im Bereich Rechenzentrum und Infrastruktur wird hinsichtlich der Transparenz das Schwergewicht klar auf die Minimierung der Energieeffizienz gelegt. Dabei müssen die eingesetzten Hardwarekomponenten klar aufzeigen, dass sie im Gegensatz zu konkurrierenden Produkten einen geringeren Energieverbrauch ausweisen. Um ein Green IT Label zu bekommen, muss das Produkt eine umfassende Liste verschiedener Kriterien in den Kategorien Material, Recyclingfähigkeit und Energieverbrauch erfüllen. Dies ist zwingend für die Ausstellung des Labels.

**Experton Group „Cloud Leader“:** das jährlich vergebene Label „Cloud Leader“ untersucht verschiedene Cloud Service Provider einerseits auf dessen Investitionstätigkeiten im Bezug ihrer Cloud-Angebote und die Klassifizierung nach Branchen und Unternehmensgrößen der Kunden. Dazu werden die einzelnen Kandidaten auf ihre Wettbewerbsstärke und die Portfolio-Attraktivität untersucht und entsprechend eingestuft. Hinsichtlich etwaiger Service-Qualitäts-Merkmale werden keine Untersuchungen und Aussagen gemacht.

**Swiss made Software:** für die Cloud Thematik kann das Label vor allem auf Software-as-a-Service eingesetzt werden. Die Vergabekriterien beziehen sich dabei lediglich auf die Entwicklung der Software. Dabei muss der Wertanteil, welcher zur Entwicklung beigetragen hat, zu mindestens 60% in der Schweiz erarbeitet worden sein. Zudem müssen die wichtigsten Entwicklungsprozesse ebenfalls in der Schweiz durchgeführt werden. Hinsichtlich der anderen Cloud Service Qualitätskriterien, werden keine weiteren Untersuchungen erhoben.

## 6.2 Zertifizierungen

**ISO:** Für den Cloud Bereich sind in diesem Zusammenhang vor allem die ISO 20000 von Wichtigkeit. Die ISO/IEC 20000 IT Service Management dient als messbarer Qualitätsstandard für das IT Service Management (ITSM). Dazu werden in der ISO/IEC 20000 die notwendigen Mindestanforderungen an Prozesse spezifiziert und dargestellt, die eine Organisation etablieren muss, um IT-Services in definierter Qualität bereitstellen und managen zu können. Innerhalb der ISO/IEC 20000 werden die diverse Anforderungen und Prozesse definiert.

Diese Punkte decken bezüglich der CSQ insbesondere Vertragliche, Datenschutz und Sicherheits- und Betriebsprozess Aspekte ab. Teilweise werden dabei auch auf einzelne Merkmale aus dem Bereich Rechenzentrum und Infrastruktur eingegangen. Das Einhalten dieser Standards wird durch die wiederkehrende Auditierung durch unabhängige Stellen gewährleistet. Bezüglich rechtlicher Fragen, stellt die Zertifizierung nur allgemein Gültige Anforderungen. Länderspezifische Ausprägungen, wie Datenschutzgesetze werden nicht explizit berücksichtigt.



**EuroCloud:** Der EuroCloud Star Audit basiert einerseits auf einem Best-Practice Ansatz, andererseits durch die Berücksichtigung von diversen Organisationen wie BSI, ETSI, ENISA. Dadurch soll gewährleistet werden, dass ein ganzheitliches Verständnis über den Umfang und die Wirksamkeit einer solchen Betriebsprüfung ermöglicht werden kann. Der Star Audit ist Modular aufgebaut und berücksichtigt verschiedene Schwerpunkte.

- Erklärung über die Zuverlässigkeit des Cloud Services, der Dienstleister und der beteiligten Unterauftragnehmer
- Untersuchung der spezifischen vertraglichen Elemente mit Blick auf
  - Auftragsdatenverarbeitung
  - Datenschutzgesetz
  - ordnungsmäßiger Buchführung
- Betriebsprozesse
- Einhaltung der Service-Level-Vereinbarungen
- Lock In Situationen und Anbieterwechsel
- Schulung und Support
- Interoperabilität

Durch die Berücksichtigung verschiedener Anforderungen in den jeweiligen Ländern, siehe beispielsweise EuroCloud Swiss „CH-Zertifizierung“, kann sichergestellt werden, dass diese auch geprüft werden.

**TüV Rheinland:** der Prüfkatalog basiert auf Standards, wie BSI, Studien sowie auf ausgewählten Vorschriften und Empfehlungen, konkretisiert und angepasst für die Cloud. Bei dem Prüfverfahren werden dabei unterschiedliche Methoden berücksichtigt und angewandt. Explizit werden dabei vor allem auf folgende Gebiete fokussiert:

- Analyse von Konzepten und Prozessen Hypervisor, Virtualisierung von Rechenzentren, Systeme, Zugriffskonzepte, Netzwerk, Systemschnittstellen, Administration, Service, Betrieb und Compliance.
- Mittels Interviews werden spezifisch der Umsetzungsgrad, die Qualität und die Nachhaltigkeit von Prozessen erhoben.
- Einhaltung von SLAs
- Architekturanalysen zur Belastbarkeit der Systeme
- Analyse der Systemsicherheit

Die Cloud-Zertifizierung hat nach erfolgreichem Abschluss eine Gültigkeit von drei Jahren und kann anschliessend erneuert werden. Während dieser Zeit überprüfen wir mit regelmässigen Audits die Gültigkeit der Cloud-Zertifikatsaussagen.

**FedRAMP:** FedRAMP ist das Ergebnis einer engen Zusammenarbeit mit Cyber- und Cloud-Experten aus verschiedenen behördlichen Organisationen in den USA und seiner Arbeitsgruppen sowie der Privatwirtschaft. Hauptzweck ist dabei die Zertifizierung von Cloud Service Providern und deren Einhaltung der behördlichen Anforderungen bezüglich Datensicherheit von Cloud Systemen und die Durchführung entsprechender Risiko-Bewertungen.

Der FedRAMP Security Assessment-Prozess definiert dabei eine Reihe von Steuerelementen für niedrige und moderate Auswirkungen Systemen basierend auf NIST SP 800-53 Kriterien. Cloud Service-Anbieter müssen bei der Umset-

zung dieser Kriterien durch eine unabhängige Organisation (3PAO) überprüfen lassen.

## 7 Mapping und Bewertung der erhobenen Varianten

Wie bereits im vorhergegangenen Kapitel erläutert, decken die einzelnen Labels nur einzelne Kriterien ab und dies nicht vollumfänglich. Das Label „Cloud Leader“ beispielsweise untersucht keine der Eigenschaften. „Green IT“ untersucht einzelne für die CSQ von geringer Bedeutung (Energieeffizienz), Aspekte der Rechenzentrum und Infrastruktur. Swiss made Software widmet sich dem Thema des Herstellungsortes einer Applikation und untersucht dabei lediglich den Ort des Entwicklungsprozesses.

Im Gegensatz dazu gehen die untersuchten Zertifikate deutlich stärker auf die Cloud Service Qualität Ausprägungen ein. Obwohl ISO 20000 keine Cloud spezifische Zertifizierung ist, legt es Standards für die Bereiche Datenschutz und Sicherheit, Rechenzentrum und Infrastruktur, sowie Betriebsprozesse fest. Durch den Prozess Service Level Management werden teilweise auch vertragliche Aspekte berücksichtigt. Auch die Certificate Cloud Services des TÜVs Rheinland decken diese Bereiche ab, zusätzlich werden rudimentäre Aspekte des Software und Interoperabilität Bereiches untersucht. FedRAMP wurde auf die Anforderungen der amerikanischen Behörden ausgerichtet. Dabei scheinen die Hauptmerkmale vor allem auf die Untersuchung der Qualität des Datenschutzes und insbesondere der Datensicherheit zu liegen.

Rechtliche Aspekte werden von diesen drei Zertifikaten nur durch die TÜV Lösung berücksichtigt, dabei wird aber nur deutsches Recht angewandt.

Der EuroCloud Ansatz und insbesondere die angestrebte Schweizer Lösung gehen auf alle wesentlichen CSQ ein. So werden in allen sechs Kategorien auf schweizerische Anforderungen angepasste detaillierte Untersuchungen durchgeführt und validiert.

Die folgende Tabelle gibt einen Überblick über die ausgewählten Labels und Zertifikate und deren Zusammenhang /Abdeckung der CSQ:

Zertifikate/ Labels	Service- Provider	Vertrag, SLA	Landesrecht, Regulatorien	Sicherheit, Datenschutz	Services (IaaS,PaaS,SaaS), Interoperabilität	Betriebs- prozesse	RZ Infra- struktur	Implemen- tierung, Schulung
ISO		X		X	IaaS,SaaS	X	X	
EuroCloud	X	X	D,A,CH	X	IaaS,PaaS,SaaS	X	X	X
TÜV Reinland		X	D	X	SaaS	X	X	
FedRAMP			US	X	SaaS	teilweise		
Green IT					IaaS		teil- weise	
Experton Group					SaaS			
Swiss made Software					SaaS			

**Eine ganzheitliche Betrachtung der Kriterien und über die einzelnen Service Modelle verteilt, wird nur bei EuroCloud erreicht. Der Audit von TÜV Reinland liegt an zweiter Stelle.**

## 8 Potenzialabschätzung

Der folgende Abschnitt soll in einem ersten Schritt kurz aufzeigen, welches Potenzial hierbei eine geeignete Zertifizierung von Providern für den Schweizer Markt mit sich bringt. In einem weiteren Schritt werden gleiche Überlegungen hinsichtlich schweizerischer Behörden aufgegriffen.

**Schweizer Markt:** Im CH-Markt sind der Enterprise-Markt eher für punktuelle SaaS und IaaS/PaaS geeignet, der KMU-Markt eher für SaaS. Cloud Services ermöglichen besonders dem KMU eine rasche Anpassung an neue wirtschaftliche Gegebenheiten. Jedoch stehen viele dieser Unternehmen in der Nutzung solcher Services noch skeptisch gegenüber. Vor allem offene Fragen rund um die Sicherheit, das Vertrauen und die Auswahl eines geeigneten Partners sind oftmals Hinderungsgründe.

Gemäss MSM Research (2013) gibt es in der Schweiz:

- ca. 300'000 kleiner Unternehmen
- ca. 3000 mittlerer Unternehmen
- ca. 300 grosse Unternehmen

Die Kleineren und mittleren Unternehmen verfügen über ein Potential für SaaS-Services und die grossen Unternehmen haben eher Potential für IaaS/PaaS Services. Für viele Unternehmen sind die IT keine Kernkompetenz und müssen diese immer teuer eingekauft und betreiben. Eine Überprüfung der Provider mit einer anerkannten Zertifizierung, kann speziell die KMUs bei der Auswahl des richtigen Partners stark unterstützen. So kann durch das entsprechende Zertifikat die Service Qualität sichergestellt werden und die potenziellen Nutzer können sich nachhaltig darauf verlassen. Eine entsprechende Zertifizierung kann hier von grossem Vorteil sein und den Markt für Cloud Services fördern.

**Schweizer Behörden:** basierend auf den drei Ebenen Bund – Kantone und Gemeinden, sind es:

- 8 Departemente und 38 Bundesämter
- 26 Kantone und 241 Kantonale Verwaltungen
- 2600 Gemeinden

Bei Zertifizierungen in der Schweizer Behörde müssen folgende Überlegungen in Betracht gezogen werden:

- Die Rahmenbedingung für Cloud Services müssen vorhanden sein
- Die Wiederverwendbarkeit und die Wirtschaftlichkeit von Cloud Services müssen gegeben sein.
- Die Servicequalität muss nachhaltig sichergestellt werden.

Einsatzgebiete für SaaS-Dienstleistungen können beim Bund und den Kantonen in den Gebieten Kommunikation & Kollaboration, Contentmanagement (CMS), Ablagen, Archiven, Finanz- & Rechnungswesen und Personalwesen zu finden sein. Werden weitere Bereiche für SaaS in Betracht gezogen, so müssen auf Grund der Wiederverwendbarkeit harmonisierte Prozesse vorhanden sein.

Im Rahmen von Standardisierungen kann die Wiederverwendbarkeit wie auf den 3 Ebenen wie folgt betrachtet werden:

	IaaS	PaaS	SaaS
Bund	Hoch	Mittel	Gering
Kantone	Hoch	Mittel	Mittel
Gemeinden	Gering	Mittel	Hoch

## 9 Empfehlungen

### 9.1 Labels

Die aufgezeigten Label Ansätze zeigen, dass diese Formate zwar Qualitätsstandards für Cloud Services teilweise definieren können, aber nicht dazu geeignet sind dessen Einhaltung auch nachhaltig zu garantieren. Labels neigen dazu ein ausgewähltes Merkmal zu untersuchen und hervorzuheben. Der Nutzen dabei scheint vor allem auf Anbieterseite zu sein. Diese können sich mit einem relativ leicht zu erwerbenden Label / Signal rühmen und für Marketingzwecke einsetzen. Für den Anwender, den Kunden bietet es bedingten Mehrwert. Im Gegenteil kann es dem potenziellen Nutzer sogar eine falsche Signalwirkung aussenden in dem es eine Sicherheit verspricht, welche aber nicht nach einer ganzheitlichen Betrachtungsweise durchgeführt wird. Um einen Vertrauensaufbau zwischen dem Anwender und dem Anbieter zu ermöglichen, ist dies jedoch gerade im Cloud-Markt von grösster Bedeutung.

**Fazit: Ein Label ist für einen nachhaltigen Cloud Service nicht geeignet.**

### 9.2 Zertifizierung

Sollen Qualitätsstandards für Cloud Services festgelegt und dessen Einhaltung überprüft werden, ist eine spezifische und ganzheitliche Zertifizierung im Sinne der Cloud Service Qualität sicher einem Label vor zu ziehen. Damit kann sich ein Service Nutzer jederzeit auf die Aussage, die Gewährleistung der angeforderten Qualität verlassen.

Die Zertifizierung ermöglicht im Gegensatz zum Label eine langfristige „Garantie“, dass der Provider die angestrebte Qualität auch bietet. Eine zertifizierte, potenzielle Wiederverwendbarkeit unter gleichen einheitlichen Servicekriterien, kann dem Kunden eine Vertrauensbasis erbringen und dabei auch für den Service-Anbieter ein Alleinstellungsmerkmal gegenüber den Mitbewerbern bieten.

**Fazit: Für die nachhaltige Sicherstellung der Servicequalität von Cloud Services ist eine EuroCloud Star Audit Zertifizierung notwendig.**

### 9.3 Datenschutz und weitere Massnahmen

Die erwähnte Datenschutzlage in der Schweiz sieht vor, dass die drei Ebenen Bund, Kantone und Gemeinden jeweils eigene Ausprägungen des Datenschutzes erheben können. Es besteht ein schweizerisches Datenschutzgesetz, aber in unserem föderalistischen System, ist es erlaubt, dass die einzelnen Parteien, wie Kantone, Gemeinden und auch öffentliche Institutionen wie Schulen eigene Anforderungen erstellen können. Dies führt dazu, dass sehr viele individuelle Ansätze für Datenschutz und Sicherheit für den jeweiligen Bedarf entstehen und die Wiederverwendbarkeit somit gefährden. Um den Erfolg von Cloud Services

und Zertifizierungen, müssen nebst der Wiederverwendbarkeit auch einheitliche Kriterien und gemeinsame Rahmenbedingungen vorhanden sein.

Für die Schaffung von gemeinsamen Rahmenbedingungen schlagen wir folgende Ansätze vor:

- **Für die Risiko Beurteilung** zur Auslagerung von Daten von Bund, Kantonen und Gemeinden soll ein Richtlinie oder ein Verfahren mit einer Klassifizierung der Daten erarbeitet werden.
- **Für die Harmonisierung von Datenschutz und Sicherheit**, soll (in Anlehnung an die BSI (deutsches Bundesamt für Sicherheit in der Informationstechnik) IT Grundschutz), eine Richtlinie für gemeinsame Anforderungen in Bezug auf Sicherheit und Datenschutz geschaffen werden, oder
- In Kombination mit einem harmonisierten Datenschutz und der Sicherheit sollen **Richtlinien für folgende Sicherheits-Szenarien** gebildet werden.

Sehr hohe Sicherheit				<b>X</b>
Hohe Sicherheit			<b>X</b>	
Mittlere Sicherheit		<b>X</b>		
Tiefe Sicherheit	<b>X</b>			
	Nicht Personen bez. Daten	Personen bezogene Daten	Besonders schützenswerte Daten	Geheime Daten

Mit der Durchdringung solcher Vorgaben kann das Vertrauen, die Servicequalität und somit das Cloud-Business, auf allen drei Ebenen gefördert werden.

- Für die **nachhaltige Sicherstellung der Servicequalität von Cloud Services** (IaaS, PaaS und SaaS) wird das Zertifizierungsverfahren nach **Star Audit** empfohlen.

Weitere Massnahmen bezüglich Zertifizierung von Cloud Services können erst nach der Studie „GovCloud“ empfohlen werden, wenn die möglichen Einsatzgebiete und entsprechende Cloud Anbieter identifiziert wurden.