

Dr. Rainer Bernnat  
Dr. Wolfgang Zink  
Dr. Nicolai Bieber  
Joachim Strach

Prof. Dr.-Ing. Stefan Tai  
Robin Fischer



**booz&co.**

---

Studie für das Bundesministerium für Wirtschaft und Technologie (BMWi)

# **Das Normungs- und Standardisierungsumfeld von Cloud Computing**

Eine Untersuchung aus europäischer und deutscher Sicht unter  
Einbeziehung des Technologieprogramms „Trusted Cloud“

**Abschlussbericht**

---

## Inhaltsverzeichnis

<b>ABBILDUNGSVERZEICHNIS .....</b>	<b>5</b>
<b>TABELLENVERZEICHNIS .....</b>	<b>5</b>
<b>1 ZUSAMMENFASSUNG.....</b>	<b>6</b>
<b>2 EINLEITUNG .....</b>	<b>14</b>
2.1 Ausgangssituation und Zielsetzung der Studie.....	14
2.2 Vorgehen und Aufbau der Studie.....	16
2.3 Cloud Computing.....	17
2.3.1 Begriffe und Definitionen .....	18
2.3.2 Grundlagen des Cloud Computing .....	19
<b>3 METHODOLOGIE ZUR UNTERSUCHUNG.....</b>	<b>22</b>
3.1 Begriffe und Definitionen der Studie .....	23
3.1.1 Begriffswelt „Akteure“ .....	23
3.1.2 Begriffswelt „Initiativen“ .....	25
3.1.3 Begriffswelt „Standards“ .....	26
3.2 Taxonomie für Standards im Cloud Computing.....	28
3.2.1 Herausforderungen im Cloud Computing.....	29
3.2.2 Ansatzpunkte der Standardisierung im Cloud Computing .....	34
3.2.3 Weitere Attribute zur Klassifizierung von Cloud-Standards und Normen .....	36
3.3 Analyseansatz der Studie .....	38
3.3.1 Fokus, Auswahl und Bewertung der Akteure .....	39
3.3.2 Fokus, Auswahl und Lückenanalyse der Standards .....	42
3.3.3 Auswahl strategischer Trends .....	48
<b>4 WICHTIGE CLOUD-STANDARDISIERUNGSORGANISATIONEN.....</b>	<b>50</b>
4.1 Deutsche Standardisierungsorganisationen.....	54
4.1.1 Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (BITKOM) .....	54
4.1.2 Deutsches Institut für Normung (DIN) .....	55
4.1.3 SaaS-EcoSystem (SaaS-ES) .....	56
4.2 Europäische Standardisierungsorganisationen.....	57
4.2.1 Europäisches Institut für Telekommunikationsnormen (ETSI) .....	57
4.2.2 EuroCloud.....	58
4.2.3 Europäischen Agentur für Netz- und Informationssicherheit (ENISA) .....	59

<b>4.3</b>	<b>Internationale Standardisierungsorganisationen .....</b>	<b>60</b>
4.3.1	Cloud Security Alliance (CSA) .....	60
4.3.2	Distributed Management Task Force (DMTF) .....	61
4.3.3	Internet Engineering Task Force (IETF) .....	62
4.3.4	Internationale Organisation für Normung (ISO) .....	63
4.3.5	International Telecommunications Union (ITU).....	64
4.3.6	National Institute of Standards and Technology (NIST) .....	65
4.3.7	Organization for the Advancement of Structured Information Standards (OASIS).....	66
4.3.8	Open Cloud Consortium (OCC) .....	67
4.3.9	Open Grid Forum (OGF) .....	68
4.3.10	The Open Group (TOG).....	68
4.3.11	Storage Networking Industry Association (SNIA) .....	69
4.3.12	TM Forum (TM-F).....	70
4.3.13	World Wide Web Consortium (W3C) .....	71
<b>5</b>	<b>RELEVANTE STANDARDS IM CLOUD-UMFELD.....</b>	<b>72</b>
<b>5.1</b>	<b>Steckbriefe aus dem Bereich „Technik“ .....</b>	<b>77</b>
5.1.1	Cloud Computing Reference Architecture (CCRA).....	77
5.1.2	Cloud Data Management Interface (CDMI) .....	80
5.1.3	Automated Audit, Assertion, Assessment, and Assurance API (Cloud Audit).....	82
5.1.4	Cloud Trust Protocol (CTP).....	84
5.1.5	Open Cloud Computing Interface (OCCI) .....	86
5.1.6	OpenStack Cloud Software (OpenStack) .....	88
5.1.7	CIM System Virtualization Model (CIMSVM) .....	90
5.1.8	Apache Hive (Hive) .....	92
5.1.9	Web Authorization Protocol (OAuth).....	93
5.1.10	Open Virtualization Format (OVF) .....	95
5.1.11	Security Content Automation Protocol (SCAP).....	97
5.1.12	Unified Service Description Language (USDL).....	99
5.1.13	Web Service Standards (WS-*) .....	101
<b>5.2</b>	<b>Steckbriefe aus dem Bereich „Management“ .....</b>	<b>103</b>
5.2.1	Eckpunktepapier Sicherheitsempfehlungen für Cloud Computing Anbieter (BSI-ESCC).....	103
5.2.2	EuroCloud Star Audit (EuroCloud-SA).....	105
5.2.3	Governance, Risk Management and Compliance Stack (GRC Stack).....	107
5.2.4	NIST Cloud Computing Use Cases (NIST-UC) .....	109
5.2.5	Statement on Standards for Attestation Engagements No. 16 (SSAE 16).....	111
<b>5.3</b>	<b>Steckbriefe aus dem Bereich „Recht“ .....</b>	<b>113</b>
5.3.1	Open Cloud Manifesto (OCM) .....	113
5.3.2	EU-Richtlinie 95/46/EG „Datenschutzrichtlinie“ (95/46/EG).....	115
<b>5.4</b>	<b>Lücken bei Standards im Cloud-Umfeld .....</b>	<b>117</b>
5.4.1	Effizienz der Dienstbereitstellung.....	117
5.4.2	Effektivität der Dienstenutzung und -steuerung .....	118
5.4.3	Transparenz der Leistungserbringung und Abrechnung .....	120
5.4.4	Informationssicherheit .....	121

5.4.5	Datenschutz.....	122
5.4.6	Interoperabilität.....	123
5.4.7	Portabilität.....	124
5.4.8	Sicherstellung eines funktionierenden Wettbewerbs .....	125
5.4.9	Compliance mit geltender Rechtslage .....	126
<b>6</b>	<b>WICHTIGE STRATEGISCHE TRENDS DER STANDARDISIERUNG IM CLOUD COMPUTING .....</b>	<b>127</b>
6.1	Einleitung und Übersicht .....	127
6.2	Strategische Trends im Einzelnen .....	128
6.2.1	Cloud-Standardisierung und staatliche Mitwirkung .....	128
6.2.2	Cloud-Zertifizierung .....	131
6.2.3	Offenheit im Cloud Computing .....	133
6.2.4	Rechtssicherheit für die Cloud .....	135
6.2.5	Cloud-Marktplätze .....	138
6.2.6	Governance im Cloud Computing .....	141
<b>7</b>	<b>HANDLUNGSEMPFEHLUNGEN ZUR STANDARDISIERUNG IM CLOUD COMPUTING AN DIE BUNDESREGIERUNG .....</b>	<b>143</b>
7.1	Handlungsrahmen, -begründung und -ziele.....	143
7.1.1	Der strategische Handlungsrahmen.....	143
7.1.2	Die Notwendigkeit ordnungspolitischen Handelns .....	146
7.1.3	Schlussfolgerung und Ableitung der Handlungsziele.....	148
7.2	Strategisches Handlungsziel I: Fokussierte inhaltliche Mitwirkung.....	150
7.2.1	Handlungsfeld 1: Schließen von Standardisierungslücken.....	150
7.2.2	Handlungsfeld 2: Unterstützung von Offenheit im Cloud Computing.....	151
7.2.3	Handlungsfeld 3: Mitwirkung bei Orientierungswissen und Vertragswesen .....	152
7.2.4	Handlungsfeld 4: Begleitende Kommunikation .....	154
7.3	Strategisches Handlungsziel II: Schaffung geeigneter Rahmenbedingungen .....	155
7.3.1	Handlungsfeld 5: Zentrale Koordination der Standardisierung .....	155
7.3.2	Handlungsfeld 6: Bereitstellung geeigneter Cloud-Zertifizierungen.....	156
7.3.3	Handlungsfeld 7: Auflegen förderpolitischer Maßnahmen .....	157
7.3.4	Handlungsfeld 8: Rechtliche Vorgaben .....	158
<b>ANHANG .....</b>		<b>159</b>
Anhang A: Vorarbeiten, Standards und Zertifizierungen mit Bezug zum Cloud Computing ...		159
Anhang B: Standardisierungsorganisationen.....		163
<b>IMPRESSUM</b>		

## Abbildungsverzeichnis

ABBILDUNG 1: EINORDNUNG DER VORLIEGENDEN STUDIE.....	14
ABBILDUNG 2: AUFBAU UND VORGEHEN DER STUDIE.....	16
ABBILDUNG 3: BEGRIFFSWELTEN DER STUDIE – ÜBERSICHT .....	23
ABBILDUNG 4: BEGRIFFSWELT „STANDARDS“ DER STUDIE.....	26
ABBILDUNG 5: EINORDNUNGSMATRIX FÜR STANDARDS IM CLOUD COMPUTING .....	29
ABBILDUNG 6: HERAUSFORDERUNGEN IM CLOUD COMPUTING .....	30
ABBILDUNG 7: DETAILLIERUNG DER HERAUSFORDERUNGEN IM CLOUD COMPUTING (1. & 2. EBENE).....	33
ABBILDUNG 8: ANSATZPUNKTE DER STANDARDISIERUNG IM CLOUD COMPUTING .....	34
ABBILDUNG 9: KATALOG DER ATTRIBUTE ZUR BESCHREIBUNG VON CLOUD-STANDARDS.....	36
ABBILDUNG 10: ÜBERGREIFENDER ANALYSEANSATZ DER STUDIE .....	39
ABBILDUNG 11: FOKUS-, AUSWAHL- UND BEWERTUNGSKRITERIEN FÜR AKTEURE .....	40
ABBILDUNG 12: FOKUS-, AUSWAHL- UND BEWERTUNGSKRITERIEN FÜR STANDARDS .....	42
ABBILDUNG 13: BETRACHTUNGSUMFANG UND FOKUS DER STUDIE.....	43
ABBILDUNG 14: VORGEHEN BEI DER ANALYSE VON STANDARDISIERUNGSLÜCKEN .....	47
ABBILDUNG 15: FOKUS- UND AUSWAHLKRITERIEN FÜR STRATEGISCHE TRENDS.....	48
ABBILDUNG 16: ÜBERSICHT VON STANDARDISIERUNGSORGANISATIONEN IM CLOUD COMPUTING .....	52
ABBILDUNG 17: ÜBERSICHT DER 20 AUSGEWÄHLTEN „CLOUD-STANDARDS“ .....	72
ABBILDUNG 18: ÜBERSICHT DER BEWERTUNG DER 20 „CLOUD-STANDARDS“ .....	74
ABBILDUNG 19: ÜBERBLICK DER STANDARDISIERUNGSLÜCKEN IM CLOUD COMPUTING .....	76
ABBILDUNG 20: EINORDNUNG DER 20 CLOUD-STANDARDS IM NORMUNGS- UND STANDARDISIERUNGSUMFELD .....	76
ABBILDUNG 21: HANDLUNGSFELDER DES AKTIONSPROGRAMMS CLOUD COMPUTING. ....	145
ABBILDUNG 22: ÜBERSICHT DER HANDLUNGSZIELE .....	149
ABBILDUNG 23: ÜBERSICHT DER HANDLUNGSFELDER .....	150

## Tabellenverzeichnis

TABELLE 1: ÜBERSICHT WICHTIGER STANDARDISIERUNGSORGANISATIONEN IM CLOUD COMPUTING....	52
TABELLE 2: ÜBERSICHT DER 20 AUSGEWÄHLTEN “CLOUD-STANDARDS“ .....	73
TABELLE 3: STRATEGISCHE TRENDS DER STANDARDISIERUNG IM CLOUD COMPUTING.....	127

## 1 Zusammenfassung

### **Zielsetzung, Ausgangssituation und Taxonomie**

Das Bundesministerium für Wirtschaft und Technologie (BMWi) hat im Frühjahr 2011 Booz & Company in Kooperation mit dem FZI Forschungszentrum Informatik beauftragt, die Studie „Das Normungs- und Standardisierungsumfeld von Cloud Computing“ durchzuführen. Sie ist in den Kontext des „Aktionsprogramms Cloud Computing“ und dessen Technologieprogramm „Trusted Cloud“ eingebettet. Deren erste Zielsetzung ist, einen Überblick über das existierende Normungs- und Standardisierungsumfeld bereitzustellen. Die deutsche Perspektive wird als Teil der Gesamtanalyse auf europäischer und internationaler Ebene berücksichtigt. Der Blick richtet sich neben Normen und Standards auch auf Vorarbeiten zur Standardisierung wie Orientierungswissen, (Referenz-) Implementierungen oder Spezifikationen, sowie Industriestandards als auch Zertifizierungen (vgl. 3.1.3). Das größte Gewicht liegt auf der Betrachtung technischer Standards; es werden aber auch Standards für das Management einbezogen und rechtliche Bezüge berücksichtigt.

Die zweite Zielsetzung der Studie sind Empfehlungen für die Trusted Cloud-Projekte hinsichtlich der Potenziale und Problemstellungen, die die Standardisierung innerhalb der Laufzeit bis Anfang 2015 mit sich bringt.<sup>1</sup>

Die Studie soll einen strategischen Aktionsrahmen und ordnungspolitische Handlungsempfehlungen erarbeiten und damit die Grundlage für eine deutsche Roadmap zur Standardisierung im Cloud Computing schaffen.

### ***Das Standardisierungsumfeld ist heterogen***

Das Normungs- und Standardisierungsumfeld im Cloud Computing findet sich – zusammenfassend betrachtet – noch in einer Frühphase. Es ist aktuell im Entstehen begriffen und gewinnt zunehmend an Eigendynamik. Diese Studie ist somit zwangsläufig eine erste Momentaufnahme.<sup>2</sup> Etablierte US-amerikanische Anbieter besitzen heute durch die Marktmacht ihrer proprietären Industriestandards den größten Einfluss auf die Standardisierung im Cloud Computing. In der zweiten Reihe positionieren sich Konsortien, die als Markteintrittsstrategie offene Standards anstreben. Bisherige Bemühungen zur Standardisierung stecken konzeptionell in den Kinderschuhen, da ein Mangel an einheitlichen Definitionen oder Orientierungswissen ein zielorientiertes gemeinsames Handeln behindert. Die Verbreitung wirklich anwendbarer und genutzter Standards für das Cloud Computing wird durch das Fehlen nationaler Regeln oder deren Harmonisierung sowie unzureichende technische Konvergenz erschwert. Viele führende Industriestaaten befinden sich im Jahr 2012 hinsichtlich Cloud Computing und seiner Standardisierung in der Orientierungs- und Planungsphase.

---

<sup>1</sup> Diese Ergebnisse stehen nur den jeweiligen Trusted Cloud-Projekten zur Verfügung.

<sup>2</sup> Kürzlich veröffentlichte Standards konnten nicht alle berücksichtigt werden (z.B. TOSCA).

### ***Die Untersuchung definiert und nutzt eine konsistente Taxonomie***

Vor diesem Hintergrund wurde zuerst eine konsistente Taxonomie für die Untersuchung des Normungs- und Standardisierungsumfeldes definiert. Sie ermöglicht ein zielgerichtetes Vorgehen, eine strukturierte Betrachtung und die begriffliche Eindeutigkeit bei Beschreibung und Bewertung. So werden Standards zum einen anhand von Herausforderungen im Cloud Computing kategorisiert, die sie adressieren („**Wofür?**“); die Untersuchung betrachtet neun übergeordnete Herausforderungen (z.B. Interoperabilität, Datenschutz; siehe 3.2.1). Zum anderen werden Standards anhand ihrer Ansatzpunkte für die Standardisierung („**Wodurch?**“) unterschieden; die Untersuchung unterscheidet 14 verschiedene Ansatzpunkte (z.B. Datei- und Austauschformate, Vertragsbedingungen; siehe 3.2.2) aus den Bereichen Technik, Management und Recht. Diese beiden Perspektiven spannen einen Raum auf, der zur Einordnung der Standards im Cloud Computing Verwendung findet (vgl. Abbildung 3.2). Das allgemeine Methodologie zur Untersuchung findet sich in Kapitel 3.

### **Standardisierungsorganisationen im Cloud Computing**

Es existiert eine Vielzahl verschiedener Akteure im Normungs- und Standardisierungsumfeld von Cloud Computing. Die Studie skizziert die wichtigsten Organisationen, die sich durch ein Mindestmaß an Engagement bei der Standardisierung im Cloud Computing und ein Mindestmaß an Partizipationsmöglichkeiten auszeichnen (im Folgenden „Standardisierungsorganisationen“). Der Auswahl liegt eine anfängliche Recherche von über 150 verschiedenen Institutionen zu Grunde. Gemäß der Zielsetzung liegt der Fokus auf Normungsorganisationen, Standardentwicklungsorganisationen, Interessensvereinigungen, Konsortien oder öffentlichen Einrichtungen. Ihnen allen ist gemein, dass sie Gremien besitzen, die Standards oder Vorarbeiten mit implizitem oder explizitem Bezug zum Cloud Computing forcieren. Forschungseinrichtungen oder privat-wirtschaftliche Unternehmen sind nicht im Fokus. Bei Letzteren bestehen keine regulären Mitwirkungsmöglichkeiten für Außenstehende.

#### ***Die 19 wichtigsten Standardisierungsorganisationen***

Eine Vorreiterrolle hat das NIST der US-Verwaltung inne, das als erstes Gremium eine Standardisierungsroadmap für das Cloud Computing erarbeitet hat. Einige internationale Standardisierungsgremien zeigen ebenfalls großes Engagement, während die überwiegende Mehrheit ihren Fokus nur langsam auf Standards für das Cloud Computing ausrichtet. Auf europäischer Ebene wird das ETSI eine koordinierende Rolle einnehmen. EuroCloud ist ein pan-europäischer Unternehmensverband der Anbieter von Cloud Computing mit großem Einfluss. In Deutschland unternehmen das DIN, der BITKOM und das BSI erste Schritte bei der Anforderungsdefinition. Wichtige zukünftige Anwender von Cloud Computing in der Wirtschaft, insbesondere im Mittelstand, zeigen zu wenig Engagement.



Folgende Übersicht zeigt die 19 wichtigsten Organisationen (vgl. 4, 3.3.1) sortiert nach ihrem thematischen und regionalen Fokus.

**Abbildung A:** Übersicht von Standardisierungsorganisationen im Cloud Computing

AUSWAHL	Allgemein	Cloud Computing	IKT, sonstige
International	ISO	CSA cloud security alliance™ OASIS Open Cloud Consortium OpenGridForum	ITU IETF SNIA™ tmforum DMTF THE Open GROUP W3C
USA	NIST		
Europa	ETSI	EuroCloud	enisa European Network and Information Security Agency
Deutschland	DIN	SaaS-EcoSystem Cloud Your Business EuroCloud DEUTSCHLAND   ECO	BITKOM

Quelle: Analyse von Booz & Company und FZI

Neben den näher betrachteten Organisationen gibt es weitere, die noch kein klares Engagement zeigen oder keine Partizipationsmöglichkeiten bieten. Einige aber von ihnen werden in Zukunft voraussichtlich eine größere Rolle spielen (siehe Einleitung zu 4).

## Existierende Standards im Cloud-Umfeld

Viele Anstrengungen sind heute noch Vorarbeiten gewidmet, z.B. Orientierungswissen, Spezifikationen oder Referenzimplementierungen. Große Verbreitung besitzen vor allem proprietäre, kommerzielle Lösungen, die derzeit zum Industriestandard aufsteigen. Gleichzeitig sind Anbieter, Anwender und Intermediäre von Cloud-Diensten in ihrer Geschäftstätigkeit einer Vielzahl von Standards ausgesetzt. Für diese Akteure stellt sich die Frage, welche bestehenden Standardisierungsansätze zum jetzigen Zeitpunkt die größte Attraktivität ausstrahlen.

Im Rahmen einer intensiven Sekundär- und Primärrecherche wurden 160 Standards identifiziert und analysiert. Der Fokus der Betrachtung liegt auf branchenübergreifenden Standards, die einen expliziten Bezug zum Cloud Computing aufweisen. Fallweise Berücksichtigung erfahren Standards mit wichtigem implizitem Bezug zu Cloud Computing (z.B. Web Services).

### Die 20 relevantesten "Cloud-Standards"

Es wurden 20 prototypische Standards (vgl. 5), Vorgaben, Zertifizierungen bzw. Vorarbeiten („Cloud-Standards“) ausgewählt. Diese werden im Detail untersucht und bewertet sowie mit weiteren ca. 35 ähnlichen Standards verglichen. Die Übersicht auf der Folgeseite fasst die Ergebnisse zusammen.



**Abbildung B:** Übersicht der 20 ausgewählten “Cloud-Standards”

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

Quelle: Analyse von Booz & Company und FZI

Die 20 Cloud-Standards besitzen nach Möglichkeit Vorbildcharakter, decken die Bereiche Technik, Management und Recht ab und finden größte Beachtung in Fachkreisen. Mit dieser Vorgehensweise soll der Überblick allgemeingültig, übersichtlich und gleichzeitig möglichst umfassend und konkret gestaltet werden (vgl. 3.3.2). Kein branchenspezifischer Standard besaß genug allgemeine Strahlkraft, um in die engere Auswahl zu gelangen. Die überwiegende Mehrheit der Standards hat internationale Relevanz. Einzelne weisen einen (leichten) europäischen bzw. nationalen Bezug auf (z.B. BSI-ESCC, USDL, NIST-UC, EuroCloud-SA, 95/46/EG).

Die Bewertung der Standards spiegelt den frühen Entwicklungsstand im Cloud Computing wider. Standards, die bereits vor dem Cloud Computing existierten, weisen eine tendenziell größere Reife auf (z.B. SCAP, WS-\*, OAuth, CIMSVM, SSAE-16) als solche, die aktuell explizit für das Cloud Computing erarbeitet werden. Die Durchsetzungsfähigkeit von Standards mit explizitem Bezug zum Cloud Computing erweist sich hingegen tendenziell höher, als bei solchen mit implizitem Bezug.

Standards, die bereits heute hohe Verbreitung und Reife besitzen, sollten effektiv genutzt werden („Use!“). Solche, die eine geringe Verbreitung genießen, sollten gefördert werden („Promote!“) und bei solchen, die sich erst in der Entwicklung befinden, sollte mitgewirkt werden („Contribute!“).

### **Standardisierungslücken im Cloud-Umfeld**

Die Standardisierungslücken und Weiterentwicklungsmöglichkeiten sind allgemein groß (vgl. 5.4). Es gibt eine recht unübersichtliche Menge teils ähnlicher oder unreifer Standards mit unklarer Relevanz am Markt. Viele existierende Standards, die nur einen impliziten Bezug zum Cloud Computing besitzen, bilden eine solide Basis (bspw. OAuth, SCAP, WS-\* oder USDL). Sie müssen aber erst noch an das Cloud Computing angepasst werden. Vielen neuen Standards, die explizit für das Cloud Computing entwickelt werden, fehlt es bislang an hinreichender Reife. In einigen Bereichen ist ein vollständiger Mangel an Standards ersichtlich.

Die Mehrzahl der Standardisierungsaktivitäten fokussiert sich auf Herausforderungen, wie Informationssicherheit, Effizienz, Interoperabilität oder Portabilität vor allem aus einer technischen Perspektive. Weiterer Bedarf nach technischen Standards besteht beispielsweise bei Standardkomponenten, Referenzarchitekturen, Benchmarks, Tests oder Protokollen und Schnittstellen.

Im Bereich der Managementstandards bestehen die größten Lücken. Es existieren keine oder nicht ausreichend umfassende Standards für Geschäftsmodelle, Dienstgütevereinbarungen, Managementmodelle sowie -prozesse, Controlling und vertragliche Regelungen. Denkbar wären auch standardisierte, verbindliche unternehmensinterne Vorschriften (Binding Corporate Rules, BCR) für Cloud-Anbieter zu Datenschutz im Zuge einer Selbstregulierung.

Das Zusammenspiel des Rechtsrahmens und der Standardisierung im Cloud Computing ist vielschichtig und wird bislang überwiegend auf Datenschutz

reduziert. Auf europäischer und deutscher Ebene ist die Klärung des grundsätzlichen strategischen regulatorischen Vorgehens notwendig.

## Standardisierungspotenziale in Deutschland

Für Deutschland und Europa stehen vor allem die Herausforderungen von Interoperabilität, Datenschutz, Rechtssicherheit und Wettbewerb im Vordergrund. Größte Priorität sollte die Schaffung einer Cloud-Zertifizierung, beispielsweise im Sinne eines Gütesiegels „Cloud Computing – Made and Secured in Germany“, besitzen. Rechtsverträglichkeitsprüfungen und die Bereitstellung von Orientierungswissen sind hierfür zentrale Voraussetzungen.

Im Technologieprogramm Trusted Cloud besteht weiteres Potenzial bei der Standardisierung etwa von Sicherheitsarchitekturen, sicheren Betreiberplattformen, Lösungen für Datenschutz und Transparenz, Identitätsmanagement, Cloud-Servicebeschreibungssprachen sowie Protokollen und Schnittstellen.

## Trends bei der Standardisierung im Cloud Computing

Zusätzlich wird der Blick mit der Beschreibung strategischer Trends bei der Standardisierung im Cloud Computing auf die Zukunft gerichtet (siehe 6). Als Ausgangspunkt wurden verschiedene Aktivitäten der letzten Jahre in Themenbereiche gruppiert. Solche Themenbereiche, die die größte fortschreitende Eigendynamik auf einen Zeithorizont bis 2015 erwarten lassen, wurden herausgegriffen und in ihrer absehbaren Entwicklung untersucht. Der Fokus liegt auf Trends mit starkem Bezug zu Europa oder Deutschland.

### Sechs wichtige strategische Trends

Folgende Übersicht fasst die sechs identifizierten Trends zusammen.

Abbildung C: Strategische Trends der Standardisierung im Cloud Computing (Kurzfassung)

Cloud-Standardisierung & staatliche Mitwirkung	<ul style="list-style-type: none"> <li>– Die <b>USA besitzen eine Vorreiterrolle</b> (z.B. <i>NIST Roadmap</i>)</li> <li>– Bei vielen Industrienationen deuten sich <b>ab 2012 zunehmende Bemühungen</b> an z.B. (Deutschland, Frankreich, Japan)</li> </ul>
Cloud-Zertifizierung	<ul style="list-style-type: none"> <li>– <b>Seit 2009 gibt es erste</b>, vergleichsweise noch unreife <b>Cloud-Zertifizierungen</b> für Standards, Experten und Geschäftspartner</li> <li>– Ein <b>hoher Automatisierungsgrad</b> der Auditierung wird <b>angestrebt</b></li> </ul>
Offenheit im Cloud Computing	<ul style="list-style-type: none"> <li>– <b>Nachzügler wollen sich zunehmend mit Hilfe offener Standards etablieren</b></li> <li>– <b>Unterschiedliche Auffassungen</b> von Offenheit</li> </ul>
Rechtssicherheit für die Cloud	<ul style="list-style-type: none"> <li>– Die bisherigen Cloud-Lösungen garantieren <b>keine Konformität mit geltendem deutschen und europäischen Recht</b></li> <li>– <b>Verbindliche Standards können Rechtssicherheit schaffen</b></li> </ul>
Cloud-Marktplätze	<ul style="list-style-type: none"> <li>– <b>Die innovative Erweiterung des Cloud Computing</b> um den Marktplatz-Gedanken wird seit 2010 verstärkt aufgegriffen</li> <li>– <b>Standards für Flexibilität &amp; Vertrauen</b> im Ökosystem <b>notwendig</b></li> </ul>
Governance im Cloud Computing	<ul style="list-style-type: none"> <li>– Es werden <b>erste Standards</b> und Anforderungsdefinitionen (z.B. <i>zu KPIs</i>) zur Governance im Cloud Computing erarbeitet</li> <li>– Standards zur <b>Adressierung komplexer Anforderungen</b> nötig</li> </ul>

Quelle: Analyse von Booz & Company und FZI

Der erste Trend (dunkelblau) fügt der Betrachtung eine themenübergreifende Perspektive hinzu. Er analysiert allgemein die Aktivitäten staatlicher Akteure bei der Standardisierung im Cloud Computing. Alle Trends besitzen unmittelbare strategische Relevanz für die Cloud-Standardisierung, da sie einen inhärenten Bezug zu den Herausforderungen im Cloud Computing aufweisen.

### **Handlungsempfehlungen für die Cloud-Standardisierung**

Für die Zukunft sind eine gesamthafte Betrachtung und eine koordinierte Zielbestimmung für die Arbeiten auf dem Feld der Cloud-Standardisierung notwendig. Dies sollte möglichst abgestimmt auf internationaler, europäischer und deutscher Ebene erfolgen. Es sollte vorrangig darum gehen, im Interesse eines funktionierenden fairen Wettbewerbs bestehende Lücken zu schließen. So bestehen sehr viele Herausforderungen hinsichtlich Interoperabilität, Portabilität, sowie besserer Transparenz, Rechtssicherheit (etwa in Bezug auf Datenschutz), Informationssicherheit und Governance, oder grundsätzlich der Offenheit für mehr Wettbewerb.

#### ***Wirtschaft und Staat sind aufgefordert zu Handeln***

Der deutschen Wirtschaft obliegt die Hauptverantwortung durch eine aktivere Rolle bei der Standardisierung ihre vitalen Interessen im Cloud Computing zu vertreten. Zugleich ist ordnungspolitisches Handeln entscheidend, da nur so einem möglichen Marktversagen frühzeitig begegnet werden kann. Cloud Computing sollte auch kein Gebiet mit unklarer Rechtslage sein; dafür birgt es zu viele Wachstumschancen. Ein rasches Handeln ist notwendig, da bis 2014 entscheidende Standardisierungsentscheidungen im Cloud Computing zu erwarten sind und damit Fakten geschaffen werden. In der gegenwärtigen Frühphase werden die Spielregeln für den Markt von morgen bestimmt. Mit fortschreitender Entwicklung sinken die Einflussmöglichkeiten.

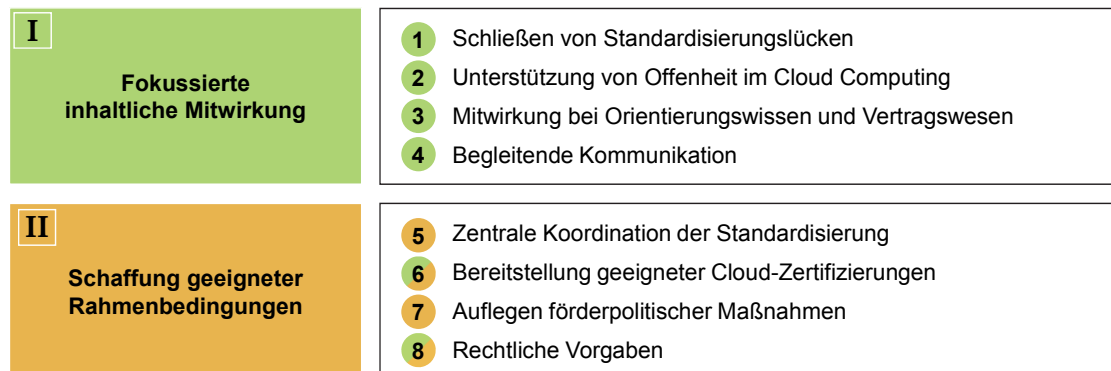
Das Handlungswirken seitens der deutschen Politik sollte sich auf zwei Ziele konzentrieren, die sich auch weitgehend auf die EU-Ebene übertragen lassen.

- **Strategisches Handlungsziel I:** Der Staat sollte in fokussierter Weise und begrenztem Maße inhaltlich bei der Standardisierung mitwirken. Der Schwerpunkt liegt auf der Anforderungsdefinition. Die eigentliche Standardisierung ist Aufgabe der Wirtschaft.
- **Strategisches Handlungsziel II:** Um ein koordiniertes und zielgerichtetes Vorgehen aller Akteure bei der Standardisierung zu ermöglichen, sollten geeignete Rahmenbedingungen bei der Standardisierung geschaffen werden. Das Handlungswirken sollte auf möglichst partizipative Instrumenten setzen.

Diese Ziele sind innerhalb des bestehenden Handlungsrahmens zu betrachten. Auf EU-Ebene sind dies vor allem die geplante Cloud-Strategie der EU-Kommission, der Expertenbericht „The Future of Cloud Computing“ und die laufenden F&E Projekte im Rahmen von FP7 zum Cloud Computing. In Deutschland bilden das Aktionsprogramm Cloud Computing, das Technologieprogramm Trusted Cloud, die angestrebte Marke „Cloud Computing – Made and Secured in Germany“ (vgl. 7.1.1) und die geplante Standardisie-

rungsroadmap den entscheidenden Rahmen. Unter Berücksichtigung dieses Handlungsrahmens wurden acht konkrete Handlungsfelder für die Bundesregierung abgeleitet, die in folgender Abbildung zusammengefasst werden.

**Abbildung D:** Übersicht der zwei Handlungsziele und acht Handlungsfelder



Quelle: Analyse von Booz & Company und FZI

Im Folgenden werden die Handlungsfelder kurz beschrieben (vgl. 7.3.1 ff.):

1. **Schließen von Handlungslücken:** Offene Standardisierungslücken sollten priorisiert werden und öffentliche Anforderungen klar formuliert werden. Bestehende Standards sollten katalogisiert werden (z.B. ähnlich eines SAGA im E-Government).
2. **Unterstützung von Offenheit im Cloud Computing:** Die Offenheit von Standards sollte durch das Setzen von Anreizen gefördert werden. Standards sollten auf Offenheit geprüft werden.
3. **Mitwirkung bei Orientierungswissen und Vertragswesen:** Orientierungswissen und dessen Eckpfeiler sollen definiert und erarbeitet werden, um Doppelarbeit zu vermeiden. Standards für das Vertragswesen sollten vom rechtlichen Rahmen abgegrenzt werden.
4. **Begleitende Kommunikation:** Standardisierungsaktivitäten, Orientierungswissen und Unterstützungsangebote sollten durch eine begleitende Öffentlichkeitsarbeit an alle Akteure kommuniziert werden, um das Bewusstsein für die Cloud-Standardisierung zu stärken.
5. **Zentrale Koordination:** Die Standardisierung muss in Deutschland über nationale, europäische und internationale Verwaltungsebenen hinweg sowie unter Einbeziehung aller Akteure zentral koordiniert werden (z.B. Standardisierungsroadmap).
6. **Bereitstellung geeigneter Zertifizierungen:** Die Marke „Cloud Computing – Made and Secured in Germany“ sollte durch geeignete Zertifizierungen im Cloud Computing untermauert werden.
7. **Auflegen förderpolitischer Maßnahmen:** Bestehende förderpolitische Maßnahmen sollten durch flankierende Maßnahmen konsequent zur Standardisierung genutzt werden.
8. **Rechtliche Vorgaben:** Der bestehende Rechtsrahmen sollte auf Angemessenheit und Implikationen für das Cloud Computing umfassend geprüft werden, um geeignete rechtliche Vorgaben abzuleiten.

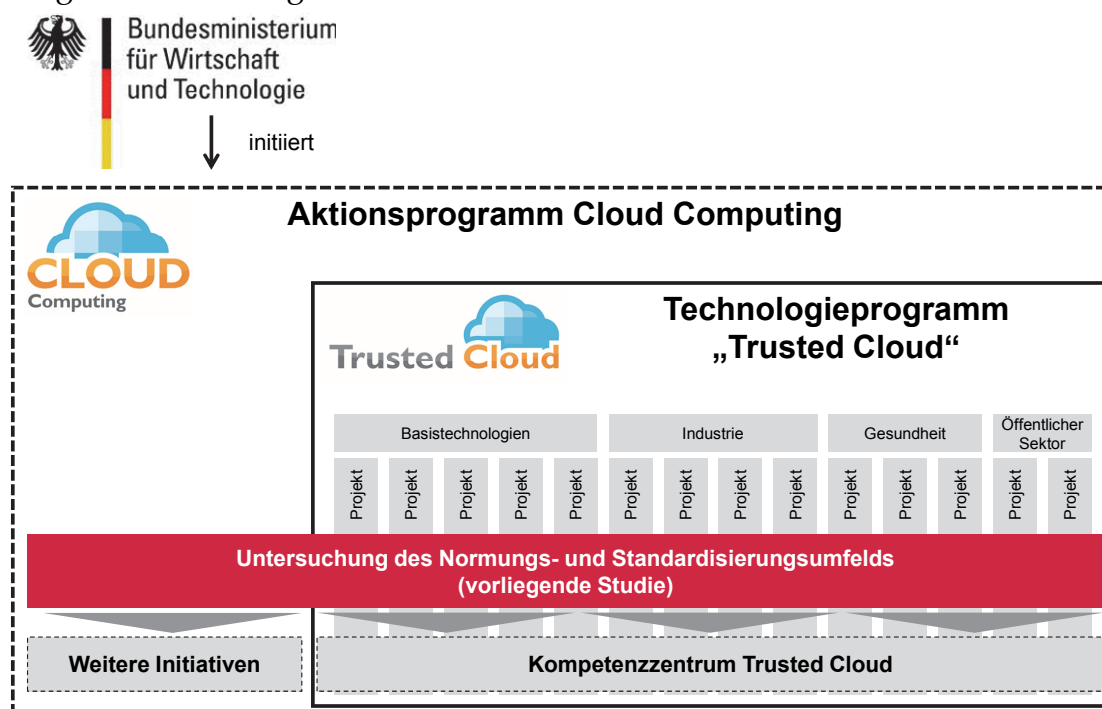


## 2 Einleitung

### 2.1 Ausgangssituation und Zielsetzung der Studie

Das Bundesministerium für Wirtschaft und Technologie (BMWi) hat Booz & Company in Kooperation mit dem FZI Forschungszentrum Informatik mit der Durchführung der Studie „Das Normungs- und Standardisierungsumfeld von Cloud Computing“<sup>3</sup> beauftragt.

Folgende Abbildung veranschaulicht den Kontext der Studie.



**Abbildung 1:** Einordnung der vorliegenden Studie

Die Untersuchung wird im Rahmen des „Aktionsprogramms Cloud Computing“ (vgl. Abbildung 1) durchgeführt, das unter Federführung des BMWi gestartet wurde und von einer Allianz aus Wirtschaft, Wissenschaft und Politik getragen wird. Hierbei sollen Zukunftschancen und Herausforderungen von Cloud Computing für den Wirtschaftsstandort Deutschland adressiert und mit konkreten Maßnahmen angegangen werden. Einer der Schwerpunktbereiche liegt dabei auf der Stärkung von Sicherheit und Vertrauen bei der Nutzung von Cloud Computing, insbesondere für kleine und mittelgroße Anwenderunternehmen (KMU) sowie Institutionen aus dem öffentlichen Sektor. Eine Fördermaßnahme des Aktionsprogramm ist das Technologieprogramm „Trusted Cloud“, mit dem das BMWi anstrebt, Forschungs- und Entwicklungsaktivitäten zu effizienten und innovativen Cloud-Infrastrukturen sowie sicheren und vertrauenswürdigen Cloud-basierten Diensten zu fördern. Als

<sup>3</sup> Abkürzung. Der vollständige Titel lautet: Untersuchung des Normungs- und Standardisierungsumfelds zum BMWi-FuE-Schwerpunkt "Sichere Internet-Dienste - Sicheres Cloud Computing für Mittelstand und öffentlichen Sektor (Trusted Cloud)".

Ergebnis von „Trusted Cloud“ werden innovative Cloud-Lösungen, Praxiserfahrungen und Geschäftsmodelle erwartet.

Vor diesem Hintergrund besteht die **erste zentrale Zielsetzung** der vorliegenden Studie darin, eine Untersuchung des aktuellen Normungs- und Standardisierungsumfeldes von Cloud Computing durchzuführen. Es soll ein Überblick über das Standardisierungsgeschehen auf internationaler, europäischer und deutscher Ebene geschaffen werden. Die **zweite Zielsetzung** ist die Analyse der Trusted Cloud-Projekte hinsichtlich ihrer Problemstellungen und Potenziale bei der Standardisierung während der Laufzeit des Technologieprogramms bis Anfang 2015. Es soll frühzeitig in der ersten Forschungsphase des Technologieprogramms eine gemeinsame Sicht des BMWi und der Trusted Cloud-Projekte auf eine mögliche Standardisierung im Technologieprogramm geschaffen werden. Dadurch soll einem potenziellen Zeit- und Ressourcenverlusten frühzeitig entgegengewirkt und die Interoperabilität und Kompatibilität zwischen den Projekten erleichtert werden.

Unter Berücksichtigung der Gesamtergebnisse soll die Studie letztlich den strategischen Aktionsrahmen und ordnungspolitische Handlungsempfehlungen für das BMWi erarbeiten, um allgemein die Grundlage für eine mögliche Roadmap zur Standardisierung im Cloud Computing für Deutschland zu schaffen.

Folgende Aufgaben und Zielsetzungen wurden im Rahmen der Ausschreibung für die Studie vorgegeben:<sup>4</sup>

- Erarbeitung einer **Übersicht über** bereits existierender Normen und **Standards** im Cloud Computing Bereich.
- **Bewertung** der Bedeutung, Anwendungs- und Zukunftsfähigkeit der bestehenden Normen und Standards.
- Darstellung von erkennbaren **Strategieentwicklungen** potenzieller Wettbewerber im Cloud Computing.
- Identifikation und Definition der Bereiche, in denen bei der Normung und Standardisierung **Technikkonvergenz** Voraussetzung für zukunftsfähige Normen oder Standards ist.
- Analyse der ausgewählten Pilotprojekte auf Probleme in Bezug auf ihre **Interoperabilität und Kompatibilität** untereinander.
- Identifizierung von sich ergebendem **Standardisierungspotenzial** und Ableitung von **Handlungsoptionen** für die „Trusted Cloud“-Projekte.
- Analyse initiiert neuer Themen bei den Regelsetzern auf Gestaltungspotenzial, Rahmenbedingungen für den nationalen Kontext und Ableitung einer **nationalen Strategie**.

---

<sup>4</sup> Verkürzte Zusammenfassung.



## 2.2 Vorgehen und Aufbau der Studie

Die vorliegende Studie ist in zwei Arbeitsstränge „Überblick Normen und Standards“ sowie „Analyse der Projekte“ gegliedert, die unterschiedliche Sichtweisen auf Normen und Standards im Cloud Computing widerspiegeln. Diese Zweiteilung findet sich sowohl im Vorgehen bei der Erstellung der Studie („blau“) als auch in ihrem Aufbau („beige“) wieder, wie es in folgender Abbildung zusammengefasst ist.

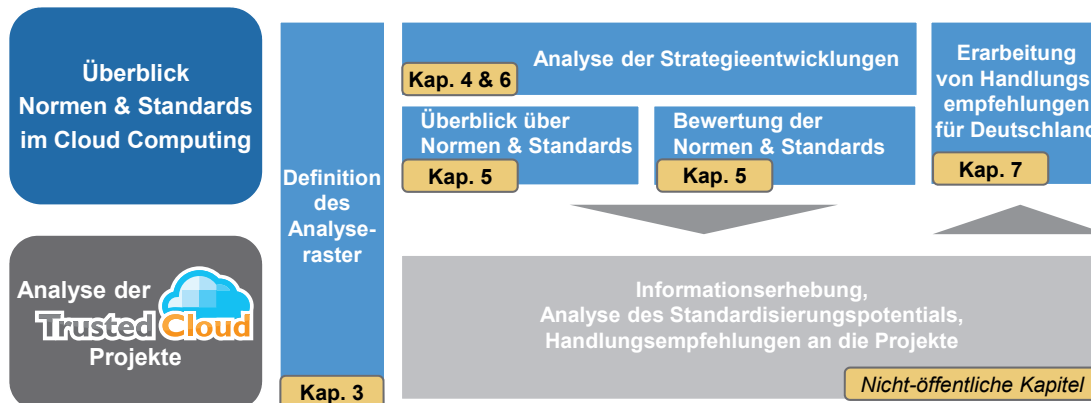


Abbildung 2: Aufbau und Vorgehen der Studie

Den Analysen der Studie – also der Erhebung und Bewertung des Cloud-Standardisierungsumfelds – liegt ein konsistentes und umfassendes Analyseraster zu Grunde (vgl. „Definition des Analyserasters“ in Abbildung 2):

- Das Analyseraster und dessen Methodologie werden gebündelt vorab in **Kapitel 2.3** beschrieben. Es umfasst Begriffe, Definitionen, eine Taxonomie für Standardisierung im Cloud Computing und den Analyseansatz der einzelnen Kapitel.

Der Rest der Studie (Kap. 4 ff.) konzentriert sich auf die Ergebnisdarstellung.

### Arbeitsstrang „Überblick Normen & Standards“:

Der erste Arbeitsstrang betrachtet Normen & Standards des Cloud-Computing aus einer allgemeinen Perspektive. Die Analysen berücksichtigen gleichermaßen die internationale, europäische und deutsche Perspektive. Dem Überblick liegen umfassende Recherchen und eine Vielzahl verschiedener Quellen zu Grunde (vgl. 3.3.2).

- In **Kapitel 4** werden 19 wichtige Organisationen, die sich bei der Standardisierung im Cloud Computing auf internationaler, europäischer oder deutscher Ebene engagieren, vorgestellt (vgl. „Analyse der Strategieentwicklungen“ in Abbildung 2). Diese *Standardisierungsorganisationen* (vgl. 3.1.1) und deren Aktivitäten bilden den zentralen Ausgangspunkt für alle weiteren Analysen.
- Unter anderem auf Basis dieser Arbeitsergebnisse folgt in **Kapitel 5** ein Überblick über aktuelle *Vorarbeiten, Standards und Zertifizierungen im Cloud Computing*. Eine relevante Auswahl von 20 „Cloud-Standards“ wird klassifiziert sowie in Steckbriefen beschrieben und bewertet. Ähnliche Standards werden vergleichend angeführt.

- In **Kapitel 5.4** werden abschließend und zusammenfassend **Lücken** („White Spots“) im Standardisierungsumfeld des Cloud Computing identifiziert und beschrieben.
- Zur Vervollständigung der Analyse bestehender Strategien werden in **Kapitel 6** sechs *strategische Trends* bei der Standardisierung im Cloud Computing identifiziert und zusammenfassend beschrieben.
- Im letzten Schritt dieses Arbeitsstranges werden in **Kapitel 7** aus den bisherigen Ergebnissen *Handlungsempfehlungen* für die Bundesregierung abgeleitet.

#### **Arbeitsstrang „Analyse der Projekte“:**

Der zweite Arbeitsstrang betrachtet die Thematik aus Sicht der 14 im Rahmen von Trusted Cloud geförderten Projekte. Hierzu ist zunächst eine eingehende Analyse der jeweiligen Projektvorgaben auf Basis der Antragsunterlagen erfolgt, die durch eine gezielte Informationsabfrage mittels eines strukturierten Erhebungsbogens ergänzt wurde. Die Ergebnisse der Problem- und Potenzialanalyse, der Konvergenzanalyse und der Handlungsempfehlungen werden den Projekten in individuellen, vertraulichen Informationspaketen zur Verfügung gestellt.

Die beiden Handlungsstränge sind eng miteinander verwoben. Einerseits dient der Arbeitsstrang „Überblick Normen & Standards“ als Strukturrahmen für die Analyse der Projekte und wichtige operative Informationsbasis für die Projekte. Andererseits war für die allgemeine Beschreibung des Normungs- und Standardisierungsumfeldes die Rückkopplung mit den Projekten wichtig, um die Praxistauglichkeit zu schärfen.

### **2.3 Cloud Computing**

Cloud Computing stellt heute ein zentrales Paradigma der IT dar. Mit dieser Entwicklung geht eine zunehmende Industrialisierung der IT durch Modularisierung, Virtualisierung und Standardisierung einher. Neben der Möglichkeit, die Komplexität bei Entwicklung und Betrieb der „in-house“-IT zu reduzieren, liegen Potenziale in der Umsetzung von Skaleneffekten (z.B. Konsolidierung von IT-Ressourcen), in geringerer Kapitalbindung sowie höherer Flexibilität und Transparenz.

Für kleinere und mittlere Unternehmen (KMU) sowie öffentliche Institutionen ist Cloud Computing besonders attraktiv, da bei herkömmlichem Ansatz hohe „sprungfixe“ Investitionen erforderlich sind, um eine moderne und wettbewerbsfähige IT-Infrastruktur zu etablieren und zu erhalten. Internes IT-Fachpersonal steht oftmals nur eingeschränkt bereit, um Verfügbarkeits-, IT-Sicherheits-, Compliance- und technische Anforderungen in voller Breite abzudecken – eine Schließung von Kompetenz- und Kapazitätslücken über den Einsatz externer Ressourcen ist i.d.R. unverhältnismäßig kostenintensiv. Vor diesem Hintergrund bietet Cloud Computing die notwendige Flexibilität, dynamisch und kosteneffizient IT-Infrastruktur und IT-Dienstleistung dem tatsächlichen Bedarf angepasst und nach tatsächlicher Nutzung abrechenbar zu beziehen.

Das wirtschaftliche Potenzial ist enorm: Die Experton Group (Studie für den BITKOM) prognostiziert einen Umsatz von Cloud Computing-Anbietern in Deutschland von 8,2 Milliarden Euro im Jahr 2015<sup>5</sup>, was einem Anteil von ca. 5% an den gesamten ITK Ausgaben in Deutschland entsprechen würde (157 Mrd. Euro in 2015 bei konstantem Wachstum von 2% p.a. ab 2010)<sup>6</sup>. Nach einer Untersuchung von Spiceworks (Studie "SMB Cloud Computing Adoption") nutzen bereits 14% der kleineren und mittleren Firmen Cloud Computing, weitere 10% planen unmittelbar den Einsatz von Cloud-Diensten und 32% besitzen kein Vertrauen in die bisherigen Cloud-Lösungen.<sup>7</sup>

In den folgenden Abschnitten wird zunächst das der Studie zugrunde liegende Verständnis von Cloud Computing als neues IT- und Geschäftsparadigma für die Bereitstellung, Nutzung und Abrechnung von IT-Ressourcen als Dienst vorgestellt (Kapitel 2.3.1).<sup>8</sup> Anschließend wird kurz ein Überblick über technologische und ökonomische Entwicklungen gegeben (Kapitel 2.3.2), die Wegbereiter des Cloud Computing darstellen.

### 2.3.1 Begriffe und Definitionen

Cloud Computing bietet die Möglichkeit, Speicherkapazitäten, Rechenleistung und Anwendungen nach kundenspezifischen Bedarfen als Dienst über das Internet zu beziehen. Das Zusammenspiel von Infrastrukturkomponenten (Server, Speicher, Netze, Middleware) und verfügbaren Diensten erscheint dem Anwender als „Wolke“ möglicher Computer- und Kommunikationsanwendungen, wodurch der Begriff des Cloud Computing geprägt wurde. Die so ermöglichte bedarfsgerechte, skalierbare und flexible Nutzung von IT-Diensten wird unterstützt durch neuartige Geschäftsmodelle, bei denen die Abrechnung je nach Funktionsumfang, Nutzungsdauer und Anzahl der Nutzer erfolgt. Zusammenfassend wird Cloud Computing unter Berücksichtigung der technischen und ökonomischen Aspekte in der Studie wie folgt definiert:

*„Unter Ausnutzung virtualisierter Rechen- und Speicherressourcen und moderner Web-Technologien stellt Cloud Computing skalierbare, netzwerk-zentrierte, abstrahierte IT-Infrastrukturen, Plattformen und Anwendungen als on-demand Dienste zur Verfügung. Die Abrechnung dieser Dienste erfolgt nutzungsabhängig.“<sup>9</sup>*

---

<sup>5</sup> Pressemitteilung des BITKOM, [http://www.bitkom.org/files/documents/BITKOM\\_PK\\_Cloud\\_Computing\\_CeBIT\\_28\\_02\\_2010\(1\).pdf](http://www.bitkom.org/files/documents/BITKOM_PK_Cloud_Computing_CeBIT_28_02_2010(1).pdf).

<sup>6</sup> ITK-Marktzahlen des BITKOM, Analyse von Booz & Company und FZI, [http://www.bitkom.org/files/documents/BITKOM\\_ITK-Marktzahlen\\_Kurzfassung\\_Maerz\\_2011.pdf](http://www.bitkom.org/files/documents/BITKOM_ITK-Marktzahlen_Kurzfassung_Maerz_2011.pdf).

<sup>7</sup> <http://www.spiceworks.com/voice-of-it/>

<sup>8</sup> Der angewandte Cloud Computing Begriff folgt der NIST-Definition sowie dem dort vorgeschlagenen Referenzmodell des Cloud Computing (vgl. NIST(2011)).

<sup>9</sup> Baun et al. (2011), S. 4.

Folgende Servicemodelle werden im Cloud Computing unterschieden:<sup>10</sup>

- **Infrastructure-as-a-Service (IaaS):**  
Die Anwender erhalten über das Internet Zugriff auf einzelne virtuelle Ressourcen, z.B. Server, Speicher, Middleware-Komponenten. Die Verwaltung (z.B. Wartung, Skalierung) dieser obliegt dem Nutzer.
- **Platform-as-a-Service (PaaS):**  
Durch die Verwendung von PaaS erhalten Anwender Zugriff auf eine Entwicklungs- und Ausführungsumgebung für Anwendungen in der Cloud. Diese baut in der Regel auf der virtualisierten Hardware auf, diese erscheint dem Anwender jedoch transparent. Verwaltungs- und Wartungsarbeiten werden durch die Plattform übernommen (z.B. Wartung, Skalierung).
- **Software-as-a-Service (SaaS):**  
Anwender nutzen Software-Anwendungen direkt über das Internet. Eine Installation auf dem eigenen PC bzw. im Rechenzentrum des Unternehmens ist nicht erforderlich.

Unter Betriebs-, Eigentums- und Organisationsaspekten können Private Clouds (für eine geschlossene Nutzergruppe) und Public Clouds (für eine große Anzahl verschiedener Nutzer) unterschieden werden. In der Realität finden sich häufig auch Nutzungskombinationen (Hybrid Clouds) von Private Clouds, Public Clouds und traditionellen sogenannten „on premise“ IT-Umgebungen.

### 2.3.2 Grundlagen des Cloud Computing

Der Erfolg des Cloud Computing basiert auf eine Reihe von technologischen und ökonomischen Entwicklungen. Diese gestalten auch das Umfeld der Normierung und Standardisierung.

Die Entwicklung von Cloud Computing wird insbesondere durch folgende technischen Entwicklungen geprägt:

- **Virtualisierung:** Die durch Cloud Computing ermöglichte Effizienzsteigerung basiert auf gemeinsamer Nutzung von Ressourcen durch Ressourcenvirtualisierung. Dies wird durch die Abstraktion gemeinsam genutzter, physischer Ressourcen in mehrere eigenständige, logische Ressourcen ermöglicht. Es kann dabei zwischen Virtualisierung von Servern, Datenspeichern, Netzen und Software unterschieden werden. In der Regel kommen dabei virtuelle Maschinen (auch Instanzen genannt) zum Einsatz.
- **Service-orientierte Architekturen:** Neben der Virtualisierung sind Service-orientierte Architekturen eine wesentliche Grundlage für Cloud Computing. Die damit verbundene lose Kopplung von Komponenten er-

---

<sup>10</sup> Auf eine ausführliche Diskussion der Konzepte IaaS, PaaS, SaaS sowie Private, Public Clouds wird in dieser Studie verzichtet. Weiterführende Literatur hierzu ist bspw.: NIST 2011, BSI 2010, Baun 2010.

möglicht die flexible (Re-)Kombination von Cloud Diensten auf Basis Nachrichten-basierter Kommunikation. Im Fall von Public Clouds erfolgt die Dienstkommunikation üblicherweise über Internetstandards (z.B. SOAP, WSDL, HTTP, TCP).

- **Grid-Computing:** Cloud Computing kann auf Grundlage von verteilten Infrastrukturen betrieben werden und profitiert dabei von Entwicklungen aus dem Bereich des Grid-Computing. Im Unterschied zu Grid-Computing müssen Cloud-Systeme jedoch nicht notwendigerweise verteilt sein und können beispielsweise auch auf leistungsstarken Servern (z.B. Mainframes) betrieben werden. Auch die Annahme von autonomen Knoten des verteilten Systems trifft in Cloud Computing in der Regel nicht zu, da das Management von Cloud-Systemen typischerweise durch einen Anbieter zentral und proprietär erfolgt.

Unter ökonomischen Gesichtspunkten lassen sich insbesondere folgende Entwicklungen beobachten, die die Entwicklung von Cloud Computing beeinflussen:

- **Internet der Dienste:** Das Internet der Dienste (engl.: „Internet of Services“) versteht Dienstleistungen als über das Internet handel- und (meist) erbringbare Güter. Insbesondere die (Kosten-) effiziente Bereitstellung und flexible Nutzung von Diensten im Internet der Dienste stellt einen Anwendungsfall von Cloud Computing dar.
- **Internet der Dinge:** Im Gedanken des Internet der Dinge (engl.: “Internet of Things”) werden „smart devices“ (z.B. Kühlschrank, Heizkörper, Smartphones, Autos) und physische Alltagsgegenstände über das Internet verbunden. Dabei werden insbesondere Systemzustände abgefragt und ggfs. durch Steuereingriffe verändert. Die Verwaltung und Bearbeitung der dabei situativ anfallenden, enorm großen Datenvolumina stellt ein Anwendungsszenario von Cloud Computing dar.
- **Mobile Apps:** Leistungsfähige mobile Endgeräte (Smartphones) stellen heute eine Plattform für mobile Anwendungen (sog. Mobile Apps) bereit. Die Vermarktung und Verbreitung dieser Anwendungen (Stichwort: App Marktplätze) wie auch der Betrieb der Anwendungen selbst wird durch die zentrale Bereitstellung von Daten über das Internet unterstützt (z.B. Nachrichten, Wetterdaten, Navigationsdaten). Die schnelle Entwicklung und Bereitstellung von Mobile Apps sind beispielhafte Problemstellungen zu deren Lösung Cloud Computing einen Beitrag leisten kann.
- **Green IT:** Die Einsparung von Energie und die Verminderung von bspw. dem CO<sub>2</sub>-Austoß von IT ist Ziel der „Green IT“-Bemühungen. Durch Virtualisierung und effizientere Ressourcen-Auslastung verspricht das Cloud Computing einen Beitrag zu leisten.
- **SmartGrids:** Die Sicherstellung einer bedarfsgerechten und intelligenten Stromversorgung stellt neuartige Herausforderungen an IT-Systeme. Der Einsatz von Cloud-Diensten kann hierbei einen wichtigen Beitrag zur Erreichung der gewünschten Ressourceneffizienz leisten.

- **Open Source:** Open Source zielt bspw. auf die Reduzierung von Lock-in Effekten oder das Überkommen des sogenannten Hold-up Problems<sup>11</sup> ab. Hierzu existieren bereits einige Lösungen für Cloud Computing, die den Aufbau von offenen Cloud-Architekturen ermöglichen sollen. Potenziale für das Cloud Computing ergeben sich insbesondere bei der Sicherstellung von Interoperabilität und Portabilität zwischen Plattformen.

---

<sup>11</sup> Ein Hold-up-Problem ergibt sich zwischen zwei Vertragspartnern (hier Cloud-Dienstanbieter und -nutzer), falls der entsprechende Vertragsgegenstand (hier der Cloud-Dienst) und damit die Kosten nicht vollständig beschrieben werden können (unvollständiger Vertrag). Nach Vertragsschluss besitzt dann eine Partei aufgrund der Investitionen der anderen die höhere Verhandlungsmacht (hier meist der Cloud-Anbieter). Die Partei mit der größeren Verhandlungsmacht kann geforderte Innovationen verlangsamen, da Anreize zur Innovation der Angebote mit steigender Verhandlungsmacht sinken.



### 3 Methodologie zur Untersuchung

Die Untersuchung des Normierungs- und Standardisierungsumfeldes von Cloud Computing in der vorliegenden Studie impliziert eine Untersuchung des Umfelds auf internationaler, europäischer und deutscher Ebene unter Berücksichtigung der besonderen Anforderungen aus dem Mittelstand und dem Technologieprogramm. Da eine Standardisierung häufig auf internationaler Ebene abläuft ist der Fokus der Untersuchung erwartungsgemäß eher allgemein und breit mit einigen europäischen und deutschen Besonderheiten.

Die Untersuchung begegnet dem grundsätzlichen Bedarf nach inhaltlicher Schärfe und Klarheit durch eine nachvollziehbare Methodik. Der Hintergrund hierfür ist eine rasante Weiterentwicklung im Cloud Computing und die Tatsache, dass sich die Standardisierung noch ganz am Anfang befindet. Entsprechend besteht grundsätzlich ein begrenztes gemeinsames Verständnis bei allen Beteiligten. Im Speziellen und im Hinblick auf die Untersuchung des Normierungs- und Standardisierungsumfeldes in dieser Studie sind folgende methodische Fragestellungen zu adressieren.

- **Festlegung des Fokus:** Die Akteure, die sich bei der Standardisierung im Cloud Computing mit verschiedenen Aktivitäten und Initiativen engagieren, sind äußerst vielfältig. Gleichzeitig ist zu klären, was unter „Standard“ im Detail zu verstehen ist. Die Festlegung des Untersuchungsfokus setzt folglich eine klare Definition der Begriffswelten von Akteuren (z.B. Normungsorganisationen), Initiativen (z.B. temporäre Arbeitsgruppen) und Standards (z.B. Industriestandard) voraus.
- **Strukturierung des Normungs- und Standardisierungsumfeldes:** Es fehlt eine zielorientierte Taxonomie zur Strukturierung des Standardisierungsumfeldes. Damit Anforderungsdefinition und Lückenanalyse zu einem effizienten Standardisierungsgeschehen führen, ist dies unumgänglich.
- **Transparenz und Konzentration auf das Wesentliche:** Das Normierungs- und Standardisierungsumfeld im Cloud Computing ist komplex und weitläufig. Daher konzentriert sich die vorliegende Studie auf die wesentlichen Akteure, Standards und Trends. Es bedarf einer nachvollziehbaren, klaren und begründeten Auswahl und Bewertung.

Entsprechend dieser Fragestellungen gliedert sich dieses Kapitel in die Unterkapitel „Begriffe und Definitionen der Studie“ (Kapitel 3.1), „Taxonomie für Standards im Cloud Computing“ (Kapitel 3.2) und „Analyseansatz der Studie“ (Kapitel 3.3).

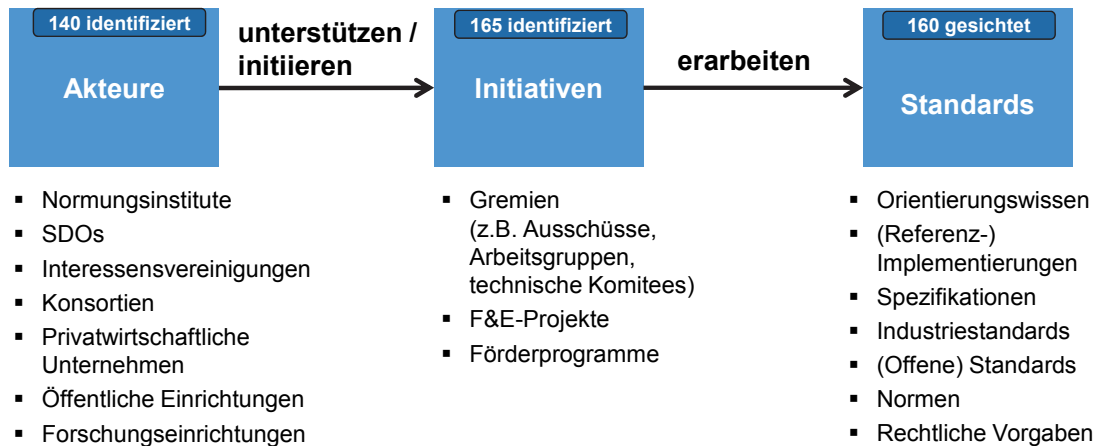
Die Methodologie, die dieser Studie zu Grunde liegt, wird gebündelt in diesem Kapitel beschrieben. Die nachfolgenden Kapitel 4 ff. können sich so auf die Darstellung, Auswertung und Bewertung der Ergebnisse konzentrieren.



### 3.1 Begriffe und Definitionen der Studie

Zunächst ist eine begriffliche Abgrenzung erforderlich, um den Fokus der Studie an einer abgestimmten Definition ausrichten zu können und so zu einem einheitlichen Verständnis beizutragen.

Folgende Abbildung zeigt überblicksartig die Begriffswelten, die der vorliegenden Studie zu Grunde liegen, und deren Sinnzusammenhang.



**Abbildung 3:** Begriffswelten der Studie – Übersicht<sup>12</sup>

Die folgenden Unterkapitel definieren die Begriffe der Abbildung.

#### 3.1.1 Begriffswelt „Akteure“

Das Cloud Computing ist in den letzten Jahren als Konzept vermehrt durch verschiedenste Akteure für Produkte und Öffentlichkeitsarbeit aufgegriffen worden. Entsprechend sind zunehmend Bemühungen bei der Standardisierung erkennbar, die sich aber in vielen Bereichen noch auf anfängliche Vorarbeiten, wie der Festlegungen von Definitionen, Anforderungen oder Use Cases, konzentrieren. In vielen Bereichen steht auch die Anpassung bestehender Spezifikationen und Standards für das Cloud Computing im Vordergrund. Insbesondere US-Anbieter versuchen ihre eigenen Cloud-Lösungen als Industriestandards durchzusetzen. Alle diese Bemühungen unterschiedlicher Reife sind für ein Verständnis der aktuellen Akteure im Cloud Computing zu berücksichtigen.

Die Gemengelage der Akteure bei der Standardisierung im Cloud Computing ist – a priori betrachtet – unübersichtlich. Sie lässt sich durch eine Vielzahl unterschiedlicher Akteure, geringe Koordination unter den Akteuren und häufige Doppelarbeit charakterisieren.

<sup>12</sup> Quelle: Analyse von Booz & Company und FZI.

Die vorliegende Studie unterscheidet folgende Akteure bei der Standardisierung im Cloud Computing:

- **Normungsorganisationen**<sup>13</sup> sind nationale, europäische oder internationale Träger mit gesetzlichem Auftrag, Normen und Standards zu entwickeln und zu veröffentlichen. Entscheidungs- sowie Konsensbildungsprozesse in Normungsorganisationen müssen öffentlich einsehbar und die erfolgte Konsensbildung nachvollziehbar sein.

**Beispiele:** ISO, CEN, DIN

- **Standardentwicklungsorganisationen** (SDOs<sup>14</sup>) sind Organisationen, deren Hauptaufgabe die (Weiter-)Entwicklung, Koordinierung und Verbreitung von Standards ist, die für eine möglichst breite Anwendung vorgesehen sind. SDOs konstituieren sich im Wesentlichen durch Gremien (siehe 3.1.2), Workshops, Meetings und Veranstaltungen. Normungsorganisationen werden gelegentlich auch zu den Standardentwicklungsorganisationen gezählt.

**Beispiele:** OASIS, W3C, ITU-T.

- **Interessensvereinigungen** sind (industrielle) Branchenverbände, Berufsgenossenschaften, Fachorganisationen oder alle anderen Vereinigungen, deren Hauptziel die konzentrierte Vertretung der Mitgliederinteressen gegenüber anderen staatlichen oder privatwirtschaftlichen Organisationen ist. Für diese Studie sind solche Interessensvereinigungen relevant, die sich bei der Standardisierung engagieren. Dies umfasst Vereinigungen auf Anbieter- sowie Anwenderseite.

**Beispiele:** BITKOM, EuroCloud.

- **Konsortien** sind zweckgebundene, befristete oder auch unbefristete Vereinigungen mehrerer rechtlich und wirtschaftlich selbstständiger Unternehmen, die zur Erfüllung einer bestimmten Aufgabe kooperieren. Für diese Studie sind solche Konsortien relevant, die sich bei der Standardisierung engagieren.
- **Privatwirtschaftliche Unternehmen** besitzen als Akteur bei der Standardisierung im Cloud Computing eine wichtige Rolle, falls von deren Cloud-Lösungen eine so große Strahlwirkung ausgeht, dass sich diese zu potenziellen Industriestandards entwickeln können.

**Beispiele:** Google, Amazon, Microsoft.

- **Öffentliche Einrichtungen** oder Agenturen im öffentlichen Raum können als Vorbereiter oder Koordinator der Standardisierung (z.B. NIST) im Cloud Computing sowie als Mitwirkende bei Standards und Zertifizierung von Standards (z.B. BSI) eine Rolle spielen.

**Beispiele:** NIST, BSI, ENISA.

---

<sup>13</sup> Engl.: De jure standards bodies

<sup>14</sup> Engl.: Standards Development Organisations (SDOs)

- **Forschungseinrichtungen** besitzen primär eine vorbereitende Rolle bei der Standardisierung im Cloud Computing, indem sie zentrale F&E-Projekte durchführen und in diesem Rahmen Spezifikationen und Anforderungen definieren.
- Der **Gesetzgeber** ist durch die Anpassung und Erarbeitung rechtlicher Vorgaben indirekt an der Standardisierung im Cloud Computing beteiligt.

Es sei darauf hingewiesen, dass die Begriffe Normungsorganisation, Standardentwicklungsorganisation, Interessensvereinigung oder Konsortium keine breite und einheitliche Verwendung erfahren und häufig auch abgewandelte Begriffe verwendet werden. Insbesondere hat sich die Verwendung des Begriffs Standardisierungsgremium (siehe 3.1.2) im Deutschen als „pars pro toto“ für Standardentwicklungsorganisationen durchgesetzt.

Zur Erhöhung der Lesbarkeit und Eindeutigkeit wird in dieser Studie vereinfachend von **Standardisierungsorganisationen** gesprochen, falls ein Akteur sich bei der Standardisierung im Cloud Computing engagiert. **Regelsetzer** sind öffentliche oder verwaltungsnahe Einrichtungen, die durch ihre Vorgaben, Förderungen und Zertifizierungen die Entwicklung im Cloud Computing und dessen Standardisierung wesentlich beeinflussen können.

### 3.1.2 Begriffswelt „Initiativen“

Eben genannte Akteure treiben die Erarbeitung und Verbreitung von Standards in **Initiativen**. Der Begriff der „Initiative“ wird im Rahmen der Studie als Sammelbegriff für alle formal organisierten Aktivitäten mit Bezug zur Standardisierung im Cloud Computing verwendet. Hierunter fallen insbesondere Arbeitsgruppen zur Standardisierung, F&E-Projekte und Förderprogramme.

- **Standardisierungsgremien** im engeren Sinn sind alle Arbeitsgruppen, Ausschüsse, technische Komitees, (Online-)Diskussionsforen, Benutzergruppen, Mailing-Listen oder ein anderer loser oder formaler Kooperationsverbund von Individuen, die sich mit einer Standardisierung beschäftigen. Der Begriff Standardisierungsgremium wird häufig als „pars pro toto“ für Standardisierungsorganisationen verwendet (siehe 3.1.1).
- **Forschungs- und Entwicklungsprojekte (F&E-Projekte)** besitzen für die Standardisierung im Cloud Computing eine vorbereitende Rolle, indem Forschungs- und Entwicklungsergebnisse zu Implementierung, Spezifikationen oder Standards führen.
- In **Förderprogrammen** stellen öffentliche Einrichtungen Gelder bereit, die zur Weiterentwicklung des aktuellen Forschungsstands im ausgeschriebenen Gebiet dienen sollen. Förderprogramme umfassen verschiedene Maßnahmen, z.B. Koordination, Öffentlichkeitsarbeit, F&E-Projekte oder auch Maßnahmen zur Standardisierung.

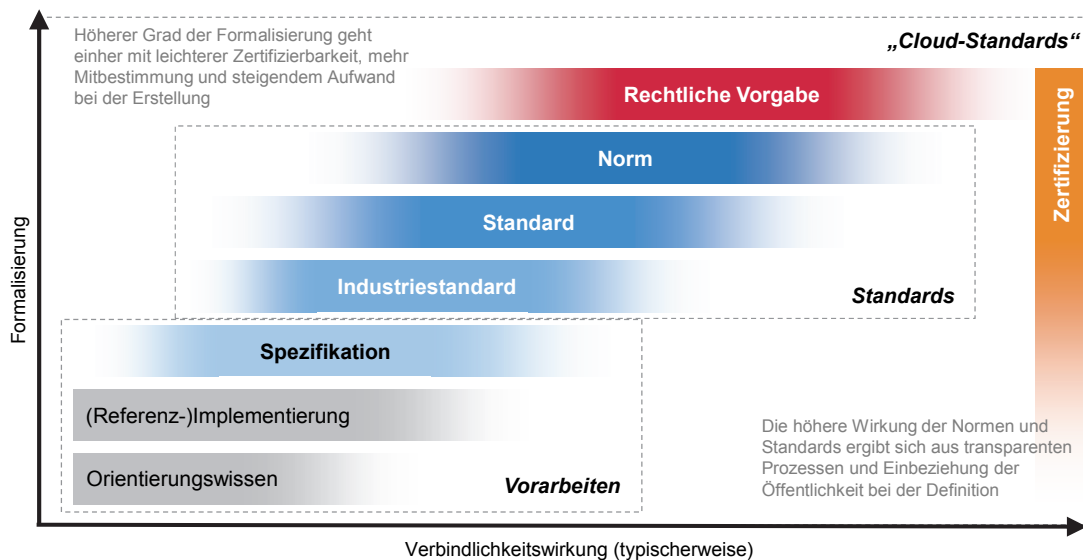
### 3.1.3 Begriffswelt „Standards“

Die begriffliche Klärung erscheint gerade auch bei „Standards“ als bedeutend, da der angelsächsische „Standards“-Begriff die Bedeutung des deutschen Begriffs „Norm“ miteinschließt. Die Studie folgt dieser Logik des erweiterten Standardbegriffs in allgemeinen Aussagen, die sowohl für Normen und Standards also auch für Normung und Standardisierung zutreffend sind. Hier beinhalten die Begriffe Standard und Standardisierung in ihrer erweiterten Bedeutung stets auch Norm und Normung.<sup>15</sup>

Bei der begrifflichen Anwendung in der vorliegenden Studie wird von der grundsätzlichen Freiwilligkeit der Anwendung von Standards ausgegangen. In ihnen selbst liegt noch keine Verbindlichkeit. Eine Anwendungspflicht kann sich jedoch sehr wohl aufgrund von Gesetzen, Rechts- oder Verwaltungsvorschriften, Verträgen oder sonstigen Rechtsgründen ergeben. In der Praxis können Standards zudem durch weichere Steuerungsinstrumente bzw. ihre Bedeutung im Markt Verbindlichkeit entfalten.

Die vorliegende Studie betrachtet nicht nur „Standards“ im engeren Sinn, sondern auch Vorarbeiten, Vorgaben und Zertifizierungen, um dem Anspruch einer umfassenden Untersuchung des Normierungs- und Standardisierungsumfeldes gerecht zu werden. Unter Vorarbeiten fallen Anforderungen, Referenzimplementierungen und Spezifikationen. Zur Erhöhung der Lesbarkeit wird bei Bedarf der Begriff „Cloud-Standards“ in Anführungszeichen gesetzt und steht vereinfachend und als Sammelbegriff für die gesamte Begriffswelt (vgl. Abbildung 4) aus Vorarbeiten, Standards, Vorgaben und Zertifizierungen.

Folgende Abbildung verdeutlicht diesen begrifflichen Zusammenhang.



**Abbildung 4:** Begriffswelt „Standards“ der Studie<sup>16</sup>

<sup>15</sup> Standards im engeren Sinne wird als Überbegriff für (Offene) Standards und Industriestandards verwandt. Vgl. hierzu die nachstehende Diskussion.

<sup>16</sup> Anmerkung: Die Darstellung besitzt illustrativen Charakter und basiert auf Trendangaben.

Die einzelnen Begriffe werden im Folgenden kurz beschrieben.

- **Orientierungswissen:** In der vorliegenden Studie werden unter „Orientierungswissen“ Anforderungen, Empfehlungen, Richtlinien, Leitfäden, Best Practice oder Use Cases für Cloud Computing subsumiert. Diese können in beliebigen Dokumenten erfasst sein (bspw. White Paper). Dokumente dieser Kategorie sind noch nicht in Form einer Spezifikation veröffentlicht und befinden sich möglicherweise vor Beginn eines Konsensbildungsprozesses.
- **(Referenz-)Implementierungen** sind in der Standardisierung von entweder vorbereitender oder ergänzender Natur. Implementierungen sind Lösungen, die ihre Praktikabilität für das Cloud Computing bereits im Einsatz zeigen, ohne zuvor in Form eines Standards spezifiziert worden zu sein. In diese Kategorie fallen beispielsweise auch wichtige etablierte Cloud-Dienste, APIs, Testbeds oder Plugfests. Referenzimplementierungen basieren auf einem Standard oder einer Spezifikation.
- **Spezifikationen** stellen den ersten Schritt in der Standardentwicklung dar. Sie beschreiben meist einen ersten Entwurf für ein Standarddokument. In der Regel werden auf Basis von Spezifikationen erste Referenzimplementierungen gebaut, die die Evaluation der Anwendbarkeit eines Standards erlauben. Spezifikationen können auch von Standardisierungsorganisationen veröffentlicht werden, erfordern aber nur einen (impliziten) Konsens unter den Verfassern. Spezifikationen beziehen sich häufig auf technische Sachverhalte, die nur spezifische Merkmale eines Produktes betreffen.
- **Standards** – im engeren Verwendungssinne – werden typischerweise von Konsortien oder industriellen Interessensverbänden spezifiziert. Neben Konsens- oder Mehrheitsentscheidung werden viele weitere Varianten zur Entscheidungsfindung in der Gruppe angewandt. Der Prozess der Entscheidungsfindung muss dabei nicht öffentlich zugänglichen Regeln folgen. Standards werden schriftlich in Dokumenten festgehalten, zielen auf allgemeine und wiederkehrende Anwendung ab und legen Regeln, Leitlinien oder Merkmale von Tätigkeiten oder Ergebnissen fest. In der Studie werden offene sowie industriespezifische Standards unterschieden:
  - Im Rahmen der vorliegenden Studie wird dann von einem **offenen Standard** gesprochen, wenn die Möglichkeit der Bewertung und Nutzung des Standards für alle gleichermaßen und frei von technischen oder juristischen Klauseln ist. Sollten einzelne Anforderungen an die Offenheit eines Standards verletzt sein,<sup>17</sup> wird in dieser Studie Standard als Bezeichnung gewählt. DIN PAS Dokumente<sup>18</sup> fallen bspw. in die Kategorie „Standard“.

---

<sup>17</sup> Vgl. hierzu auch <http://fsfe.org/projects/os/def.de.html>.

<sup>18</sup> Das DIN subsumiert unter „Spezifikation“ sowohl Standards, Spezifikationen als auch Empfehlungen. Deshalb findet die DIN-Terminologie in dieser Studie keine Anwendung.

- Bei **Industriestandards** wird häufig von „de-facto“-Standards, wie z.B. die Bluetooth-Protokolle der Bluetooth-SIG oder das IrDa-Protokoll der Infrared Data Association, gesprochen. Gedanklich ergänzt werden können diese um proprietäre herstellerspezifische Lösungen, die im Markt eine entsprechende Bedeutung erlangt haben (bspw. Amazon Machine Images).

**Synonym:** De-facto Standard.

- Eine **Norm** ist ein Dokument, das durch ein festgelegtes, nachvollziehbares Normungsverfahren im Konsens erstellt wurde und von einer anerkannten Normungsorganisation (z.B. nationale Normungsinstitute) angenommen wurde. Im Rahmen des Normungsprozesses werden Entwürfe der Öffentlichkeit zur Diskussion zur Verfügung gestellt. Eine Norm zielt auf eine allgemeine und wiederkehrende Anwendung. Sie legt Regeln, Leitlinien oder Merkmale für Tätigkeiten oder deren Ergebnisse fest. Allgemein beziehen sich Normen eher auf Produkte, die bereits erste Verbreitung im Markt gefunden haben.<sup>19</sup>

**Synonym:** De-jure Standard.

- **Rechtliche Vorgaben** sind im Gegensatz zu Standards und Normen zentrale Vorgaben der Exekutive, die rechtlich bindend sind. Sie können Normen und Standards einbeziehen oder deren Einhaltung vorgeben, um diesen Verbindlichkeit zu geben. Schwächere Vorgaben sind weiterhin bi- und multilaterale Verträge, die einen einheitlichen und verbindlichen Rahmen für Marktteilnehmer der entsprechenden Rechtssphären schaffen.

**Synonym:** Rechtsnorm

Neben der Klassifizierung von Standards steht der Begriff der Zertifizierung in einem orthogonalen Zusammenhang.

- Unternehmen, hier Anbieter und Anwender von Cloud-Lösungen, können zur Bestätigung der Einhaltung von Kriterienlisten, Standards oder rechtlichen Vorgaben **Zertifikate** erwerben. Die Aussagekraft von Zertifikaten wie auch die Nachvollziehbarkeit des Vorgangs der Zertifizierung steigt dabei mit dem Grad der Formalisierung und Verbindlichkeitswirkung.

### 3.2 ***Taxonomie für Standards im Cloud Computing***

Existierende Ansätze zur Klassifizierung von Standards im Cloud Computing unterscheiden bspw. Anforderungen der Cloud-Föderation von Anforderungen des Konfigurationsmanagements von Cloud-Diensten. Zudem werden Beiträge zur Vereinheitlichung der Begriffswelt von Anwendungsfällen oder Anforderungen des Cloud Computing unterschieden.<sup>20</sup>

Diese Studie verwendet zur grundlegenden Klassifizierung von Standards ein Vorgehen, das die Zielorientierung und inhaltliche Strukturierung gleichwer-

---

<sup>19</sup> Vgl. DIN EN 45020:2006.

<sup>20</sup> Vgl. NTT 2011.



tig behandelt. So werden Standards zum einen anhand der Herausforderungen im Cloud Computing eingeordnet, die sie adressieren („Wofür?“, vgl. Kapitel 3.2.1). Zum anderen werden Standards anhand ihrer Ansatzpunkte für die Standardisierung („Wodurch?“, vgl. Abschnitt 3.2.2 ) eingeordnet. Durch die Kombination beider Perspektiven ergibt sich die in dieser Studie verwendete Einordnungsmatrix, die näherungsweise das Normungs- und Standardisierungsumfeld aufspannt und mit der sich Standards im Cloud Computing einordnen lassen.

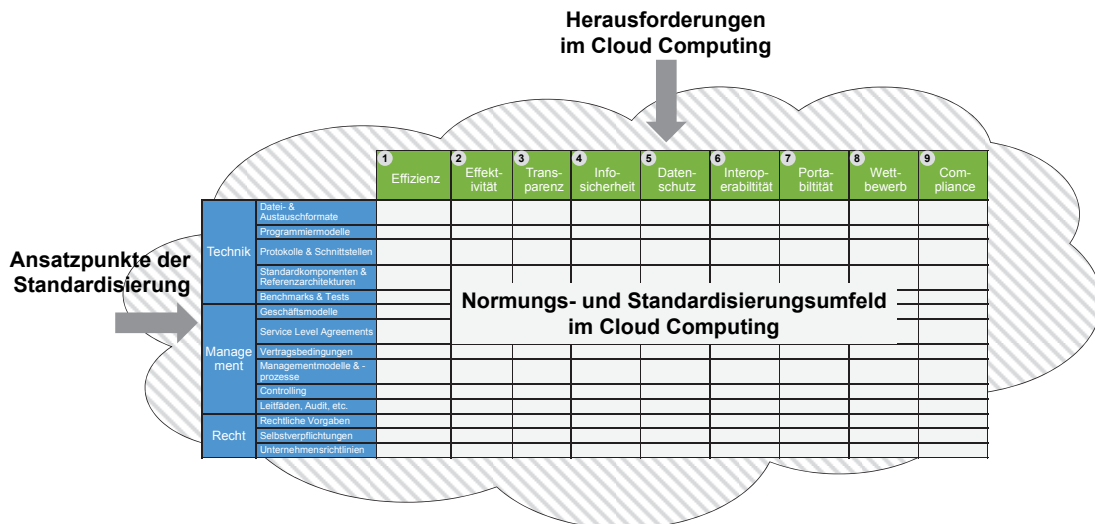


Abbildung 5: Einordnungsmatrix für Standards im Cloud Computing

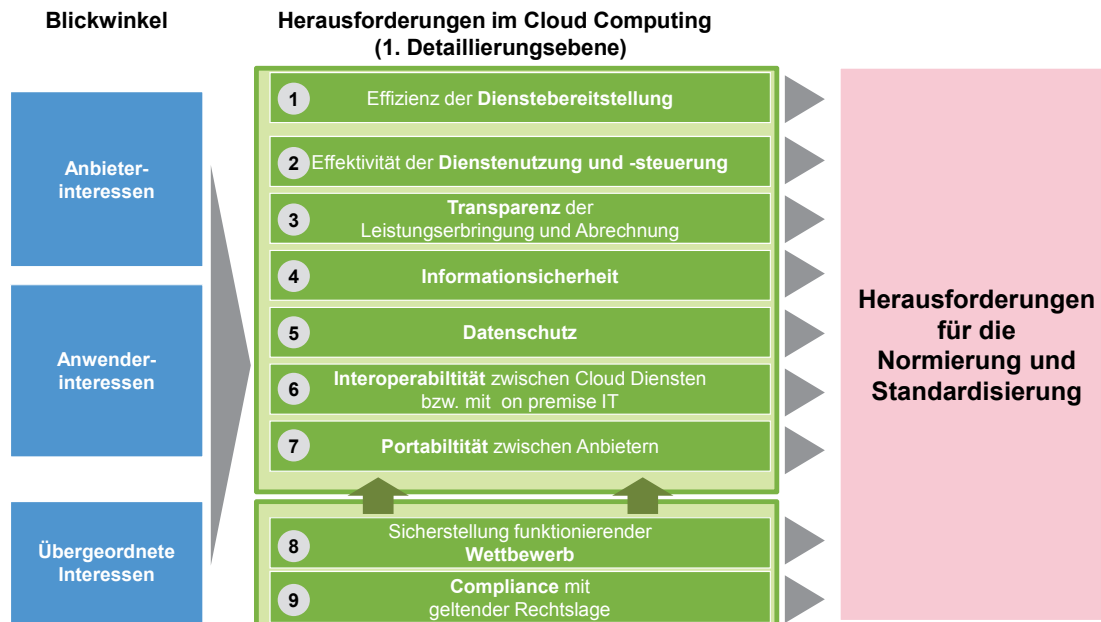
### 3.2.1 Herausforderungen im Cloud Computing

Auf Basis von Literaturstudien wurden neun besonders relevante Herausforderungen im Cloud Computing identifiziert. Jeder Herausforderung wurde ein primärer Blickwinkel zugeordnet, der für eine bestimmte Akteursgruppe besonders relevant ist. Im Folgenden werden die übergeordneten Herausforderungen kurz beschrieben. Sie bilden die Grundlage für die Identifikation der Herausforderungen für die Standardisierung im Cloud Computing (vgl. Abbildung 6).

- **Anbieter von Cloud-Diensten** sind zuvorderst an einer möglichst effizienten und damit aus der eigenen Sicht wirtschaftlich vorteilhaften Dienstebereitstellung interessiert.
- Die Interessen der **Anwender von Cloud-Diensten** sind vielschichtiger. Neben der Effektivität der Dienstenutzung und -steuerung sind dies übergreifende Anforderungen nach Transparenz, Informationssicherheit und Datenschutz. Letzterer wurde aufgrund seiner – insb. in Deutschland – maßgeblichen Bedeutung für das Cloud Computing bewusst nicht unter Informationssicherheit subsummiert. Darüber hinaus erwarten Anwender von Cloud-Diensten Interoperabilität sowie Portabilität von Daten und Diensten zwischen verschiedenen Cloud-Anbietern.
- Eine Sonderrolle kommt zwei weiteren eher **aus übergeordneten Interessen getriebenen Herausforderungen** zu: Zum einen ist dies die Sicherstellung eines funktionierenden Wettbewerbs zwischen Anbietern, wodurch



wettbewerbsverzerrende Lock-in Effekte vermieden werden sollen. Zum anderen ist dies die Sicherstellung von Compliance. Beide Herausforderungen stehen hierbei nicht auf der gleichen Ebene, wie die zuvor genannten. Sie sind diesen übergeordnet. So fördert bspw. erhöhte Portabilität und Interoperabilität aber auch verbesserte Transparenz den Gedanken des funktionierenden Wettbewerbs. Datenschutz hingegen ist wiederum ein Teilbereich der Compliance.



**Abbildung 6:** Herausforderungen im Cloud Computing

In dieser Studie berücksichtigte Herausforderungen wurden für den Betrachtungszweck wo notwendig auf einer zweiten Ebene differenziert. Die folgenden Abschnitte beschreiben alle berücksichtigten Herausforderungen in einem Überblick (vgl. Abbildung 7):

**Effizienz der Dienstbereitstellung (1):** Die Bereitstellung von Cloud-Diensten kann durch den Einsatz von Standards effizienter erfolgen. Vier Bereiche sind hierbei zu unterscheiden.

- 1a) Zunächst ist aus Sicht der Anbieter die *Nutzung von Entwicklungstools und -komponenten* von Vorteil, da aufwändige Eigenentwicklungen im Entwicklungsprozess vermieden werden können.
- 1b) Der *Aufbau skalierbarer Architekturen* stellt zudem eine Herausforderung dar. Hier müssen insbesondere auch Eigenschaften wie Redundanz, Fehlertoleranz und Multi-Tenenacy berücksichtigt werden.
- 1c) Eine weitere Herausforderung beim effizienten Betrieb ist *Ressourcenmanagement und Flexibilität*. Dies bezieht sich zunächst auf technische Ressourcen wie Hardware und Software aber auch auf Personalressourcen im Sinne der Kapazitätsplanung und Standardisierung von Qualifikationsanforderungen.
- 1d) Gerade im Cloud-Kontext sind die Erwartungen an die *Verfügbarkeit der Dienste* sehr hoch. Sie hängen von diversen Einflussfaktoren ab (z.B. Rechenzentrumshardware, Netzverfügbarkeit bis hin zum An-

wender). Schon bei der Messung der Verfügbarkeiten ergeben sich Standardisierungsprobleme.

**Effektivität der Dienstenutzung und -steuerung (2):** Um die Nutzung von Cloud-Diensten effektiv zu ermöglichen, werden zunächst Lösungen benötigt, die den Dienst an sich bereitstellen (z.B. HTML, Remote-Desktop Protokolle, Standards für Shell-Zugriffe, Web Service Standards). Da diese aber allgemein verfügbar und meist standardisiert sind, werden sie im Weiteren nicht separat betrachtet. Eine höhere Relevanz kommt den folgenden Herausforderungen zu:

- 2a) Vor der eigentlichen Nutzung von Cloud-Services sind etwaige Fragen zur *Vertragsgestaltung inkl. Haftungsfragen* zu klären.
- 2b) Während der Nutzung ist einer der Haupterfolgskriterien die Möglichkeit zur eigenständigen *Steuerung der Dienste durch den Anwender*.
- 2c) Im Falle von Problemen während der Nutzung sollte es standardisierte *Governance- und Eskalationsmechanismen* geben.

**Transparenz der Leistungserbringung und Abrechnung (3):** Die oftmals recht anonyme Auftraggeber-Auftragnehmerbeziehung im Cloud-Computing bringt eine Reihe potenzieller Transparenzprobleme mit sich.

- 3a) Zunächst bestehen die Anforderungen, dass die *Abrechnung inkl. Lizenzmanagement* transparent für den Anwender ist. Je komplexer die Abrechnungsmodelle und je mehr Einflussfaktoren involviert sind, desto komplexer, intransparenter und weniger planbar wird die Abrechnung und damit die Kostenbelastung für den Anwender.
- 3b) Weiterhin sollte Transparenz bzgl. der Leistungsseite bestehen. So kommt der Erfüllung und Überwachung des vereinbarten Service-Levels in Form von Service Level Agreements (SLAs) eine wichtige Rolle zu. Die Studie subsumiert solche Anforderungen im Bereich *Qualitätssicherung und Überwachung SLA*.
- 3c) Gerade vor dem Hintergrund des Datenschutzes und besonderer Vorschriften in bestimmten Branchen kann es von hoher Relevanz sein, Transparenz über *Art und Ort der Datenverarbeitung* zu erhalten. Dies widerspricht dem Kerngedanken des Cloud Computing zunächst, der den Bezug von Cloud-Diensten aus einer intransparenten „Wolke“ zu jeder Zeit und an jeden Ort vorsieht.

**Informationssicherheit (4):** Von vielen Beobachtern werden Sicherheitsaspekte als das Haupthindernis für eine schnelle Verbreitung von Cloud Computing gesehen.

- 4a) *Identitäts- und Rechtemanagement*: Die Verwaltung einer potenziellen Vielfalt von Identitäten sowie die Konfiguration eines effizienten Rechtemanagements für Cloud-Dienste – insb. bei der Verwendung einer föderierten Cloud-Architektur – könnte durch einheitliche Standards zur Verwaltung von Benutzern ermöglicht werden.
- 4b) *Vertraulichkeit und Integrität*: Im Cloud Computing werden Daten verschiedener Akteure verarbeitet. Daraus resultieren unterschiedliche

Anforderungen in Bezug auf das benötigte Niveau an Vertraulichkeit und Integrität.<sup>21</sup> Es gilt den gesamten Lebenszyklus von Daten zu betrachten. Dies beginnt bei der technischen Übermittlung und Speicherung und endet erst bei deren Löschung. Themenbereiche sind u.a. Verschlüsselung und Schlüsselmanagement, anonymisierte Datenverarbeitung, etc.

4c) **Zugriffsschutz, Logging, Abwehr von Angriffen:** Eine sichere Trennung von Mandanten sowie Zugriffskontrolle, die sichere Identifizierung und Authentisierung umfasst, und die gezielte Autorisierung<sup>22</sup> sowie zugehörige Protokollierungsmechanismen sind wesentliche Funktionen für funktionierende Informationssicherheit. Diese sollten als übergreifende Lösungen unter Einbezug aller Akteure betrieben werden können.<sup>23</sup> Darüber hinaus sollten Standards einen Beitrag zum zuverlässigen Schutz vor Angriffen bereitstellen.

4d) **Nachweis und Zertifizierung:** Neben der rein technischen Erfüllung von Sicherheitsanforderungen sind Nachweis, Zertifizierung und Auditierung der IT-Sicherheit von ebenso großer Bedeutung.

**Datenschutz (5):** Datenschutz als Schutz von personenbezogenen, personenbeziehbaren und sensiblen Daten vor Missbrauch, ist gerade in Deutschland eine der größten Herausforderungen im Kontext des Cloud Computing. Die Sicherstellung der Datenschutz-Compliance bspw. durch geeignete Anbieterauswahl, regelmäßige Kontrolle oder Einforderung einer transparenten Dokumentation stellt viele Unternehmen vor eine große Herausforderung. Gerade für die Mehrzahl der KMUs, ohne entsprechendes Fachpersonal, ist dies derzeit eine große Herausforderung.

**Interoperabilität (6):** Cloud-Interoperabilität wird in der vorliegenden Studie aus drei Gesichtspunkten betrachtet:

6a) **Migration in die bzw. aus der Cloud:** Hierfür werden Fähigkeiten, die es ermöglichen Infrastruktur-, Middleware- oder Anwendungskomponenten sowie vollständige Anwendungen und Daten in die Cloud zu verlagern oder aus der Cloud zu entfernen, benötigt.

6b) **Integrationsfähigkeit in on-premise IT:** Ferner stellt die Sicherstellung der Interoperabilität von on-premise Systemen und Applikationen und Cloud-Diensten in Form einer Hybrid Cloud eine Herausforderung dar.

6c) **Cloud-Föderation:** Hierfür wird die Fähigkeit Infrastrukturen, Plattformen und Anwendungen unterschiedlicher Anbieter verlässlich und oft ad-hoc miteinander verbinden zu können benötigt. Eine Grundlage

---

<sup>21</sup> Impliziert alle Daten, beispielsweise personenbezogene Daten, Benutzerdaten, Nutzungsprofile oder allgemein Metadaten.

<sup>22</sup> Z.B. Beschränkung des Zugriffs auf Benutzerdaten für Administratoren

<sup>23</sup> Z.B. Übergreifendes ID-Management bzw. „ID-Federation“.

hierfür können einheitliche oder kompatible Schnittstellen bilden, so dass keine individuelle Integration von Diensten notwendig ist.

**Portabilität zwischen Anbietern (7):** Zur Vermeidung von Lock-in Effekten ist es notwendig, dass Dienste und Daten unter Verwendung von einheitlichen Standards einfach und auf regulärer Basis zwischen unterschiedlichen Cloud-Anbietern portiert werden können.

7a) **Dienst-Portabilität** beschreibt Fähigkeiten zur Portierung von Cloud-Diensten. Mit Portabilität (auch „Plattformunabhängigkeit“) wird die Eigenschaft eines Cloud-Dienstes bezeichnet, auf unterschiedlichen Cloud Computing-Plattformen ausführbar zu sein.

7b) **Daten-Portabilität** beschreibt Fähigkeiten zur Portierung von Daten, die von den Kunden bei einem Anbieter abgelegt sind, um dem Kunden einen Wechsel zwischen verschiedenen Anbietern zu ermöglichen. Standards könnten u.a. einheitliche Datenformate, Exit-Vereinbarungen, z.B. mit Datenintegritätszusicherung und Kostenanzeige, umfassen.

**Sicherstellung eines funktionierenden Wettbewerbs (8):** Aufgrund der Skaleneffekte seitens der Anbieter und potenzieller Lock-in-Effekte, besteht im Cloud Computing die Gefahr einer Beeinträchtigung des Wettbewerbs zwischen den Anbietern und Herausbildung von marktbeherrschenden Akteuren. Gerade in Deutschland und Europa ist die Sicherstellung eines funktionierenden Wettbewerbs, der auch die Teilhabe von mittelständischen Unternehmen gewährleistet, von zentraler Bedeutung.

**Compliance mit geltender Rechtslage (9):** Unter Compliance wird meist die Einhaltung von Gesetzen und Richtlinien sowie freiwilliger Vereinbarungen verstanden. Dies ist insb. eine Herausforderung, da der Nutzer von Cloud-Diensten nur eine geringe Transparenz über die Regeleinhaltung des Anbieters hat. Besonders relevant ist dies in den Bereichen IT-Sicherheit, Datenschutz sowie im kommerziellen Bereich.

Folgende Abbildung fasst diese Herausforderungen zusammen.



**Abbildung 7:** Detaillierung der Herausforderungen im Cloud Computing (1. & 2. Ebene)

### 3.2.2 Ansatzpunkte der Standardisierung im Cloud Computing

Standards können über unterschiedliche Mittel eine Standardisierung herbeiführen. Im Rahmen dieser Studie werden die „Mittel der Standardisierung“ als Ansatzpunkte der Standardisierung verstanden. Diese lassen sich im Cloud-Umfeld in die drei grundlegenden Bereiche Technik, Management und Recht unterscheiden. Analog zur Vorgehensweise bei den Herausforderungen werden die Ansatzpunkte wie folgt auf einer zweiten Ebene differenziert.

Bereich	Ansatzpunkte	Beispiele
Technik	Datei- & Austauschformate	OVF, EC2, USDL, CIM SVM...
	Programmiermodelle	MapReduce, JAQL, PIG, HIVE
	Protokolle & Schnittstellen	OCCI, CDMI, CloudAudit, Google DLF, ...
	Standardkomponenten & Referenzarchitekturen	OpenStack, OSGI, NIST RM, IBM RM, DMTF, CTP, ...
	Benchmarks & Tests	Benchmarking Suites, Security Assessment, ....
Management	Geschäftsmodelle	IaaS, PaaS, SaaS-Betreibermodelle, ...
	Service Level Agreements	WS-Agreement, Business SLAs, ...
	Vertragsbedingungen	EVB-IT, EU SVK, Bausteine für AGB, EULA
	Managementmodelle & -prozesse	ISO 27001/27002, ITIL, COBIT, ...
	Controllingmodelle & -prozesse	SSAE, SAS 70, ....
Recht	Leitfäden, Audit, etc.	BSI Eckpunktepapier, NIST UC, EuroCloud LRD&C
	Rechtliche Vorgaben	EU Datenschutzrichtlinie, BDSG, Safe Harbor
	Selbstverpflichtungen	Open Cloud Manifesto, ...
	Unternehmensrichtlinien	Interne Policies, ...

**Abbildung 8:** Ansatzpunkte der Standardisierung im Cloud Computing

**Technik:** Hierunter werden technische Standards gefasst. Im Bereich der Informationstechnologie lassen sich die folgenden konkreten Ausprägungen identifizieren:

- **Datei- und Austauschformate** dienen der Übermittlung und Speicherung von (teil-)strukturierten Daten. Dies können neben Dokumenten, Bildern oder Mediendateien auch Virtual Machine Images sein.
- **Programmiermodelle** bilden die Grundlage für Erstellung und Ausführung von Quellcode. Über die Vorgabe von Programmierkonzepten und -abstraktionen werden die Bausteine von Programmiersprachen definiert. Besonders durch den dem Cloud Computing zugeschriebenen Paradigmenwechsel können neuartige Programmiermodelle benötigt werden.
- **Protokolle und Schnittstellen** beschreiben hingegen einen dynamischen Ablauf zum Austausch von Information zwischen zwei Komponenten, Anwendungen oder Akteuren. Neben dem Zugriff zur eigentlichen Nutzung (z.B. Speicherung von Daten) werden Schnittstellen zum Management und zur Konfiguration verwendet.
- **Standardkomponenten und Referenzarchitekturen** erleichtern den Aufbau und die Verwendung von Cloud-Infrastrukturen und Cloud-Diensten. Durch standardisierte Designvorgaben, bspw. Referenzarchitekturen, können Best Practice auf eigene Cloud-Dienste übertragen werden. Dies kann auch die Verständlichkeit, Vergleichbarkeit und Interoperabilität von Angeboten erleichtern. Die Betrachtung des gesamten Lebenszyklus trägt zur Vollständigkeit bei.
- **Benchmarks und Tests** helfen die Leistungsfähigkeiten unterschiedlicher Cloud-Dienste, bspw. durch die Vorgabe von Lastprofilen und



Kennzahlen, zu bemessen und zu beurteilen. Darüber hinaus erlauben standardisierte Tests die Verifizierung von z.B. Sicherheitsanforderungen.

**Management:** In diesem Bereich werden Standards eingegliedert, die die kommerzielle Abwicklung sowie das Management auf der Seite von Cloud-Anbietern und Cloud-Anwendern unterstützen.

- *Geschäftsmodelle* bilden die Grundlage für den wirtschaftlichen Betrieb von Cloud-Diensten. Bei der Erarbeitung von Geschäftsmodellen gilt es, zum einen potenzielle Markt- und Kundensegmente, Absatzahlen oder Ressourcenbedarf zu bestimmen. Zusätzlich müssen auch Faktoren wie die Preisgestaltung, Beschaffung oder Personalplanung berücksichtigt werden. Im Bereich des Cloud Computing ist insb. der Bereich einer einheitlichen Leistungsbeschreibung für die Standardisierung relevant.
- *Service Level Agreements (SLA)* erhöhen die Effizienz in der Vertragsgestaltung, erlauben dedizierte Vertragsverhandlungen und erlauben die Festlegung und Sicherstellung gezielter Anforderungen an den Diensteanbieter. SLAs können so signifikant zur Vertrauensbildung beitragen.
- *Vertragsbedingungen* bieten im Bereich des Cloud Computing ausreichend Raum für Standardisierungsbemühungen. Beispielsweise als Rahmenverträge, die durch SLAs ergänzt werden, Endbenutzer-Lizenzvereinbarungen oder Vertragsbausteine in unterschiedlichen Sprachen.
- *Managementmodelle und -prozesse* (z.B. im Sinne der im IT-Servicemanagement weit verbreiteten ITIL-Bibliotheken) können helfen, einheitliches Vorgehen und Begrifflichkeiten sicherzustellen und Best Practice Prozesse zu fördern.
- *Controllingmodelle und -prozesse* können durch Vorgaben, bspw. zur Abrechnung und Rechnungslegung, oder dem Risikomanagement von bspw. IT-Systemen einheitliche Dokumente zur Dokumentation der Geschäftstätigkeit fördern. Dies kann ggfs. zur Vereinfachung von Zertifizierungen beitragen.
- *Leitfäden, Audit etc.* können allgemein sowohl potenziellen Anbietern als auch Nutzern von Cloud-Diensten hilfreich sein. Dies wird durch den Transport von Orientierungswissen, bspw. in Form von Best Practice, ermöglicht.

**Recht:** Regelungen und Vorschriften, die den geltenden Rechtsrahmen für die Akteure im Cloud Computing abstecken, können in drei Gruppen unterschieden werden.

- *Rechtliche Vorgaben* stellen verbindliche Vorgaben, die auf entsprechenden Gesetzen, Richtlinien, Verordnungen o.ä. basieren.

- **Selbstverpflichtungen** fassen mehr oder weniger freiwillige Vereinbarungen und Kodizes zusammen, die z.B. von (Branchen-)Verbänden herausgegeben werden.
- **Unternehmensrichtlinien** stellen die schwächste Form von Regelungen und Vorschriften zum geltenden Rechtsrahmen dar. Die Verabschiedung von Unternehmensrichtlinien erlaubt Unternehmen, sich bei der Geschäftstätigkeit bspw. strengeren Richtlinien zu unterwerfen als durch Selbstverpflichtungen oder rechtliche Vorgaben gefordert.

## 3.2.3 Weitere Attribute zur Klassifizierung von Cloud-Standards und Normen

Der „Bezug zum Cloud Computing“ ist ein maßgeblicher Einflussfaktor für die Entscheidung hinsichtlich der Berücksichtigung eines Standards in dieser Studie. Darüber hinaus bilden – wie oben ausgeführt – die mit dem Standard adressierten Herausforderungen des Cloud Computing und die Ansatzpunkte der Standardisierung die maßgeblichen Bezugspunkte für die Einordnung innerhalb der Cloud-Standard Taxonomie. Zur weiteren, einheitlichen Beschreibung der Standards im Cloud Computing sind jedoch weitere Attribute notwendig. Die folgenden Eigenschaften eines Cloud-Standards dienen der steckbriefhaften Beschreibung und Bewertung (vgl. Abbildung 9), der in dieser Studie als besonders relevant erachteten Standards.

<b>BASIS- INFORMATION</b>	<b>Status</b>	Entwurf / In Arbeit / Veröffentlicht
	<b>Formalisierung</b>	Empfehlung / Spezifikation / Industriestandard / Standard / Referenzimplementierung / EU-Richtlinie
	<b>Bezug zu CC</b>	Implizit / Explizit
	<b>Initiator</b>	< Name der Standardisierungsorganisation >
	<b>Beteiligte</b>	Ca. Anzahl + Bekannte Unternehmen als Treiber
	<b>Link</b>	<Link zu den Standarddokumenten>
<b>GELTUNGS- BEREICH</b>	<b>Service-Modell</b>	IaaS/ PaaS/ SaaS/ Alle
	<b>Nutzergruppe</b>	Anbieter/ Intermediäre/ Nutzer/ Alle
	<b>Branche</b>	Bezeichnung für Branche/ Übergreifend
	<b>Deployment</b>	Private/ Public/ Alle
	<b>Geographie</b>	DE/ EU/ Global
	<b>Unternehmensgröße</b>	Kleinunternehmen/ Großunternehmen/ Alle
<b>BEWERTUNG</b>	<b>Reifegrad</b>	Gering/ Mittel/ Hoch/ Produkt
	<b>Durchsetzungsfähigkeit</b>	Gering/ Mittel/ Hoch
	<b>Partizipationsmöglichkeit</b>	Keine/ Eingeschränkt/ Offen
<b>ÄHNLICHE STANDARDS</b>		<Ähnliche Standards.Kürzel>

Abbildung 9: Katalog der Attribute zur Beschreibung von Cloud-Standards

**Basisinformationen:** Zunächst erscheint es naheliegend die verfügbaren grundlegenden Informationen für jeden Standard kurz zu benennen. In dieser Studie wurden hierfür folgende Eigenschaften erhoben:

- **Status:** Dokumente zur Definition von Standards können während der Erhebungsphase in unterschiedlichen Status vorliegen. Die Studie unterscheidet Entwurfsfassungen, fortgeschrittene Arbeitsdokumente und offiziell veröffentlichte Dokumente.
- **Formalisierung:** Im Laufe der Standardisierung durchlaufen die Standarddokumente unterschiedliche Formalisierungsstatus. Die Studie



unterscheidet die Formalisierung nach Arten von Standards wie in Abschnitt 3.1.3 erläutert.

- **Bezug zum CC:** Standards können impliziten oder expliziten Bezug zum Cloud Computing aufweisen.
- **Initiator:** Die Angabe der jeweiligen Standardisierungsorganisation, des Normungsgremiums bzw. des Initiators ergänzt die Beschreibung der Standards.
- **Beteiligte:** Die Akzeptanz und Verbreitung von Standards hängt unter anderem von der Anzahl und Prominenz der Unterstützer eines Standards ab. Unterstützer werden im Attribut Beteiligte berücksichtigt.
- **Link:** Über die Angabe von Links wird der Zugriff auf weiterführende Informationen ermöglicht.

**Geltungsbereich:** Neben den grundlegenden Informationen werden Standards nach ihren Anwendungsbereichen anhand folgender Eigenschaften charakterisiert:

- **Service-Modell:** Diese Eigenschaft beschreibt den für den Standard relevante Typisierung als Cloud-Dienst: Es sind Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) und Infrastructure-as-a-Service (IaaS) zu unterscheiden – eine Mehrfachzuordnung ist möglich.
- **Benutzergruppe:** Ein Standard kann jeweils speziell aus Sicht eines Anbieters oder eines Nutzers von Cloud-Diensten relevant sein. Darüber hinaus kann die Relevanz für weitere Nutzergruppen angegeben werden, die als Intermediäre zusammengefasst werden. Eine Mehrfachzuordnung ist möglich.
- **Branche:** Auch wenn spezifisch für eine bestimmte Branche entwickelte Standards weniger im Fokus dieser Studie stehen, so ist doch die Relevanz ggf. je nach Industriezweig unterschiedlich. Eine besondere Rolle spielt hierbei die Unterscheidung in öffentlichen und privaten Sektor, die unter diesem Stichwort betrachtet wird. Ist keine Branchenrelevanz erkennbar, werden Standards als übergreifend gekennzeichnet.
- **Deployment:** Analog zur mittlerweile weit verbreiteten Terminologie der Deployment Modelle des Cloud Computing wird die Relevanz der Standards für Public Clouds, Private Clouds oder Hybrid Clouds (Ausprägung: Alle) unterschieden – ein Standard kann für verschiedene Modelle sinnvoll nutzbar sein.
- **Geographie:** Insbesondere bei rechtlichen Standards ist die Gültigkeit bzw. Verbindlichkeit eines Standards ggf. nur auf eine bestimmte Region begrenzt (z.B. EU, Deutschland, USA). Aufgrund der globalen Vernetzung durch das Internet ist dies bei technischen Standards meist weniger relevant.
- **Unternehmensgröße:** Standards, insbesondere im Bereich des Managements, können den Aufbau bestimmter Strukturen in Organisationen erfordern. Zudem sind bestimmte Standards nur unter Abgabe von Lizenzgebühren einsetzbar. Beide Punkte sind Beispiele dafür, dass man-

che Standards auf Grund von Ressourcenmangel nicht unbedingt von KMUs eingesetzt werden können. Daher erscheint die Einschätzung der Anwendbarkeit relevant.

Die Attribute zur Bewertung der Standards werden in folgenden Unterkapitel unter 3.3.2 „Bewertung“ beschrieben.

### 3.3 Analyseansatz der Studie

Das Normierungs- und Standardisierungsumfeld von Cloud Computing ist komplex und weitläufig. Die vorliegende Studie konzentriert sich auf die wesentlichen Akteure, Standards und Trends. Das folgende Kapitel definiert jeweils den Fokus der Untersuchung, begründet die Auswahl und beschreibt den Bewertungsansatz.

Der Untersuchung des Normierungs- und Standardisierungsumfeldes liegt eine umfassende Primär- und Sekundärrecherche zu Grunde. Der Schwerpunkt liegt auf der Sekundärrecherche. Die Untersuchung wird durch ausgewählte Experteninterviews, Forschungsergebnisse und Primärerhebungen aus den Trusted Cloud-Projekten angereichert.

Die Analyse basiert auf einer breiten initialen Sichtung möglicher Akteure, Initiativen und Standards sowie ausgewählter (Referenz-)Projekte und (Referenz-)Dienste (siehe Begriffsdefinitionen in 3.1), die potenzielle Relevanz für die Standardisierung im Cloud Computing auf deutscher, europäischer und internationaler Ebene besitzen. Die Untersuchung sowie deren Inhalte, Struktur und Vorgehen erfolgt entlang eines transparenten und nachvollziehbaren Analyserasters<sup>24</sup>.

Im Anhang findet sich ein Auszug der gesichteten Standardisierungsorganisationen und Standards. Detaillierte Rechercheergebnisse der Untersuchung können bei Bedarf beim BMWi angefragt werden.

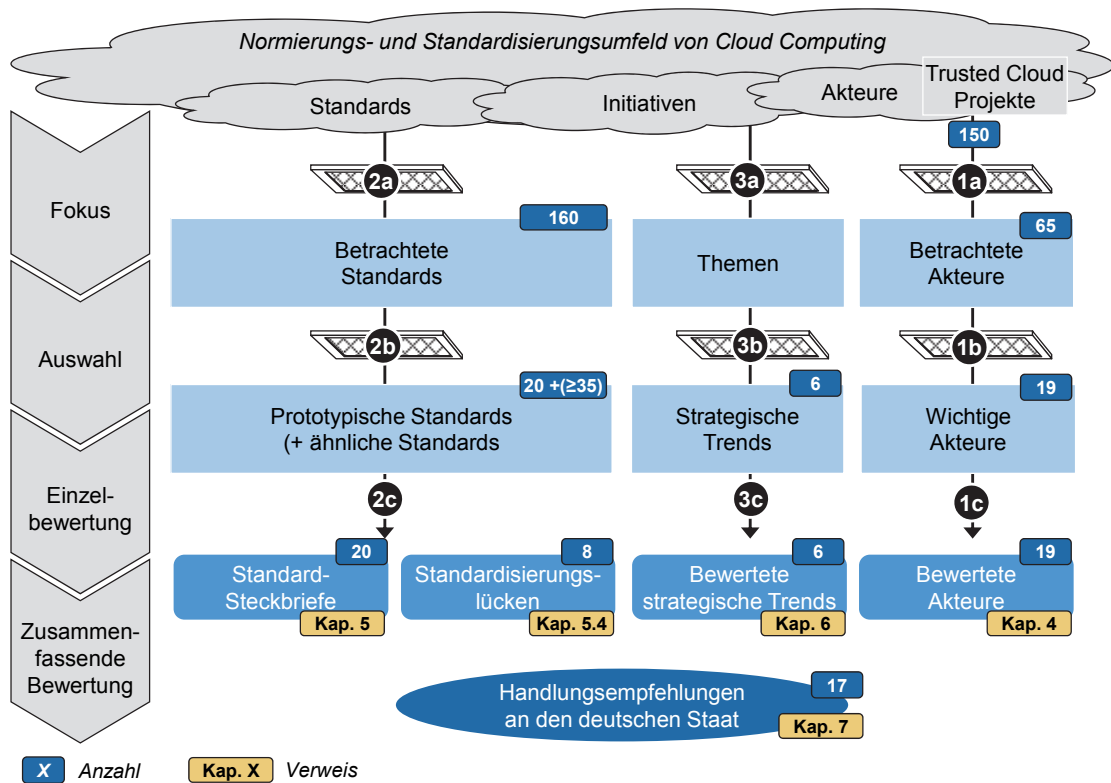
Der Analyseansatz besteht für Akteure, als auch Trends und Standards aus vier Schritten.

- **Fokus:** Festlegung des Fokus (vgl. Kapitel 2.3) der Untersuchung und Eingrenzung der Rechercheergebnisse, die näher betrachtet werden.
- **Auswahl:** Konzentration der Untersuchung auf das Wesentliche (vgl. Kapitel 2.3) durch Festlegung transparenter Auswahlkriterien.
- **Einzelbewertung:** Beschreibung und Bewertung ausgewählter Rechercheergebnisse unter Verwendung einheitlicher Bewertungskriterien.
- **Zusammenfassende Bewertung:** Übergreifende und zusammenfassende Analyse und Bewertung aller Ergebnisse zur Ableitung von Handlungsempfehlungen.

Die Abbildung auf der Folgeseite illustriert diesen Analyseansatz überblicksartig. Für jeden Zwischenschritt wird die Anzahl der Zwischenergebnisse als kleines Rechteck rechts oben angegeben.

---

<sup>24</sup> In Form eines strukturierten Tabellendokumentes.



**Abbildung 10:** Übergreifender Analyseansatz der Studie<sup>25</sup>

Die detaillierte Beschreibung der Einzelschritte wird in den folgenden Unterkapiteln vorgenommen.

### 3.3.1 Fokus, Auswahl und Bewertung der Akteure

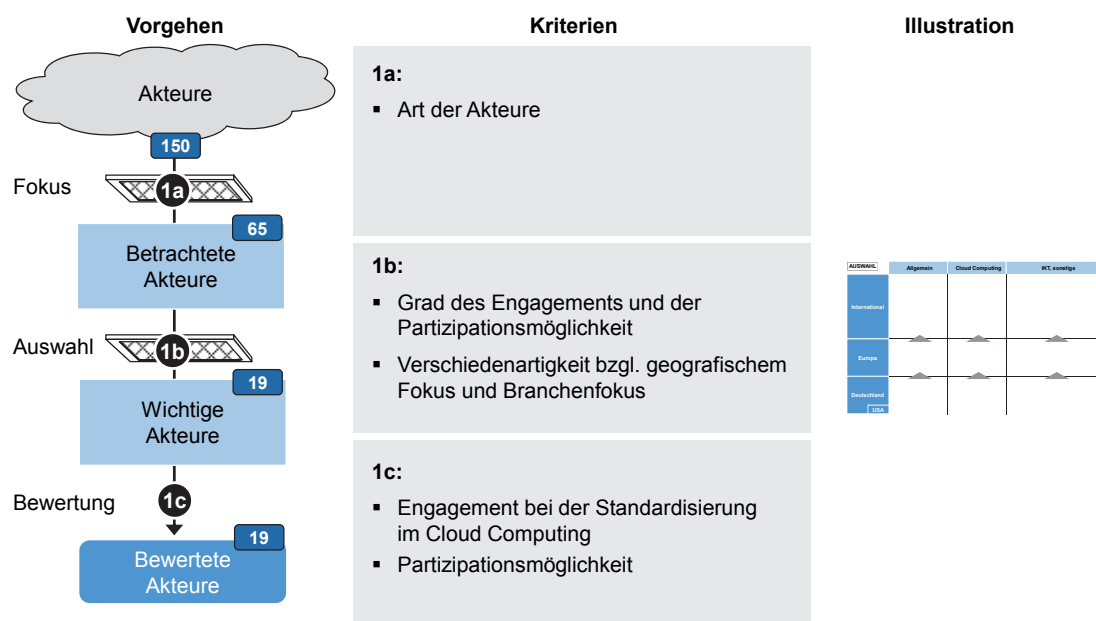
An dieser Stelle wird das methodische Vorgehen bei der Festlegung des Fokus, der Auswahl und Bewertung der Akteure ausgeführt. Die Ergebnisse, also die beschriebenen und bewerteten 19 Steckbriefe der Standardisierungsorganisationen, finden sich in Kapitel 4. Dem Vorgehen liegen die Ergebnisse einer initialen ungefilterten Recherche von über 150 verschiedenen Akteuren aller Arten, wie Normungsorganisationen, Standardentwicklungsorganisationen, Interessensvereinigungen, Konsortien, privatwirtschaftlicher Unternehmen, öffentlicher Einrichtungen oder Forschungseinrichtungen (siehe 3.1.1) als Ausgangspunkt zu Grunde. Die Recherche stützt sich auf öffentlich verfügbare Informationen aus dem Internet (z.B. Studien), existierenden Bestandsaufnahmen (insb. der IETF<sup>26</sup> oder das „Cloud Standards Wiki“<sup>27</sup>), Ergänzungen aus Experteninterviews sowie Pressearchive.

<sup>25</sup> Quelle: Analyse von Booz & Company und FZI.

<sup>26</sup> <http://tools.ietf.org/id/draft-khasnabish-cloud-sdo-survey-01.txt>

<sup>27</sup> <http://cloud-standards.org>

Folgende Abbildung zeigt und illustriert die Fokus-, Auswahl- und Bewertungskriterien für die Akteure.



**Abbildung 11:** Fokus-, Auswahl- und Bewertungskriterien für Akteure.<sup>28</sup>

## Fokus

Die Beschreibung der Akteure im Normierungs- und Standardisierungsumfeld von Cloud Computing folgt dem Ziel einen Ausgangspunkt für mögliche Partizipationsmöglichkeiten bei diesen Akteuren zu schaffen.

Entsprechend liegt der Fokus auf den Akteuren, die ein Mindestmaß an Engagement bei der Cloud-Standardisierung bzw. ein Mindestmaß an Partizipationsmöglichkeit im Allgemeinen erkennen lassen. Dies sind solche Akteure (ca. 65<sup>29</sup>), wie sie in 3.1.1 als *Standardisierungsorganisationen* definiert werden, also vor allem – aber nicht ausschließlich – Normungsorganisationen, Standardentwicklungsorganisationen, Interessenvereinigungen oder Konsortien. Forschungseinrichtungen und privatwirtschaftliche Unternehmen fallen nicht in den Fokus. Gerade letztere (z.B. US-amerikanische Anbieter) treiben und nehmen faktisch maßgeblichen Einfluss auf die Standardisierung. Es bestehen allerdings keine regulären Mitwirkungsmöglichkeiten für Außenstehende.

## Auswahl

Die Auswahl folgt dem Ziel eine möglichst ausgewogene und prägnante Darstellung der Standardisierungsorganisationen zu erreichen. An die betrachteten Standardisierungsorganisationen (ca. 65) werden folgende Auswahlkriterien angelegt. Auf dieser Grundlage werden 19 der wichtigsten Standardisierungsorganisationen ausgewählt.

<sup>28</sup> Quelle: Analyse von Booz & Company und FZI.

<sup>29</sup> Anzahl identifizierter Akteure.

- **Grad des Engagements und der Partizipationsmöglichkeit:** Der Grad des Engagements der Akteure bei der Standardisierung im Cloud Computing und der Partizipationsmöglichkeit (analog zur den Bewertungskriterien).
- **Verschiedenartigkeit bzgl. geografischem Fokus und Branchenfokus:** Verschiedenartigkeit der Akteure bei deren geografischen Arbeitsfokus (International, Europa, Deutschland) und deren inhaltlichem Branchenfokus (Allgemein, Cloud Computing, IKT und Sonstige). Einen Sonderfall spielt die USA, die durch ihre zentrale Bedeutung beim Cloud Computing stichpunktartig berücksichtigt wird.

### *Bewertung*

Das erste Auswahlkriterium steht in direkter Wechselwirkung mit den Bewertungskriterien. Im Zuge der Bewertung findet eine Verfeinerung der Auswahl statt. Die Bewertung der Standardisierungsorganisationen erfolgt nach folgenden Kriterien:

- **Engagement bei der Standardisierung im Cloud Computing:** Das Engagement, das die Standardisierungsorganisation bei der Standardisierung im Cloud Computing erkennen lässt. Dies umfasst vor allem bisheriges Engagement und solche Ankündigungen, die als verlässlich eingestuft werden. Für das Engagement werden folgende fünf Einstufungen definiert:
  - „*Sehr gering/kein*“: Unwesentliche Standardisierungsbemühungen, weder mit implizitem noch mit explizitem Bezug zum Cloud Computing.
  - „*Gering*“: Vor allem Mitwirkung bei Standards mit implizitem Bezug zum Cloud Computing oder solchen mit explizitem Bezug, aber geringer Reife.
  - „*Mittel*“: Mitwirkung bei einem Standard, der in der vorliegenden Studie als besonders relevant betrachtet wird (siehe 3.3.2) oder von ähnlicher Bedeutung ist.
  - „*Hoch*“: Mitwirkung bei mehreren Standards, die in der vorliegenden Studie als besonders relevant betrachtet werden oder umfangreiche Mitwirkung bei Standards, die impliziten Bezug besitzen.
  - „*Sehr hoch*“: Besonders umfangreiche Mitwirkung bei mehreren bedeutenden Standards mit implizitem oder explizitem Bezug zum Cloud Computing.
- **Partizipationsmöglichkeit:** Möglicher Grad der Partizipation in Gremien der Standardisierungsorganisation. Die Ausprägungen erfolgen entsprechend der Definition für Standards in Abschnitt 3.3.2.

Die Standardisierungsorganisationen werden zuerst kurz allgemein an Hand ihrer Ziele, Aufgaben und Mitglieder charakterisiert. Danach werden relevante Gremien zur Standardisierung sowie relevante Standards mit implizitem und explizitem Bezug zur Standardisierung angeführt. Abschließend werden

die Partizipationsmöglichkeiten durch die Angabe beispielsweise der Mitgliedsstufen, der Beitragslogik, Stimmrechte oder Partizipationsrechte konkretisiert.

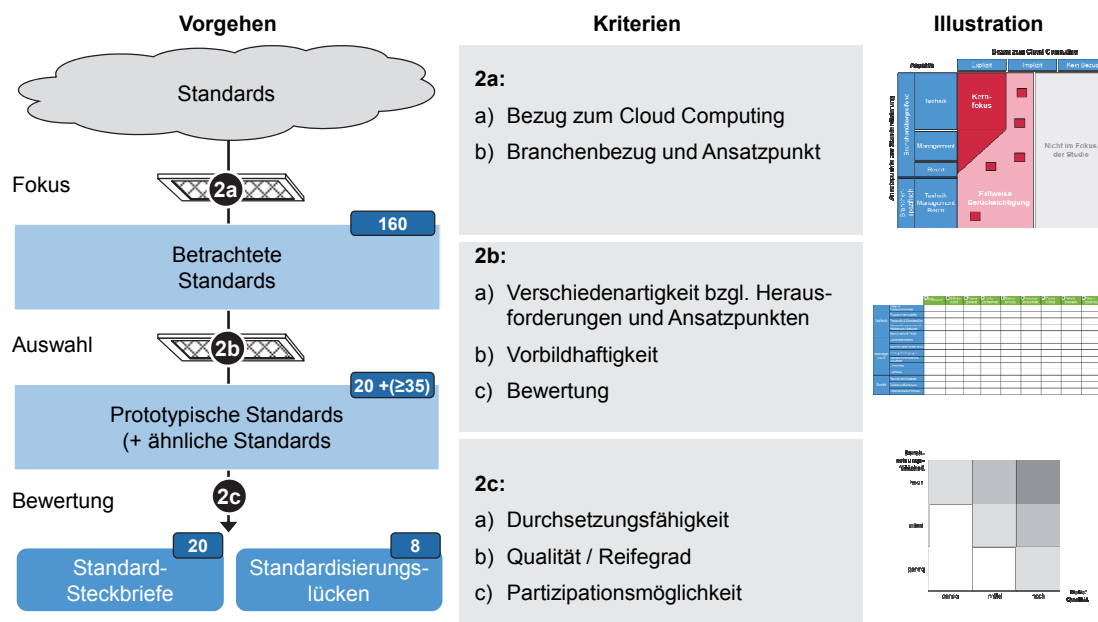
## 3.3.2 Fokus, Auswahl und Lückenanalyse der Standards

An dieser Stelle wird das methodische Vorgehen bei der Festlegung des Fokus, der Auswahl und der Bewertung der Standards sowie bei der Lückenanalyse beschrieben. Die Ergebnisse der Untersuchung, also die Standardsteckbriefe und Lückenanalyse, finden sich in Kapitel 5.

Die Untersuchung von Standards, die besondere Bedeutung für das Cloud Computing besitzen, schließt Vorarbeiten, Standards sowie Zertifizierungen gemäß der Begriffsdefinitionen in 3.1.3 ein. Der Recherche liegt eine Vielzahl verschiedener Quellen zu Grunde:

- Bestehende Übersichten von Cloud-Standards (z.B. NIST Cloud Standards Inventory<sup>30</sup>) und Cloud-Standardisierungsroadmaps,
- Gremien der recherchierten Standardisierungsorganisationen,
- White Paper, Leitfäden, Studien, Anforderungsdokumente, die öffentlich über das Internet verfügbar sind,
- Pressearchive und Fachzeitschriften sowie
- Interviews mit Experten, z.B. aus den Trusted Cloud-Projekten.

Folgende Abbildung zeigt und illustriert die Fokus-, Auswahl- und Bewertungskriterien für die Standards, wie sie in der Studie Verwendung finden.





## Fokus

Die Erfassung, Analyse und Aufbereitung des Standardisierungsumfeldes von Cloud Computing hat zum Ziel, einen handlungsorientierten Überblick über existierende Standards im Cloud Computing zu schaffen. Offene Bereiche („White Spots“) sollen identifiziert werden, in denen ein gestalterischer Beitrag zur Etablierung von Standards in Deutschland, aber auch darüber hinaus geleistet werden kann.

Anbieter, Anwender und Intermediäre von Cloud Diensten sind in ihrer Geschäftstätigkeit einer Vielzahl von Standards ausgesetzt. Um diese Standardvielfalt in einem ersten Schritt auf einen überschaubaren Umfang zu reduzieren und diese anschließend in ihrer Relevanz bewerten zu können, wurden die Standards anhand des im Folgenden definierten Betrachtungsumfangs in die Studie aufgenommen.

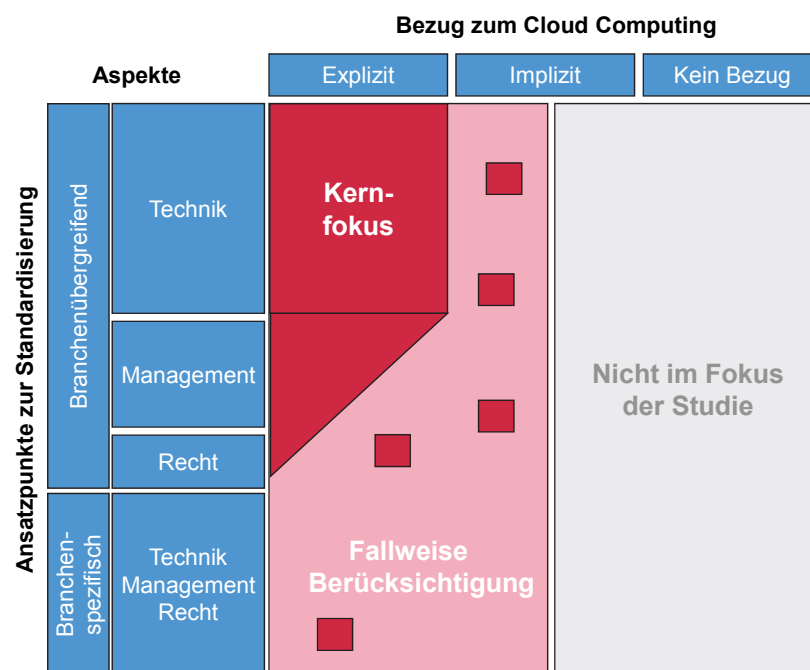


Abbildung 13: Betrachtungsumfang und Fokus der Studie

- **Bezug zum Cloud Computing:** Der Fokus der Studie lässt sich zunächst anhand der Dimension „Bezug zum Cloud Computing“ einschränken. Hier werden Standards, die einen expliziten Bezug zum Cloud Computing haben, von Standards unterschieden, die einen impliziten Bezug zu Cloud Computing haben, d.h. einen Geltungsbezug zu Basistechnologien oder zu Grundprinzipien des Cloud Computing (siehe auch Kapitel 2.3). Vollständig außerhalb des Fokus dieser Studie sind Standards, die weder einen expliziten noch impliziten Bezug zum Cloud Computing aufweisen.
- **Ansatzpunkte zur Standardisierung:** Entlang der zweiten Dimension „Ansatzpunkte zur Standardisierung“ werden zunächst Standards unterschieden, die nur für spezifische Branchen von Relevanz sind, sowie Standards, die ein branchenübergreifendes Wirkungsfeld haben. In

beiden Fällen, werden Standards auf zweiter Ebene entlang der Ansatzpunkte Technik, Management und Recht unterschieden.

*Der Kernfokus der Studie liegt auf branchenübergreifenden Standards, die einen expliziten Bezug zu Cloud Computing besitzen.* Es wird erwartet, dass der Standardisierungsgrad im Bereich Technik am höchsten ist, so dass dieser Bereich auch einen natürlichen Schwerpunkt der Studie bildet. Eine generelle Erörterung des Rechtsrahmens der Geschäftstätigkeit liegt nicht im Fokus der vorliegenden Studie. Standards mit implizitem Bezug zum Cloud Computing finden fallweise, also bei hinreichender Relevanz für eine Berücksichtigung in Deutschland, Einzug in die Studie, insbesondere dann, wenn die Relevanz nicht auf den ersten Blick ersichtlich ist.

Branchenspezifische Standards adressieren spezifische Anforderungen (wie bspw. in der Energie- und Chemie-Branche oder dem Gesundheitswesen) und sind oftmals Technologie-agnostisch. Dies bedeutet im Umkehrschluss, dass ein disruptiver Technologiewechsel im Unternehmen, wie ihn das Cloud Computing mit sich bringt, wenig Auswirkung auf existierende branchenspezifische Standards hat. Branchenspezifische Standards werden deshalb nur fallweise berücksichtigt. In der Studie werden ferner jene Einzelfälle berücksichtigt, in denen branchenspezifische Cloud-Standards existieren und Potenziale zur Generalisierung bestehen.

In Summe werden in der vorliegenden Studie etwa 160 Standards identifiziert, die diesem Fokus entsprechen.

### *Auswahl*

Das Ziel ist eine möglichst kompakte Auswahl vielversprechender Standards für das Cloud Computing, die gleichzeitig ein großes inhaltliches Spektrum von Standards zeigt und inhaltliche Dopplungen vermeidet. Entsprechend unterliegt die Auswahl der Standards, die nachfolgend in der Studie als Steckbriefe beschrieben und bewertet werden, folgenden Kriterien:

- **Verschiedenartigkeit:** Die ausgewählten Standards sollen ein möglichst großes inhaltliches Spektrum abdecken. Das Spektrum wird durch die Herausforderungen und Ansatzpunkte gemäß der definierten Taxonomie (siehe 3.2) aufgespannt.
- **Vorbildhaftigkeit:** Die Auswahl der Standards soll keine inhaltlichen Dopplungen besitzen. Es werden möglichst reife und umfangreiche Standards mit prototypischem Charakter ausgewählt. Ähnliche Standards werden in den Steckbriefen erwähnt (vgl. 3.2.3) und in Vergleich mit dem prototypischen ausgewählten Standards gesetzt.

Unter Anwendung dieser Kriterien werden die 20 Standards ausgewählt, die gemessen an der **Bewertung** die größte Relevanz besitzen. In der Studie konnten mehr als 35 weitere ähnliche Standards identifiziert werden.

### **Bewertung**

Die Bewertung der Standards erfolgt nach folgenden Kriterien und Ausprägungen. Die im Rahmen der Studie vorgenommene Bewertung der Cloud-Standards wurde in Workshops und Expertengesprächen validiert.

- **Reifegrad:** Auf Grundlage des Status und der Formalisierung eines Standards sowie der inhaltlichen Analyse wird der Reifegrad eines Cloud-Standards eingestuft. Dabei wird insbesondere auch die zeitliche Entwicklung des Standards berücksichtigt. Die möglichen Ausprägungen sind:
  - *Gering:* Der Standard wurde noch nicht spezifiziert oder die Spezifikation ist nur sehr rudimentär. Es existieren noch keine vollständigen Referenzimplementierungen.
  - *Mittel:* Es liegt eine erste Standardspezifikation vor sowie evtl. darauf aufbauende Überarbeitungen vor. Es gibt wenige Referenzimplementierungen.
  - *Hoch:* Für den Standard existieren bereits mehrere, überarbeitete Spezifikationen oder die aktuelle Spezifikation hat trotz vielfacher Anwendung bestand. Es existieren zahlreiche Implementierungen. Im Fall von bereits breiter Verwendung wird der Reifegrad als Produkt klassifiziert.
- **Durchsetzungsfähigkeit:** Unter Berücksichtigung der an einem Standard Beteiligten sowie der Initiatoren wird eine Einschätzung der Durchsetzungsfähigkeit im Cloud Computing vorgenommen. Dazu wurde auch der aktuelle Bedarf und Standardisierungsdruck des Standards berücksichtigt. Neben der Anzahl der Unterstützer wird auch die Qualität der Unterstützer (bspw. Marktmacht oder Standardisierungserfahrung) berücksichtigt. Prognosen versprechen Potenzial in den Abstufungen:
  - *Gering:* Der Bedarf der Standardisierung ist vorhanden. Es fehlt jedoch eine breite, qualitative hochwertige Masse an Unterstützern.
  - *Mittel:* Der Bedarf für Standards ist hoch. Es gibt einige Unterstützer. Darunter befinden sich auch solche von hoher Qualität.
  - *Hoch:* Der Bedarf für Standards ist dringend. Es gibt ausreichende Masse und Qualität der Unterstützer. Die Koordination der Standardisierungsbemühen ist sichergestellt.
- **Partizipationsmöglichkeit:** Die Möglichkeiten zur Mitwirkung bei der (Weiter-)Entwicklung von Standards durch die öffentlichen Verwaltung, Unternehmen oder Personen hängen stark von der Standardisierungsorganisation ab. Je nach Standardisierungsorganisation sind Par-

tizipationsmöglichkeiten unterschiedlich stark beschränkt bzw. unterliegen zahlreichen Vorgaben zur Regelung der Beitragsrechte<sup>32</sup>:

- *Keine/gering*: Eine Mitwirkung bei der Standardisierung ist nicht möglich oder es existieren nur sehr eingeschränkte, in ihrer Umsetzung wenig transparente Mitwirkungsmöglichkeiten. Dies ist typischerweise bei de-facto-Standards der Fall.
- *Mittel*: Die Möglichkeit zur Mitwirkung bei der Standardisierung setzt eine persönliche oder organisationale Mitgliedschaft voraus. Hierfür sind zeitgebundene, meist hohe Mitgliedsbeiträge zu entrichten. Die Partizipation ist auf einzelne Arbeitsgruppen beschränkt. In der Regel ist auch der Zugriff auf Arbeitsmaterialien und die Lizenzierung der Standards Arbeitsgruppen-spezifisch geregelt und kann weitere Kosten verursachen.
- *Hoch*: Die Partizipation bei Weiterentwicklung eines Standards kann eine Mitgliedschaft bei der Standardisierungsorganisation voraussetzen. Die Höhe der Mitgliedsbeiträge stellt jedoch in der Regel kein Hindernis für die Partizipation dar (bspw. durch gestaffelte Beitragsmodelle). Zusatzbeiträge für den Beitritt zu Arbeitsgruppen oder zur Lizenzierung des Standards fallen nicht an.
- *Offen/sehr hoch*: Standardisierungsvorhaben, die keine Einschränkungen der Partizipation vorsehen oder diese an einen kostenfreien Beitritt zur Organisation binden, werden als offen gekennzeichnet. Die Verwendung der Standards kann unter Einhaltung von gebührenfreien Lizenzmodellen erfolgen.

### **Lückenanalyse**

Die Studie hat neben der Identifikation und Bewertung von Vorarbeiten, Standards und Zertifizierungen im Cloud Computing auch die Analyse von gegenwärtigen Lücken der Standardisierung zum Ziel. Unter Standardisierungslücken werden dabei solche Ansätze der Standardisierung verstanden, deren inhaltliche Reife und/oder Breite bislang nicht in ausreichendem Maße bearbeitet wird, um die Herausforderungen im Cloud Computing zu adressieren.

Zur Identifikation der gegenwärtigen Lücken in der Standardisierung des Cloud Computing wird ein zweistufiges Vorgehen gewählt, das in der Abbildung auf der Folgeseite illustriert wird.

---

<sup>32</sup> Details zu den Beitragsmodellen sowie Mitwirkungsmöglichkeiten und -pflichten einzelner Standardisierungsorganisationen finden sich in Kapitel 4.



dig ausschöpfen. Die Dringlichkeit der Standardisierung ist eher langfristig einzuschätzen.

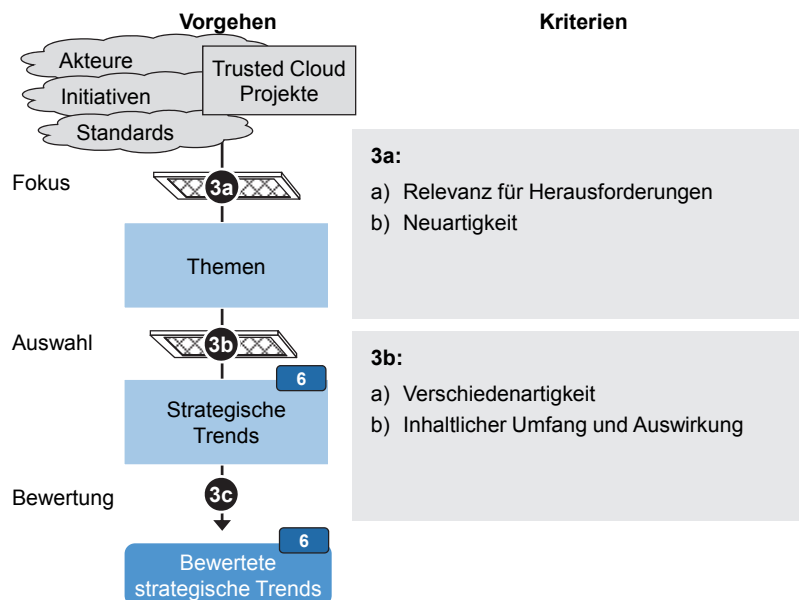
- *Erhöht:* Eine Standardisierungslücke ist erhöht, wenn Potenzial der Standardisierung offensichtlich ist, existierende Standards dieses aber noch nicht vollständig ausschöpfen. Die Dringlichkeit der Standardisierung ist eher mittelfristig einzuschätzen.
- *Hoch:* Eine Standardisierungslücke ist hoch, wenn Potenzial der Standardisierung offensichtlich ist, existierende Standards dieses aber unzureichend ausschöpfen oder nicht vorhanden sind. Die Dringlichkeit der Standardisierung ist eher kurzfristig einzuschätzen.

Die Identifikation von Lücken der Standardisierung schließt die ganzheitliche Betrachtung der aktuellen Standardlage zur Erörterung des Normierungs- und Standardisierungsumfelds im Cloud Computing ab. Gleichzeitig wird hierdurch ein wichtiger Grundstein für die Ableitung von Handlungsempfehlungen gelegt.

### 3.3.3 Auswahl strategischer Trends

An dieser Stelle wird das methodische Vorgehen bei der Festlegung des Fokus, der Auswahl und Bewertung der strategischen Trends ausgeführt. Die Ergebnisse der Untersuchung, also die Beschreibung der Trends erfolgt in Kapitel 6.

Folgende Abbildung zeigt die Fokus- und Auswahlkriterien für die strategischen Trends.



**Abbildung 15:** Fokus- und Auswahlkriterien für strategische Trends<sup>33</sup>

Folgende Themen und Quellen liegen der Auswertung der strategischen Trends zu Grunde:

<sup>33</sup> Quellen: Analyse von Booz & Company und FZI.



- Themen in White Paper, Leitfäden, Studien, Anforderungsdokumenten und von Standards,
- Themen bei Gremien der Standardisierungsorganisationen,
- Trends und Themen in Pressearchiven und Fachzeitschriften sowie
- Trends und Themen, die in Experteninterviews und durch die Trusted Cloud-Projekte genannt werden.

### *Fokus*

Der Fokus liegt auf Themen mit starkem, aber nicht notwendigerweise ausschließlichem, Bezug zu Deutschland, die folgende Kriterien erfüllen.

- **Relevanz für Herausforderungen:** Die Themen besitzen alle unmittelbare strategische Relevanz für die Cloud-Standardisierung, da sie einen inhärenten, im Einzelfall aber unterschiedlichen, Bezug zu den Herausforderungen im Cloud Computing (siehe 3.2.1) besitzen.
- **Neuartigkeit:** Es existieren in den letzten Jahren Aktivitäten zu diesen Themen, die auch kürzlich Momentum zeigen.

### *Auswahl*

Folgende Auswahlkriterien werden an die Grundgesamtheit der Themen angelegt, um die strategischen Trends, die in der vorliegenden Studie ausgewertet werden, auswählen zu können.

- **Verschiedenartigkeit:** Die strategischen Trends besitzen im wechselseitigen Vergleich untereinander und gemessen an der Taxonomie eine möglichst hohe Verschiedenartigkeit. Inhaltliche Überschneidungen werden möglichst reduziert, sind dieser Vorgehensweise allerdings inhärent, da die Trends real existierende Strukturen widerspiegeln und diese bündeln.
- **Inhaltlicher Umfang und Auswirkung:** Ein strategischer Trend ist möglichst übergreifend und inhaltlich umfassend. Er lässt aktuell die größte Eigendynamik auf einen Zeithorizont bis 2015 erkennen.

### *Bewertung*

Die Bewertung der Trends wird qualitativ vorgenommen. Es werden unter anderem Aspekte, wie Innovationspotenzial, Dringlichkeit und Eigendynamik berücksichtigt.

## 4 Wichtige Cloud-Standardisierungsorganisationen

Die Beschreibung ausgewählter Standardisierungsorganisationen soll zu Beginn durch die grundsätzliche Standardisierungsmechanik am freien Markt und kurzen Fallbeispielen einer Standardisierung motiviert werden.

Standardisierung kann als ein Prozess betrachtet werden, der abhängig von der Produktreife, der Marktstruktur und den Standardisierungsthemen durch verschiedene Akteure getrieben wird. Eine Standardisierung wird in der Regel durch neuartige Technologien und Produkte aus Wissenschaft und Forschung sowie der Wirtschaft eingeleitet.

Privatwirtschaftliche Unternehmen und wissenschaftliche Einrichtungen können zwei strategisch grundsätzlich verschiedene Strategien verfolgen: Der Versuch eigene Standards am Markt durchzusetzen oder die Festlegung von Standards im Rahmen von Kooperationen bzw. in Standardisierungsgremien. Auf einem freien Markt besitzen a priori beide Strategien ihre Berechtigung. Nicht selten ist auch ein Wechselspiel zwischen beiden festzustellen. Entscheidend sind der Zeitpunkt und der tatsächliche Einfluss der Standardisierungsarbeit in Gremien. Am Ende einer prototypischen Standardisierung steht eine breit akzeptierte Norm beispielsweise der Internationalen Organisation für Normung (ISO).

Folgende Beispiele sollen diesen Prozess verdeutlichen:

- Der MP3 Standard wurde überwiegend durch eine Forschungsallianz unter der Federführung des Fraunhofer IIS entwickelt.<sup>34</sup> Abstimmungen gab es lediglich im Rahmen einer MPEG-Audiogruppe.<sup>35</sup> Der ursprüngliche MP3 Standard hat sich weitestgehend unverändert durchgesetzt und wurde erst nachdem er breite Akzeptanz besaß in die ISO (ISO/IEC 11172-3, ISO/IEC 13818-3) eingebracht.
- Blu-ray hingegen hat sich in einem „Formatkrieg“, der am offenen Markt ausgetragen wurde, gegen seine Wettbewerber HD DVD und VMD durchgesetzt. Toshiba stellte seine HD DVD Technik in 2008 ein und brachte danach ein Blue-ray-Abspielgerät heraus.<sup>36</sup>
- Bei DVDs kam es 1995 an einem verhältnismäßig frühen Zeitpunkt in der Standardisierung zu einer gemeinsamen Einigung zwischen den Anbietern. Dies ist wesentlich auf den Druck der Filmindustrie zurückzuführen, die ein Szenario wie bei der Markteinführung von Videorekordern unbedingt vermeiden wollte und die der Leittragende unterschiedlicher Formate gewesen wäre.

Aus staatlicher Sicht kann auf die Standardisierung durch verschiedene partizipative oder regulatorische Instrumente Einfluss genommen werden. Pri-

---

<sup>34</sup> <http://www.iis.fraunhofer.de/bf/amm/diemp3geschichte/entwicklung/>

<sup>35</sup> <http://www.iis.fraunhofer.de/bf/amm/diemp3geschichte/team/>

<sup>36</sup> [http://www.toshiba.co.jp/about/press/2008\\_02/pr1903.htm](http://www.toshiba.co.jp/about/press/2008_02/pr1903.htm)

vatwirtschaftliche Anbieter und Anwender bewegen sich hingegen auf dem freien Markt und sind auf Standardisierungsgremien oder ihre Marktmacht zur Durchsetzung ihrer Interessen angewiesen.

Cloud Computing befindet sich am Anfang des Standardisierung-Prozesses. Derzeit wird die Standardisierung insbesondere durch die großen US-amerikanischen Anbieter (z.B. Google, Amazon) bestimmt, die überwiegend danach streben die „de-facto“ Standards ihrer eigenen Cloud-Lösungen im Wettbewerb durchzusetzen. Eine zweite Gruppe bildet sich um Anbieter (z.B. AMD, Cisco, VMware, IBM, Microsoft oder viele KMU), deren Lösungen noch weniger Marktanteile besitzen und die deshalb auf Kooperationen mit anderen setzen (siehe 6.2.3).

Für Anbieter mit geringerer Marktmacht und die Gruppe der Anwender stellt sich eine Beeinflussung des faktischen Standardisierungsgeschehens im Cloud Computing folglich als Herausforderung dar. Dies gilt insbesondere für viele deutsche Anbieter sowie Anwender in der Wirtschaft und insbesondere im Mittelstand. Eine naheliegende Strategie besteht darin sich selbst in Interessensgruppen zu organisieren und den eigenen Einfluss gebündelt in existierenden Standardisierungsgremien einzubringen. Folglich können so eigene Anforderungen eingebracht werden und gleichzeitig auch die Bedeutung bestehender Gremien gestärkt werden.

Vor diesem Hintergrund, stehen bei der Beschreibung von Standardisierungsorganisationen (siehe Definition in 3.1.1) in diesem Kapitel alle diejenigen im Vordergrund (siehe Methodologie in 3.3.1), die sich durch ein Mindestmaß an Engagement bei der Standardisierung im Cloud Computing und ein Mindestmaß an Partizipationsmöglichkeiten auszeichnen.





In diesem Kapitel wird – gemäß dieser Perspektive – eine Auswahl der für diese Studie bedeutendsten Standardisierungsorganisationen skizziert. Dabei müssen stets Abhängigkeiten zwischen deutscher, europäischer und internationaler Ebene berücksichtigt werden. Sofern besondere Abstimmungspotenziale auf nationaler Ebene bestehen, wie dies im Fall der NIST in den USA der Fall ist, wird dies berücksichtigt. Alle ausgewählten Standardisierungsorganisationen haben gemein, dass sie ein Standardisierungsgremium besitzen, das sich mit Themen beschäftigt, die entweder einen expliziten oder impliziten Bezug zum Cloud Computing aufweisen. Die ursprüngliche fachliche Ausrichtung der Organisationen und deren Teilnehmer muss dagegen nicht unmittelbar eine Beziehung zum Cloud Computing erkennen lassen. Der Fokus der Darstellung in diesem Kapitel liegt ausdrücklich nicht auf Vollständigkeit, hierfür sei auf laufende Aktivitäten verwiesen, z.B. der IETF<sup>37</sup> oder das „Cloud Standards Wiki“<sup>38</sup>.

---

<sup>37</sup> <http://tools.ietf.org/id/draft-khasnabish-cloud-sdo-survey-01.txt>

<sup>38</sup> <http://cloud-standards.org>

Folgende Abbildung gibt einen Überblick der in dieser Studie betrachteten Standardisierungsorganisationen, die sich durch ihr Engagement im Cloud Computing für eine Beschreibung in diesem Kapitel qualifiziert haben.

AUSWAHL	Allgemein	Cloud Computing	IKT, sonstige
International	ISO		
USA	NIST		
Europa	ETSI	EuroCloud	ENISA (European Network and Information Security Agency)
Deutschland	DIN		

**Abbildung 16:** Übersicht von Standardisierungsorganisationen im Cloud Computing<sup>39</sup>

Folgende Abbildung fasst das Engagement dieser Organisationen bei der Standardisierung im Cloud Computing beispielhaft zusammen.

**Tabelle 1:** Übersicht wichtiger Standardisierungsorganisationen im Cloud Computing<sup>40</sup>

Fokus	Organisation	Cloud-Standardisierungsengagement (Beispiele)
International	Allg. ISO (Internationale Organisation für Normung)	OSIMM, OVF, SOA, Orientierungswissen, Anforderungen sowie Koordination der Cloud-Standardisierung (z.B. in JTC 1/SC 38)
	CC CSA (Cloud Security Alliance)	Best Practices, Orientierungswissen und Standards im Bereich Sicherheit für das Cloud Computing (z.B. GRC Stack)
	CC OCC (Open Cloud Consortium)	Cloud-Infrastruktur für Forschungszwecke, Cloud Computing-Testumgebungen, Referenzimplementierungen, MaS-tone Benchmark
	IKT DMTF (Distributed Management Task Force)	OVF, System Virtualization Management Standards (VMAN), Management-Datenmodell
	IKT IETF (Internet Engineering Task Force)	Internetprotokolle und -standards, wie FTP, http/HTTPS, TCP/IP, X.509 Certificates, PKI oder OAuth; Übersicht von Cloud-Standardisierungsgrößen
	IKT ITU (International Telecommunications Union)	Cloud-Definition, Ökosystem, Use Cases Anforderungen & Architektur, Sicherheit im CC, Cloud-Infrastruktur, Lückenanalyse. Aktionsplan
	IKT OASIS (Organization for the Advancement of Structured Information Standards)	Begriffe, Use Cases und Lücken zu Cloud-Identität (in IDCloud), viele implizit relevante Standards (z.B. SAML, ODF, SOA, WS-*)

<sup>39</sup> Analyse von Booz & Company und FZI.

<sup>40</sup> Analyse von Booz & Company und FZI.

Fokus		Organisation	Cloud-Standardisierungsengagement (Beispiele)
International	IKT	OGF (Open Grid Forum)	Open Cloud Computing Interface (OCCI) oder GridFTP
	IKT	SNIA (Storage Networking Industry Association)	Cloud Data Management Interface (CDMI), Storage Management Initiative Specification (SMI-S), eXtensible Access Method (XAM)
	IKT	TOG (The Open Group)	Standards zur Integration von Cloud Computing in bestehende Firmenarchitekturen, z.B. Cloud Computing Reference Architecture (CCRA)
	IKT	TM-F (TM Forum)	Anpassungen von Frameworks für das CC, Cloud Billing, Cloud SLA Mgmt., Cloud Security & Risk, Cloud Business Process Framework
	IKT	W3C (World Wide Web Consortium)	USDL Inkubator, allgemeine Web-Standards (z.B. HTML, XML, CSS, WSDL, XML Encryption, XML Digital Signature oder SOAP)
USA		NIST (National Institute of Standards and Technology)	Cloud Computing-Standardisierungsroadmap, Referenzarchitekturen, Taxonomie, Use Cases, Orientierungswissen, Koordination
Europa	Allg.	ETSI (Europäisches Institut für Telekommunikationsnormen)	Standards, Lückenanalyse und Testsysteme zu Interoperabilität, Anforderungen, Use Cases, Koordination, Standardisierungsroadmap
	CC	EuroCloud	Umfangreicher Leitfaden zu Recht, Datenschutz und Compliance, EuroCloud Star Audit ("SaaS-Gütesiegel")
	IKT	ENISA (Europäische Agentur für Netz- und Informationssicherheit)	Cloud Computing – SME Survey, Cloud Computing Information Assurance Framework, Cloud Computing Risk Assessment
Deutschland	Allg.	DIN (Deutsches Institut für Normung)	Spiegelgremien zur ISO JTC 1/SC 38 im NIA-01-38 „Verteilte Anwendungsplattformen und Dienste“
	CC	SaaS-ES (SaaS-EcoSystem)	Zertifikat „Trust in Cloud“ für SaaS und Cloud-Lösungen, Zertifikat „Cloud Experte“
	IKT	BITKOM (Bundesverband Informationswirtschaft, Telekommunikation & neue Medien)	Leitfaden des Arbeitskreis „Cloud Computing & Outsourcing“, Betreiber von Cloud-Practice.de (z.B. vertragliche Regelungen, Use Cases)

Neben obigen Standardisierungsorganisationen gibt es viele weitere Organisationen, die noch kein klares Engagement bei der Cloud-Standardisierung zeigen oder keine Partizipationsmöglichkeiten bieten. Einige könnten aber in Zukunft eine größere Rolle spielen und finden deshalb an dieser Stelle kurze Erwähnung.

Auf deutscher Ebene sind dies beispielsweise die Deutsche Kommission Elektrotechnik Elektronik Informationstechnik (DKE), der Bundesverband der deutschen Industrie (BDI), der Bundesverband mittelständische Wirtschaft (BVMW) oder der Bundesverband IT-Mittelstand (BITMi e.V.). Auf staatlicher Seite sind das Bundesamt für Sicherheit in der Informationstechnik (BSI), der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit<sup>41</sup> und die Bundesnetzagentur zu nennen.

<sup>41</sup> Gemeinsam mit den Datenschutzbehörden der Länder, z.B. dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD).

Andere Standardisierungsorganisationen auf nationaler Ebene sind beispielsweise das Cloud Computing Forum (CCF) in Korea, das Global Inter-Cloud Technology Forum (GICTF) in Japan, die Cloud Operations and Security Arbeitsgruppe in Japan oder die China Communications Standards Association (CCSA).

Auf europäischer Ebene ist zu erwarten, dass neben der ETSI auch die European Grid Infrastructure (EGI), die Networked European Software and Services Initiative (NESSI) und die Europäische Agentur für Netz- und Informationssicherheit (ENISA) eine Rolle spielen werden. Im Europäischen Komitee für Normung (CEN) gibt es bisher keine Bemühungen im Cloud Computing.

Weitere Standardisierungsorganisationen auf internationaler Ebene, die erst seit kurzem existieren bzw. nur geringe Standardisierungsbeiträge erkennen lassen, sind das Cloud Computing Interoperability Forum (CCIF), das Open Cloud Consortium (OCC), die Object Management Group (OMG), das Cloud Standards Customer Council (CSCC) oder die Open Data Center Alliance.

### 4.1 Deutsche Standardisierungsorganisationen

#### 4.1.1 Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (BITKOM)

	Eckdaten	
	Gründungsjahr	1999
	Hauptsitz	Berlin
	Fokus	Deutschland / ITK
	Internet	<a href="http://www.bitkom.org">www.bitkom.org</a>

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) ist der Branchenverband der deutschen Informations- und Telekommunikationsbranche. BITKOM vertritt mehr als 1.600 Unternehmen, davon über 1.000 Direktmitglieder. Zunächst agierte BITKOM nur als Dachverband. Inzwischen wirkt BITKOM auch an fachlichen Themen in diversen Gremien und Projekten mit. BITKOM hat sich als Ziel gesetzt die politischen und wirtschaftlichen Rahmenbedingungen für die ITK-Branchen durch Interessenvertretung zu optimieren. BITKOM engagiert sich für strategische ITK-Politik, die die Politikebenen von der EU über Bund und Länder bis zu den Kommunen umfasst.

Mit Cloud Computing setzen sich mehrere BITKOM-Arbeitskreise der Kompetenzbereiche IT-Services, Software, Sicherheit, IT-Infrastruktur & Digital Office sowie Umwelt & Nachhaltigkeit auseinander. Seit 2008 besitzt BITKOM auch den Arbeitskreis „Cloud Computing & Outsourcing“<sup>42</sup>, der

<sup>42</sup> <http://www.bitkom.org/de/themen/61490.aspx>




sich explizit mit dem Cloud Computing beschäftigt. Im Rahmen dieses Arbeitskreises wurde der „Leitfaden Cloud Computing“<sup>43</sup> erarbeitet und im Oktober 2009 veröffentlicht. BITKOM wirkt auch beim Aktionsprogramm Cloud Computing des BMWi mit und ist einer der Schirmherren des Portals [www.Cloud-Practice.de](http://www.Cloud-Practice.de), das verschiedenstes Know-How (z.B. zu vertraglichen Regelungen, Datenschutz, Informationssicherheit oder Compliance) sowie Use Cases bündelt.

BITKOM ist auch Mitglied in Deutschland sicher im Netz e.V., einer Initiative für mehr Online-Sicherheit.

BITKOMs Mitwirkung bei der Standardisierung im Cloud Computing fokussiert sich folglich überwiegend auf die Anforderungsdefinition, Interessensvertretung und der Bereitstellung von Orientierungswissen.

Die Mitgliedschaft in dem BITKOM ist deutschen ITK-Unternehmen vorbehalten und setzt die Entrichtung eines Mitgliedbeitrags voraus. Darüber hinaus werden keine weiteren Bedingungen an die Mitgliedschaft geknüpft.

### 4.1.2 Deutsches Institut für Normung (DIN)

	Eckdaten	
	Gründungsjahr	1917
	Hauptsitz	Berlin
	Fokus	Deutschland / Allgemein
	Internet	<a href="http://www.din.de">www.din.de</a>

Das Deutsche Institut für Normung e. V. (DIN) ist die bedeutendste nationale Normungsorganisation in Deutschland, die privatwirtschaftlich mit dem rechtlichen Status eines gemeinnützigen Vereins organisiert ist. Durch Abschluss eines Normenvertrages mit der Bundesrepublik Deutschland 1975 ist das DIN als die nationale Normungsorganisation in den europäischen und internationalen Normungsorganisationen anerkannt. Die Hauptaufgabe des DIN besteht darin, gemeinsam mit den Vertretern der interessierten Kreise (z.B. Hersteller, Handel, Industrie, Wissenschaft, Verbraucher, Prüfinstitute und Behörden) Normen, Spezifikationen und Standards zu erarbeiten. Heute ist die Normungsarbeit des DIN zu fast 90 Prozent europäisch und international ausgerichtet. Das DIN vertritt somit vor allem deutsche Interessen auf europäischer und internationaler Ebene.

Im Rahmen des Normenausschuss Informationstechnik und Anwendungen (NIA) des DIN, existiert das Arbeitsgebiet „Verteilte Anwendungsplattformen und Dienste“ (NIA-01-38), das von besonderer Bedeutung für das Cloud Computing ist. Das Gremium umfasst vor allem die nationalen Spiegelgremien zu der „Studiengruppe zu Cloud Computing“ (ISO/IEC JTC 1/SC 38/SG


<sup>43</sup> [http://www.bitkom.org/de/themen/36129\\_61111.aspx](http://www.bitkom.org/de/themen/36129_61111.aspx)

1), zu „Web services“ (ISO/IEC JTC 1/SC 38/WG 1), zu „Service Oriented Architecture (SOA)“ (ISO/IEC JTC 1/SC 38/WG 2) und seit März 2010 zu „Cloud computing“ (ISO/IEC JTC 1/SC 38/WG 3). In dieser Rolle wirkt das NIA-01-38 bei vielen wichtigen Normen und Standards, wie OSIMM, OVF, W3C SOAP, W3C Web Services oder SOA mit und erstellt Studien.

Im NIA-01-38 sind derzeit Experten aus folgenden Organisationen vertreten: Microsoft Deutschland GmbH, IBM Deutschland GmbH, SAP AG, Fraunhofer-Institut für Offene Kommunikationssysteme (FOKUS), Fraunhofer-Institut für Software und Systemtechnik (ISST), das Ministerium des Innern und für Sport Rheinland-Pfalz, die Hochschule für Technik und Wirtschaft (HTW) und das Bundesamt für Sicherheit in der Informationstechnik (BSI).

Die Mitarbeit an der Normungstätigkeit unterliegt, wie in allen Normenausschüssen des DIN einer Geschäftsordnung und erfordert die Entsendung durch eine autorisierende Stelle. Gäste können sich unter bestimmten Umständen bei der zuständigen Geschäftsstelle im DIN zur befristeten Teilnahme anmelden.

### 4.1.3 SaaS-EcoSystem (SaaS-ES)

	Eckdaten	
	Gründungsjahr	2010 (Mai)
	Hauptsitz	Frankfurt
	Fokus	Deutschland / Cloud Comp.
	Internet	<a href="http://www.saasecosystem.org">www.saasecosystem.org</a>

SaaS-EcoSystem e.V. ist ein Unternehmensnetzwerk zum Thema SaaS und Cloud Computing. SaaS-EcoSystem ist ein eingetragener Verein (e.V.) mit derzeit 18 Mitgliedern, die sich überwiegend aus mittelständischen Softwareanbietern (ISV) zusammensetzen.<sup>44</sup> Das Ziel von SaaS-EcoSystem ist die Bewerbung, Förderung und wirtschaftliche Etablierung von SaaS bzw. Cloud Computing in Deutschland mit einem Fokus auf mittelständische Anbieter und Nutzer. SaaS-EcoSystem bietet Softwareanbietern (ISV) Leistungen zur Geschäftsstrategie, Lösungsarchitektur, IT-Umsetzung, dem Betriebsmodell und der Vermarktung (Marketing & Vertrieb). Leistungen an Nutzer umfassen Geschäftsstrategien, Auswahlstrategien, Entscheidungsunterstützung und Implementierung.

SaaS-EcoSystem hat das Zertifikat „Trust in Cloud“ für SaaS und Cloud-Lösungen und das Zertifikat „Cloud Experte“ für Experten erarbeitet. Beide Zertifikate besitzen gemessen an der Anzahl bisheriger Zertifizierungen eine

---


<sup>44</sup> Die beiden namhaftesten und größten Mitglieder sind IBM Deutschland GmbH und die FUJITSU Enabling Software Technology GmbH.

noch geringe Verbreitung. Die Vertrauensbildung der Zertifikate ist gering, da es sich im Wesentlichen um Fragebogen-basierte Ansätze handelt.

Die Mitgliedschaft unterliegt keinen grundsätzlichen Einschränkungen. Für die Mitgliedschaft wird ein Beitrag erhoben. Bevorzugte Mitglieder von SaaS-EcoSystem sind mittelständische Softwareanbieter im Cloud-Umfeld.

## 4.2 Europäische Standardisierungsorganisationen

### 4.2.1 Europäisches Institut für Telekommunikationsnormen (ETSI)

	Eckdaten	
	Gründungsjahr	1988
	Hauptsitz	Sophia-Antipolis, Frankreich
	Fokus	Europa / IKT
	Internet	<a href="http://www.etsi.org">http://www.etsi.org</a>

Das Europäische Institut für Telekommunikationsnormen (ETSI)<sup>45</sup> ist eine der drei großen Normungsorganisationen in Europa. ETSI ist ein gemeinnütziges Institut mit dem Ziel, europaweit einheitliche Standards im Bereich der Telekommunikation zu schaffen. Das Institut hat 655 Mitglieder aus über 50 Ländern, darunter Netzbetreiber, Diensteanbieter, Verwaltungen, Anwender und Hersteller.

ETSI besaß bei der Standardisierung im Cloud Computing ursprünglich einen besonderen Schwerpunkt auf Interoperabilität. In 2010 wurden im Rahmen der „Specialist Task Force on ICT GRID Technologies Interoperability and Standardization“ (STF 331) erste Berichte mit Bezug zum Cloud Computing erarbeitet: Ein White Paper „Grid and Cloud Computing Technology: Interoperability and Standardization for the Telecommunications Industry“, drei technische Berichte zu Interoperabilitätslücken und eine technische Spezifikation eines Testsystems für Interoperabilität.

Ebenfalls in 2010 wurde das ehemalige „Technical Committee GRID“ (TC GRID) in „Technical Committee CLOUD“ (TC CLOUD) umbenannt. Mit dem TC CLOUD beschäftigt sich das ETSI zukünftig mit der kompletten inhaltlichen Breite von Cloud Computing. Das TC CLOUD arbeitet an einem Entwurf für „Standardisation Requirements for Cloud Services“ und „Use Cases for Cloud Service Scenarios“.<sup>46</sup>

Seit Ende 2011 übernimmt auf EU-Ebene verstärkt das ETSI die koordinierende Rolle bei der Cloud-Standardisierung. Unter anderem führt das ETSI die Standardisierungsroadmap für e-Infrastrukturen aus dem SIENA<sup>47</sup> Projekt

<sup>45</sup> Engl.: European Telecommunications Standards Institute.


<sup>46</sup> Veröffentlicht im Januar 2011.

<sup>47</sup> <http://www.sienainitiative.eu>

fort. ETSI plant die Erarbeitung einer Standardisierungsroadmap für Interoperabilität im Cloud Computing.

Unternehmen können sich um eine Mitgliedschaft bei der ETSI bewerben. Die Mitgliedschaft ist gebührenpflichtig und ermöglicht die Teilnahme an technischen Komitees und Arbeitsgruppen.

### 4.2.2 EuroCloud

	Eckdaten	
	Gründungsjahr	2010 (Jan.) bzw. 2009 (Dez.)
	Hauptsitz	Paris bzw. Köln
	Fokus	Europa bzw. Deutschland / Cloud Computing
	Internet	<a href="http://www.eurocloud.org">www.eurocloud.org</a> <a href="http://www.eurocloud.de">www.eurocloud.de</a>

EuroCloud Europe ist ein paneuropäischer Unternehmensverband der Anbieter von Cloud Computing. Der Dachverband EuroCloud Europe vertritt die Interessen der europäischen Cloud Computing-Branche gegenüber der europäischen Politik und IT-Verbänden wie SNIA (Storage Networking Industry Association), BSA (Business Software Alliance) oder SIIA (Software and Information Industry Association). EuroCloud ist derzeit in 27 europäischen Ländern präsent und es existieren 17 nationale Verbände.

In Deutschland ist dies Eurocloud Deutschland\_eco e.V. mit derzeit 73 Mitgliedern, der dem eco – Verband der deutschen Internetwirtschaft e.V. mit rund 500 Mitgliedern angegliedert ist.


EuroCloud Deutschland umfasst die Kompetenzgruppen Cloud Managed Services, Interoperabilität & Standards, Recht & Compliance und SaaS-Gütesiegel. Zentrale Ergebnisse der bisherigen Arbeit sind der detaillierte „EuroCloud Leitfaden: Recht, Datenschutz und Compliance“<sup>48</sup> und das EuroCloud Star Audit ("SaaS-Gütesiegel"), das Parallelen zu einem Sterneranking für Hotels aufweist.

Die Mitgliedschaft im EuroCloud Deutschland\_eco e.V. ist kostenfrei, setzt jedoch eine Firmenmitgliedschaft im eco e.V. voraus. Auf europäischer Ebene sind Sponsorships von EuroCloud Europe möglich. Gold Sponsoren sind beispielsweise Microsoft, Joyent oder Equinix. Gold Sponsoren können u.a. Workshopleiter bestimmen.

---

<sup>48</sup> <http://www.eurocloud.de/2010/12/02/eurocloud-leitfaden-recht-datenschutz-compliance/>

#### 4.2.3 Europäischen Agentur für Netz- und Informationssicherheit (ENISA)

	Eckdaten	
	Gründungsjahr	2004
	Hauptsitz	Heraklion, Kreta, Griechenl.
	Fokus	Europa / IKT
	Internet	<a href="http://www.enisa.europa.eu">www.enisa.europa.eu</a>

Die Europäische Agentur für Netz- und Informationssicherheit (ENISA) wurde 2004 von der Europäischen Union gegründet. Sie beschäftigt derzeit ca. 50 Mitarbeiter. Auf deutscher Ebene besteht insbesondere eine Kooperation mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI).

Ihr Zuständigkeitsschwerpunkt ist die Netz- und Informationssicherheit innerhalb der europäischen Union.<sup>49</sup> Eine Aufgabe der ENISA ist demnach die „Verfolgung der Entwicklung von Standards und Normen“.

Ein Arbeitsergebnis mit implizitem Bezug zur Standardisierung im Cloud Computing ist der im Oktober 2008 veröffentlichte Bericht „Technology-induced challenges in Privacy & Data Protection in Europe“.

Direkten Bezug zum Cloud Computing besitzt das „Cloud Computing – SME Survey“<sup>50</sup>, das „Cloud Computing Information Assurance Framework“<sup>51</sup> und insbesondere das „Cloud Computing Risk Assessment“<sup>52</sup>, die alle im November 2009 veröffentlicht wurden.

Alle Aktivitäten der ENISA sind als vorbereitende Arbeiten für die eigentliche Standardisierung im Cloud Computing relevant.

Die Mitwirkung bei der ENISA ist über den Verwaltungsrat (Management Board) möglich, der die ENISA überwacht. Er setzt sich aus Delegierten der Mitgliedstaaten, der Europäischen Kommission und Interessenvertretern der Wirtschaft, des Verbraucherschutzes und aus der Forschung zusammen.

<sup>49</sup> Zuständigkeitsbereich, Ziele und Aufgaben der ENISA sind im Detail in der Verordnung Nummer 460/2004 des Europäischen Parlamentes und Rates vom 10. März 2004 beschrieben.


<sup>50</sup> <http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-sme-survey>

<sup>51</sup> <http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-information-assurance-framework>

<sup>52</sup> <http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment>

## 4.3 Internationale Standardisierungsorganisationen

### 4.3.1 Cloud Security Alliance (CSA)

	Eckdaten	
	Gründungsjahr	2008 (Dez.)
	Hauptsitz	K.A.
	Fokus	International / Cloud Comp.
	Internet	<a href="http://www.cloudsecurityalliance.org">www.cloudsecurityalliance.org</a>

Die Cloud Security Alliance (CSA) ist eine nicht gewinnorientierte Organisation, die sich aus einer Koalition von Anbieterfirmen, Verbänden und Einzelpersonen zusammensetzt und insgesamt mehr als 25'000 Mitglieder<sup>53</sup> besitzt. Ihr Ziel ist die Verbreitung und die breite Anwendung von Best Practices zur Sicherheit im Cloud Computing.

Die CSA umfasst eine Vielzahl von Arbeitsgruppen und Initiativen: „Architecture and Framework“, „GRC, Audit, Physical, BCM, DR“, „Legal Issues: Contracts and E-Discovery“, „Portability, Interoperability and Application Security“, „Information Management and Data Security“, „Data Center Operations and Incident Response“, „Information Lifecycle Management and Storage“, „Virtualization and Technology Compartmentalization“ oder „Security as a Service“.

Die CSA veröffentlicht Best Practices, Orientierungswissen und Standards für das Cloud Computing: „Governance, Risk Management and Compliance Stack“ (GRC Stack, siehe 5.2.3), „Consensus Assessments Initiative“, „Cloud Controls Matrix (CCM)“, „Cloud Trust Protocol“, „Cloud Metrics“, „Common Assurance Maturity Model“, „CloudSIRT“, „Top Threats to Cloud Computing“, „Security as a Service“, „CloudAudit“, „Security Guidance“ (V3.0), „Trusted Cloud Initiative“<sup>54</sup> oder das „Certificate of Cloud Security Knowledge“ (CCSK).

Die CSA beansprucht für sich auch in Zukunft eine Führungsrolle bei der Entwicklung neuer Sicherheitsstandards im Cloud Computing.


Die CSA ist grundsätzlich offen für eine Mitgliedschaft von Unternehmen, Verbänden, Einrichtungen und auch Einzelpersonen. Die jährlichen Mitgliedsgebühren für ein Unternehmen belaufen sich derzeit auf 10.000 USD.

<sup>53</sup> Die CSA besitzt mehr 100 Firmenmitglieder.

<sup>54</sup> [www.trusted-cloud.com](http://www.trusted-cloud.com). Diese Initiative besitzt keinen Bezug zum deutschen Technologieprogramm Trusted Cloud.



#### 4.3.2 Distributed Management Task Force (DMTF)

	Eckdaten	
	Gründungsjahr	1992
	Hauptsitz	Portland, Oregon, USA
	Fokus	International / IKT
	Internet	<a href="http://www.dmtf.org">www.dmtf.org</a>

Die Distributed Management Task Force (DMTF) ist eine nicht gewinnorientierte Industrievereinigung, deren Aufgabe die Entwicklung von Standards für das Systems-Management sowie die Förderung der Interoperabilität von Lösungen für das Systems-Management durch Standards ist. Mit der Virtualization Management Initiative (VMAN) hat die DMTF eine auch für das Standardisierungsumfeld des Cloud Computing relevante Initiative gestartet.

Der Standardisierungsfokus der DMTF liegt auf technischen Ansatzpunkten für IaaS. Es werden in erster Linie die Herausforderungen wie Portabilität und Interoperabilität adressiert.

Die umfassend angelegte Standardisierungs-Agenda zur Unterstützung des Managements von virtualisierten Ressourcen erarbeitet Standards, die das Verwalten der virtuellen Ressourcen entlang des Lebenszyklus (Develop, Package/Distribute, Deploy, Manage, Retire) betrachten. Ein erstes Ergebnis der Initiative ist der Vorschlag zum Open Virtualization Format (OVF), das vor allem die Phasen Develop, Package/Distribute und Deploy abdeckt. In Zukunft sollen sogenannte „System Virtualization Management Standards (VMAN)“ einheitlich definierte Funktionen definieren, die ein einfaches und durchgängiges Management von beliebigen virtualisierten Umgebungen ermöglichen. Es wird auf etablierten Arbeiten zum Server-Management (SMASH – Systems Management Architecture for Server Hardware) sowie dem grundlegenden DMTF Management-Datenmodell (CIM – Common Information Model) aufgebaut, um Anbietern die Möglichkeit zu bieten physische und virtuelle Ressourcen gleichzeitig zu verwalten.

Erste Ansätze für VMAN sind bereits beschrieben und als Whitepaper veröffentlicht.<sup>55</sup> Technische Aspekte werden überwiegend von der Arbeitsgruppe „Systems Virtualization, Partitioning and Clustering (SVPC)“ bearbeitet. Die Weiterentwicklung der Standardisierung des Cloud Managements wird in den Arbeitsgruppen „Cloud Management Work Group (CMWG)“, „Cloud Auditing Data Federation (CADF)“ und „Open Cloud Standards Incubator“ vorangetrieben.


Die Mitarbeit in Form von Feedback zu Standards, Spezifikation, Profilen und White-Papern der DMTF ist nach Unterzeichnung der DMTF-Feedback Po-

<sup>55</sup> Vgl. CIM System Virtualization Model (Whitepaper), DSP2013\_1.0.0, [www.dmtf.org/vman](http://www.dmtf.org/vman).

licy<sup>56</sup> grundsätzlich allen Interessierten offen gestellt. Es gibt drei mögliche Stufen für eine Mitgliedschaft bei der DMTF:

- „Leadership“ (12.000 USD/Jahr<sup>57</sup>, mit Stimmrecht),
- „Participation“ (6.000 USD/Jahr<sup>57</sup>, Teilnahme in Arbeitsgruppen) und
- „Monitoring“ (2.500 USD/Jahr, erweiterte Informationen).

### 4.3.3 Internet Engineering Task Force (IETF)

	Eckdaten	
	Gründungsjahr	1986
	Hauptsitz	-- <sup>58</sup>
	Fokus	International / IKT
	Internet	<a href="http://www.ietf.org">www.ietf.org</a>

Die Internet Engineering Task Force (IETF) ist eine offene Vereinigung von freiwilligen Experten, deren Ziel die Entwicklung und Verbreitung von Internetstandards ist. Sie konstituiert sich im Wesentlichen durch regelmäßige IETF-Meetings und Arbeitsgruppen, die über E-Mail oder Foren kommunizieren und jedem zugänglich sind. Die Arbeit der IETF konzentriert sich auf die Lösung technischer Probleme im Internet, die kurzfristig adressierbar sind. Typischerweise wird die Interoperabilität zwischen Produkten verschiedener Hersteller über das Internet angestrebt. Die Arbeitsgruppen entwerfen, prüfen und testen zu diesem Zweck Spezifikationen von Protokollen.

Die IETF besitzt aktuell keine Arbeitsgruppen, die sich speziell mit Protokollen für das Cloud Computing befassen. Derzeit werden Lösungen für das Cloud Computing im Rahmen der regulären IETF-Meetings diskutiert, beispielsweise die „Cloud Computing and Networking bar BOFs“ in Anaheim (IETF-77), Maastricht (IETF-78), und Beijing (IETF-79)<sup>59</sup>. Es werden insbesondere Ergebnisse aus den Arbeitsgruppen IETF/APP Decade<sup>60</sup>, IETF/TSV/nfsv4<sup>61</sup> und IETF/OPS/netconf als relevant für eine Anpassung für das Cloud Computing betrachtet. Es ist anzunehmen, dass das IETF in diesem Bereich zukünftig wesentliche Beiträge zur Standardisierung im Cloud Computing leisten kann.

---

<sup>56</sup> Die Unterzeichnung der Feedback Policy überträgt der DMTF bspw. das Recht der ausschließlichen, nicht widerruflichen und lizenzfreien Nutzung des Feedbacks (vgl. <http://www.dmtf.org/standards/feedback>).

<sup>57</sup> 50% Rabatt für Endnutzer oder Regierungseinrichtungen.

<sup>58</sup> Die IETF ist keine Körperschaft und ist ohne Rechtsform.

<sup>59</sup> Präsentationen auf <http://trac.tools.ietf.org/area/app/trac/wiki/Clouds>.

<sup>60</sup> <https://datatracker.ietf.org/wg/decade/>


<sup>61</sup> <http://tools.ietf.org/wg/nfsv4/charters>

Zusätzlich erscheint es wahrscheinlich, dass auch viele zentrale Internetstandards, wie FTP, http/HTTPS, TCP/IP, X.509 Certificates, PKI oder OAuth auf ihre Anpassung für das Cloud Computing untersucht werden.

Die IETF stellt selbst keine Körperschaft dar und besitzt dadurch keine Rechtsform. Die Teilnahme an den IETF-Meetings oder Mitwirkung in Arbeitsgruppen steht jedem offen. Entscheidungen liegen keine strikten Konsensbildungsprozesse zu Grunde. Vielmehr wird ein grober Konsens als ausreichend betrachtet. Es besteht keine förmliche Mitgliedschaft oder Mitgliedsvoraussetzung.

Die IETF arbeitet in enger Kooperation mit dem W3C und der ISO / IEC.

### 4.3.4 Internationale Organisation für Normung (ISO)

	Eckdaten	
	Gründungsjahr	1947
	Hauptsitz	Genf, Schweiz
	Fokus	International / Allgemein
	Internet	<a href="http://www.iso.org">www.iso.org</a>

Die Internationale Organisation für Normung (ISO) ist eine Nichtregierungsorganisation, die sich als Netzwerk aus derzeit 162 nationalen Normungsorganisationen mit gesetzlichem Auftrag (z.B. DIN, AFNOR, ANSI) zusammensetzt. Ihre Hauptaufgabe ist die Entwicklung und Veröffentlichung von internationalen Standards gemäß Konsensverfahren.

ISO's technisches Komitee JTC 1 / SC 38 "Distributed application platforms and services (DAPS)"<sup>62</sup> umfasst folgende Arbeitsgruppen bzw. Studiengruppe, die besonderer Bedeutung für das Cloud Computing besitzen.


- Web services (ISO/IEC JTC 1/SC 38/WG 1),
- Service Oriented Architecture (SOA) (ISO/IEC JTC 1/SC 38/WG 2),
- Cloud computing (ISO/IEC JTC 1/SC 38/WG 3) und
- Studiengruppe zu Cloud Computing (ISO/IEC JTC 1/SC 38/SG 1).

Die Arbeitsgruppen arbeiten beispielsweise an folgenden Normen und Standards: OSIMM, OVF, W3C SOAP, W3C Web Services, SOA, etc. Die Studiengruppe beschäftigt sich insbesondere mit der Erarbeitung von Definitionen, Orientierungswissen oder Anforderungen sowie der Koordination. Die DIN ist für Deutschland aktives Mitglied in JTC 1 / SC 38 (siehe auch 4.1.2). Unternehmen können über folgende Standardisierungsorganisationen, die mit dem JTC 1 / SC 38 zusammenarbeiten, auf die Arbeit einwirken: DMTF, INLAC, ITU, OASIS und SNIA.

<sup>62</sup> [http://www.iso.org/iso/standards\\_development/technical\\_committees/list\\_of\\_iso\\_technical\\_committees/iso\\_technical\\_committee.htm?commid=601355](http://www.iso.org/iso/standards_development/technical_committees/list_of_iso_technical_committees/iso_technical_committee.htm?commid=601355)

ISO's technisches Komitee SC27 arbeitet an den Leitlinien "Information technology – Security techniques – Security in cloud computing" (ISO/IEC 27017), das auf ISO/IEC 27002 basiert. Laut Komitee wird es keine spezifische Zertifizierung zur Sicherheit im Cloud Computing geben. ISO/IEC 27001 wird nach Anpassungen auch für das Cloud Computing als ausreichend erachtet.

### 4.3.5 International Telecommunications Union (ITU)

	Eckdaten	
	Gründungsjahr	1865
	Hauptsitz	Genf, Schweiz
	Fokus	International / IKT
	Internet	<a href="http://www.itu.int">www.itu.int</a>

International Telecommunications Union (ITU) ist eine Spezialagentur der Vereinten Nationen, die sich für den IKT-Bereich verantwortlich zeichnet. Sie besitzt drei Tätigkeitsbereiche: ITU-T (Telecommunication Standardization Sector), ITU-R (Radiocommunication Sector) und ITU-D (Telecommunication Development Sector). Die ITU-T besitzt folglich einen ausschließlichen Fokus auf Standardisierung.

Die ITU-T hat im Februar 2010 auf einem ihrer Mitgliedertreffen in Genf die ITU-T Focus Group on Cloud Computing (FG Cloud)<sup>63</sup> eingerichtet. Die FG Cloud setzt sich zum Ziel im Rahmen der Kompetenzen und Aufgabenbereiche der ITU-T bei der Standardisierung im Cloud Computing mitzuwirken. Sie umfasst derzeit folgende Arbeitsgruppen:

WG1: Cloud Computing Vorteile & Anforderungen

- WA 1-1 Cloud Definition, Ökosystem & Taxonomie
- WA 1-2 Uses Cases Anforderungen & Architektur
- WA 1-3 Sicherheit im Cloud Computing
- WA 1-4 Infrastruktur- & Netzwerkeinsatz für die Cloud
- WA 1-5 Cloud-Dienste & Ressourcenmanagement, Plattformen und Middleware
- WA 1-6 Cloud Computing Vorteile & erste Anforderungen aus einer IKT-Perspektive


WG2: Lückenanalyse & Roadmap für Cloud-Standardisierung in d. ITU-T

- WA 2-1 Überblick der Aktivitäten von Standardisierungsorganisationen im Cloud Computing
- WA 2-2 Lückenanalyse & Aktionsplan für die Entwicklung relevanter ITU-T Cloud-Standards

<sup>63</sup> <http://www.itu.int/en/ITU-T/focusgroups/cloud/>

Viele Arbeitsergebnisse und Mailinglisten der FG Cloud sind für Gäste nach einer Registrierung zugänglich. Die Mitwirkungsmöglichkeiten bei der ITU sowie bei der der FG Cloud sind vom eigenen Mitgliederstatus abhängig. Die ITU unterscheidet Mitgliedsstaaten, Sektorenmitglieder und Partner.<sup>64</sup>

#### 4.3.6 National Institute of Standards and Technology (NIST)

	Eckdaten	
	Gründungsjahr	1901
	Hauptsitz	Gaithersburg, MD, USA
	Fokus	USA / Allgemein
	Internet	<a href="http://www.nist.gov">www.nist.gov</a>

Das National Institute of Standards and Technology (NIST) ist eine Bundesbehörde des Wirtschaftsministeriums der Vereinigten Staaten von Amerika. Das NIST ist die US-weit bedeutendste öffentliche Forschungseinrichtung für Technologieentwicklung. Ziel der NIST ist die Förderung von Innovation und industrieller Wettbewerbsfähigkeit in den USA durch das Vorantreiben von Messtechnik, Standards und Technologie. Die NIST ist kein offizielles nationales Normungsinstitut der USA, sondern koordiniert unter dem National Technology Transfer and Advancement Act (NTTAA) mit dem Standards and Coordination Office (SCO) technische Standardisierungs- und Konformitätsaktivitäten im öffentlichen und privaten Sektor. Die NIST überwacht auch Standardisierungsaktivitäten weltweit.

Bereits vor der Erscheinung der Nationalen Cloud Computing-Strategie der USA wurde das NIST damit beauftragt die Einführung von Cloud Computing in allen Regierungsbereichen zu beschleunigen und zu sichern. Seither treibt das NIST die nationalen und internationalen Bestrebungen zur Entwicklung von Standards und Richtlinien für Cloud Computing maßgeblich voran. Dies soll – gemäß Vorgabe – in enger Abstimmung mit Standardisierungseinrichtungen, der Privatwirtschaft sowie sonstigen Beteiligten erfolgen.

Das NIST unterhält derzeit eine Cloud Computing Standards Roadmap (CCSRWG) Arbeitsgruppe sowie vier weitere Arbeitsgruppen zum Cloud Computing: Reference Architecture and Taxonomy Working Group (CCRATWG), Standards to Acceleration to Jumpstart the Adoption of Cloud Computing (SAJACC), Security Working Group (CCSWG) und Target Business Use Cases Working Group (CCBUCSWG).

Das NIST betreibt die Cloud Computing Collaboration Site<sup>65</sup> zur Online-Zusammenarbeit. Diese Seite umfasst auch ein Cloud Standards Inventory<sup>66</sup>.


<sup>64</sup> <http://www.itu.int/members/>

<sup>65</sup> <http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/WebHome>

Neben der Erarbeitung des SCAP<sup>67</sup> (siehe 5.1.11), fokussiert sich die NIST bisher auf die Erarbeitung von Definitionen, Orientierungswissen und Leitfäden im Cloud Computing: NIST Use Cases, NIST Definition of Cloud Computing (NIST SP 800-145), NIST Cloud Computing Reference Architecture (NIST SP 500-292) oder NIST Cloud Computing Synopsis and Recommendations (NIST-SP800-146). Im Juli 2011 erschien die erste Auflage der NIST Cloud Computing-Standardisierungsroadmap (NIST SP500-291).

Das NIST ermöglicht eine beschränkte Mitwirkung über Tools zur Online-Partizipation und koordiniert sich mit vergleichbaren Gremien.

### 4.3.7 Organization for the Advancement of Structured Information Standards (OASIS)

	Eckdaten	
	Gründungsjahr	1992
	Hauptsitz	Boston, USA
	Fokus	International / IKT
	Internet	<a href="http://www.oasis-open.org">www.oasis-open.org</a>

Die Organization for the Advancement of Structured Information Standards (OASIS) ist eine nicht gewinnorientierte Standardentwicklungsorganisation, die offene Standards für die Informationsgesellschaft (weiter-)entwickelt, harmonisiert und verbreitet. Standards von OASIS mit sehr großer Verbreitung sind beispielsweise XML- und Webservice-Standards. OASIS beschäftigt sich unter anderem mit folgenden weiteren Bereichen: Sicherheit, SOA, Smart Grid, elektronische Veröffentlichungen oder Notfallmanagement.

OASIS betrachtet Cloud Computing als eine natürliche Fortsetzung und Erweiterung von SOA- und Netzwerkmanagementmodellen. Viele OASIS Standards besitzen einen impliziten Bezug zum Cloud Computing:

- Sicherheit-, Zugangs- und Identitätsverfahrensstandards, z.B. OASIS SAML, XACML, SPML, WS-Security Policy oder WS-Trust.
- Standards für Inhalts-, Formatkontrolle und Datenimport / -export, z.B., OASIS ODF.
- Registrierungs-, Repository- und Verzeichnisstandards, z.B. OASIS ebXML und UDDI.
- SOA Methoden und Modelle, Netzwerkmanagement, Servicequalität und Interoperabilität, z.B. OASIS SOA-RM, and BPEL.
- Webservice-Standards, wie WS-Security, WS-I Web Services Profile, WS-Reliable Messaging und weitere.

<sup>66</sup> <http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/StandardsInventory>

<sup>67</sup> Security Content Automation Protocol (SCAP), <http://scap.nist.gov/>




OASIS hat zusätzlich das "Identity in the Cloud Technical Committee" (IDCloud) eingerichtet, das sich

- mit der Harmonisierung von Definition / Terminologien / Wortschatz zur Identität im Kontext von Cloud Computing,
- mit der Identifikation und Definition von Use Cases und Profilen und
- mit der Identifikation von Lücken in existierenden Identitätsmanagementstandards für die Cloud

beschäftigt. Kürzlich wurde das technische Komitee OASIS Topology and Orchestration Specification for Cloud Applications (TOSCA) eingerichtet.

OASIS staffelt seinen Mitgliederstatus nach "Foundational Sponsor", "Sponsor" und "Contributor". Alle drei Stufen besitzen allerdings die wichtigsten Mitwirkungsrechte<sup>68</sup>, wie Teilnahme an Arbeitsgruppen, Abstimmung zu Standards oder Einrichtung neuer Arbeitsgruppen. Die Abstufung unterscheidet sich im Wesentlichen hinsichtlich Öffentlichkeitsarbeit und Marketing. Die jährlichen Mitgliedsgebühren unterscheiden sich für Unternehmen (Contributor: 3.000-8.000 USD), Forschungseinrichtungen (Contributer: 1.100 USD) und öffentliche Einrichtungen (1.100 USD).

#### 4.3.8 Open Cloud Consortium (OCC)

	Eckdaten	
	Gründungsjahr	Keine Angabe
	Hauptsitz	Illinois, USA
	Fokus	International / Cloud Comp.
	Internet	<a href="http://www.opencloudconsortium.org">www.opencloudconsortium.org</a>

Das Open Cloud Consortium (OCC) ist ein gemeinnütziger Zusammenschluss von 9 Unternehmen, 5 Universitäten, 4 öffentlichen Einrichtungen. Es

- betreibt eine gemeinsame Cloud-Infrastruktur (z.B. Open Science Data Cloud) für Forschungszwecke,
- koordiniert und betreibt Cloud Computing-Testumgebungen (z.B. Open Cloud Testbed) und
- entwickelt Referenzimplementierung, Benchmarks und Standards (z.B. MalStone Benchmark).


Die Gremien der OCC umfassen

- die Open Science Data Cloud (OSDC) Arbeitsgruppe,
- das Projekt Matsu,
- das OCC Virtual Network Testbed und
- die Open Cloud Testbed Arbeitsgruppe.

<sup>68</sup> <http://www.oasis-open.org/join/benefits-matrix>

Alle Mitglieder, bis auf die AIST aus Japan, sind US-amerikanisch. Die Partizipationsmöglichkeiten für Unternehmen und Einrichtungen außerhalb der USA werden derzeit als faktisch gering eingeschätzt.

### 4.3.9 Open Grid Forum (OGF)


	Eckdaten	
	Gründungsjahr	2006
	Hauptsitz	Muncie (IN), USA
	Fokus	International / IKT
	Internet	<a href="http://www.ogf.org">www.ogf.org</a>

Das Open Grid Forum (OGF) ist eine Standardentwicklungsorganisation, die sich aus Anwendern, Anbietern und Entwicklern zusammensetzt. Die OGF legt ihren inhaltlichen Schwerpunkt auf die Bereiche Grid-Computing und weitere Formen verteilter Datenverarbeitung. Beide Bereiche haben einen starken Bezug zum Cloud Computing, weshalb das OGF Cloud Computing inzwischen ebenfalls als einen seiner Schwerpunktbereich betrachtet.

OGF unterhält die Open Cloud Computing Interface (OCCI) Working Group, die sich für die Erarbeitung des OCCI Standards (siehe 5.1.5) verantwortlich zeichnet. Ein Standard des OGF mit implizitem Bezug zum Cloud Computing ist beispielsweise GridFTP.

Der OGF Prozess zur Erarbeitung offener Standards lehnt sich eng an den Prozessen der IETF an. Der Mitgliedsstatus des OGF für Organisationen staffelt sich in Platinum, Gold, Silber und Projekt. Mitglieder aller Stufen besitzen das Recht Leiter für Arbeitsgruppen zu stellen. Die Stufen unterscheiden sich vor allem durch ihren Einfluss im Management Board und Marketingmöglichkeiten. Die jährlichen Mitgliedsgebühren erstrecken sich von 1.500 USD für eine Projektmitgliedschaft einer nicht-gewinnorientierten Organisation bis zu 30.000 USD für gewinnorientierte Platinum-Mitglieder.

### 4.3.10 The Open Group (TOG)

	Eckdaten	
	Gründungsjahr	1996
	Hauptsitz	Keine Angabe
	Fokus	International / IKT
	Internet	<a href="http://www.opengroup.org">www.opengroup.org</a>

The Open Group (TOG) ist eine Standardentwicklungsorganisation, die die Entwicklung offener und anbieterunabhängiger Standards und Zertifizierungen im IT-Bereich vorantreibt. Sie besitzt derzeit mehr als 300 Mitglieder. Am


bekanntesten ist die Organisation für ihre Zertifizierung von UNIX und die Veröffentlichung von UNIX-Spezifikationen.

Im Jericho Forum der TOG werden Standards entwickelt, die die Sicherheit bei einer Geschäftstätigkeit über weltweite offene Netzwerke erhöhen sollen.

Die Open Group Cloud Work Group<sup>69</sup> der TOG beschäftigt sich mit Standards, die es erlauben Cloud Computing-Technologien in bestehende Firmenarchitekturen zu integrieren, um deren Vorteile, wie Kostenreduktion, Skalierbarkeit oder Agilität, zu nutzen. In der Arbeitsgruppe sollen die Perspektiven der Anbieter und der Anwender bzw. von Firmen jeder Größe gleichermaßen berücksichtigt werden. Das wichtigste Ergebnis der Arbeitsgruppe ist bisher die „Cloud Computing Reference Architecture“ (CCRA, siehe 5.1.1), die im Februar 2011 veröffentlicht wurde.

Der Mitgliedsstatus der TOG staffelt sich in Platinum, Gold, Silber, wissenschaftliche und Konsortial-Mitglieder. Gold-Mitglieder haben Zugang zu allen Foren und Arbeitsgruppen, Silber-Mitglieder nur zu einem Forum, aber allen Arbeitsgruppen. Platinum-Mitglieder haben den größten Einfluss auf das Management Board. Jährliche Mitgliederbeiträge bewegen sich von 2.500 USD für die Silber-Mitgliedschaft für kleine IT-Firmen bis zu mehr als 40.000 USD für eine Platinum-Mitgliedschaft großer Firmen.

#### 4.3.11 Storage Networking Industry Association (SNIA)

	Eckdaten	
	Gründungsjahr	1997
	Hauptsitz	Keine Angabe (USA)
	Fokus	International / IKT
	Internet	<a href="http://www.snia.org">www.snia.org</a>

Die Storage Networking Industry Association (SNIA) ist eine nicht gewinnorientierte Handelsvereinigung<sup>70</sup>, deren Ziel die Verbesserung und Steigerung der Vertrauenswürdigkeit bisheriger Netzwerkspeichertechnologie und -anwendungen ist. Die SNIA konzentriert sich deshalb auf die Entwicklung und Unterstützung von Standards, Technologien und Fortbildung in diesem Bereich. Sie besitzt ungefähr 400 Unternehmen als Mitglieder.

Die SNIA treibt die „Cloud Storage Initiative“, die als wichtiges Ergebnis das „Cloud Data Management Interface“ (CDMI, siehe 5.1.1) erarbeitet hat.

Weitere Gremien mit implizitem Bezug zum Cloud Computing sind: Data Management Forum, the Green Storage Initiative, the Ethernet Storage Forum, Storage Management Initiative, Solid State Storage Initiative, the Storage Security Industry Forum und XAM Initiative.


<sup>69</sup> <http://www.opengroup.org/cloudcomputing/>

<sup>70</sup> Registriert unter 501(c)(6).

Aus diesen gehen die "Storage Management Initiative Specification" (SMI-S) und die "eXtensible Access Method" (XAM) als zwei wichtige Arbeitsergebnisse hervor.

Alle beitragspflichtigen Mitgliederstufen der SNIA besitzen die Rechte in Gremien mitzuarbeiten oder abzustimmen. Lediglich die Mitwirkung im Management Board ist den „Vendoren“ vorbehalten.

### 4.3.12 TM Forum (TM-F)

	Eckdaten	
	Gründungsjahr	1988
	Hauptsitz	Morristown, USA
	Fokus	International / IKT
	Internet	<a href="http://www.tmforum.org">www.tmforum.org</a>

Das TM Forum ist eine nicht gewinnorientierte Industrievereinigung der Medien- und IKT-Branche, deren Ziel die Informationsbereitstellung und Unterstützung ihrer Mitglieder bei der Bereitstellung profitabler Dienstleistungen ist. Ihre Aufgabenbereiche umfassen Branchenstudien, Benchmarks, Technologie-Roadmaps, Best Practice-Ratgeber, Softwarestandards/-schnittstellen sowie zertifizierte Weiterbildung, Konferenzen und Veröffentlichungen. Derzeit besitzt das TM Forum mehr als 700 Unternehmen in 75 Ländern als Mitglieder.


Ein Kernstück von TM Forums Arbeit ist Frameworkx, eine Sammlung von Standards und unterstützenden Diensten für den Geschäftsbetrieb.

TM Forum's "Cloud & New Services Initiative" erarbeitet Anpassungen von Frameworkx für das Cloud Computing und besitzt die Vision eines weltweit offenen Marktplatzes für Cloud-Dienste, der auf einheitlichen Standards basiert. Das TM Forum besitzt den strukturellen Vorteil, dass es viele Teilnehmer der Wertschöpfungskette (z.B. Firmenkunden, Cloud-Anbieter, Technologieunternehmen) vereint.

Kollaborationsprojekte der Initiative umfassen: Cloud Billing, Cloud SLA Management, Cloud Security & Risk, Cloud Frameworkx/QSP (Quick Start Packs), Cloud Business Process Framework, Service Provider Leadership Council (SPLC) Cloud Requirements, Software Enabled Services Management Solution, IPsphere und B2B Product Trading.

Das "Enterprise Cloud Leadership Council" ist nur für Unternehmen zugänglich, die bereits Mitglied sind und bereits ein hohes Ansehen innerhalb dem TM Forum besitzen. Eine Mitwirkung bei konkreten Kollaborationsprojekten gestaltet sich einfacher.

**4.3.13 World Wide Web Consortium (W3C)**

	Eckdaten	
	Gründungsjahr	1994
	Hauptsitz	Keine Angabe (USA)
	Fokus	International / IKT
	Internet	<a href="http://www.w3c.org">www.w3c.org</a>

Das World Wide Web Consortium (W3C) ist die wichtigste Standardentwicklungsorganisation für das Internet, deren Hauptaufgabe die Entwicklung von Protokollen und Richtlinien ist. Sie umfasst derzeit mehr als 300 Organisationen als Mitglieder und beschäftigt 60 Mitarbeiter.

W3C's weitläufig bekannte Standards, wie HTML, XML oder CSS, sind auch für das Cloud Computing relevant, da viele der Cloud-Lösungen auf der heutigen Netzwerk- und Internet-Technologie aufbauen. Weitere relevante Standard sind WSDL, XML Encryption, XML Digital Signature oder SOAP.

Besondere Relevanz besitzt das W3C Incubator<sup>71</sup> Gremium zu USDL (siehe 5.1.12). USDL könnte zukünftig als Grundlage für eine Beschreibungssprache für Cloud-Dienste dienen.

Die Device APIs Working Group<sup>72</sup> erarbeitet Client-seitige APIs, die die Entwicklung von Web-Anwendungen und Web-Widgets ermöglichen.

Bisher ist kein Cloud-spezifisches Gremium bei der W3C in Planung.

Das W3C ist bestrebt mögliche Standards unter Einbeziehung einer breiten Öffentlichkeit zu optimieren. Deshalb unterscheidet das W3C „Community und Business Group“ und „W3C Working Groups“. Die Mitarbeit in ersteren ist jedem möglich, die in letzteren nur Mitgliedern. Die W3C kennt nur eine Mitgliederstufe. Die Mitgliedschaft steht jeder Art von Organisation und Einzelperson offen. Mitglieder haben volle Mitwirkungs- und Stimmrechte in Gremien. Mitgliedsgebühren staffeln sich nach Umsatz, Art und Sitz der Organisation.

<sup>71</sup> <http://www.w3.org/2005/Incubator/usdl/>

<sup>72</sup> <http://www.w3.org/2009/dap/> bzw. <http://www.w3.org/2009/05/DeviceAPIC charter>

## 5 Relevante Standards im Cloud-Umfeld

Die Analyse des Standardisierungsumfeldes soll einen Überblick über existierende Standards im Cloud Computing schaffen und diese in den Kontext des Technologieprogramms Trusted Cloud einordnen. Darüber hinaus sollen offene Bereiche („White Spots“), in denen ein gestalterischer Beitrag zur Etablierung von Standards in Deutschland, aber auch darüber hinaus geleistet werden kann, identifiziert werden.

Entsprechend gliedert sich dieses Kapitel in eine Beschreibung ausgewählter Standards anhand eines Steckbriefs (siehe 5.1, 5.2 und 5.3) und der Beschreibung von Standardisierungslücken (siehe 5.4). Für eine detaillierte Beschreibung des methodischen Vorgehens wird auf Kapitel 3.3.2 verwiesen. Im Folgenden wird ein Überblick über die Ergebnisse gegeben.

### Übersicht über relevante Standards im Cloud-Umfeld

Anbieter, Anwender und Intermediäre von Cloud-Diensten sind in ihrer Geschäftstätigkeit einer Vielzahl von Standards ausgesetzt. Im Rahmen einer intensiven Recherche wurden ca. 160 Normen, Standards, Vorgaben, Zertifizierungen und Vorarbeiten erhoben (siehe Anhang A).<sup>73</sup> Um den Überblick allgemeingültig, übersichtlich und gleichzeitig möglichst umfassend und konkret zu gestalten, wird eine Auswahl von 20 prototypischen „Cloud-Standards“ getroffen, die mit weiteren 35 ähnlichen verglichen werden. Bei diesen Ergebnissen handelt es sich um eine Momentaufnahme von Anfang 2012, deren Aktualität durch die große aktuelle Dynamik begrenzt wird.

Folgende Übersicht zeigt die 20 ausgewählten relevanten Cloud-Standards.

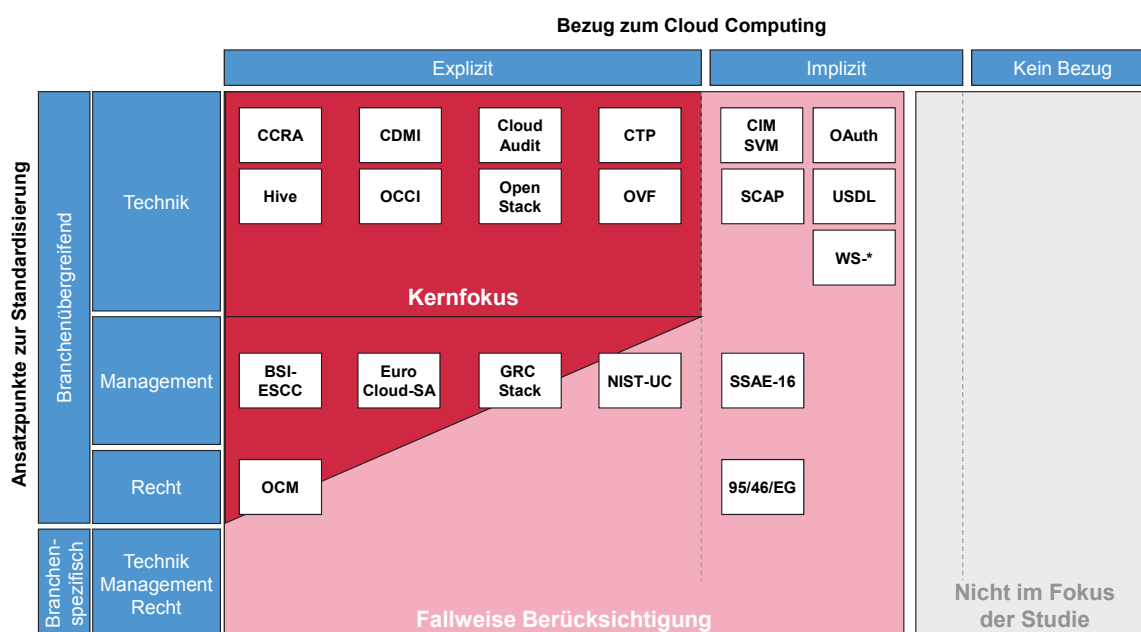


Abbildung 17: Übersicht der 20 ausgewählten „Cloud-Standards“<sup>74</sup>

<sup>73</sup> Siehe Begriffswelt „Standards“ in Kapitel 3.1.3.

<sup>74</sup> Analyse von Booz & Company und FZI.



Die 20 Cloud-Standards besitzen nach Möglichkeit Vorbildcharakter, decken die Bereiche Technik, Management und Recht ab (siehe Definition „Ansatzpunkte“ in 3.2.2) und finden größte Beachtung in Fachkreisen. Der Fokus der Betrachtung liegt auf branchenübergreifenden Standards, die einen expliziten Bezug zu Cloud Computing aufweisen. Fallweise Berücksichtigung erfahren Standards mit wichtigem implizitem Bezug zu Cloud Computing (z.B. Web Service Standards). Kein branchenspezifischer Standard besaß genug allgemeine Strahlkraft, um in die engere Auswahl zu gelangen. Die überwiegende Mehrheit der Standards hat internationale Relevanz. Einzelne weisen einen (leichten) europäischen bzw. deutschen Bezug auf (z.B. BSI-ESCC, USDL, NIST-UC, EuroCloud-SA, 95/46/EG).

Folgende Übersicht listet die 20 Cloud-Standards nach deren Abkürzung und weist weitere Basisinformationen wie deren vollständigen Namen, Kurzbeschreibung, inhaltlicher Fokus (Cloud Computing - CC, Informations- und Kommunikationstechnologie - IKT, Allgemein - Allg.), Formalisierung (siehe 3.1.3) und Initiator (siehe Anhang B) sowie ähnliche Standards aus.

**Tabelle 2:** Übersicht der 20 ausgewählten „Cloud-Standards“<sup>75</sup>

Fokus	Standards, Zertifizierungen, Vorgaben und Vorarbeiten	Ähnliche	Formalisierung	Initiator
Technik	<b>CC</b> <u>CCRA (Cloud Computing Reference Architecture)</u> : Referenzarchitektur für Cloud Service Angebote	Referenzarchitekturen der NIST oder des BSI	Spezifikation	TOG
	<b>CC</b> <u>CDMI (Cloud Data Management Interface)</u> : API zum Zugriff auf Daten in IaaS, DaaS Szenarios	XAM, iSCSI, NFS, WebDAV	Spezifikation	SNIA
	<b>CC</b> <u>Cloud Audit (Automated Audit, Assertion, Assessment, and Assurance API)</u> : API zum Zugriff auf Auditinformationen	SCAP	Spezifikation	CSA
	<b>CC</b> <u>CTP (Cloud Trust Protocol)</u> : Einheitliche Techniken und Nomenklatur zur Erhöhung der Transparenz	SCAP, OCRL	Orientierungswissen	CSA
	<b>CC</b> <u>OCCI (Open Cloud Computing Interface)</u> : API zum Management von Clouds (insb. IaaS)	DeltaCloud, Libcloud, APIs von EC2, Rackspace, Eucalyptus, vCloud u.w.	Industriestandard	OGF
	<b>CC</b> <u>OpenStack (OpenStack Cloud Software)</u> : Rahmenwerk zum Aufbau von Cloud-Infrastrukturen	OpenNebula, Nimbus (Schnittstellen: CMDI, OCCI, OVF)	Industriestandard	(Diverse)
	<b>IKT</b> <u>CIMSVM (CIM System Virtualization Model)</u> : Objektmodell und Schnittstellen für Virtuelle Systeme & Komponenten	- -	Spezifikation	DMTF
	<b>IKT</b> <u>Hive (Apache Hive)</u> : Programmiermodell für Datenabfragen	JAQL, PIG	Industriestandard	Apache
	<b>IKT</b> <u>OAuth (Web Authorization Protocol)</u> : Protokoll und Schnittstelle zum Identitätsmanagement	OpenID, WS-Federation, SAML	Standard	IETF
	<b>IKT</b> <u>OVF (Open Virtualization Format)</u> : Dateiformat für Virtuelle Maschinen	AMI, EMI	Offener Standard	DMTF, ANSI, ISO

<sup>75</sup> Analyse von Booz & Company und FZI.

Fokus		Standards, Zertifizierungen, Vorgaben und Vorarbeiten	Ähnliche	Formalisierung	Initiator
Technik	IKT	<b>SCAP (Security Content Automation Protocol):</b> Protokoll und Schnittstelle zum Abruf von Sicherheitsinformationen	CloudAudit	Industriestandard	NIST
	IKT	<b>USDL (Unified Service Description Language):</b> Beschreibungssprache für virtuelle Dienstleistungen	WSDL, UDDI, WADL, OWL-S, SNN, WSMO, e3Value, PAS1018 u.w.	Spezifikation	W3C
	IKT	<b>WS-* (Web Service Standards):</b> Spezifikationen, Standards und Normen für Web Services	WSDL, WS-Policy, WS-Agreement, WS-Security, WS-I u.w.	Standard	OASIS, OGF, W3C
Management	CC	<b>BSI-ESCC (Eckpunktepapier Sicherheitsempfehlungen für Cloud Computing Anbieter):</b> Leitfaden	Andere Anforderungsdokumente	Orientierungswissen	BSI
	CC	<b>EuroCloud-SA (EuroCloud Star Audit):</b> Zertifikat für Anbieter von Cloud-Diensten	EuroPriSe, TiC	Zertifizierung	EuroCloud
	CC	<b>GRC Stack (Governance, Risk Management and Compliance Stack):</b> Rahmenwerk zu Risikobewertung von Anbietern	CloudAudit, CCM, CAIQ, CTP	Orientierungswissen	CSA
	CC	<b>NIST-UC (Cloud Computing Use Cases):</b> Leitfaden für Anwendungsfälle im Cloud Computing mit Fokus auf US-Behörden	Use Cases von OGF oder DMTF	Orientierungswissen	NIST
	Allg.	<b>SSAE-16 (Statement on Standards for Attestation Engagements No. 16):</b> Zertifikat für Anbieter von Cloud-Diensten	CobiT, BSI-100, ISAE 3402, ITIL, SAS 70, IDW PS 330/951/FAIT1	Zertifizierung	AICPA
Recht	CC	<b>OCM (Open Cloud Manifesto):</b> Selbstverpflichtung zu Offenheit für Cloud-Anbieter	--	Industriestandard	(Diverse)
	Allg.	<b>95/46/EG (EU-Richtlinie 95/46/EG „Datenschutzrichtlinie“):</b> Datenschutzvorgaben der EU	Bundesdatenschutzgesetz, Datenschutzgesetze d. Länder, Safe Harbor	Rechtliche Vorgabe	EU

Die Cloud-Standards werden in dieser Reihenfolge in den folgenden Kapiteln untersucht, bewertet und mit den 35 ähnlichen Standards verglichen.

Folgende Matrix fasst das Ergebnis der Bewertung der 20 Cloud-Standards nach erwarteter Durchsetzungsfähigkeit und aktuellem Reifegrad zusammen.

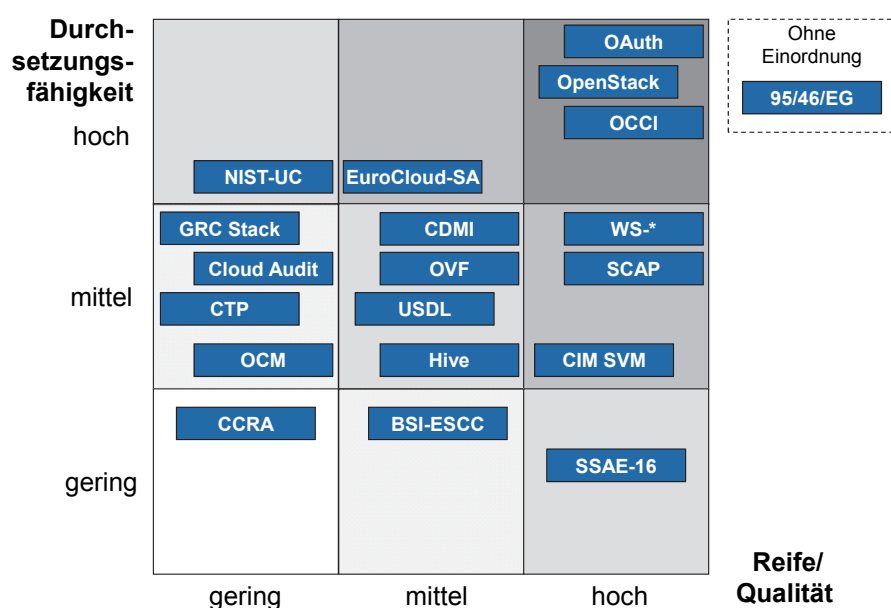


Abbildung 18: Übersicht der Bewertung der 20 „Cloud-Standards“

Die Bewertung basiert auf einer ersten sorgfältigen Prüfung durch Booz & Company und das FZI, die aber keinen abschließenden Anspruch auf Korrektheit besitzt, sondern vielmehr im Fortgang kontinuierlich erneuert werden muss. Standards, die bereits heute hohe Verbreitung und Reife besitzen, sollten effektiv genutzt werden („Use!“). Solche, die eine geringe Verbreitung genießen, sollten beworben werden („Promote!“) und bei solchen, die sich erst in der Entwicklung befinden, sollte mitgewirkt werden („Contribute!“).

Aus den vorgenommenen Analysen, lassen sich bereits erste Erkenntnisse zur aktuellen Standardisierungssituation im Cloud Computing ableiten:

- Der Mehrheit der Cloud-Standards lässt sich dem technischen Bereich zuordnen. Management- und dedizierte rechtliche Standards lassen sich weit weniger finden.
- Die Mehrzahl der Standardisierungsaktivitäten fokussieren die Herausforderungen Effizienz, Interoperabilität und Portabilität.
- Im Bereich des Managements sind derzeit fast ausschließlich Leitfäden oder ähnliche Standarddokumente anzutreffen. Cloud-Standards für Geschäftsmodelle, Dienstgütevereinbarungen, Managementmodelle oder -prozesse sowie Controlling existieren nicht.
- Viele existierende Standards, die nur einen impliziten Bezug zum Cloud Computing besitzen, besitzen einen höheren Reifegrad, müssen aber ggf. erst noch an das Cloud Computing angepasst werden.
- Die Durchsetzungsfähigkeit von Cloud-Standards, die mit explizitem Bezug zum Cloud Computing erarbeitet werden, wird tendenziell höher eingestuft als bei solchen mit implizitem Bezug.

### *Lücken bei Standards im Cloud-Umfeld*

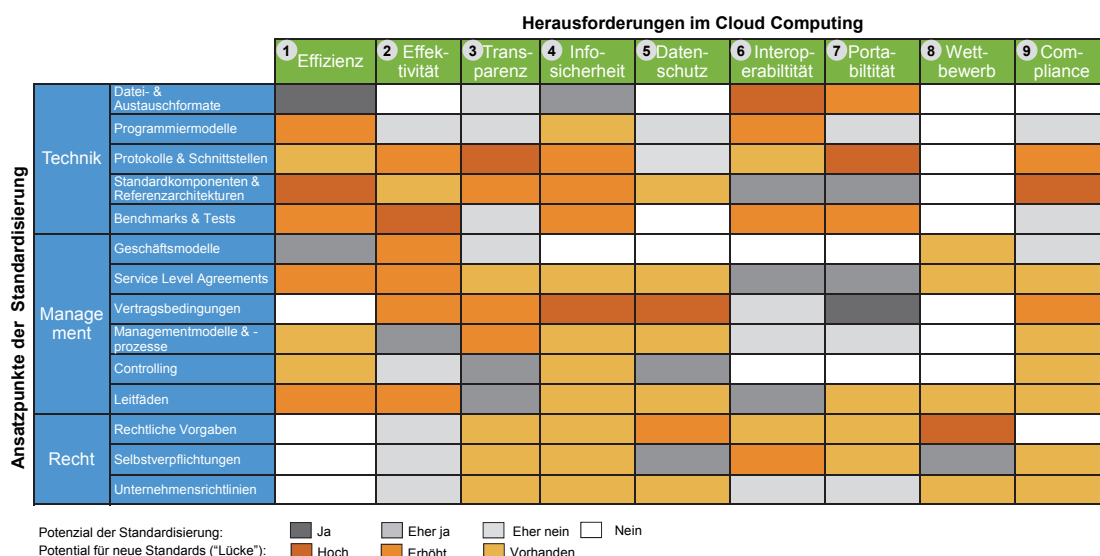
Die übergreifende Bewertung des Portfolios von Cloud-Standards sowie die damit verbundene Identifikation von Standardisierungslücken erlauben die ganzheitliche Betrachtung des Normierungs- und Standardisierungsumfeldes. Gleichzeitig wird hierdurch ein wichtiger Grundstein für die Ableitung von Handlungsempfehlungen gelegt. Eine detaillierte Beschreibung des methodischen Vorgehens bei der Identifikation von Standardisierungslücken findet sich in Kapitel 3.3.2.

Unter Lücken werden solche Ansatzpunkte der Standardisierung verstanden, deren inhaltliche Reife und/oder Breite bislang nicht in ausreichendem Maße bearbeitet wurde, um die Herausforderungen im Cloud Computing zu adressieren.<sup>76</sup> Die Ursachen hierfür können vielfältiger Natur sein. So ist in einigen Bereichen (bspw. Interoperabilität, Portabilität) festzustellen, dass die Nachfrage nach Standards und damit der Druck auf Cloud-Anbieter noch zu gering sind. In anderen Bereiche, z. B. PaaS-Lösungen, sind das Begriffsbild und vor allem die technischen Konzepte noch so wenig entwickelt, dass sinnvolle Ansatzpunkte für Standards nur schwer zu erkennen sind.

---

<sup>76</sup> Siehe hierzu auch die Ausführungen in Kapitel 3.3.2.

Die folgende Übersicht illustriert dieses Gesamtergebnis der Lückenanalyse im Normungs- und Standardisierungsumfeld von Cloud Computing.



**Abbildung 19:** Überblick der Standardisierungslücken im Cloud Computing<sup>77</sup>

Die folgende Abbildung zeigt im Vergleich, wie sich die 20 ausgewählten Cloud-Standards im Normungs- und Standardisierungsumfeld einordnen.

**Herausforderungen im Cloud Computing**

		1 Effizienz	2 Effektivität	3 Transparenz	4 Info-sicherheit	5 Daten-schutz	6 Interop-erabilität	7 Porta-bilität	8 Wett-bewerb	9 Com-pliance
Technik	Datei- & Austauschformate	CIMSVM, OVF, USDL, WS-*		USDL, WS-*	SCAP, WS-*		CIMSVM, OVF, SCAP, USDL, WS-*	CIMSVM, OVF, USDL		
	Programmiersprachen	Hive					Hive	Hive		
	Protokolle & Schnittstellen	CDMI, CIMSVM, CTP, OCCL, OpenStack, WS-*	CDMI, CTP, OCCL, OpenStack	CloudAudit, CTP, WS-*	CTP, OAuth, SCAP, WS-*		CDMI, CIMSVM, OCCL, OpenStack, SCAP, WS-*	CIMSVM, OCCL, OpenStack		CloudAudit
	Standardkomponenten & Referenzarchitekturen	CDMI, CIMSVM, CTP, CCRA, OpenStack	CDMI, CTP, CCRA, OpenStack	CTP, CCRA	CTP, CCRA, BSI-ESCC	BSI-ESCC	CDMI, CIMSVM, OpenStack	CIMSVM, OpenStack		
	Benchmarks & Tests									
Management	Geschäftsmodelle	USDL		USDL			USDL	USDL		
	Service Level Agreements	USDL		USDL			USDL	USDL		
	Vertragsbedingungen	USDL		USDL			USDL	USDL		
	Managementmodelle & -prozesse	GRC	GRC		GRC, SSAE-16					GRC
	Controlling				SSAE-16					
Recht	Leitfäden	CTP, EuroCloud-SA, GRC	CTP, EuroCloud-SA, GRC, NIST-UC	CTP, EuroCloud-SA, NIST-UC	CTP, BSI-ESCC, EuroCloud-SA, GRC, NIST-UC	BSI-ESCC, EuroCloud-SA, NIST-UC	NIST-UC	EuroCloud-SA		EuroCloud-SA, GRC
	Rechtliche Vorgaben					95/46/EG				
	Selbstverpflichtungen			OCM	OCM		OCM	OCM	OCM	
	Unternehmensrichtlinien									

**Abbildung 20:** Einordnung der 20 Cloud-Standards im Normungs- und Standardisierungsumfeld<sup>78</sup>

Zusammenfassend lassen sich folgende, augenscheinliche Lücken in der Standardisierung hervorheben:

- Standardkomponenten & Referenzarchitekturen zur ganzheitlichen Leistungsüberwachung der Cloud-Dienste, Infrastrukturen und Ressourcen.
- Benchmarks & Tests zur Überprüfung und Dokumentation der Effektivität der Dienstenutzung.

<sup>77</sup> Analyse von Booz & Company und FZI.

<sup>78</sup> Analyse von Booz & Company und FZI.

- Protokolle & Schnittstellen zur Sicherstellung von Transparenz durch automatisierten Informationsaustausch.
- Standardisierte Vertragsbedingungen zur Gewährleistung der Informationssicherheit und Sicherstellung des Datenschutzes speziell auch für kleine und mittlere Unternehmen.
- Umfassende Protokolle & Schnittstellen zur Unterstützung von Interoperabilität von Cloud-Diensten.
- Standardisierte Protokolle & Schnittstellen zum Austausch von Daten und Diensten im Sinne der Portabilität.
- Rechtliche Vorgaben zur Sicherstellung des funktionierenden Cloud Wettbewerbs.
- Standardkomponenten & Referenzarchitekturen zum Management von Compliance.

## 5.1 Steckbriefe aus dem Bereich „Technik“

### 5.1.1 Cloud Computing Reference Architecture (CCRA)

BASIS- INFORMATION	Status	Entwurf
	Formalisierung	Orientierungswissen
	Bezug zu CC	Explizit
	Initiator	The Open Group
	Beteiligte	IBM
	Link	<a href="http://www.opengroup.org/cloudcomputing/">http://www.opengroup.org/cloudcomputing/</a>
TAXONOMIE	Ansatzpunkte	▪ T – Standardkomponenten & Referenzarchitekturen
	Herausforderungen	▪ Effizienz ▪ Effektivität ▪ Transparenz ▪ Informationssicherheit
GELTUNGS- BEREICH	Service-Modell	Alle
	Nutzergruppe	Anbieter
	Branche	Übergreifend
	Deployment	Alle
	Geographie	Global
	Unternehmensgröße	Alle
BEWERTUNG	Reifegrad	Gering
	Durchsetzungsfähigkeit	Gering
	Partizipationsmöglichkeit	Mittel
ÄHNLICHE STANDARDS		NIST RA, BSI RA

**Kurz-Charakterisierung:** Referenzarchitekturen stellen Modellentwürfe zur standardisierten und methodisch einheitlichen Beschreibung eines anzustrebenden Sollzustands für einen ausgewählten Problembereich dar. Das von der IBM erarbeitete und seit Februar 2011 bei The Open Group (TOG) zur Standardisierung eingereichte Cloud Computing Reference Model (CCRA) beschreibt auf Grundlage von Best Practices, wie Anforderungen im Cloud Computing durch Architekturentscheidungen umgesetzt werden können. Hierdurch soll insbesondere sichergestellt werden, dass die dem Cloud Computing zugeschriebenen Vorteile (bspw. Skalierbarkeit oder Ressourceneffizienz) von allen Beteiligten realisiert werden können.

Die CCRA basiert auf der durch TOG standardisierten Referenzarchitektur für Service-orientierte Architekturen (SOA RA).<sup>79</sup> So ist das CCRA kompatibel mit dem im SOA RA vorgestellten Schichtenmodell.<sup>80</sup> Auch die in SOA RA durch ein Schalenmodell vorgenommene Unterscheidung von Integrations-, Qualitäts-, Informations- und Governance-Aspekten wird in CCRA übernommen. Hier wird durch Ergänzung einer Schale zur Verwaltung der Sicherheit, Elastizität, Leistungsfähigkeit und Konsumentenfreundlichkeit (engl.: consumability) auf die spezifischen Anforderungen des Cloud Computing eingegangen.

Zur Strukturierung der CCRA werden die Komponenten anhand von drei Cloud-Akteuren unterschieden:

- *Cloud Service Consumer* (hier: Unternehmen, Personen oder IT-Systeme), die Cloud-Dienste nutzen.
- *Cloud Service Provider*, die Cloud-Dienste betreiben.
- *Cloud Service Creator*, die Cloud-Dienste gestalten, implementieren und weiterentwickeln.

Der Fokus der CCRA liegt in der Identifikation von Komponenten, die von Cloud Service Providern zur Verfügung gestellt werden müssen. Diese unterteilen sich in Cloud-Infrastrukturen, Cloud-Dienste und eine sogenannte Common Cloud Management Plattform (CCMP) zum Management von Cloud-Diensten:

- **Cloud-Infrastruktur:** Als Cloud-Infrastruktur werden die für den Betrieb von Cloud-Diensten benötigten Rechen-, Speicher- und Netzwerk-Ressourcen zusammengefasst. Zusätzlich finden auch sonstige Anlagen (wie bspw. Racks, Räume, Gebäude) Berücksichtigung.
- **Cloud-Dienste:** Neben den Cloud-typischen Diensten auf Infrastruktur-, Plattform- und Software-Ebene sieht das CCRA auch den Betrieb von Geschäftsprozessen nach dem „as-a-Service“-Prinzip vor. Zusätzlich finden Cloud-Dienste, die durch ein Ökosystem von unabhängigen Cloud-Anbietern bereitgestellt werden können Berücksichtigung.
- **Common Cloud Management Plattform (CCMP):** Die Unterstützung von bspw. Service oder Business Managern stellt die Kernaufgabe der CCMP dar. Hierzu werden die vorgeschlagenen Komponenten in „Operational Support Services (OSS)“ und „Business Support Services (BSS)“ unterschieden. Über je eine Schnittstelle für Cloud Service Consumers, Cloud Service Creators und Cloud Service Providers können Akteur-spezifische Ausschnitte aus der beschriebenen Gesamtfunktionalität gebildet werden.

---

<sup>79</sup> Vgl. TOG, SOA RA (<http://www.opengroup.org/projects/soa-ref-arch/>).

<sup>80</sup> Dieses beginnt auf Hardwareebene mit der Beschreibung von „operativen Systemen“ (engl.: operational systems). Darauf aufbauend können Dienstkomponenten (engl.: service components), Dienste (engl.: services), Geschäftsprozesse (engl.: business processes) und Konsumentenschnittstellen (engl.: consumer interfaces) beschrieben werden.



**Bewertung:** Die von der IBM erarbeitete CCRA zeichnet sich durch ihre inhaltliche Breite aus. Gleichzeitig kann die Entwurfsversion jedoch nur eine geringe Detailtiefe aufweisen. Die vorgenommenen Beschreibungen von Referenzkomponenten bleiben oft auf Stichwortniveau. Eine Diskussion von Architekturentscheidungen findet kaum statt. Die Reife von CCRA wird dementsprechend als gering eingestuft. Das Potenzial von CCRA sich zum künftigen Standard zu entwickeln, hängt eng mit dem generellen Bedarf für eine Referenzarchitektur – über die Notwendigkeit zur Schaffung einer gemeinsamen Begriffswelt hinaus – zusammen. Darüber hinaus ist zu beachten, dass eine Reihe konkurrierender Vorschläge (siehe „Ähnliche Standards“) existiert. Unter Berücksichtigung dieser Punkte, geht die Studie von einer eher geringen Durchsetzungsfähigkeit von CCRA aus. Die Möglichkeit zur Partizipation bei der Weiterentwicklung von CCRA ist im Rahmen der durch TOG moderierten Arbeitsgruppen möglich. Dies setzt jedoch eine Mitgliedschaft bei TOG voraus. Das Niveau der Partizipation ist als „mittel“ einzustufen.

**Ähnliche Standards:** Alle untersuchten Referenzarchitekturen weisen ähnliche Strukturen und ähnliche Umfänge auf. Die Unterschiede lassen sich folglich nur in Details, die durch die jeweiligen Blickwinkel beeinflusst sind, ausmachen. So unterscheidet sich die vom NIST vorgestellte Referenzarchitektur (NIST-RA) in der Berücksichtigung weiterer Cloud-Akteure. Es werden bspw. Komponenten zur Unterstützung eines Cloud-Auditors, Cloud-Brokers und Cloud-Carriers gefordert. Eine Rolle zur Berücksichtigung von Erstellern von Cloud-Diensten existiert nicht. Auch NIST-RA befindet sich noch auf einem geringen Reifenniveau. Es bleibt abzuwarten, ob NIST-RA und CCRA künftig inhaltlich weiter konvergieren werden.

Das BSI schlägt in seinem Eckpunktepapier zur Sicherheit im Cloud Computing (BSI-ESCC) ebenfalls eine Referenzarchitektur für Cloud Computing vor (BSI-RA). Diese hat die CCRA und NIST-RA zum Vorbild und verweist zur tiefergehenden Ausgestaltung der BSI-RA auf eben diese. Die potenzielle Durchsetzungsfähigkeit einer deutschen Referenzarchitektur wird als eher gering bewertet.

## 5.1.2 Cloud Data Management Interface (CDMI)

<b>BASIS- INFORMATION</b>	<b>Status</b>	Veröffentlicht
	<b>Formalisierung</b>	Industriestandard
	<b>Bezug zu CC</b>	Explizit
	<b>Initiator</b>	SNIA CSI
	<b>Beteiligte</b>	> 100
	<b>Link</b>	<a href="http://www.snia.org/cdmi/">http://www.snia.org/cdmi/</a>
<b>TAXONOMIE</b>	<b>Ansatzpunkte</b>	<ul style="list-style-type: none"> <li>▪ T – Protokolle und Schnittstellen</li> <li>▪ T – Standardkomponenten &amp; Referenzarchitekturen</li> </ul>
	<b>Herausforderungen</b>	<ul style="list-style-type: none"> <li>▪ Effizienz</li> <li>▪ Effektivität</li> <li>▪ Interoperabilität</li> </ul>
<b>GELTUNGS- BEREICH</b>	<b>Service-Modell</b>	IaaS
	<b>Nutzergruppe</b>	Anbieter, Nutzer
	<b>Branche</b>	Übergreifend
	<b>Deployment</b>	Alle
	<b>Geographie</b>	Global
	<b>Unternehmensgröße</b>	Alle
<b>BEWERTUNG</b>	<b>Reifegrad</b>	Mittel
	<b>Durchsetzungsfähigkeit</b>	Mittel bis hoch
	<b>Partizipationsmöglichkeit</b>	Mittel
<b>ÄHNLICHE STANDARDS</b>		XAM, iSCSI, NFS, WebDAV

**Kurz-Charakterisierung:** Das von der Storage Network Industry Association (SNIA) vorgestellte Cloud Data Management Interface (CDMI) beschreibt eine standardisierte Funktions- und Management-Schnittstelle für Cloud Storage Dienste. Nutzer von Cloud Storage Diensten sollen damit in die Lage versetzt werden, gleichzeitig von unterschiedlichen Anbietern Cloud-Dienste einsetzen und steuern zu können (Cloud Föderation). Über die Vorgabe einer Referenzarchitektur für Cloud Storage Dienste trägt der Standard zudem zur Sicherstellung eines effizienten Ressourcenmanagements auf Seite der Cloud Anbieter bei.

Im Rahmen der vorgenommenen Standardisierung wurden existierende Cloud Storage Angebote analysiert und deren Schnittstellen konsolidiert. Die im Frühjahr 2011 als Arbeitsentwurf der SNIA veröffentlichte Standardversion basiert schlägt vor Daten in Container zu abstrahieren. Die Strukturierung und Administration der Daten erfolgt dann unter Verwendung der Container. So können bspw. Zugriffsberechtigungen über Domänen-Container („domain container“) verwaltet werden. Erweiterte Funktionalitäten, wie das Bereitstellen von Informationen bzgl. des Funktionsumfangs einzelner Cloud Storage Angebote, werden ebenfalls in Containern („capability container“) abgebildet. Zur Stapelverarbeitung von Daten sieht der Standard sogenannte „queue container“ vor.

Im Standard werden Interaktionen grundsätzlich in Datenzugriffe („data path“) und Managementzugriffe („control path“) unterschieden. Über die HTTP-Methoden GET, PUT und DELETE wird der vollständige Lebenszyklus der Daten abgebildet. Zugriffe auf die Management-Schnittstelle werden ebenfalls über HTTP realisiert und ermöglicht bspw. das Anfragen der Systemfähigkeiten („capabilities“) über einen Verzeichnisdienst, wie auch die Definition und das Verwalten von Zugriffsbeschränkungen („ACL“) auf Container-Ebene. Zur Verschlüsselung des Datenaustauschs wird bisher ausschließlich TLS über HTTP vorgesehen. Weitere Ausbaustufen des Standards sehen

die Einbeziehung von ergänzenden Funktionen wie etwa Rechnungsverwaltung, Monitoring oder Versionierung vor. Darüber hinaus soll es in Zukunft möglich sein, über einen zu definierenden Erweiterungsmechanismus den Standard für die eigenen Anforderungen zu ergänzen.

**Bewertung:** Die Dokumente zur Spezifikation des CDMI-Standards liegen bisher in Form von Arbeitsversionen vor. Diese weisen jedoch bereits eine hohe Formalisierung auf. Auf dieser Grundlage wird der Standardisierung von CDMI aktuell ein mittlerer Reifegrad zugeordnet. Die Durchsetzungsfähigkeit des Standards kann als mittel bis hoch eingestuft werden. Dies liegt in den bereits vorhandenen Referenzimplementierungen durch NIST SAJACC und andere Anbieter begründet. Zudem kann erwartet werden, dass mit der SNIA, als standardtreibende Organisation und Industrievereinigung der Speichernetzwerkhersteller, ein Multiplikator existiert, um die Verbreitung und damit die Durchsetzungsfähigkeit des Standards zu treiben. Die Möglichkeiten der Partizipation im Standardentwicklungsprozess auf mittlerem Niveau eingestuft. Die aktive Beteiligung an der Weiterentwicklung von CDMI setzt eine kostenpflichtige SNIA-Mitgliedschaft voraus und ist auf Mitglieder der Cloud Storage Initiative (CSI) beschränkt. Das Beitragen von allgemeinen Kommentaren zu veröffentlichten Dokumenten ist auch nicht assoziierten Interessenten möglich. Hierfür muss das SNIA „Feedback Contribution Agreement“ akzeptiert werden, dass unter anderem die Abtretung aller Rechte an eingebrachten Kommentaren an die SNIA vorsieht.

**Ähnliche Standards:** Es existieren zahlreiche, standardisierte Protokolle für entfernte Zugriffe auf Daten und Dateisysteme über Netzwerke, darunter sind iSCSI, NFS und WebDAV auf Grund ihrer Marktrelevanz hervorzuheben. Diese erreichen jedoch insb. im Bereich des Datenmanagements nicht den Funktionsumfang der vorgestellten CDMI Schnittstellen. Auf Grund der nativen Unterstützung vieler Betriebssysteme können Sie jedoch in bestimmten Anwendungskontexten eine Alternative für entfernte Datenzugriffe darstellen. Ebenfalls von der SNIA entwickelt, stellt die eXtensible Access Method (XAM) eine Alternative für Einsatzzwecke, in denen über Netzwerke auf Dateisysteme zugegriffen werden soll. XAM befindet sich derzeit im Standardisierungsprozess durch die ANSI.

### 5.1.3 Automated Audit, Assertion, Assessment, and Assurance API (Cloud Audit)

BASIS- INFORMATION	Status	Veröffentlicht
	Formalisierung	Spezifikation
	Bezug zu CC	Explizit
	Initiator	CSA
	Beteiligte	> 100
	Link	<a href="http://cloudaudit.org/">http://cloudaudit.org/</a>
TAXONOMIE	Ansatzpunkte	▪ T – Protokolle und Schnittstellen
	Herausforderungen	▪ Transparenz ▪ Compliance
GELTUNGS- BEREICH	Service-Modell	Alle
	Nutzergruppe	Alle
	Branche	Übergreifend
	Deployment	Public
	Geographie	Global
	Unternehmensgröße	Alle
BEWERTUNG	Reifegrad	Gering
	Durchsetzungsfähigkeit	Mittel
	Partizipationsmöglichkeit	Sehr hoch
ÄHNLICHE STANDARDS		SCAP

**Kurz-Charakterisierung:** Automated Audit, Assertion, Assessment, and Assurance API (A6) – nun CloudAudit genannt – soll Anbietern von Cloud-Diensten ermöglichen, Betriebs-, Sicherheits-, Audit- und Vertraulichkeitsinformationen standardisiert bereitzustellen. Nutzer von Cloud-Diensten sowie Intermediäre sollen durch CloudAudit den Abruf dieser Informationen automatisieren können. Dabei sollen auch Korrektheitsprüfungen anhand von Signaturen unterstützt werden.

Die aktuell veröffentlichte erste Version der Spezifikation beschreibt eine Schnittstelle zur Bereitstellung der Daten sowie Namenskonventionen, die den Abruf der Daten über HTTP ermöglichen. Sie wurde durch die Networking Group der IETF im Juli 2010 veröffentlicht.<sup>81</sup> CloudAudit unterstützt demnach den Zugriff auf strukturiert und unstrukturiert vorliegende Auditdaten. Damit Anbieter von Cloud-Diensten ihre Informationen Standardkonform bereitstellen, müssen Informationen entsprechend den definierten Verzeichnis- und Namensstrukturen abgelegt und über einen Webserver veröffentlicht werden. Aktuelle Begleitdokumente zum Standard definieren Namenskonventionen für Zertifikate und Informationen zu bspw. COBIT, HIPAA, ISO 27002, NIST SP800-53 und PCI DSS.

Künftige Versionen des Standards sollen die aktuelle Schnittstellenspezifikation um weitergehende Interaktionsmöglichkeiten erweitern. So sollen gezielte Nachfragen nach bestimmten Zertifikaten oder Benachrichtigungsfunktionen für Nutzer bei der Veröffentlichung von neuen oder aktualisierten Zertifikaten unterstützt werden. Darüber hinaus soll der Standard künftig Rahmenwerke für automatisierte Compliance-Prüfungen vorgeben.

<sup>81</sup> Die Dokumentstatus laut IETF Klassifikation lautet „Internet-Draft“.

CloudAudit beinhaltet bisher keine Vorgaben in Bezug auf Zugriffskontrollen, ID- und Rechtemanagement oder Verschlüsselung. Der Standard folgt diesbezüglich der Annahme, dass Nutzer wie Intermediäre in einem vorgelagerten Schritt bereits für den Zugriff authentisiert und autorisiert wurden. Die Weiterentwicklung und Verwaltung von CloudAudit (A6) wird durch die Cloud Security Alliance (CSA) getrieben.

**Bewertung:** Der Standard wird in den Bereich der Standards mit geringem Reifegrad klassifiziert. Dies liegt vor allem darin begründet, dass die aktuelle Spezifikation nur einen sehr eingeschränkten Funktionsumfang beschreibt. Der Standard unterstützt zudem die Verwendung unstrukturierter Datentypen also bspw. auch das Ablegen von Zertifikaten in Bild oder Textformaten. Hierdurch wird die angestrebte automatische Analyse der Auditinformationen erschwert. Eine Lösung für diese Herausforderung ist derzeit nicht im Standard enthalten. Die Durchsetzungsfähigkeit wird auf mittlerem Niveau eingestuft, da der Standard auf Grund der beabsichtigten Einfachheit ohne großen Aufwand zu implementieren ist. Zudem werden die Aktivitäten zur Entwicklung von CloudAudit seit Oktober 2010 zentral von der Cloud Security Alliance (CSA) koordiniert. Die gleichzeitige Eingliederung von CloudAudit in das von der CSA unterstützte Rahmenwerk zur Unterstützung von Governance, Risikomanagement und Compliance (GRC-Stack) trägt zudem zu guten Verbreitungschancen des Standards bei. Die Einreichung einer Standardspezifikation bei der IETF ist angedacht. Die inhaltliche Mitarbeit an CloudAudit (A6) ist nicht an eine CSA-Mitgliedschaft gebunden und steht allen Interessierten frei. Die Partizipationsmöglichkeit wird als „sehr hoch“ eingestuft.

**Ähnliche Standards:** Für den spezielleren Bereich der Bereitstellung von Informationen über das generelle Sicherheitsniveau sowie aktuelle Informationen zum Sicherheitsstatus von IT-Systemen kann das von der NIST entworfene Security Content Automation Protocol (SCAP) eine Alternative darstellen (vgl. Kapitel 5.1.11).

### 5.1.4 Cloud Trust Protocol (CTP)

BASIS- INFORMATION	Status	Entwurf
	Formalisierung	Orientierungswissen
	Bezug zu CC	Explizit
	Initiator	CSA
	Beteiligte	CSC
	Link	<a href="https://cloudsecurityalliance.org/research/initiatives/cloud-trust-protocol/">https://cloudsecurityalliance.org/research/initiatives/cloud-trust-protocol/</a>
TAXONOMIE	Ansatzpunkte	<ul style="list-style-type: none"> <li>▪ T – Protokolle und Schnittstellen</li> <li>▪ T – Standardkomponenten und Referenzarchitekturen</li> <li>▪ M – Leitfäden</li> </ul>
	Herausforderungen	<ul style="list-style-type: none"> <li>▪ Effizienz</li> <li>▪ Effektivität</li> <li>▪ Transparenz</li> <li>▪ Informationssicherheit</li> </ul>
GELTUNGS- BEREICH	Service-Modell	Alle
	Nutzergruppe	Alle
	Branche	Übergreifend
	Deployment	Public
	Geographie	Global
	Unternehmensgröße	Alle
BEWERTUNG	Reifegrad	Gering
	Durchsetzungsfähigkeit	Mittel
	Partizipationsmöglichkeit	Gering
ÄHNLICHE STANDARDS		SCAP, OCRL

**Kurz-Charakterisierung:** Durch den Einsatz des Cloud Trust Protocol (CTP) sollen Nutzer von Cloud-Diensten dazu ermächtigt werden, auf einem angemessenen Informationsstand wohl informierte Entscheidungen über die Auswahl und den Einsatz benötigter Cloud-Dienste zu treffen.

Das ursprünglich unter Federführung des IT-Dienstleisters CSC (Computer Sciences Corporation) entwickelte CTP folgt hierzu der Grundphilosophie, dass digitales Vertrauen nur über Transparenz erreicht werden kann.<sup>82</sup> Diese bisher veröffentlichten Arbeitsdokumente der Initiative zur Entwicklung des CTP fokussieren auf die Darstellung von standardisierten Softwarekomponenten sowie technischen Designvorgaben und Referenzarchitekturen zur Herstellung von Transparenz.

Die Konzeption von CTP baut auf 24 Kernbausteinen (EOT, engl. „elements of transparency“) auf. Dienst-Anwender sollen für jedes EOT individuelle Informationen abrufen können. Es gibt u. a. EOT für Audit-Protokolle, Schwachstellen- (engl. „vulnerability“) und Fehlerberichte (engl. „incident“) sowie Informationen zur Separierung von Daten (engl. „data separation affirmation“). In Summe sollen so alle notwendigen Informationen über die aktuelle Sicherheitskonfiguration sowie operative Eigenschaften von Cloud-basierten Informationssystemen beurkundet und dadurch letztlich Vertrauen in Cloud Computing geschaffen werden. CTP verzichtet auf die Definition eines grundlegenden Datenmodell zur Beschreibung der eingesetzten Infrastrukturkomponenten (engl. „Assets“) und Konfigurationen.<sup>83</sup> Das verwendete

<sup>82</sup> Vgl. Knode & Egan (2010), Digital Trust in the Cloud: Into the Cloud with CTP – A Precise for the Cloud Trust Protocol.

<sup>83</sup> Im Unterschied zu Ansätzen wie bspw. CIM SVM (vgl. hierzu Kapitel 5.1.7).



te Infrastrukturmodell soll ad-hoc und vom gemeinsamen Bild der Infrastruktur von Anbieter und Nutzer bestimmt sein.<sup>84</sup>

CTP ist heute Bestandteil des von CSA entwickelten Governance, Risk Management und Compliance (GRC) Rahmenwerks. Die Weiterentwicklung und Verwaltung wird durch die CSA getrieben.

**Bewertung:** Der Reifegrad von CTP muss als gering klassifiziert werden. Es existiert derzeit keine offizielle Arbeitsversion einer Standardspezifikation. Bisherige Veröffentlichungen sind häufig nur in der Form von Präsentationsunterlagen vorzufinden. Entsprechend schwierig ist die Einschätzung der Durchsetzungsfähigkeit des potentiellen Standards. Diese wird noch als mittel eingestuft. Begründet ist dies in der einerseits vielversprechenden und umfangreichen Ausrichtung des Konzepts. Gleichzeitig trägt die Eingliederung von CTP in das von der CSA unterstützte Rahmenwerk Governance, Risikomanagement und Compliance („GRC-Stack“) zur Verbreitung des Standards bei. Andererseits muss die Durchsetzungsfähigkeit auf Grund der bisher noch nicht eingeleiteten Standardisierungsmaßnahmen sowie der geringen Detailtiefe vorhandener Dokumente kritisch hinterfragt werden. Auch bleibt abzuwarten, ob sich neben CSC weitere Unternehmen an der Standardentwicklung beteiligen werden. Die Bewertung der Partizipationsmöglichkeit ist auf Grund weniger Informationen erschwert und wird auf Grundlage der frei verfügbaren als „gering“ eingestuft. Bisher veröffentlichte Dokumente legen den Schluss nahe, dass CSC bisher alleiniger Treiber der Vorarbeiten zum Standard ist. Es ist unklar, inwiefern eine Beteiligung am Entwicklungsprozess durch eine CSA-Mitgliedschaft ermöglicht wird.

**Ähnliche Standards:** Im Bereich der expliziten Cloud-Standards wurden im Rahmen der Studie keine Alternativen identifiziert. Die nachfolgend beschriebenen Standards weisen jedoch impliziten Bezug zum Cloud Computing auf.

Das Security Content Automation Protocol (SCAP) kann eine Alternative zum Austausch von Informationen zur Sicherstellung der Transparenz in Bezug auf Sicherheitsinformationen darstellen. Durch die Fokussierung auf sicherheitsrelevante Informationen liegt hier bereits eine Spezifikation als Arbeitsversion vor. Vor allem im Hinblick auf die Spezifikation der Schnittstellen, kann der Status im Vergleich zu CTP als reifer eingeschätzt werden.

Zur Sicherstellung von Transparenz und Compliance kann zudem die Open Checklist Reporting Language (OCRL) eine angemessene Alternative darstellen. OCRL beschreibt ein XML-Format zur automatisierten Analyse von Systemstatus sowie deren Einbettung in druckfertige Berichte. Ähnlich wie CTP ist der Reifegrad von OCRL gering. Auch erscheint dieses Projekt derzeit wenig aktiv und es fehlen Sponsoren für eine weite Verbreitung.

---

<sup>84</sup> Es können also in unterschiedlichen Anbieter-Anwender-Konstellationen verschieden Detaillierungen der Infrastruktur zum Einsatz kommen.

### 5.1.5 Open Cloud Computing Interface (OCCI)

BASIS- INFORMATION	Status	Veröffentlicht
	Formalisierung	Industriestandard
	Bezug zu CC	Explizit
	Initiator	OGF
	Beteiligte	- -
	Link	<a href="http://www.occi-wg.org/">http://www.occi-wg.org/</a>
TAXONOMIE	Ansatzpunkte	▪ T – Protokolle & Schnittstellen
	Herausforderungen	▪ Effizienz ▪ Effektivität ▪ Interoperabilität ▪ Portabilität
GELTUNGS- BEREICH	Service-Modell	IaaS, (PaaS, SaaS)
	Nutzergruppe	Anbieter, Nutzer
	Branche	Übergreifend
	Deployment	Alle
	Geographie	Global
	Unternehmensgröße	Alle
BEWERTUNG	Reifegrad	Hoch
	Durchsetzungsfähigkeit	Hoch
	Partizipationsmöglichkeit	Hoch bis sehr hoch
ÄHNLICHE STANDARDS		DeltaCloud, EC2 API, Eucalyptus API, Libcloud, Rackspace API, OpenStack Compute API, VMWare vCloud API, Microsoft Azure

**Kurz-Charakterisierung:** Das von der Open Cloud Computing Initiative des Open Grid Forums (OGF) entwickelte Open Cloud Computing Interface (OCCI) definiert ein REST-basiertes Protokoll und eine Schnittstelle, die eine Reihe von Ressourcenverwaltungsaufgaben im Cloud Computing unterstützen soll.

Ursprünglich sollte der Funktionsumfang ähnlich zu üblichen Fernwartungsprogrammen sein und war auf IaaS Betriebsmodelle beschränkt. Die seit April 2011 als Version 1.1 vorliegenden Standardspezifikationen beinhalten darüber hinausgehende Funktionen zur Unterstützung von PaaS oder SaaS Betreibermodellen. Neben typischen Anforderungen für IaaS-Angebote, wie bspw. das Hinzufügen oder Freigeben von Cloud Ressourcen, definiert OCCI Funktionen zum Betrieb von Monitoringdiensten oder zur Steuerung der Skalierungseigenschaften der verwendeten Ressourcen.

Im Zuge der Standardisierung von OCCI wurde von Beginn an auf Erweiterbarkeit des Standards gesetzt, sodass auf den Anwendungsbedarf angepasste, nicht notwendigerweise durch die Standardisierungsorganisation vorgegebene Ergänzungen möglich sind. OCCI selbst, wird ebenfalls modular durch das Zusammenspiel von drei Dokumenten spezifiziert:

- **OCCI Core (GFD.183):** Hier werden die Kernelemente des Standards definiert. Alle weiteren Spezifikationen bauen auf diesen Kernelementen auf. So ermöglicht bspw. die Definition von *Mixin*-Objekten, die Abbildung der skalierbaren Infrastruktur durch dynamisches Hinzufügen von Rechen- oder Speicherkapazitäten zur Systemlaufzeit.
- **OCCI Infrastruktur (GFD.184):** In diesem Profil werden die Ressourcen einer IaaS-Domäne spezifiziert. Dies beinhaltet Attribute und Funktionen. Im Standard werden folgende Hauptbestandteile einer IaaS-Architektur unterschieden: Compute, Network und Storage.

- **OCCI HTTP Rendering (GFD.185):** Das HTTP Rendering Profile definiert schließlich das Interaktions- und Kommunikationsprotokoll also die Serialisierung und Sicherung der Aufrufe. Hierfür wird eine über HTTP anzusprechende, RESTful OCCI API spezifiziert. Zur Verschlüsselung der Kommunikation stützt sich OCCI auf TLS.

**Bewertung:** Es sind bereits einige Referenzimplementierungen des OCCI-Standards am Markt zu finden, z. B. OpenStack, Eucalyptus oder OpenNebula. Darüber hinaus ermöglicht das verfügbare OCCI Compliance Testing Tool automatisierte Tests der Regelkonformität. Der Reifegrad von OCCI wird folglich als hoch eingestuft. Im Hinblick auf die mögliche Durchsetzungsfähigkeit von OCCI ist zu begrüßen, dass bereits heute die Kompatibilität zu Standards wie CDML, JSON oder OVF<sup>85</sup> sichergestellt ist. Durch die hierdurch angestrebte Interoperabilität<sup>86</sup> sowie die Erweiterbarkeit des Standards wird die Durchsetzungsfähigkeit als ebenfalls hoch eingeschätzt. Derzeit ist eine Reihe von aktiven Weiterentwicklungen des Standards zu beobachten, bspw. zur Berücksichtigung von Abrechnungsaspekten oder zur Erweiterung des Monitorings auf beliebige SLAs. Die Möglichkeiten zur Beteiligung an OCCI sind unterschiedlich zu bewerten. Grundsätzlich setzt eine Mitarbeit bei OGF Standards eine OGF-Mitgliedschaft voraus. Dies ist in der Regel nicht Arbeitsgruppen-spezifisch. Speziell für OCCI existiert jedoch ein Aufruf an alle Interessierten zur Beteiligung an der Standardisierung. Die Partizipationsmöglichkeit wird als „hoch“ bis „sehr hoch“ eingestuft.

**Ähnliche Standards:** Neben OCCI existieren weitere Standardinitiativen, die ebenfalls die Definition einer einheitlichen Managementschnittstelle für Cloud-Dienste zum Ziel haben. Hier sind insbesondere die als Apache-Projekte entwickelten DeltaCloud und LibCloud zu nennen. Beiden Lösungen weisen einen ähnlichen Funktionsumfang sind jedoch bislang nur für Ruby und C/C++ bzw. Python verfügbar. Als im Bereich Public Cloud verwandte, jedoch im Funktionsumfang auf IaaS Betriebsmodelle beschränkte Standards, können der de-facto Standards Amazon EC2 API genannt werden. Die Open Source Varianten Eucalyptus API sowie OpenStack Compute stellen wie bereits genannt Referenzimplementierungen von OCCI dar. Daneben gibt es eine Reihe von weiteren proprietären Schnittstellen von Cloud Infrastruktur Anbietern wie Microsoft oder Rackspace. Diese decken ebenfalls eine Reihe von IaaS Funktionen ab. Im Bereich der Private Clouds stehen die proprietären Schnittstellen der Anbieter von Virtualisierungslösungen wie VMWare, Microsoft oder XEN in Konkurrenz.

---

<sup>85</sup> Hinweis: Beim Einsatz von OVF muss derzeit noch beachtet werden, dass OCCI in seiner Rendering Spezifikation nur text/occi, text/plain und text/uri-list zur Verfügung stellt. Aus diesem Grund müssen OVF-Attribute stets noch zuerst in OCCI-Attribute umgewandelt werden. Gleiches gilt in umgekehrter Richtung.

<sup>86</sup> Hinweis: OCCI ist derzeit bereits zu IaaS-Angeboten wie R2AD, Eucalyptus, OpenStack oder OpenNebula.org interoperabel.

### 5.1.6 OpenStack Cloud Software (OpenStack)

BASIS- INFORMATION	Status	Veröffentlicht
	Formalisierung	Referenzimplementierung
	Bezug zu CC	Explizit
	Initiator	Rackspace, NASA
	Beteiligte	> 100: AMD, Dell, Citrix, HP, Intel
	Link	<a href="http://www.openstack.org">http://www.openstack.org</a>
TAXONOMIE	Ansatzpunkte	<ul style="list-style-type: none"> <li>▪ T – Protokolle und Schnittstellen</li> <li>▪ T – Standardkomponenten und Referenzarchitekturen</li> </ul>
	Herausforderungen	<ul style="list-style-type: none"> <li>▪ Effizienz</li> <li>▪ Effektivität</li> <li>▪ Interoperabilität</li> <li>▪ Portabilität</li> </ul>
GELTUNGS- BEREICH	Service-Modell	IaaS, PaaS
	Nutzergruppe	Alle
	Branche	Übergreifend
	Deployment	Alle
	Geographie	Global
	Unternehmensgröße	Alle
BEWERTUNG	Reifegrad	Hoch
	Durchsetzungsfähigkeit	Hoch
	Partizipationsmöglichkeit	Sehr hoch
ÄHNLICHE STANDARDS		Referenzimplementierungen: OpenNebula, Nimbus Schnittstellen: CDML, OCCl, OVF (sowie dort genannte)

**Kurz-Charakterisierung:** Die unter dem Namen OpenStack Cloud Software bekannten Projekte haben die Entwicklung eines „Open Standard Cloud Operating System“ zum Ziel. Damit soll der Aufbau von Private und Public Clouds auf Basis einer Quell-offenen Infrastruktur ermöglicht werden.

Die Gründung des OpenStack Projekts geht auf eine gemeinsame Initiative der NASA und Rackspace zurück. Mittlerweile wird die OpenStack Community von mehr als 100 Firmen unterstützt. Darunter befinden sich neben Cloud Startups oder Kleinunternehmen auch zentrale Hard- und Softwareunternehmen wie AMD, Dell, Citrix, Cisco, HP, Intel, Dell und Citrix.

Die folgenden zu OpenStack gehörenden Projekte stehen als Apache-Projekte zur Verfügung und sind unter den Apache 2.0 Lizenzbedingungen zur freien Verwendung erhältlich:

- **OpenStack Compute (Codename: Nova):** Ziel der Compute-Komponente ist die Bereitstellung und das Management großer Verbünde virtueller Maschinen (auch engl. „instances“). Hierdurch sollen redundant ausgelegte und skalierbare Cloud Rechenressourcen bereitgestellt werden können. Nova definiert dazu Schnittstellen und Werkzeuge. Zur Sicherstellung der Interoperabilitäts- und Portabilitätsanforderungen erfolgen die Entwicklungen unabhängig von den tatsächlich eingesetzten Virtualisierungstechnologie.
- **OpenStack Storage (CodeName: Swift):** Ziel der Storage-Komponente ist die Bereitstellung eines skalierbaren Speichers zur Ablage von Langzeitdaten, wie z. B. „Images“ virtueller Maschinen. Die Bereitstellung eines verteilten Dateisystems, das kontinuierliche Lese- und Schreibzugriffe unterstützt, entspricht nicht den Anforderungen und ist daher nicht beabsichtigt. Vielmehr stellt Swift für große, eher statische Dateien Skalierbarkeit, Redundanz und Beständigkeit des Spei-

chers über besondere Architekturen, Mechanismen und Werkzeuge sicher.

- **OpenStack Image Service (Codename: Glance):** Ziel der Image Service-Komponenten ist die Unterstützung des Auffindens, der Registrierung und der Bereitstellung von Virtual Disk Images. Diese Images stellen Snapshots einer OpenStack Compute Instanz dar und können über die Storage-Komponente (Swift) abgelegt werden. Hierfür werden eine Vielzahl von Dateiformaten unterstützt, bspw. OVF, EC2, VMDK (VMware), VHD (Xen, Microsoft) oder VDI (Oracle).

Die von OpenStack verwendeten Schnittstellen orientieren sich bisher eng an dem durch Amazon vorgegebenen Funktionsumfang. Alle Schnittstellen werden als RESTful Services bereitgestellt.

**Bewertung:** Zur Steuerung der Fortentwicklung der OpenStack-Projekte existieren zentrale Strukturen, die die u. a. Beiträge einzelner Unterstützer konsolidieren und das Release Management überwachen. In der kurzen Geschichte von OpenStack ist bereits eine Reihe von Wiederveröffentlichungen zu beobachten. Der Reifegrad von OpenStack wird daher als hoch eingestuft. Die mögliche Durchsetzungsfähigkeit der im Rahmen von OpenStack entwickelten Standardlösungen und -schnittstellen wird auf Grund der Zusammensetzung und Masse der Unterstützer als hoch eingeschätzt. Hierbei ist zu beachten, dass die großen Cloud-Anbieter wie Amazon, Google oder auch Microsoft bislang keine Unterstützer von OpenStack sind. Die Möglichkeit der Beteiligung an der Entwicklung von OpenStack wird als „sehr hoch“ eingestuft, da eine Community-basierten Entwicklung der Projekte erfolgt. Ein Austausch zwischen den Unterstützern wird bspw. durch die halbjährig veranstalteten Entwicklerkonferenzen unterstützt.

**Ähnliche Standards:** Die zu OpenStack vergleichbaren Standards lassen sich in zwei Bereiche untergliedern. Zum einen sind ähnliche Referenzimplementierungen wie OpenNebula oder Nimbus zu nennen. Beide sind vom Funktionsumfang mit OpenStack zu vergleichen. Die Auswahl der richtigen Alternative obliegt somit der Prüfung im Einzelfall. Im Bereich der Verwaltung und Steuerung von Cloud-Rechenressourcen sind zum anderen insbesondere die Entwicklungen von OVF und OCCI sowie die dort genannten „ähnlichen Standards“ vergleichbar. Für den Bereich der Storage-Komponenten gilt dies auch für CDMI. Im Bereich der Image-Services ist OVF verwandt. Bereits heute stellt OpenStack bspw. für OCCI eine Referenzimplementierung dar. Für die Zukunft ist zu beobachten, inwieweit OpenStack sich zu einem eigenständigen Industriestandard entwickelt. Es wird jedoch erwartet, dass OpenStack auch in Zukunft Konformität zu den genannten, verwandten Standards anstrebt.



### 5.1.7 CIM System Virtualization Model (CIMSVM)

<b>BASIS- INFORMATION</b>	<b>Status</b>	In Arbeit
	<b>Formalisierung</b>	Spezifikation
	<b>Bezug zu CC</b>	Implizit
	<b>Initiator</b>	DMTF
	<b>Beteiligte</b>	-
	<b>Link</b>	<a href="http://dmtof.org/standards/vman">http://dmtof.org/standards/vman</a>
<b>TAXONOMIE</b>	<b>Ansatzpunkte</b>	<ul style="list-style-type: none"> <li>▪ T – Datei- und Austauschformate</li> <li>▪ T – Protokolle und Schnittstellen</li> <li>▪ T – Standardkomponenten und Referenzarchitektur</li> </ul>
	<b>Herausforderungen</b>	<ul style="list-style-type: none"> <li>▪ Effizienz</li> <li>▪ Interoperabilität</li> <li>▪ Portabilität</li> </ul>
<b>GELTUNGS- BEREICH</b>	<b>Service-Modell</b>	IaaS
	<b>Nutzergruppe</b>	Anbieter, Nutzer
	<b>Branche</b>	Übergreifend
	<b>Deployment</b>	Alle
	<b>Geographie</b>	Global
	<b>Unternehmensgröße</b>	Alle
<b>BEWERTUNG</b>	<b>Reifegrad</b>	Mittel
	<b>Durchsetzungsfähigkeit</b>	Mittel
	<b>Partizipationsmöglichkeit</b>	Hoch
<b>ÄHNLICHE STANDARDS</b>		- -

**Kurz-Charakterisierung:** Das von der Arbeitsgruppe System Virtualization, Partitioning, and Clustering (SVPC) der DMTF entwickelte Common Information Model System Virtualization Model (CIMSVM) beschreibt einen Standard zum Management von virtualisierten Systemen sowie zugehörigen Ressourcen. Durch Definition eines Objektmodells und die Spezifikation von Management-Schnittstellen, leistet das CIMSVM einen Beitrag zur Adressierung der Herausforderungen des Ressourcenmanagements sowie zur Interoperabilität und Portabilität virtueller Ressourcen im Cloud Computing. Der Geltungsbereich des CIMSVM ist nicht auf Cloud Computing beschränkt. Es soll vielmehr ein Standard für alle Anwendungsbereiche der Virtualisierung von Systemen und Ressourcen erarbeitet werden. Auf Grund des engen inhaltlichen Zusammenhangs ist ein impliziter Bezug zum Cloud Computing festzustellen.

Das CIMSVM baut auf dem umfangreichen Common Information Model (CIM)<sup>87</sup> der DMTF auf. Es erweitert das bestehende Modell zum Management von Rechnern und Rechenressourcen in Unternehmen um zusätzliche Konzepte und Attribute der Virtualisierung. Darüber hinaus werden weitergehende Möglichkeiten zur Abbildung von Abhängigkeiten zwischen virtuellen Systemen und ihren Ressourcen berücksichtigt.

<sup>87</sup> Das CIM definiert ein Basisobjektmodell für Informationen für das Management von IT-Systemen, Netzwerken, Anwendungen und Diensten. Damit ermöglicht es den Austausch dieser Information zwischen IT-Systemen und deren Anbietern (vgl. <http://www.dmtf.org/standards/cim>).



In Analogie zum CIM wird das CIMSVM durch eine Reihe detaillierter Profile (bspw. Ressource Allocation Profile (DSP1041), System Virtualization Profile (DSP1042)) ergänzt. Dies dient der Reduzierung der Komplexität innerhalb abgeschlossener Einsatzbereiche. In Summe sind derzeit neun Kernprofile zur vollständigen Spezifikation des CIMSVM vorgesehen.<sup>88</sup> Diese sind zum Teil bereits als offizielle DMTF Standarddokumente verfügbar. Die Weiterentwicklung des CIMSVM sowie zugehöriger Profile erfolgt durch die DMTF, insb. durch die Arbeitsgruppe SVPC.

**Bewertung:** Die Erarbeitung des Standards befindet sich derzeit noch in Arbeit. Die Konsensbildung ist folglich noch nicht abgeschlossen. Dennoch ist das vorgestellte Metamodell bereits sehr umfangreich und konzeptuell gut aufgestellt. Entsprechend wird CIMSVM ein mittlerer Reifegrad zugeordnet. Ein Zeitplan für die Veröffentlichung der ersten offiziellen Standardversion liegt derzeit nicht vor. Dennoch wird das Potenzial zur Durchsetzungsfähigkeit auf mittlerem Niveau eingestuft. Die hohe Aktivität der Initiative zur Weiterentwicklung des Standards sowie die guten Erfahrungen bzgl. der Akzeptanz des übergeordneten Common Information Models (CIM) tragen zu einer tendenziell positiven Zukunftsprognose bei. Die Möglichkeit der Mitwirkung an der Weiterentwicklung des Standards ist als „hoch“ zu charakterisieren. Die aktive Beteiligung an CIMSVM setzt eine kostenpflichtige DMTF-Mitgliedschaft voraus, diese ist jedoch nicht auf die einzelne Initiativen beschränkt. Interessierten steht es offen, sich durch direktes Feedback in den Arbeitsgruppen zu beteiligen. Die Notwendigkeit, alle Rechte am Feedback oder an sonstigen Beiträgen abzutreten, kann jedoch ein Hindernis zur freien Kooperation darstellen.

**Besonderheiten:** Das auf Erweiterbarkeit ausgerichtete Metamodell des Standards ermöglicht es Anbietern von Virtualisierungstechnologien eigene mit der Kernspezifikation des Standards konforme Profile zu erarbeiten. So können Spezifika eigener Produkte berücksichtigt werden. Die Notwendigkeit diese frühzeitig in die Standardentwicklung einzubringen kann so umgangen werden.

**Ähnliche Standards:** Im Rahmen der Studie wurden keine ähnlichen Standards identifiziert.

---

<sup>88</sup> DSP1041, DSP1042, DSP1043, DSP1044, DSP1045, DSP1049, DSP1050, DSP1057, DSP1059.

### 5.1.8 Apache Hive (Hive)

BASIS- INFORMATION	Status	Veröffentlicht
	Formalisierung	Industriestandard
	Bezug zu CC	Explizit
	Initiator	Apache
	Beteiligte	> 100 – Facebook, Yahoo!, Amazon
	Link	<a href="http://hive.apache.org">http://hive.apache.org</a>
TAXONOMIE	Ansatzpunkte	▪ T – Programmiermodelle
	Herausforderungen	▪ Effektivität ▪ Interoperabilität ▪ Portabilität
GELTUNGS- BEREICH	Service-Modell	IaaS
	Nutzergruppe	Alle
	Branche	Übergreifend
	Deployment	Alle
	Geographie	Global
	Unternehmensgröße	Alle
BEWERTUNG	Reifegrad	Produkt
	Durchsetzungsfähigkeit	Mittel
	Partizipationsmöglichkeit	Sehr hoch
ÄHNLICHE STANDARDS		JAQL, PIG

**Kurz-Charakterisierung:** Das durch die Apache Software Foundation entwickelte Hive Rahmenwerk erlaubt den Aufbau einer Data-Warehouse Infrastruktur, die auf das Hadoop File System (HDFS) aufsetzt. Die zur Datenabfrage verwendete Hive Query Language (HiveQL) stellt ein Programmiermodell zur Definition von Datenabfragen dar. Hive ist dabei an die SQL-Syntax angelehnt.

Zur Bearbeitung der in HiveQL definierten Datenabfragen wird intern eine Abbildung auf Map/Reduce-Funktionen vorgenommen. Über Erweiterungsmechanismen wird zudem sichergestellt, dass für aufwändigere Abfragen, die nicht in HiveQL formuliert werden können, Programmcode zum direkten Aufruf von Map/Reduce-Funktionen eingesetzt werden kann. Dies erlaubt bspw. auch die Erweiterung um benutzerdefinierte Skalar- (kurz: UDF), Aggregations- (kurz: UDAF) und Tabellenfunktionen (kurz: UDTF).

Apache Hive wurde ursprünglich von Facebook entwickelt, um das im Einsatz befindliche HDFS um typische Data-Warehouse Funktionen wie das Partitionieren, die Analyse oder die Indexierung von Daten zu erweitern. Im Sommer 2008 hat Facebook den Hive Quellcode veröffentlicht, der nun unter Federführung der Apache Software Foundation weiterentwickelt wird.

**Bewertung:** Hive befindet sich derzeit in einer Reihe von Produkten im Einsatz.<sup>89</sup> So bietet bspw. Amazon mit Elastic-MapReduce eine kommerzielle Implementierung des Hive Rahmenwerks an. Der Reifegrad wird folglich als Produkt-reif eingestuft. Der Durchsetzungsfähigkeit von Hive als Standard für Abfragesprachen wird ein mittleres Potenzial zugeschrieben. Dies liegt einerseits im speziellen Anwendungsfall begründet. Zugleich existieren aber auch konkurrierende Ansätze (bspw. Apache Pig oder JAQL). Dem O-

<sup>89</sup> Vgl. <https://cwiki.apache.org/confluence/display/Hive/PoweredBy>.

penSource-Gedanken entsprechend ist die Partizipationsmöglichkeit als „sehr hoch“ entsprechend der Apache-Lizenzbedingungen einzustufen.

**Ähnliche Standards:** Vergleichbare Aspekte zu Programmiermodellen – insb. zu Abfragesprachen für sehr große Datenvolumina – werden in den Standards Query Language for JavaScript Object Notation (JAQL) und Apache Pig entwickelt. Beide basieren, ähnlich wie Hive, auf dem Map/Reduce-Verfahren. JAQL wurde ursprünglich von IBM entwickelt und hat zum Ziel, in JSON beschriebene Daten möglichst einfach verändern und analysieren zu können. Zu beachten ist, dass die Weiterentwicklung von JAQL eingestellt wurde. Der Ansatz findet jedoch in IBMs BigInsights eine kommerzielle Weiterentwicklung. Apache Pig wurde ursprünglich von Yahoo! entwickelt und wird nun ebenfalls als Apache Projekt weiterentwickelt. Im Unterschied zu den in Hive und JAQL verwendeten imperativen Programmiermodellen folgt Pig einem deklarativen Ansatz.

### 5.1.9 Web Authorization Protocol (OAuth)

BASIS- INFORMATION	Status	Veröffentlicht
	Formalisierung	Standard
	Bezug zu CC	Implizit
	Initiator	IETF
	Beteiligte	Yahoo!, Facebook, Microsoft
	Link	<a href="http://tools.ietf.org/html/rfc5849">http://tools.ietf.org/html/rfc5849</a> <a href="http://oauth.net/core/1.0/">http://oauth.net/core/1.0/</a>
TAXONOMIE	Ansatzpunkte	▪ T – Protokolle & Schnittstellen
	Herausforderungen	▪ Informationssicherheit
GELTUNGS- BEREICH	Service-Modell	Alle
	Nutzergruppe	Anbieter, Anwender, Broker
	Branche	Übergreifend
	Deployment	Alle
	Geographie	Global
	Unternehmensgröße	Alle
BEWERTUNG	Reifegrad	Produkte
	Durchsetzungsfähigkeit	Hoch
	Partizipationsmöglichkeit	Sehr hoch
ÄHNLICHE STANDARDS		OpenID, WS-Federation, SAML

**Kurz-Charakterisierung:** Das durch die Internet Engineering Task Force (IETF) standardisierte Web Authorization Protocol (OAuth) spezifiziert eine Schnittstelle und ein Protokoll zur Identifikation von Nutzern. Zugleich wird die Autorisierung von Zugriffen auf Schnittstellen und Daten zwischen unterschiedlichen Diensteanbietern unterstützt. Diensteanbieter müssen im Ergebnis kein eigenes Identitäts- und Rechtemanagement betreiben, um fremden Nutzern oder Diensten Zugriff auf Ressourcen zu gewähren.

Ein typisches Anwendungsszenario stellt die Autorisierung von Web- oder Mobile-Clients für Cloud-basierte Dienste (bspw. Twitter, Dropbox, Facebook, Amazon Web Services) dar.

Technisch wird der Zugriff über den Austausch von Schlüsseln (engl. Tokens) für die Autorisierung von Zugriffen auf Web-Schnittstellen ermöglicht. Dabei muss jeder Client einmalig – vor dem ersten Zugriff auf die geschützte Ressource – einen Schlüssel (engl. „Request-Token“) – vom Diensteanbieter anfor-

dern. Der Protokollablauf ermöglicht dann, den „Request-Token“ in einen sogenannten Zugangsschlüssel (engl. „Access-Token“) einzutauschen. Hierfür ist die einmalige Eingabe des Benutzernamens und Passworts durch den Anwender notwendig. Bei erfolgreicher Zuteilung des Zugangsschlüssels können alle zukünftigen Anfragen mittels dieses Schlüssels signiert werden. Dies ermöglicht dem Dienstanbieter die Autorisierung des Zugriffs. Eine Wiederholung der Eingabe der Benutzername-Passwort-Kombination ist nun überflüssig.

Die Entwicklung von OAuth startete im November 2006 und war von der Notwendigkeit der Entwicklung eines auf OpenID-basierenden Identitätsdiensts für Twitter motiviert. Die Dringlichkeit der Entwicklung eines einheitlichen Standards zum Identitäts- und Rechtemanagement zeigte sich unter anderem in der frühen Unterstützung der OAuth-Initiative durch Dienstanbieter wie Yahoo, Facebook oder Microsoft. Die erste Entwurfsversion der Spezifikation wurde bereits im Oktober 2007 fertiggestellt. Seit April 2010 ist ein durch das IETF standardisierte „Request for comments“ verfügbar. Es sind bereits aktive Arbeiten an der Version 2.0 beobachtbar, die den Standard durch Vereinfachung des Protokolls, vor allem im Hinblick auf Nutzerfreundlichkeit und Skalierbarkeit, verbessern sollen.<sup>90</sup>

**Bewertung:** Das Web Authorization Protokoll (OAuth) wird bereits in kommerziell verfügbaren Diensten verwendet. Es besitzt einen hohen Reifegrad und findet bereits vielfach Anwendung in Cloud-Diensten. Die Durchsetzungsfähigkeit kann als hoch eingestuft werden, da bereits heute viele Cloud-Dienste auf OAuth bauen und ein breites Spektrum an Programmbibliotheken für die Verwendung von OAuth existiert.<sup>91</sup> Die Durchsetzungsfähigkeit profitiert dabei von der Möglichkeit zum Einsatz von Erweiterungsmechanismen, die Anpassungen des Standards für unterschiedliche Einsatzzwecke ermöglichen. Die Weiterentwicklung des Standards wird hauptsächlich von der OAuth-Initiative sowie der IETF Working Group getrieben. Die Partizipationsmöglichkeiten an der Entwicklung von OAuth werden als „sehr hoch“ eingestuft. Es ist erkennbar, dass der Standard bereits eine hohe Reife erreicht hat. Dadurch ist die Offenheit gegenüber Anpassungswünschen, die die Grundlagen des Standards betreffen, jedoch als eher gering einzustufen.

**Ähnliche Standards:** Im primär für das Cloud Computing relevanten Bereich der WebIDs ist vor allem OpenID als ähnliche Standard zu nennen. OpenID unterscheidet sich von OAuth in der Notwendigkeit der wiederholten Verwendung von Benutzername und Passwort zur Autorisierung. Darüber hinaus bedarf OpenID der vorherigen Konfiguration von Trust-Domänen zwischen Anbietern, um die Möglichkeit der Autorisierung grundsätzlich zu er-

---

<sup>90</sup> Ende April 2011 wurde die erste Entwurfsversion auf den Seiten des IETF online gestellt. Seither erfolgten einige Überarbeitungen (vgl. <http://tools.ietf.org/wg/oauth/draft-ietf-oauth-v2/>).

<sup>91</sup> Es gibt unter anderem Programmbibliotheken für folgende Programmiersprachen: Java, Objective-C, PHP, RubyOnRails, Python, .NET etc.

möglichen. Im allgemeineren Bereich des Service-oriented Computing über SOAP/WSDL wird ein föderiertes Identitätsmanagement bspw. durch WS-Federation unterstützt. Generell kann zum Aufbau eines verteilten Benutzer-managements auch auf die Security Assertion Markup Language (SAML) zurückgegriffen werden.

### 5.1.10 Open Virtualization Format (OVF)

<b>BASIS- INFORMATION</b>	<b>Status</b>	Veröffentlicht
	<b>Formalisierung</b>	Standard
	<b>Bezug zu CC</b>	Explizit
	<b>Initiator</b>	DMTF
	<b>Beteiligte</b>	>100
	<b>Link</b>	<a href="http://www.dmtf.org/standards/ovf">http://www.dmtf.org/standards/ovf</a>
<b>TAXONOMIE</b>	<b>Ansatzpunkte</b>	▪ T – Datei- & Austauschformate
	<b>Herausforderungen</b>	▪ Effizienz ▪ Interoperabilität ▪ Portabilität
<b>GELTUNGS- BEREICH</b>	<b>Service-Modell</b>	IaaS
	<b>Nutzergruppe</b>	Alle
	<b>Branche</b>	Übergreifend
	<b>Deployment</b>	Alle
	<b>Geographie</b>	Global
	<b>Unternehmensgröße</b>	Alle
<b>BEWERTUNG</b>	<b>Reifegrad</b>	Hoch
	<b>Durchsetzungsfähigkeit</b>	Mittel bis hoch
	<b>Partizipationsmöglichkeit</b>	Hoch
<b>ÄHNLICHE STANDARDS</b>		AMI, EMI

**Kurz-Charakterisierung:** Das von der Distributed Management Task Force (DMTF) entwickelte Open Virtualization Format (OVF) soll zur Verbesserung der Portabilität von Virtual Appliances beitragen. OVF spezifiziert offene, sichere, portierbare und erweiterbare Dateiformate zur Beschreibung von Virtual Appliances. Das Bündeln und die Verteilung der gewünschten Software erfolgt auf Plattform-unabhängige Art und Weise, kann aber durch Erweiterungen auf Spezifika der eingesetzten Virtualisierungskomponenten (bspw. spezielle Hypervisortypen) angepasst und optimiert werden.

Ein OVF-Dateipaket (Open Virtual Appliance or Application, OVA)<sup>92</sup> beinhaltet mindestens einen OVF-Deskriptor zur Verwaltung von Meta-Informationen sowie beliebige viele Image-Dateien (Betriebssystempartition und weitere virtuelle Festplatten) und weitere Manifest- sowie Zertifikatsdateien zur Beschreibung der benötigten virtuellen Hardware bzw. Validierung der Paketinhalte. Die in OVF spezifizierten Betriebssystem- und Speicherdateien können direkt ausgeführt werden, sind jedoch nicht für die Ausführung optimiert. Die in Betracht kommende Virtualisierungshardware, kann zur Steigerung der Ausführungseffizienz eigene Formate verwenden.

<sup>92</sup> Eine OVA-Datei bündelt die notwendigen OVF-Dateien im TAR-Format. Die Bündelung aller benötigten Dateien in einer OVA-Datei ist optional.

OVF ist Bestandteil der sich künftig vergrößernden Familie von DMTF-Standards zum „Virtualization Management“, deren Entwicklung von der Virtualization MANagement Initiative (VMAN) getrieben wird.

**Bewertung:** Durch die kontinuierliche Arbeit der DMTF ist OVF seit 2010 nicht nur in der DMTF-Version 1.1.0 sondern auch als ANSI-Standard (INCITS 469-2010)<sup>93</sup> verfügbar. Die Weiterentwicklung des Standards wird durch die Arbeitsgruppe „System Virtualization, Partitioning, and Clustering (SVPC)“ verantwortet. Der Reifegrad kann entsprechend als hoch betrachtet werden. Die Durchsetzungsfähigkeit des Standards kann als mittel bis hoch eingestuft werden. Dies liegt u. a. in der zunehmenden Verbreitung Tools begründet, die OVF unterstützen. Darüber hinaus kann erwartet werden, dass durch die DMTF ein Multiplikator existiert, der die Verbreitung und damit die Durchsetzung des Standards treibt. Die Möglichkeiten der Partizipation im Standardentwicklungsprozess sind als „hoch“ einzustufen. Die aktive Beteiligung an der Weiterentwicklung von OVF setzt eine kostenpflichtige DMTF-Mitgliedschaft voraus. Das Beitragen von allgemeinen Kommentaren zu veröffentlichten Dokumenten für Dritte ist möglich.

**Ähnliche Standards:** In Konkurrenz zum OVF-Standard, stehen Amazons Industriestandard Amazon Machine Images (AMI) sowie die OpenSource Alternative Eucalyptus Machine Images (EMI). Im direkten Vergleich zwischen OVF und AMI/EMI fällt vor allem der bei letzteren vorhandene enge Bezug zu jeweiligen Implementierungsdetails auf.<sup>94</sup> Nach der gängigen Anwendungspraxis besteht ein AMI aus einer Datei, die das Kernbetriebssystem und installierte Anwendungen beinhaltet, sowie eine Datei mit Verweisen auf Dateien, die die zu verwendeten System-Kernels (Amazon Kernel Images, ARI) und RAM-Disks (Amazon RAM Disk Image, ARI) beschreiben.<sup>95</sup> Die Verwendung von AMI erzwingt die Einhaltung spezieller Vorgaben für das zu verwendende Datei- und Systemlayout. Der Aufbau von EMI als offener Nachbau von AMI ist identisch. Dies verhindert letztlich die Wirkung von AMI/EMI als Ansatzpunkt zur Erreichung der gewünschten Portabilität für Virtual Appliances. OVF scheint zur Realisierung von Portabilität besser geeignet. Es definiert zudem erweiterte Sicherheits- und Integritätsfunktionalitäten, die bspw. eine automatische Validierung von Dateiinhalten erlauben.

---

<sup>93</sup> ANSI, INCITS 469-2010, <http://webstore.ansi.org/RecordDetail.aspx?sku=INCITS+469-2010>.

<sup>94</sup> AMI sind an EC2 und S3, EMI an Eucalyptus und Walruss gekoppelt.

<sup>95</sup> <http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/AMIs.html>



### 5.1.11 Security Content Automation Protocol (SCAP)

BASIS- INFORMATION	Status	Veröffentlicht
	Formalisierung	Industriestandard
	Bezug zu CC	Implizit
	Initiator	NIST
	Beteiligte	US-Behörden, MITRE
	Link	<a href="http://scap.nist.gov">http://scap.nist.gov</a>
TAXONOMIE	Ansatzpunkte	<ul style="list-style-type: none"> <li>▪ T – Datei- &amp; Austauschformate</li> <li>▪ T – Protokolle und Schnittstellen</li> </ul>
	Herausforderungen	<ul style="list-style-type: none"> <li>▪ Informationssicherheit</li> <li>▪ Interoperabilität</li> </ul>
GELTUNGS- BEREICH	Service-Modell	Alle
	Nutzergruppe	Alle
	Branche	Öffentliche Verwaltung
	Deployment	Alle
	Geographie	USA
	Unternehmensgröße	Alle
BEWERTUNG	Reifegrad	Hoch
	Durchsetzungsfähigkeit	Mittel
	Partizipationsmöglichkeit	Gering
ÄHNLICHE STANDARDS		CloudAudit, CTP

**Kurz-Charakterisierung:** Das Security Content Automation Protocol (SCAP) beschreibt eine Auswahl von Standardspezifikationen für Datei- und Austauschformate sowie Protokolle und Schnittstellen zur Beschreibung und zum Austausch von Informationen über Sicherheitskonfigurationen und -schwachstellen. Dadurch sollen insbesondere das Sicherheitsmanagement von IT-Systemen, die Interoperabilität von Sicherheitslösungen und die Kommunikation von Sicherheitsinformationen standardisiert werden.

Das Security Content Automation Protocol (SCAP), wurde vom NIST und vom U.S. Wirtschaftsministerium initiiert. Es liegt seit September 2011 in Version 1.2 vor. Software-Produkte können anhand von SCAP Use Cases auf ihre Konformität als Produzent oder Konsument von Sicherheitsinformationen getestet werden. Neben konkreten Software-Produkten können auch Quellen für Sicherheitsinformationen auf ihre Konformität getestet werden.

Insgesamt werden elf Standardspezifikationen in fünf Gruppen (engl. „SCAP Components“) beschreiben:

- Als erste Komponenten werden **Beschreibungssprachen** (engl. „languages“) zur Erstellung von sowohl maschinen-lesbaren als auch für Menschen zu interpretierende Prüflisten aufgeführt. Zu diesen gehören das Extensible Configuration Checklist Description Format (XCCDF), die Open Vulnerability and Assessment Language (OVAL) und die Open Checklist Interactive Language (OCIL).
- Die zweite Gruppe beschreibt Standards zur Definition von **Berichtsformaten** (engl. „reporting formats“) für die Zusammenstellung von IT-Sicherheitsinformationen. Hierzu gehören das Asset Reporting Format (ARF) und der Asset Identification (AI) Katalog.
- Die dritte Gruppe wird durch **Fachbegriffsmodelle** (engl. „enumerations“) gebildet. Dazu gehören die Common Platform Enumeration (CPE) zur Benennung von Hardware, Betriebssystemen und Anwen-

dungen, die Common Configuration Enumeration (CCE), für Sicherheitskonfigurationen von Software, sowie die Liste der Common Vulnerabilities and Exposures (CVE), zur Benennung von Softwarebedingten Sicherheitsschwachstellen.

- **Kennzahlen- und Bewertungssysteme** bilden die vierte Gruppe der SCAP Komponenten. Hierzu zählen das Common Vulnerability Scoring System (CVSS) und das Common Configuration Scoring System (CCSS)
- Die letzte Gruppe der Standards dient der Sicherstellung der **Integrität** des Informationsaustauschs. Hierfür sieht SCAP das Trust Model for Security Automation Data (TMSAD) vor und erlaubt dadurch die Nutzung von digitalen Signaturen zur Sicherung der Kommunikation.

Im Rahmen des NIST SCAP Validation Program können Unternehmen ihre Software für SCAP zertifizieren lassen können. Diese Zertifizierungen sind ein Jahr gültig und können verlängert werden. Hierzu müssen die entsprechenden Tests erneut bestanden werden.

**Bewertung:** Die NIST ist Herausgeber des SCAP und übernimmt dadurch auch die Verantwortung für die Pflege und Weiterentwicklung des Standards. Zur Verabschiedung neuer Standardversionen liegt ein öffentlicher Prozess vor. Der Reifegrad von SCAP kann insgesamt als hoch eingestuft werden. Die Durchsetzungsfähigkeit von SCAP als Standard zur Beschreibung, Analyse und Austausch von Sicherheitsinformationen im Cloud Computing kann nicht eindeutig beantwortet werden. Zunächst ist festzustellen, dass bislang keine Cloud-spezifischen Sicherheitsanforderungen Berücksichtigung finden. Auch ist die Frage, inwiefern existierende Tests zur Sicherstellung der Konformität auf Cloud-Anwendungsbereiche übertragen werden können. Zugleich bietet SCAP jedoch eine fundierte Ausgangslage für den automatisierten Austausch von Sicherheitsinformationen im Cloud Computing. Abschließend ist zu beachten, dass die entwickelten Standards sowie die hierfür erarbeiteten Anforderung aus der Sicht der US-Behörden verfasst wurden. Länderspezifische Anpassungsmöglichkeiten, die bspw. durch europäisches oder deutsches Recht notwendig würden, sind bislang nicht vorgesehen. Formalisierte Partizipationsmöglichkeiten zur Weiterentwicklung von SCAP bspw. durch die Einbringung eigener Anforderungen sind nicht bekannt.

**Ähnliche Standards:** CloudAudit und CTP sind verwandte Standards.<sup>96</sup> Einige der in SCAP referenzierten Standards werden durch die MITRE gepflegt. Hierfür existieren über das MITRE Adoption Program Alternativen zum NIST SCAP Validation Program.

---

<sup>96</sup> Zur weiteren Beschreibung der Ähnlichkeit wird auf die jeweiligen Kapitel verwiesen.

### 5.1.12 Unified Service Description Language (USDL)

<b>BASIS- INFORMATION</b>	<b>Status</b>	In Arbeit
	<b>Formalisierung</b>	Spezifikation
	<b>Bezug zu CC</b>	Implizit
	<b>Initiator</b>	W3C, SAP
	<b>Beteiligte</b>	> 10
	<b>Link</b>	<a href="http://www.w3.org/2005/Incubator/usdl/">http://www.w3.org/2005/Incubator/usdl/</a>
<b>TAXONOMIE</b>	<b>Ansatzpunkte</b>	<ul style="list-style-type: none"> <li>▪ T – Datei- &amp; Austauschformate</li> <li>▪ M – Geschäftsmodelle</li> <li>▪ M – Service Level Agreements</li> <li>▪ M – Vertragsbedingungen</li> </ul>
	<b>Herausforderungen</b>	<ul style="list-style-type: none"> <li>▪ Effizienz</li> <li>▪ Transparenz</li> <li>▪ Interoperabilität</li> <li>▪ Portabilität</li> </ul>
<b>GELTUNGS- BEREICH</b>	<b>Service-Modell</b>	Alle
	<b>Nutzergruppe</b>	Alle
	<b>Branche</b>	Übergreifend
	<b>Deployment</b>	Alle
	<b>Geographie</b>	Global
	<b>Unternehmensgröße</b>	Alle
<b>BEWERTUNG</b>	<b>Reifegrad</b>	Mittel
	<b>Durchsetzungsfähigkeit</b>	Mittel
	<b>Partizipationsmöglichkeit</b>	Sehr hoch
<b>ÄHNLICHE STANDARDS</b>		Beispiele: WSDL, UDDI, WADL, OWL-S, WSMO, e3Value, SNN, TEXO Service Ontology, DIN PAS 1018, SML, SaaS-DL

**Kurz-Charakterisierung:** Die Unified Service Description Language (USDL) definiert eine plattformneutrale Beschreibungssprache für Dienste und Dienstleistungen im Internet (engl.: Internet-of-Services). Ziel von USDL ist die Sicherstellung von Interoperabilität und Portabilität, indem Dienste auffindbar, vergleichbar und handelbar beschrieben werden. USDL ermöglicht nicht nur die Beschreibung von funktionalen Aspekten der Dienste (z. B. Schnittstellen und Protokolle), sondern auch eine standardisierte Beschreibung von betriebswirtschaftlichen, operationalen und rechtlichen Aspekten der Anwendung von Diensten.<sup>97</sup>

Zur Sicherstellung der Wartbarkeit und Erweiterbarkeit des Standards ist die Sprachdefinition modular aufgebaut und basiert auf der Meta Object Facility (MOF) der OMG. Neben den zentralen Modulen für allgemeine Sprachaspekte und die Dienstbeschreibung sind einzelne Module zur Beschreibung von Diensteseigenschaften aus den Bereichen Recht, Bepreisung, (Geschäfts-)Partner, Dienstgüte, Technik, Funktion und Interaktion berücksichtigt. Als besonderer Anspruch sollen USDL-Dienstbeschreibungen sowohl vom Menschen als auch von IT-Systemen gelesen und interpretiert werden können. Hierfür werden im Standard unter anderem Technologien des Semantic Webs eingesetzt.

Die Entwicklung von USDL ist ein Ergebnis des vom BMWi geförderten Leuchtturmprojekts „THESEUS“. USDL wurde durch SAP im Rahmen des THESEUS Anwendungsfall „TEXO“ entwickelt und 2009 erstmals der Öffent-

<sup>97</sup> USDL – Webbasierte Dienstleistungen auf dem Vormarsch - <http://news.sap-im-dialog.com/usdl-webbasierte-dienstleistungen-auf-dem-vormarsch/> - Abgerufen am 11.08.11

lichkeit vorgestellt. USDL wurde nicht explizit für den Einsatz zur Beschreibung von Cloud Services entwickelt, hat aber aufgrund der Erweiterbarkeit sowie der umfassend angelegten Anwendbarkeit den Anspruch, auch für die Beschreibung von Cloud Services (SaaS) anwendbar zu sein. Ebenfalls aus dem TEXO-Projekt stammen eine Reihe von Softwarekomponenten und -tools, die für die Erstellung und Verarbeitung von USDL-Beschreibungen eingesetzt werden können.

**Bewertung:** Die USDL-Spezifikation wird von einer durch Attensity, DFKI, SAP, und Siemens gegründeten Arbeitsgruppe des World Wide Web Consortium (W3C) als Vorbereitung für eine mögliche Standardisierung überarbeitet. Dabei sind regelmäßig Versionsaktualisierungen erschienen. Der Reifegrad des Standards wird als „in Arbeit“ eingestuft. Beachtung verdient jedoch, dass die aktuell vorliegenden Dokumente bereits sehr ausgereift und umfangreich sind. USDL hat noch keinen Standardisierungsprozess durchlaufen. Aufgrund des modularen Aufbaus von USDL bestehen Erweiterungs- oder Anpassungsmöglichkeiten für unterschiedliche Bedarfe. Der Prognose für eine hohe Durchsetzungsfähigkeit von USDL im Cloud Computing steht derzeit noch die geringe Beteiligung etablierter Akteure im Cloud Computing wie auch das Fehlen eines klaren Cloud Computing-Anwendungsfalls gegenüber. Die Durchsetzungsfähigkeit des Standards wird daher als mittel bewertet. Die Beteiligung an der Standardisierung bzw. an den Vorarbeiten steht allen Interessenten auf organisatorischer und persönlicher Basis offen. Entgegen der üblichen W3C-Verfahren, die einen formalen Beitritt zur W3C Arbeitsgruppe voraussetzen, können Diskussionsbeiträge und Änderungswünsche zu USDL auch ohne offizielle Mitgliedschaft geleistet werden. Die Möglichkeit zur Partizipation wird als „sehr hoch“ bewertet.

**Ähnliche Standards:** Zur Beschreibung von Diensten existiert eine Vielzahl von sowohl wissenschaftlichen als auch industriellen Spezifikationen. Diese lassen sich grob in die Bereiche Service-oriented Computing (bspw. WSDL, UDDI, WADL), semantische Dienstbeschreibungen (bspw. OWL-S, WSMO), Beschreibung von Servicenetzwerken (bspw. e3Value, SNN) oder Service Systemen (bspw. TEXO Service Ontology) sowie Ansätzen zur Beschreibung der ökonomischen Aspekte von Diensten (bspw. DIN PAS 1018) unterteilen.<sup>98</sup> Diese decken im Vergleich zu USDL nur Teilaspekte ab, können in einzelnen Aspekten daher aber auch detaillierter sein. Eine Alternative zur Beschreibung von Cloud Services kann die von der W3C als „Recommendation“ veröffentlichte Service Modeling Language (SML)<sup>99</sup> darstellen. Diese bezieht auch Informationen über die für die Erbringung notwendigen IT-Ressourcen mit in die Dienstbeschreibung ein. Auch hier kann der Bezug zum Cloud Computing nur implizit hergeleitet werden. Die im Vergleich zu USDL gerin-

---

<sup>98</sup> Eine ausführlichere Diskussion der Gemeinsamkeiten von USDL und verwandten Ansätzen findet sich in der USDL Spezifikation 3.0 <http://www.internet-of-services.de/index.php?id=570>.

<sup>99</sup> <http://www.w3.org/TR/2009/REC-sml-if-20090512/>

gere Ausdrucksmächtigkeit kann durch den expliziten Bezug zu IT-Systemen sowie die weiter vorangeschrittene Standardisierung je nach Anwendungsfall unterschiedlich stark ins Gewicht fallen. Eine auf WS-\* basierenden Initiative zur Beschreibung von Cloud Service stellt die Software-as-a-Service Description Language (SaaS-DL) dar. SaaS-DL soll insbesondere die Modell-basierte Entwicklung von SaaS-Diensten unterstützen.

### 5.1.13 Web Service Standards (WS-\*)

<b>BASIS- INFORMATION</b>	<b>Status</b>	Veröffentlicht
	<b>Formalisierung</b>	Standard
	<b>Bezug zu CC</b>	Implizit
	<b>Initiator</b>	OASIS, OGF, W3C
	<b>Beteiligte</b>	Diverse
	<b>Link</b>	<a href="http://www.oasis-open.org/">http://www.oasis-open.org/</a> <a href="http://www.w3.org/">http://www.w3.org/</a> <a href="http://www.ogf.org/">http://www.ogf.org/</a>
<b>TAXONOMIE</b>	<b>Ansatzpunkte</b>	<ul style="list-style-type: none"> <li>▪ T – Datei- &amp; Austauschformate</li> <li>▪ T – Protokolle &amp; Schnittstellen</li> </ul>
	<b>Herausforderungen</b>	<ul style="list-style-type: none"> <li>▪ Effizienz</li> <li>▪ Transparenz</li> <li>▪ Informationssicherheit</li> <li>▪ Interoperabilität</li> </ul>
<b>GELTUNGS- BEREICH</b>	<b>Service-Modell</b>	Alle
	<b>Nutzergruppe</b>	Alle
	<b>Branche</b>	Übergreifend
	<b>Deployment</b>	Alle
	<b>Geographie</b>	Global
	<b>Unternehmensgröße</b>	Alle
<b>BEWERTUNG</b>	<b>Reifegrad</b>	Produkt
	<b>Durchsetzungsfähigkeit</b>	Mittel
	<b>Partizipationsmöglichkeit</b>	Je nach Standardisierungsorganisation
<b>ÄHNLICHE STANDARDS</b>		--

**Kurz-Charakterisierung:** Web Services sind eine Technologie zur Umsetzung von Service-orientierten Architekturen. Historisch wurde die Entwicklung von Web Services von der Notwendigkeit zur losen Kopplung von verteilten Systemen über bspw. Unternehmensgrenzen getrieben. Vorherrschende Technologien (bspw. CORBA) resultierten bis dahin in enger Verzahnung von Objektmodellen. Die Sicherstellung von Interoperabilität gestaltete sich deshalb mühsam. Web Services traten in diese Lücke und ermöglichen das nötige Maß an Interoperabilität durch lose Kopplung auf Grundlage von Internet-standards wie HTTP, URI, MIME und XML. Durch die Einführung der Web Service Description Language (WSDL) wird die Abstraktion der tatsächlich zur Implementierung verwendeten Technologie sichergestellt.

Im Laufe der Verbreitung von Web Services wurde eine Reihe von Standards zur Erweiterung der Technologie erarbeitet. So existieren Standards zur Beschreibung von Web Services (WS-Policy), zur Sicherstellung von Dienstgüteanforderungen (WS-Agreement, WS-AtomicTransaction, WS-Business Activity, WS-ReliableMessaging, WS-Security) und zur Unterstützung der Kompo-



sition von Diensten (BPEL, WS-Coordination).<sup>100</sup> Web Service Standards lassen sich dabei modular kombinieren und entsprechend ihres Fokus in der sogenannten „Web Service Plattform Architecture“ einordnen.

Die Entwicklung der Standards erfolgte dabei nicht koordiniert durch eine zentrale Stelle. Vielmehr konkurrierten unterschiedlichen Standardisierungsorganisationen bei der Standardgestaltung bevor die Standardisierung überwiegend durch das W3C und OASIS konsolidiert wurde. Einen Ausdruck dieser Entwicklung stellt auch die Gründung der „Web Service Interoperability Organization“ dar. Diese fördert durch die Spezifikation von Web Service Profilen und die Bereitstellung von Testwerkzeugen die Interoperabilität von Web Service Standards.<sup>101</sup> So existieren derzeit bspw. das „WS-I Basic Profile“<sup>102</sup>, „WS-I Basic Security Profile“<sup>103</sup> zur Sicherung von Web Services, „WS-I Reliable Secure Profile“<sup>104</sup> zur Gewährleistung der Zuverlässigkeit und Sicherheit der Kommunikation sowie das Transport-orientierte „Simple SOAP Binding Protocol“<sup>105</sup>.

**Bewertung:** Web Service Standards sind vielfältig im Einsatz. Der Reifegrad ist allgemein als Produktreif zu bewerten. Die Akzeptanz von Web Service Standards für den Einsatz Cloud Computing ist jedoch vielfältig durch den erzeugten Mehraufwand des Einsatzes gehemmt. Hierzu trägt auch die Konkurrenz der REST-basierten Kommunikation von Diensten bei, die leichtgewichtiger ist, aber weniger Garantien, z.B. zur Dienstgüte, bieten kann. Es lassen sich erste Initiativen beobachten, die Konzepte und Lösungen bspw. zur Sicherstellung von Dienstgüteanforderungen auf REST-basierte Protokolle & Schnittstellen übertragen.<sup>106</sup> Die Durchsetzungsfähigkeit von WS-\* wird für Cloud Computing entsprechend auf einem mittleren Niveau eingestuft. Die Möglichkeiten der Partizipation zur Gestaltung von Web Service Standards

---

<sup>100</sup> Neben der hier genannten Auswahl von Web Service Standards existieren weitere Spezifikationen. Eine weiterführende Diskussion der jeweiligen Spezifikationen und deren Zusammenspiel ist nicht Aufgabe dieser Studie. Hierfür wird auf die existierende Fachliteratur verwiesen.

<sup>101</sup> Seit Ende 2010 werden die Aktivitäten der Web Service Interoperability Organization durch die OASIS weiter geführt.

<sup>102</sup> „WS-I Basic Profile“ beschreibt das Zusammenspiel von WSDL, UDDI, WS-Addressing sowie binären Dateianhängen (vgl. <http://ws-i.org/Profiles/BasicProfile-2.0-2010-11-09.html>).

<sup>103</sup> „WS-I Basic Security Profile“ baut auf „WS-I Basic Profile“ auf und beschreibt das Zusammenspiel dieser Standards und WS-Security (vgl. <http://www.ws-i.org/Profiles/BasicSecurityProfile-1.1.html>).

<sup>104</sup> „WS-I Reliable Secure Profile“ beinhaltet Vorgaben zur Sicherstellung der Interoperabilität beim Einsatz von WS-ReliableMessaging und WS-SecureConversation (vgl. <http://www.ws-i.org/Profiles/ReliableSecureProfile-1.0-2010-11-09.html>).

<sup>105</sup> „Simple SOAP Binding Protocol“ macht Vorgaben zur Verwendung von SOAP als Transportprotokoll für WSDL-basierte Web Services (vgl. <http://www.ws-i.org/Profiles/SimpleSoapBindingProfile-1.0.html>).

<sup>106</sup> Die OGF diskutiert bspw. über eine REST-basierte Variante für WS-Agreement (vgl. [http://ogf.org/gf/event\\_schedule/materials.php?event\\_id=19](http://ogf.org/gf/event_schedule/materials.php?event_id=19)).



sind abhängig von der jeweils verantwortlichen Standardisierungsorganisation und entsprechend als offen bzw. eingeschränkt zu bewerten. Die Übertragung von Web Service Standards auf REST-basierte Schnittstellen befindet sich erst in den Anfängen. Hier sind vielfältige, informelle Beiträge in unterschiedlichen Gremien möglich.<sup>107</sup>

**Ähnliche Standards:** Neben den bereits beschriebenen Bezügen zu verwandten Technologien und der dort vorhandenen Standards sind keine ähnlichen Standards bekannt.

## 5.2 Steckbriefe aus dem Bereich „Management“

### 5.2.1 Eckpunktepapier Sicherheitsempfehlungen für Cloud Computing Anbieter (BSI-ESCC)

BASIS- INFORMATION	Status	Veröffentlicht
	Formalisierung	Orientierungswissen
	Bezug zu CC	Explizit
	Initiator	BSI
	Beteiligte	--
TAXONOMIE	Link	<a href="https://www.bsi.bund.de/ContentBSI/Presse/Pressemitteilungen/Presse2011/Mindestanforderungen-Cloud-Computing-Dienste_10052011.html">https://www.bsi.bund.de/ContentBSI/Presse/Pressemitteilungen/Presse2011/Mindestanforderungen-Cloud-Computing-Dienste_10052011.html</a>
	Ansatzpunkte	<ul style="list-style-type: none"> <li>▪ T – Standardkomponenten &amp; Referenzarchitekturen</li> <li>▪ M – Leitfäden, etc.</li> </ul>
	Herausforderungen	<ul style="list-style-type: none"> <li>▪ Informationssicherheit</li> <li>▪ Datenschutz</li> </ul>
GELTUNGS- BEREICH	Service-Modell	Alle
	Nutzergruppe	Alle
	Branche	Übergreifend
	Deployment	Private/ Public/ Alle
	Geographie	DE
	Unternehmensgröße	Alle
BEWERTUNG	Reifegrad	Mittel
	Durchsetzungsfähigkeit	Gering
	Partizipationsmöglichkeit	--
ÄHNLICHE STANDARDS		--

**Kurz-Charakterisierung:** Das vom Bundesamt für Sicherheit in der Informationstechnik erarbeitete Eckpunktepapier „Sicherheitsempfehlungen für Cloud Computing Anbieter“ (BSI-ESCC) beschreibt Mindestanforderungen zur Informationssicherheit für Cloud-Dienste. Das Papier beschreibt konkrete Empfehlung, die nationalen und internationalen Geltungsanspruch besitzen. Sie wollen als Diskussionsgrundlage verstanden werden und sind als solche erweiterbar und erlauben Veränderungen, wenn die Gegebenheiten dies erfordern. Wo existent stützt sich das BSI-ESCC bei der Anwendung auf internationale Standards. Das angewandte Verständnis von Cloud Computing ist eng an die Vorgaben der NIST angelehnt.

Das Kernstück des BSI-ECC stellt die Bewertung identifizierter Herausforderungen und Empfehlungen zu Adressierung dieser durch die Cloud-Anbieter dar. Im Ergebnis soll die Sicherheit von Cloud-Diensten zu erhöht bzw. lang-

<sup>107</sup> Siehe Fußnote 106.

fristig gewährleistet werden. Dabei werden elf Sicherheitsbereiche unterschieden: Sicherheitsmanagement beim Anbieter, Sicherheitsarchitektur, ID- und Rechtemanagement, Kontrollmöglichkeiten durch den Nutzer, Monitoring, Notfallmanagement, Portabilität und Interoperabilität, Sicherheitsprüfung und -nachweis, Anforderungen an das Personal, Vertragsgestaltung und schließlich Datenschutz und Compliance.

Das Papier diskutiert für jeden Bereich mögliche Schutzmaßnahmen, die Cloud-Anbieter umsetzen sollten, um die Sicherheit im Cloud Computing sicherzustellen. Die Priorisierung der Schutzmaßnahmen erfolgt anhand von drei Kategorien: Basisanforderungen (B), Daten mit hohen Vertraulichkeitsanforderungen (C+, engl. „confidentiality“) und Daten, die eine hohe Verfügbarkeit (A+, engl. „availability“). Das BSI-ESCC bewertet die Anforderungen von Private und Public Clouds dabei unterschiedlich.

**Bewertung:** Die Bewertung des Reifegrads, der Durchsetzungsfähigkeit sowie der Partizipationsmöglichkeiten bei Leitfäden wird grundsätzlich als nur mäßig zielführend eingeschätzt. Dies liegt in der Natur dieser Dokumente begründet. Einerseits stellen Leitfäden häufig eine initiale Bestandsaufnahme von Anforderungen und ersten Lösungsideen dar, die Naturgemäß nur einen oberflächlichen Charakter besitzen. Gleichzeitig ist die Einschätzung der Durchsetzungsfähigkeit auf Grund der häufig vorhandenen Vielzahl an Leitfäden schwierig. Auch ist zu einem späteren Zeitpunkt nicht mit Sicherheit festzustellen, welche Maßnahmen auf Grundlage welches Leitfadens umgesetzt wurden. Schließlich stellen Leitfäden im Moment der Veröffentlichung meist abgeschlossene Projekte dar, die in der Regel nicht mehr weiterentwickelt werden. Dennoch wird der Reifegrad des BSI-ESCC auf mittlerem Niveau eingestuft, was in der umfangreichen Erhebung und dem methodischen Vorgehen begründet liegt.

**Ähnliche Standards:** In der Kategorie der Leitfäden mit überwiegendem Fokus auf Ansatzpunkte aus dem Bereich des Managements existieren eine Reihe weiterer Empfehlungen. So beschreibt der von EuroCloud veröffentlichte Leitfaden LRD&C Anforderungen zum Datenschutz, Risikomanagement und Compliance. In diese Kategorie fallen auch WAPBP und CSA. Grundsätzliche Fragen zu Schutzniveaus von IT-Systemen werden bspw. in ISO27001 definiert.

### 5.2.2 EuroCloud Star Audit (EuroCloud-SA)

<b>BASIS- INFORMATION</b>	<b>Status</b>	Veröffentlicht
	<b>Formalisierung</b>	Zertifizierung
	<b>Bezug zu CC</b>	Explizit
	<b>Initiator</b>	EuroCloud
	<b>Beteiligte</b>	> 100
	<b>Link</b>	<a href="http://www.eurocloud.de">http://www.eurocloud.de</a>
<b>TAXONOMIE</b>	<b>Ansatzpunkte</b>	▪ M – Leitfäden
	<b>Herausforderungen</b>	<ul style="list-style-type: none"> <li>▪ Effizienz</li> <li>▪ Effektivität</li> <li>▪ Transparenz</li> <li>▪ Informationssicherheit</li> <li>▪ Datenschutz</li> <li>▪ Portabilität</li> <li>▪ Compliance</li> </ul>
<b>GELTUNGS- BEREICH</b>	<b>Service-Modell</b>	SaaS
	<b>Nutzergruppe</b>	Anbieter
	<b>Branche</b>	Übergreifend
	<b>Deployment</b>	Public
	<b>Geographie</b>	EU, DE
	<b>Unternehmensgröße</b>	Alle
<b>BEWERTUNG</b>	<b>Reifegrad</b>	Mittel
	<b>Durchsetzungsfähigkeit</b>	Mittel
	<b>Partizipationsmöglichkeit</b>	Hoch
<b>ÄHNLICHE STANDARDS</b>		EuroPriSe, TiC

**Kurz-Charakterisierung:** Ziel der EuroCloud Star Audit Zertifizierung ist die Schaffung einer Orientierungs- und Entscheidungshilfe bei der Auswahl von SaaS Angeboten für Cloud-Anwender. Hierzu erarbeitete EuroCloud eine Reihe von Fragebögen, welche die Bewertung der von Cloud-Anbietern eingesetzten Maßnahmen zum Betrieb und der Bereitstellung von SaaS-Angeboten ermöglichen sollen. Grundlage für den Zertifizierungskatalog stellen die unter anderem im BSI-ESCC und ENISA-Report identifizierte Risiken des Cloud Computing dar.

Die „EuroCloud Star Audit SaaS“-Zertifizierungen sind modular aufgebaut und unterscheiden sich nach der Art der Leistung, die zu zertifizierende Unternehmen erbringen. So können Rechenzentrums-Betreiber das sogenannte „EuroCloud Star Audit SaaS Ready“ erhalten. Dieses stellt gleichzeitig die Grundlage für die Zertifizierung von Anbieter von Cloud-Diensten im Rahmen der Zertifizierung „EuroCloud Star Audit SaaS App“. Werden Cloud-Dienste aus einer Hand angeboten, können beide Zertifizierung zur „EuroCloud Star Audit SaaS“ kombiniert werden.

Untersuchungsgegenstände bei der Auditierung sind Vertragswerke im Hinblick auf Compliance-Anforderungen, eingesetzte Rechenzentrumsinfrastrukturen, Maßnahmen zum Datenschutz und zur Datensicherheit, Betriebsprozesse zur Sicherstellung von Verfügbarkeit und Notfallmanagement sowie die Risikobewertung von Implementierungsdetails (Schnittstellen, Konzepte, Support) der SaaS-Dienste.

Für jede Zertifizierung ist die Tiefe in den drei Stufen „Trusted Cloud Service (3 Sterne)“, „Trusted Cloud Service Advanced (4 Sterne)“ und „Trusted Cloud Service Advanced High Availability (5 Sterne)“ wählbar. Mit steigender Tiefe der Zertifizierung soll die Vertrauenswürdigkeit eines Cloud-Dienstes gestei-

gert werden. Auf Seiten des Zertifikatsempfängers steigen mit der Tiefe der Zertifizierung auch die Kosten.

Die Zertifizierung erfolgt entsprechend eines Lizenzierungsmodells. Zertifikate sind 24 Monaten gültig. Durch ein sogenanntes Rezertifizierungsverfahren können Zertifikate in einem vereinfachten Prozess erneut zertifiziert werden. Sollten sich auf Grund von neuen technischen, wirtschaftlichen oder rechtlichen Rahmenbedingungen neuartige Risiken des Cloud Computing ergeben, können die Fragebogen angepasst werden. Im Rahmen des Rezertifizierungsverfahrens ist stets der aktuelle Fragebogenkatalog für die Zertifizierung maßgeblich. Die Auditierung soll durch unabhängige Auditoren, die Experten im jeweiligen Bereich sind, durchgeführt werden. Hierdurch soll unter anderem die Objektivität und Neutralität gewährleistet sein.

**Bewertung:** Der breit angelegte Umfang der EuroCloud-Zertifizierungen verspricht einen großen Beitrag bei der Vertrauensbildung. Gleichzeitig stellt er jedoch eine Herausforderung bei der Gestaltung nachvollziehbarer Bewertungskriterien. Aus Sicht der Cloud-Anwender sind diese notwendig, um verstehen zu können, welche Risiken durch die Zertifizierung reduziert werden. Im derzeitigen Stand der Standardisierung ist dies noch nicht durchgehend gewährleistet. Darüber hinaus bleibt unklar, wie die Zertifizierung von Rechenzentrums- und Cloud-Anbietern in Zusammenhang mit den von ihnen angebotenen Diensten steht. Fraglich bleibt, wie innerhalb der 24-Monate während der Zertifizierung mit neuen Releases umgegangen wird, wenn bspw. eine „EuroCloud Star Audit SaaS App“-Zertifizierung erfolgte. Entsprechend wird dem „EuroCloud Star Audit SaaS“ ein mittleres Reifenniveau zugeordnet.

Grundsätzlich ist die Nachfrage nach Zertifizierungen zum Aufbau von Vertrauen und Sicherheit im Cloud Computing groß. „EuroCloud Star Audit SaaS“ stellt einen ersten Vorschlag für ein solches Zertifikat dar, das sich derzeit noch in einer Erprobungsphase befindet. Bislang sind nur wenige prominente Cloud-Anbieter zertifiziert. Die potenzielle Durchsetzungsfähigkeit wird daher ebenfalls auf einem mittleren Niveau eingestuft. Insbesondere wird sich erst künftig zeigen, inwiefern das definierte Lizenz- und Preismodell für kleine und mittelständige Unternehmen passend ist.

Die Partizipationsmöglichkeit an der Weiterentwicklung der Zertifikate ist im Rahmen einer EuroCloud-Mitgliedschaft möglich und daher als „hoch“ zu bewerten.

**Ähnliche Standards:** Zertifikate können einen wichtigen Beitrag für die Vertrauensbildung bspw. durch die Erleichterung der Risikoeinschätzung im Cloud Computing haben. Jedoch existieren bislang nur wenige Zertifizierungsansätze.

Im Rahmen der von SaaS-Ecosystem getriebenen „Trust-in-Cloud“-Initiative wurde ebenfalls eine Check-Liste zum Vergleich unterschiedlicher Cloud-Angebote erarbeitet. Darauf aufbauend können Cloud-Dienste zertifiziert werden. Dies geschieht ebenfalls auf Basis eines jährlichen Lizenzmodells. Der Fokus auf Cloud-Dienste unterscheidet Trust-In-Cloud vom Anbieterorientierten Zertifikat „EuroCloud Star Audit SaaS“.

Das „EuroPriSe European Privacy Seal“ hat keinen spezifischen Fokus auf Cloud Computing, stellt aber einen ersten Standard für die Zertifizierung der Einhaltung der Europäischen Datenschutzrichtlinien dar. Ähnlich zum Vorgehen bei „Trust-in-Cloud“ liegt auch hier der Fokus der Zertifizierung auf individuellen Cloud Angeboten. Das „EuroPriSe European Privacy Seal“ kann ergänzend zu den „EuroCloud Star Audit SaaS“- oder „Trust-in-Cloud“-Zertifikaten eingesetzt werden.

### 5.2.3 Governance, Risk Management and Compliance Stack (GRC Stack)

<b>BASIS- INFORMATION</b>	<b>Status</b>	In Arbeit
	<b>Formalisierung</b>	Orientierungswissen
	<b>Bezug zu CC</b>	Explizit
	<b>Initiator</b>	CSA
	<b>Beteiligte</b>	> 100
	<b>Link</b>	<a href="https://cloudsecurityalliance.org/research/initiatives/grc-stack/">https://cloudsecurityalliance.org/research/initiatives/grc-stack/</a>
<b>TAXONOMIE</b>	<b>Ansatzpunkte</b>	<ul style="list-style-type: none"> <li>▪ M – Managementmodelle &amp; -prozesse</li> <li>▪ M – Leitfäden</li> </ul>
	<b>Herausforderungen</b>	<ul style="list-style-type: none"> <li>▪ Effizienz</li> <li>▪ Effektivität</li> <li>▪ Informationssicherheit</li> <li>▪ Compliance</li> </ul>
<b>GELTUNGS- BEREICH</b>	<b>Service-Modell</b>	Alle
	<b>Nutzergruppe</b>	Alle
	<b>Branche</b>	Übergreifend
	<b>Deployment</b>	Alle
	<b>Geographie</b>	Global
	<b>Unternehmensgröße</b>	Alle
<b>BEWERTUNG</b>	<b>Reifegrad</b>	Gering
	<b>Durchsetzungsfähigkeit</b>	Mittel
	<b>Partizipationsmöglichkeit</b>	Mittel
<b>ÄHNLICHE STANDARDS</b>		CloudAudit, CCM, CAIQ, CTP, LRD&C

**Kurz-Charakterisierung:** Das von der Cloud Security Alliance erarbeitete Rahmenwerk für Governance, Risk Management und Compliance (GRC) bildet einen übergeordneten Rahmen (engl. „stack“) für die zunächst eigenständigen Entwicklungen der Komponenten der Cloud Controls Matrix (CCM), dem damit eng verbundenen Cloud Consensus Assessments Initiative Questionnaire (CAIQ), und Cloud Audit.<sup>108</sup> Der weiteren Verzahnung der drei Initiativen dient das Cloud Trust Protocol (CTP).<sup>109</sup>

In der Gesamtheit der Spezifikationen beinhaltet der GRC-Stack Bewertungskriterien und Kontrollziele sowie entsprechende Schnittstellen zum Abruf der für das angestrebte, effektive Management von Cloud Services benötigten Da-

<sup>108</sup> Auf Grund der ursprünglichen Eigenständigkeit der Cloud Audit Bemühungen sowie des klaren technischen Fokus der bisherigen Dokumente zum Standard wird Cloud Audit im Rahmen der technischen Standards separat behandelt (vgl. Abschnitt 5.1.3).

<sup>109</sup> Neben der bereits separat beschriebenen Technischen Aspekte des Cloud Trust Protocol (vgl. hierzu Kapitel 5.1.4 wird in diesem Abschnitt insbesondere der Beitrag von CTP zur Standardisierung des Managements von Cloud Service betrachtet.

ten.<sup>110</sup> Die Auswahl der vorgeschlagenen Bewertungskriterien und Kontrollziele basiert auf der Analyse bewährter Best Practices, Standards und allgemeingültiger Richtlinien zum Management von IT-Systemen. Der Einsatzbereich des GRC Stacks umfasst bewusst sowohl Anbieter wie Nutzer von Cloud-Diensten. Eine Unterscheidung der Anwendbarkeit zwischen den Cloud-Servicekategorien (d.h. IaaS, PaaS, SaaS) wird im GRC-Stack nicht vorgenommen. Nachfolgend werden die managementorientierten Bestandteile des GRC Stacks – also. CCM und CAIQ – in einem kurzen Überblick dargestellt.

Die *Cloud Control Matrix (CCM)* stellt ein Rahmenwerk zur Bewertung des Risikos von Cloud Anbietern zur Verfügung. Dabei werden für das Management von Cloud Diensten relevante Herausforderungen „Steuerungsbereiche“ (engl. „control areas“) identifiziert und Empfehlungen zur Ausübung der Steuerung (engl. „control specification“) dargestellt.<sup>111</sup> Dazu wurden und werden in Zukunft allgemeine Rahmenwerke für das Management von IT-Systemen (wie bspw. COBIT 4.1, HIPAA, ISO 27001, NIST SP800) auf einen möglichen Beitrag zum Management von Cloud Diensten untersucht und nach Anwendbarkeitsbereichen (bspw. IaaS, PaaS, SaaS oder Anwender und Anbieter) klassifiziert.<sup>112</sup> Im Ergebnis bietet CCM Anbietern von Cloud-Diensten eine Möglichkeit der standardisierten Schwachstellenanalyse der Organisation und Infrastruktur zum Betrieb der eigenen Cloud Serviceangebote bspw. in den Bereichen Release Management, Sicherheitsarchitektur sowie der Gestaltung des operativen Betriebs durch Unternehmenspolicies, Dokumentationen oder Ressourcenplanung. Für Nutzer von Cloud-Diensten stellt CCM ein Rahmenwerk zur Analyse der durch den Provider zugesicherten Sicherheitsgarantien auf einheitliche Weise dar.

Passend zu den in CCM definierten Steuerungsbereichen stellt die CSA mit dem Consensus Assessments Initiative Questionnaire (CAIQ) einen Fragebogen zur Durchführung der Schwachstellenanalyse bereit.<sup>113</sup> Darin wird für jede in CCM vorgegebenen Steuerungsbereich eine Entscheidungsfrage zugeordnet. Für den Fall einer negativen Bewertung gibt CCM zudem Hilfestellungen zur Behebung der identifizierten Unzulänglichkeiten.

**Bewertung:** Der Bewertung des GRC Stacks liegen die Analyse der einzelnen Komponenten sowie die Bewertung des Rahmenwerks zugrunde. Die Reife der vorliegenden Dokumente wird insgesamt als gering bewertet. Hervorzu-

---

<sup>110</sup> Im Rahmen der Studie wurden die technischen Aspekte, die durch CloudAudit und CTP abgedeckt werden bereits in eigenständigen Kapiteln dargestellt (vgl. Kapitel 5.2.2 und 5.1.4). Hier werden nun die Managementaspekte fokussiert.

<sup>111</sup> In der zum Zeitpunkt der Studienerstellung aktuellen Fassung vom 26.08.2011 (Version 1.2) werden insgesamt 98 Steuerungsbereiche aufgeführt.

<sup>112</sup> Siehe hierzu [https://cloudsecurityalliance.org/wp-content/uploads/2011/03/CSA-CAIQ-Question-Set-v1-1\\_FINAL\\_v6.xlsx](https://cloudsecurityalliance.org/wp-content/uploads/2011/03/CSA-CAIQ-Question-Set-v1-1_FINAL_v6.xlsx).

<sup>113</sup> Durch die Abhängigkeit der Anwendung von CAIQ und CCM ist stets darauf zu achten das beide in derselben Versionsnummer verwendet werden.



heben ist der fortgeschrittene Arbeitsstand zur Analyse der Cloud Controls Matrix, welcher jedoch noch wenige Hinweise zur Anwendung der CCM oder CAIQ vorgibt.<sup>114</sup> Die Möglichkeit einer potentiellen Durchsetzung des GRC Stacks bis zur Marktadoption wird als mittel bewertet. Positiv für einen möglichen Erfolg des Standards wirkt sich die hohe Anzahl an namhaften Unterstützern für den GRC Stack aus. Gleichzeitig bleiben inhaltlich Fragen zur Konzeption des Stacks sowie der einzelnen Komponenten. Auf Grund der noch früheren Standardisierungsphase sind für beide teils nur Entwurfsdokumente verfügbar. Die Möglichkeit der Partizipation am weiteren Standardisierungsprozess ist als „mittel“ einzustufen, da eine Mitgliedschaft bei der CSA vorausgesetzt wird. Darüber hinaus ist derzeit nicht offensichtlich, wie Entscheidungsprozesse geregelt sind.

**Ähnliche Standards:** In Zielsetzung und Umfang wurden im Rahmen der Studie keine ähnlichen Standards oder Standardisierungsbestrebungen identifiziert. Es wird nochmals darauf hingewiesen das der GRC Stack aus den vier ursprünglich eigenständigen Standardinitiativen Cloud Audit, CCM, CAIQ und CTP hervorging.

#### 5.2.4 NIST Cloud Computing Use Cases (NIST-UC)

BASIS- INFORMATION	Status	In Arbeit
	Formalisierung	Orientierungswissen
	Bezug zu CC	Explizit
	Initiator	NIST
	Beteiligte	--
	Link	<a href="http://www.nist.gov/itl/cloud/use-cases.cfm">http://www.nist.gov/itl/cloud/use-cases.cfm</a>
TAXONOMIE	Ansatzpunkte	▪ M – Leitfäden
	Herausforderungen	▪ Effektivität ▪ Transparenz ▪ Informationssicherheit ▪ Datenschutz ▪ Interoperabilität
GELTUNGS- BEREICH	Service-Modell	Alle
	Nutzergruppe	Alle
	Branche	Öffentlicher Sektor
	Deployment	Public
	Geographie	USA
	Unternehmensgröße	Alle
BEWERTUNG	Reifegrad	Gering
	Durchsetzungsfähigkeit	Hoch
	Partizipationsmöglichkeit	Keine/gering
ÄHNLICHE STANDARDS		OGF-UC, DMTF-UC, CCUCDG-1, CCUCDG-2

**Kurz-Charakterisierung:** Das NIST veröffentlichte im Mai 2010 die Cloud Computing Use-Cases (NIST-UC). Darin werden Anforderungen an Cloud-Dienste anhand von Anwendungsfällen beschrieben. Diese Anwendungsfälle sollen künftig als Grundlage zur Evaluation des Einsatzes von Cloud-Diensten in US-Behörden dienen.

<sup>114</sup> Eine Analyse der Standards Cloud Audit und CTP findet sich in den Kapiteln 5.2.2 und 5.1.4.

Jeder Anwendungsfall wird einheitlich, anhand folgender Struktur beschrieben: Zunächst wird angegeben, welche der möglichen zwölf Akteure<sup>115</sup> im Anwendungsfall beteiligt sind, welche Ziele erreicht werden sollen und welche Annahme (bspw. zur Systemkonfiguration) dem jeweiligen Anwendungsfall zu Grunde liegen. Darauf aufbauend werden sogenannte Erfolgsszenarien und damit verbunden Interaktionen zwischen den Akteuren beschrieben. Dabei werden ausdrücklich auch mögliche Fehler und das gewünschte Verhalten der Cloud-Dienste im Fehlerfall beschrieben. So darf bspw. kein Nutzer angelegt werden, falls keine korrekten Zahlungsinformationen bei der Erstellung eines Nutzerkontos angegeben wurden. Die Beschreibung eines Anwendungsfalls kann durch Anhängen zusätzlicher Anforderungsdateien vervollständigt werden.

Insgesamt werden durch das NIST 24 Anwendungsfälle für den Einsatz von Cloud Computing in der öffentlichen Verwaltung aufgeführt. Diese lassen sich in vier Themengebieten klassifizieren:

Im Bereich des *Cloud-Dienstmanagements* werden bspw. Anwendungsfälle zum Verwaltung von Benutzerkonten dokumentiert. Darüber hinaus werden Anforderungen zum Transport von Daten in bzw. aus der Cloud, zum Löschen von Daten, zum Management von IaaS-Diensten oder zur Abfrage der durch Cloud-Dienste unterstützten Funktionalitäten beschrieben.

Der zweite Themenbereich beschreibt Anforderungen in Bezug auf *Interoperabilität*. Darin werden bspw. Funktionen zum Transport von Daten zwischen Cloud-Anbietern oder zur Migration von Warteschlangen-basierten Anwendungen in die Cloud gefordert. Zusätzlich fällt die Beschreibung von Anforderung hinsichtlich der erforderlichen Portabilität von Daten und Diensten unter den Bereich Interoperabilität.

Die Anwendungsfälle im Bereich *Cloud Sicherheit* beschreiben Szenarien zum Identitätsmanagement, zur Überwachung der Sicherheit und zur Regelung der Datenfreigabe zu Gunsten Dritter.

Der letzte Themenbereich gibt einen Ausblick auf künftige, *komplexere Anwendungsfälle* im Cloud Computing. Dies beinhaltet Cloud Management Broker, die Unterstützung von Eigentumsübergängen eines Datums zwischen Cloud-Anwendern innerhalb einer Cloud sowie Aspekte der Fehlertoleranz.

**Bewertung:** Das NIST beschreibt alle Anwendungsfälle einheitlich gemäß der skizzierten Vorlage. Jedoch erscheint die Auswahl der einzelnen Anwendungsfälle und bspw. dort möglicher Fehler als pragmatisch. Eine Information zur Vollständigkeit der ausgewählten Anwendungsfälle fehlt. Der Reifegrad wird daher als gering eingestuft. Die Durchsetzungsfähigkeit wird jedoch als hoch eingestuft. Dies liegt darin begründet, dass zu erwarten ist, dass

---

<sup>115</sup> Die zwölf möglichen Akteure im Cloud Computing gemäß NIST-UC lauten: unidentified-user, cloud-subscriber, cloud-subscriber-user, cloud-subscriber-administrator, cloud-user, payment-broker, cloud-provider, transport-agent, legal-representative, identity-provider, attribute-authority, cloud-management-broker.

das NIST die beschriebenen Anwendungsfälle zur Bewertung von Cloud-Diensten für den Einsatz in US-Behörden verwenden will. Dies erfordert von allen potenziellen Cloud-Anbietern, die Abdeckung dieser Anwendungsfälle. Eine Partizipationsmöglichkeit bei der Weiterentwicklung der Standards ist nicht möglich, da Anforderungen aus Sicht der US-Behörden beschrieben werden.

**Ähnliche Standards:** Neben den durch das NIST beschriebenen Anwendungsfällen existieren weitere Kataloge zur Beschreibung des Einsatzgebiet von Cloud-Computing in Organisationskontexten. So erarbeiteten die DMTF und die OGF ebenfalls Use-Case-Dokumente zur Beschreibung von Einsatzszenarien des Cloud Computing. Auch die Cloud Computing Use Case Group hat Anwendungsfälle für Cloud Computing erarbeitet (vgl. CCUCDG-1 und CCUCDG-2).

### 5.2.5 Statement on Standards for Attestation Engagements No. 16 (SSAE 16)

BASIS- INFORMATION	Status	Veröffentlicht
	Formalisierung	Zertifizierung
	Bezug zu CC	Implizit
	Initiator	AICPA
	Beteiligte	Personengebunden
	Link	www.ssae16.com
TAXONOMIE	Ansatzpunkte	<ul style="list-style-type: none"> <li>▪ M – Managementmodelle &amp; -prozesse</li> <li>▪ M – Controllingmodelle &amp; -prozesse</li> </ul>
	Herausforderungen	▪ Informationssicherheit
GELTUNGS- BEREICH	Service-Modell	Alle
	Nutzergruppe	Alle
	Branche	Übergreifend
	Deployment	Public
	Geographie	Global
	Unternehmensgröße	Großunternehmen
BEWERTUNG	Reifegrad	Mittel bis hoch
	Durchsetzungsfähigkeit	Mittel
	Partizipationsmöglichkeit	Mittel
ÄHNLICHE STANDARDS		CobiT, BSI-100 Standardfamilie, ISAE 3402, ISO 27001, IDW PS 330, IDW PS 951, IDW RS FAIT1, ITIL, SAS 70, CloudAudit

**Kurz-Charakterisierung:** Das „Statement on Standards for Attestation Engagements No. 16 (SSAE 16)“ beschreibt einen Standard zur Berichterstattung über interne Kontrollsysteme von Dienstleistungsunternehmen durch Auditoren. Die Durchführung einer SSAE 16 Auditierung ermöglicht Dienstleistungsunternehmen, den Nachweis der Angemessenheit und Wirksamkeit des im Unternehmen eingesetzten internen Kontrollsystems. SSAE 16 ersetzt das bisherige „Statement on Auditing Standards No. 70 (SAS 70)“, um die internationale Reichweite der Berichtsstandards zu vergrößern.<sup>116</sup> Beide werden

<sup>116</sup> Eine detaillierte Diskussion der Unterschiede und Gemeinsamkeiten zwischen SSAE 16 und SAS 70 ist nicht im Fokus dieser Studie. In diesem Zusammenhang wird auf die unter [www.ssae16.com](http://www.ssae16.com) und [www.sas70.com](http://www.sas70.com) verfügbaren Dokumente hingewiesen. Mit Einführung von SSAE 16 wurde auch das internationale Äquivalent „International Standards for Assurance Engagements (ISAE) No. 3402 (ISAE 3402)“ eingeführt.

bzw. wurden vom „American Institute of Certified Public Accountants (AICPA)“ erarbeitet und weiterentwickelt.

Bei der Durchführung eines Audits der internen Kontrollsysteme können Dienstleistungsunternehmen SSAE 16 zwischen einem Typ1- oder Typ2-Nachweis wählen.<sup>117</sup> Bei Typ1-Auditierungen wird auf Basis der Dokumentation der internen Mechanismen die Ist-Situation der internen Kontrollsysteme dokumentiert. Hierzu wird geprüft, ob das Management grundsätzlich in der Lage ist Risiken für den laufenden Betrieb zu erkennen und Gegenmaßnahmen zur Verfügung stehen. Bei Typ2-Prüfungen erfolgt eine Beurteilung zur Effektivität der aus Typ1 bekannten internen Kontrollen. Die Kontrollmechanismen dürfen dabei auch manuell ausgeführt werden. Komplettiert werden Typ2-Auditierungen durch Einschätzung des Auditors zur Wirksamkeit der getesteten Kontrollen.

Im Ergebnis sollen SSAE 16 Auditierungen die Zuverlässigkeit und Sicherheit im Umgang mit ausgelagerten Daten und Geschäftsprozessen nachweisen. SSAE 16 wurde ursprünglich für den Einsatz in typische Outsourcing-Szenarien entwickelt. Die Möglichkeit zur Erschaffung einer Vertrauensbasis zwischen Cloud-Anbietern und Cloud-Nutzer kann jedoch auch einen Beitrag im Cloud Computing leisten. Dies bestätigten auch die erst kürzlich erfolgten SSAE 16 bzw. SAS 70 Auditierungen großer Cloud-Anbieter wie bspw. Amazon Web Services, Google, Microsoft Azure oder Rackspace.

**Bewertung:** Der Reifegrad des SSAE 16 Prüfstandards wird grundsätzlich als hoch eingestuft. Dies ist auch in der durch SAS 70 vorhandenen Standardhistorie begründet. Die Anwendbarkeit von SSAE 16 im Cloud Computing fußt jedoch auf der Prämisse von Outsourcing-Beziehungen. Diese sind klassisch auf längere Laufzeiten angelegt. Im aktuellen Status bleiben insbesondere Fragen im Hinblick auf die Durchführbarkeit von Audits bei tiefen Lieferketten und sich ständige wechselnden Geschäftsbeziehungen zwischen Cloud-Anbietern. Wie bereits beschreiben, ist eine erste Marktakzeptanz von SSAE 16 insbesondere bei großen Cloud-Anbietern zu beobachten. Speziell bei kleinen und mittelständischen Anbietern ist die Durchsetzungsfähigkeit von SSAE 16 aufgrund der damit verbunden regelmäßigen Kosten jedoch abzuwarten. Im Ergebnis wird für SSAE 16 eine mittlere Durchsetzungsfähigkeit erwartet. Die Partizipation bei der Pflege und Weiterentwicklung von SSAE 16 ist auf Mitglieder der AICPA beschränkt. Es werden persönliche Mitgliedschaften angeboten, deren Beiträge je nach Partizipationsintensität gestaffelt sind. Die Partizipationsmöglichkeit wird auf mittlerem Niveau bewertet.

**Ähnliche Standards:** Neben dem beschriebenen historischen Zusammenhang zwischen SSAE 16 und SAS 70 sowie dem internationalen Pendant „International Standards for Assurance Engagements No. 3402 (ISAE 3402)“ existiert für den deutschsprachigen Raum zudem der vom Institut für Wirtschaftsprüfer herausgegebene Prüfungsstandard zur „Prüfung des internen Kontrollsys-

---

<sup>117</sup> Diese Unterscheidung existierte bereits in SAS 70 und wurde für SSAE 16 übernommen.

tems beim Dienstleistungsunternehmen für auf das Dienstleistungsunternehmen ausgelagerte Funktionen (IDW PS 951)“. Dieser stellt ein auf deutsche Anforderungen angepasstes Abbild von SAS 70 dar. Im weiteren Umfeld der Sicherstellung der Funktionsfähigkeit von IT-Systemen im betrieblichen Einsatz sind insbesondere auch ISO 27001, die BSI-100 Standardfamilie „IT-Grundschatz“, IDW PS 330, IDW RS FAIT 1 sowie CobiT und ITIL zu nennen.<sup>118</sup> Allen ist der fehlende Bezug zu Cloud-spezifischen Anforderungen wie Flexibilität der Ressourceneinbindung oder Skalierbarkeit gemein. Im Rahmen der Prüfung erteilte Zertifikate könnten durch den Einsatz von Cloud Audit standardisiert und automatisiert abgerufen werden. Cloud Audit definiert jedoch keine standardisierten Vorgaben hinsichtlich der Auditierungs- bzw. Zertifizierungsprozesse selbst.

### 5.3 Steckbriefe aus dem Bereich „Recht“

#### 5.3.1 Open Cloud Manifesto (OCM)

BASIS- INFORMATION	Status	Veröffentlicht
	Formalisierung	Industriestandard
	Bezug zu CC	Explizit
	Initiator	- -
	Beteiligte	> 100, bspw. IBM, SAP, Sun, Cisco, ECM.
	Link	<a href="http://www.opencloudmanifesto.org">http://www.opencloudmanifesto.org</a>
TAXONOMIE	Ansatzpunkte	▪ R – Selbstverpflichtungen
	Herausforderungen	▪ Transparenz ▪ Informationssicherheit ▪ Interoperabilität ▪ Portabilität ▪ Wettbewerb
GELTUNGS- BEREICH	Service-Modell	Alle
	Nutzergruppe	Anbieter
	Branche	Übergreifend
	Deployment	Alle
	Geographie	Global
	Unternehmensgröße	Alle
BEWERTUNG	Reifegrad	Gering
	Durchsetzungsfähigkeit	Mittel
	Partizipationsmöglichkeit	Sehr hoch
ÄHNLICHE STANDARDS		- -

**Kurz-Charakterisierung:** Das im März 2009 vorgestellte Open Cloud Manifesto (OCM) beschreibt in einer Selbstverpflichtung die Absicht, Cloud Computing grundsätzlich offen zu gestalten und so bspw. Lock-in Situationen zu vermeiden. Dabei liegt die Vorstellung zu Grunde, dass Cloud Computing ohne das Internet nicht existieren könnten und daher ebenso eine für alle offene Plattform darstellen sollte. OCM definiert sechs grundlegende Prinzipien für offenes Cloud Computing, die Wahlmöglichkeiten, Flexibilität und Agilität für Cloud-Anwender sicherstellen sollen:

<sup>118</sup> Ein detaillierter Vergleich der hier genannten Standards wurde durch das BSI erarbeitet: [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschatz/Hilfsmittel/Do ku/studie\\_ueberblick-standards.pdf](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschatz/Hilfsmittel/Do ku/studie_ueberblick-standards.pdf)

- Cloud-Anbieter müssen zusammenarbeiten, um die Herausforderungen der Verbreitung von Cloud Computing durch offene Kollaboration und den sinnvollen Einsatz von Standards zu treiben.
- Cloud-Anbieter dürfen Ihre Markposition nicht ausspielen, um Cloud-Anwender durch Lock-in Situationen an ihre Plattform zu binden.
- Cloud-Anbieter sollen existierende Standards wann immer sinnvoll anwenden. Doppeltentwicklungen sollen vermieden werden.
- Die Anzahl neuer Cloud-Standards sollte so gering wie möglich gehalten werden.
- Alle Anstrengungen zur Entwicklung einer offenen Cloud sollten von Kundenbedürfnissen getrieben sein und nicht allein durch technische Anforderungen der Cloud-Anbieter motiviert sein.
- Die Cloud Computing Community sollte zusammenarbeiten und sicherstellen, dass Entwicklungsbemühungen nicht überlappen oder gar im Konflikt stehen.

**Bewertung:** Das Open Cloud Manifesto wurde im März 2009 in kurzer Zeit von einem kleinen, ausgewählten Kreis verabschiedet und anschließend weiteren Cloud-Anbietern zur Unterschrift vorgelegt. Konkrete Vorgaben zur Umsetzung einer offenen Cloud werden im OCM nicht getroffen. Unterstützer des OCM verschreiben sich folglich den genannten sechs Prinzipien für offenes Cloud Computing. Der Reifegrad des OCM wird auf Grundlage der fehlenden Präzision der Anforderungen und Mittel für offenes Cloud Computing als gering eingestuft. Die unklaren Verantwortlichkeiten der Weiterentwicklung des OCM, sowie die fehlende Unterstützung von wesentlichen Cloud-Anbietern (bspw. Amazon oder Microsoft) lassen ein mittleres Potenzial zur Durchsetzungsfähigkeit von OCM erkennen. Dazu trägt auch bei, dass es keine Regelungen für Sanktionen bei Verstößen gegen das OCM gibt. Alle Cloud-Anbieter können grundsätzlich als Unterstützer des OCM auftreten, indem sie dieses unterzeichnen. Die Veröffentlichung und Verwendung von OCM erfolgt unter Annahme der Creative Commons Attribution-Share Alike-Lizenz. Die Partizipationsmöglichkeit wird als „sehr hoch“ bewertet. Dabei gilt es zu beachten, dass derzeit keine Organisation die Weiterentwicklung von OCM treibt. Es fehlen daher Strukturen die eine geregelte Partizipation über die Unterstützung hinaus Sicherstellen könnten.

**Ähnliche Standards:** Bisher sind keine weiteren Selbstverpflichtungen bekannt.



### 5.3.2 EU-Richtlinie 95/46/EG „Datenschutzrichtlinie“ (95/46/EG)

BASIS- INFORMATION	Status	Veröffentlicht
	Formalisierung	Rechtliche Vorgabe
	Bezug zu CC	Implizit
	Initiator	EU
	Beteiligte	--
	Link	<a href="http://europa.eu/legislation_summaries/information_society/data_protection/14012_de.htm">http://europa.eu/legislation_summaries/information_society/data_protection/14012_de.htm</a>
TAXONOMIE	Ansatzpunkte	▪ R – Rechtliche Vorgaben
	Herausforderungen	▪ Datenschutz
GELTUNGS- BEREICH	Service-Modell	Alle
	Nutzergruppe	Alle
	Branche	Übergreifend
	Deployment	Alle
	Geographie	EU
	Unternehmensgröße	Alle
BEWERTUNG	Reifegrad	--
	Durchsetzungsfähigkeit	--
	Partizipationsmöglichkeit	Hoch
ÄHNLICHE STANDARDS		2001/497/EG, 2002/16/EG, 2004/915/EG, BDSG, DSGVO, KOM(2010) 609, Safe Harbor, weitere branchenspezifische Vorgaben wie §291a SGB V (eGK)

**Kurz-Charakterisierung:** Der europäische Rat und das europäische Parlament haben 1995 die Richtlinie 95/46/EG, auch bekannt als die Datenschutzregelung erlassen. Darin werden die Ziele und Mittel zur Etablierung einer europaweiten Datenschutzrichtlinie festgeschrieben.

Grundsätzlich steht dem Gesamtziel der Europäischen Union eine Handels- und Wirtschaftsunion zu sein, der Schutz von personenbezogenen Daten entgegen. Dies rührt daher, dass gemeinschaftlicher Handel den freien Verkehr von Waren und damit zwingend auch die Übermittlung personenbezogener Daten erfordert. Gleichzeitig sind in der EU jederzeit die Grundrechte und Grundfreiheiten der Bürger zu schützen.

Mit der Datenschutzrichtlinie will die EU zur Sicherstellung der Grundrechte und Grundfreiheiten den Datenschutz sicherstellen und insbesondere auch das Datenschutzniveau der Mitgliedstaaten angleichen. Dazu definiert 95/46/EG neben den Begriffen des personenbezogenen und sensiblen Datums auch Rechte und Pflichten für die Verarbeitung dieser Daten. So dürfen etwa Bürger der EU, die den Schutz ihrer personenbezogenen Daten verletzt sehen, nach Abschnitt V von ihrem Auskunftsrecht über die Verwendung der personenbezogenen Daten Gebrauch machen. Bestätigt sich der Verdacht einer unsachgemäßen Verarbeitung und Verwendung der Daten, können sie eine Berichtigung, Löschung oder Sperrung dieser verlangen. Darüber hinaus wird die Übermittlung von Personenbezogener Daten in Drittländer geregelt. Dies geschieht in Kapitel IV und sieht die Übermittlung nur vor, wenn dieses Drittland ein angemessenes Schutzniveau vorweisen kann. In Summe nehmen die EU-Vorgaben zum Datenschutz durch die Definition des rechtlichen Rahmens für Standards zur Datenverarbeitung im Allgemeinen (und damit auch für das Cloud Computing) Einfluss auf die Standardisierung.

Bereits 1995 wurde erkannt, dass durch neue technologische Errungenschaften der Austausch und die Verarbeitung von Daten über die Ländergrenzen

hinweg immer schneller und einfacher durchführbar sind. Um dieser schnellen Entwicklung gerecht zu werden, erfolgte 1997 die Umsetzung der Richtlinie speziell für den Telekommunikationsbereich, welche bereits fünf Jahre später durch die Richtlinie 2002/58/EG für den breiteren Anwendungsbereich der elektronischen Kommunikation ersetzt wurde.

Aktuell arbeitet die Kommission an einer kompletten Neufassung der Richtlinie. Dazu wurde eine Online-Konsultation an der sich verschiedene Firmen und Interessengruppen beteiligt haben durchgeführt<sup>119</sup> und ein neues Gesamtkonzept zum Datenschutz in der EU erarbeitet. Diese wurde am 4.11.2010 von der Kommission dem Europäischen Parlament sowie weiteren Beteiligten vorgelegt.<sup>120</sup> Unter anderem wird darin als einer der Ursachen für die Notwendigkeit zur erneuten Überprüfung und Anpassung des Rechtsrahmens explizit auf Cloud Computing hingewiesen. Gemäß dem Gesamtkonzept sollen in den Bereichen „Stärkung der Rechte des Einzelnen“, „Stärkung der Binnenmarktsituation“ und „globale Dimension des Datenschutzes“ Überarbeitungen mit Bezug zur Standardisierung erfolgen.<sup>121</sup> So wird die Erarbeitung eines EU-Standardmusters „Datenschutzhinweise“ beabsichtigt, dass Personen ermöglichen soll auf standardisierte Weise Informationen zum Datenschutz abrufen können.<sup>122</sup> Das EU-Standardmuster sollen künftig zwingend von den „für die Verarbeitung Verantwortlichen“ (Anbietern von Cloud-Diensten) zur Information der Nutzer verwendet werden. Zudem wird durch die Kommission vorgeschlagen, die Einführung von EU-Zertifizierungsregeln zum Datenschutz zu untersuchen. Anbieter von Cloud-Diensten<sup>123</sup> soll es hierdurch ermöglicht werden, dass sie einen Nachweis zur Einhaltung der Pflichten zum Datenschutz im Rahmen der Selbstregulierung erbringen können. Schließlich wird künftig diskutiert werden, ob über die Einführung von standardisierten, verbindlichen unternehmensinternen Vorschriften (Binding Corporate Rules, BCR) ein Beitrag zur Klärung und Vereinfachung der Bestimmungen im internationalen Datentransfer geleistet werden kann.

---

<sup>119</sup> Vergleich hierzu auch die Ausführungen im Kapitel 6.2.1.

<sup>120</sup> Die Mitteilung der Kommission ist an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen adressiert.

<sup>121</sup> Das Gesamtkonzept für den Datenschutz in der Europäischen Union sieht zudem eine Überarbeitung im Bereich der „polizeilichen und justiziellen Zusammenarbeit in Strafsachen“ vor. Auf Grund des nicht direkt herstellbaren Bezugs zur Standardisierung wird dieser Bereich hier nur zur Vollständigkeit, ohne weitere Diskussion erwähnt.

<sup>122</sup> Dies beinhaltet die Information der Betroffenen darüber „wie, von wem und aus welchem Grund ihre Daten erfasst und verarbeitet werden, wie lange sie aufbewahrt werden und ob sie Zugriff auf ihre Daten haben und die Berichtigung oder Löschung der Daten verlangen können.“ (KOM(2010) 609, S. 6f.)

<sup>123</sup> Der explizite Bezug findet sich im Originaltext nicht. Hier wird allgemein von „für die Verarbeitung Verantwortlichen“ gesprochen. Die Abweichung ist Ergebnis des Übertrags auf den Anwendungsbereich Cloud Computing im Rahmen der Studie.

**Bewertung und Abgrenzung zu ähnlichen Standards:** Eine inhaltliche Bewertung des Reifegrads und der Durchsetzungsfähigkeit der europäischen Datenschutzvorgaben erscheint im Rahmen der Studie nicht zielführend. Die Möglichkeit zur Beteiligung bei der Erarbeitung der neuen Datenschutzregelung wird als „hoch“ bewertet. Hierbei sind parlamentarische Verfahrensweisen zu beachten und die gegebenen Möglichkeiten, wie die z. B. durch öffentliche Konsultationen möglich wäre, auszunutzen.

#### **5.4 Lücken bei Standards im Cloud-Umfeld**

Im folgenden Unterkapitel werden die Standardisierungslücken im Cloud Computing im Detail untersucht. Eine Zusammenfassung der Ergebnisse findet sich in der Einleitung zu Kapitel 5.

Die Lückenanalyse im Normungs- und Standardisierungsumfeld wird strukturiert entlang der Taxonomie (vgl. Kapitel 3.2) durchgeführt. Entsprechend wird für jede der Herausforderungen im Cloud Computing (vgl. Kapitel 3.2.1) kurz diskutiert, welche Ansatzpunkte bislang noch nicht ausreichend adressiert werden. Soweit möglich werden Gründe hierfür benannt. Die Diskussion der Standardisierungslücken erfolgt entlang der in Kapitel 3.2.1 definierten Ansatzpunkte in den Bereichen Technik, Management und Recht. In einer Einleitung wird für jede Herausforderung kurz der Einfluss von länderspezifischen Anforderungen (bspw. durch sich unterscheidende Rechtsrahmen) auf die Standardisierung diskutiert.

##### **5.4.1 Effizienz der Dienstebereitstellung**

Die Standardisierung im Bereich der Effizienz der Dienstebereitstellung wird ausschließlich von internationalen Organisationen getrieben. Dies verwundert nicht, da die effiziente Bereitstellung von Diensten eine technische wie organisatorische Herausforderung darstellt, die ortsunabhängig sichergestellt werden muss.

Unter den technischen Ansatzpunkten ist zu beobachten, dass existierende Standards zu Programmiermodellen, Protokollen & Schnittstellen sowie Standardkomponenten & Referenzarchitekturen das Gesamtspektrum des Standardisierungsbedarfs nur zum Teil abdecken.

So fehlen Programmiermodelle, die Standards für Abfragesprachen und Programmbibliotheken bspw. zur Veredelung von Daten vorgeben. Im Bereich der Protokolle & Schnittstellen sowie bei Standardkomponenten & Referenzarchitekturen werden Aspekte des ganzheitlichen Monitorings von Ressourcen und Cloud-Diensten bislang nicht adressiert.

Nur wenige Standards für Benchmarks & Tests der Effizienz von Cloud-Diensten konnten identifiziert werden. Speziell für Cloud-Speicherdienste ist bspw. das Yahoo! Cloud Serving Benchmark (YCSB)<sup>124</sup> ein erster Schritt in die Richtung von standardisierten Leistungsvergleichen. Hierzu soll YCSB künf-

---

<sup>124</sup> Siehe [http://research.yahoo.com/Web\\_Information\\_Management/YCSB](http://research.yahoo.com/Web_Information_Management/YCSB).

tig eine Sammlung von Testabläufen und einheitlichen Belastungsprofilen zur Verfügung stellen. Allgemein erscheinen Standards für Benchmarks & Test besonders relevant, da sie Anbietern von Cloud-Diensten ermöglichen bspw. die Skalierbarkeit ihres Systems bei unterschiedlichen, aber einheitlich definierten Lastprofilen zu analysieren. Ähnliche Szenarien sind für die Überprüfung und das Testen der Effizienz des eingesetzten Ressourcenmanagements wie auch der Sicherstellung der Verfügbarkeit von Cloud-Diensten wünschenswert.

Auch die Komposition von Cloud-Diensten auf technischer und organisatorischer Ebene ist noch nicht hinreichend adressiert. Hier fehlen bspw. Standards zur Beschreibung und Überwachung von Dienstkompositionen unter Berücksichtigung von bspw. Abhängigkeiten zwischen den benötigten Komponenten und zugehörigen Ressourcen oder gar Prozessen. Speziell für Plattform-Angebote fehlt es derzeit noch eine der notwendigen, leichtgewichtigen Werkzeugunterstützung für Cloud-Anbieter.

Im Managementbereich der Standardisierung ist zu beobachten, dass existierende Standards für Service Level Agreements bislang nur unzureichend auf die für Cloud-Dienste speziellen Anforderungen eingehen. Aus Sicht der Anbieter sind hier Standards wünschenswert die bspw. die Bestimmung von sinnvollen Service Levels für ein Cloud-Dienstangebot auf Basis der eingesetzten Infrastruktur ermöglichen. Leitfäden und Audits geben bislang nur oberflächliche Empfehlungen für den Aufbau von skalierbaren Architekturen, flexibles Ressourcenmanagement oder das Management der Verfügbarkeit der angebotenen Cloud-Dienste. Dies stellt insbesondere für kleine und mittelständische Unternehmen eine Hürde beim Aufbau eines Cloud-Dienstangebots dar. Existierende Managementmodelle und -prozesse zur Verwaltung und Steuerung der im Unternehmen eingesetzten IT-Systeme zeigen bspw. Schwächen bei der Berücksichtigung der durch Cloud Computing ermöglichten Dynamik in der Bereitstellung von Ressourcen. Dies reicht von der Verabschiedung flexibler Budgetrahmen bis hin zur notwendigen Verschlinkung der Entscheidungsprozesse im Hinblick auf die potenziell schnelle und wiederkehrende Abfolge von Entscheidungssituationen. Darüber hinaus sind derzeit keine für den Einsatz im Cloud Computing bestimmten Controlling-Standards vorhanden. Es wird tendenziell davon ausgegangen, dass hier eine Lücke der Standardisierung vorhanden ist. So ist bspw. fraglich, wie die Möglichkeiten der flexiblen Budgetierung berücksichtigt werden. Diese stellt eine ökonomische Voraussetzung zur Realisierung der gewünschten Skalierung dar.

Die Relevanz der Standardisierung zur Sicherstellung der Effizienz in der Dienstebereitstellung wird grundsätzlich als gering eingestuft. Standards sind in diesem Bereich nicht zu finden.

### **5.4.2 Effektivität der Dienstenutzung und -steuerung**

Die untersuchten Standards weisen keine Merkmale auf, die Ihre Anwendbarkeit auf einzelne Rechtsräume beschränken. Generell ist dies im Bereich der „Effektivität der Dienstenutzung und -steuerung“ auch für die Zukunft

nicht zu erwarten. Eine Ausnahme stellen potenzielle Regelungen zur Klärung von Vertrags- und Haftungsfragen dar, da die Sicherstellung der Effektivität überwiegend ein unternehmerisches Ziel darstellt. Hier bleibt abzuwarten, ob spezifische Cloud Regelungen notwendig werden.<sup>125</sup>

Standards zur technischen Sicherstellung der Effektivität zeichnen sich durch einen tendenziell eher hohen Reifegrad aus. Insbesondere die Standardisierung von Schnittstellen zur Steuerung von Infrastrukturdiensten sind weit fortgeschritten (bspw. CDMI, OCCI, OpenStack) und können erste Implementierungen nachweisen. Eine Lücke besteht jedoch noch in der Integration der bisher isoliert entwickelten Standards (bspw. CDMI und OCCI) zu einer einheitlichen Management-Schnittstelle bspw. zur Konfiguration von sowohl Rechen- als auch Datendiensten.<sup>126</sup> Darüber hinaus fehlen auch Standards zum Testen der von Cloud-Anbietern bereitgestellten Funktionen zur Sicherstellung der Effektivität. Standards sollten Methoden und Werkzeuge bereitstellen, um z.B. die zur Selbstverwaltung angebotenen Funktionen automatisiert, über Checklisten u.ä. bewerten zu können. Hier könnten die existierenden Leitfäden zur Beschreibung von Cloud-Anwendungsfällen Ansatzpunkte bieten.

Die technische und ökonomische Beschreibung der Dienstgüte von Cloud-Angeboten bezieht sich heute überwiegend auf Eigenschaften, bspw. Verfügbarkeit oder Durchsatzvolumina. Zur kontinuierlichen Sicherstellung der Effektivität der Dienstenutzung- und -bereitstellung werden jedoch auch Ansätze benötigt, um solche nicht-funktionalen Eigenschaften auch für Dienste zur Selbstverwaltung definieren und überwachen zu können. Hierzu könnten bspw. die Verfügbarkeit von Governance und Eskalationsmechanismen oder die benötigte Zeit bis zu Umsetzung eines Change-Requests angegeben werden.

Die durch Cloud Computing angestrebte Automatisierung in der Verwaltung und Steuerung von Diensten erfordert neben technischen Voraussetzungen auch die Anpassung organisatorischer Abläufe. So ist die Vorgabe von Managementmodellen und -prozessen zur organisatorischen Verankerung des Self-Service-Prinzips bei Cloud-Anwendern bisher unzureichend adressiert. Erste Ansätze hierzu finden sich im Kontext der durch den GRC-Stack beschriebenen Standards. Diese Ansätze beinhalten bislang jedoch keine Hinweise zur Umsetzung der Vorgaben innerhalb einer Organisation. Weitere potenzielle Felder für Standardisierungsbestrebungen könnten sich im Bereich der Erarbeitung von Vorgaben zur Gestaltung von Geschäftsmodellen oder Vertragsbedingungen zur Sicherung der Effizienz ergeben. Überarbeitete Rahmenwerke (bspw. Gesetze oder Richtlinien) könnten zudem Einfluss auf die Effektivität der Dienstenutzung und -steuerung nehmen.

---

<sup>125</sup> Vgl. hierzu auch die Ausführungen zur Rechtssicherheit in der Cloud in Kapitel 6.2.4.

<sup>126</sup> Diese Lücke der Standardisierung ist eng mit der Sicherstellung der Interoperabilität von Cloud-Standards verbunden.



### 5.4.3 Transparenz der Leistungserbringung und Abrechnung

Die Standardisierung im Bereich der „Transparenz“ weist länderspezifische Anforderungen auf. Insbesondere die Managementstandards erfordern angepasste bzw. anpassbare Standards, bspw. für die Zertifizierung von Cloud-Diensten. Auch im Bereich der Dienstbeschreibungen sind Länderspezifika zu berücksichtigen.

Existierende, *technische Standards* leisten nur einen ersten Beitrag zur Sicherstellung von Transparenz. So sind bisherige Ansätze zu *Protokollen & Schnittstellen* entweder noch nicht über den Status einer Idee (bspw. CTP) hinaus gekommen, beschreiben eine sehr eingeschränkte Funktionalität (bspw. CloudAudit) oder sind nicht für die leichtgewichtige, REST-basierte Kommunikation einzusetzen (bspw. WS-\*). Bislang fehlen Standards, die einen Beitrag zur Automatisierung von Auditierungsprozessen bspw. durch umfassende Schnittstellen unterstützen. Im Rahmen der Studie konnten darüber hinaus keine Standards zum Abruf von Abrechnungsinformationen identifiziert werden. Eine Lücke der Standardisierung stellt folglich die Weiterentwicklung solcher Protokolle & Schnittstellen dar. Ein erster Schritt hierfür könnte die Einführung einer einheitlichen Terminologie und vergleichbaren Skalen für die Beschreibung und Messung von Ressourcenverbräuchen darstellen.

Auch konnten keine Standards für *Programmiermodelle* zur Sicherstellung der Transparenz oder des Benchmarking und Testen der Transparenz identifiziert werden. Diesen Bereichen wird jedoch eher eine geringe Relevanz für die Standardisierung im Hinblick auf die Sicherstellung der Transparenz beigegeben und weist daher keinen akuten Handlungsbedarf auf.

Im Hinblick auf *Standardkomponenten & Referenzarchitekturen* konnten keine Standards zur automatisierten Dienstgüteüberwachung identifiziert werden. Standards zur Bereitstellung von Informationen zu Art und Ort der Datenverarbeitung könnten darüber hinaus bspw. einen wesentlichen Beitrag zur Schaffung von Transparenz und damit von Vertrauen im Cloud Computing schaffen. Solche Standards existieren derzeit jedoch nicht. Die in CTP vorgeschlagene Idee eines Trust Brokers zur Sicherstellung von Vertrauen in Cloud Computing beschreibt eine weitere Lücke der aktuellen Standardisierungsbemühungen mit konkretem Handlungsbedarf. Die Weiterentwicklung der Idee sowie die Bereitstellung einer entsprechenden Standardkomponente oder standardisierter Schnittstellen könnten einen wesentlichen Beitrag zur Schaffung von Transparenz und Interoperabilität von Cloud Brokern im Cloud Computing leisten. Auch für eine eventuelle organisatorische Ausgestaltung zum Betrieb einer solchen Komponente durch eine unabhängige Schiedsinstanz fehlen bislang Konzepte.

Die Forderung nach erhöhter Transparenz erfordert im Bereich der *Managementansätze* neue Entscheidungsmodelle, die insbesondere schlankere Freigabeprozesse für Leistungs-, Audit- oder Sicherheitsinformationen im Cloud Computing vorgeben. Standardisierte *Managementmodelle & -prozesse* könnten hier einen Rahmen für die organisatorische Umsetzung der Transparenzanforderung vorgeben. Auch die Ausgestaltung von Standardvorlagen für Ver-



*träge*, die den erhöhten Transparenzanforderungen im Cloud Computing gerecht werden, könnte eine mögliches Feld künftiger Standardisierungsbemühungen darstellen.

Weiter besteht Handlungsbedarf für die Standardisierung von *Selbstverpflichtungen*. OCM gibt ein erstes Beispiel vor, jedoch bleiben bislang insbesondere Fragen zur Verbindlichkeit und zu Sanktionsmaßnahmen bei einem möglichen Verstoß gegen die unterschriebene Verpflichtung offen. Eine weitere Lücke der Standardisierung im Bereich der Sicherstellung von Transparenz kann schließlich in der Festschreibung von Rechten zum Datenabruf (ähnlich zum Auskunftsrecht im Datenschutz) liegen. Dazu könnte auch der Entwurf von einheitlichen, freiwilligen Unternehmensrichtlinien bspw. zur Regelmäßigkeit und Frequenz der Veröffentlichung von Informationen zur Schaffung eines Rechtsrahmens für erhöhte Transparenz beitragen.

### 5.4.4 Informationssicherheit

Die Vorgaben zur Informationssicherheit unterscheiden sich je nach gültigem Rechtsraum. Daher ist davon auszugehen, dass Standards für Informationssicherheit spezifisch für unterschiedliche Rechtsräume gestaltet werden müssen oder zumindest anpassbar gestaltet sein sollten. Anforderungen zur Informationssicherheit ergeben sich in allen Einsatzszenarien der IT-gestützten Datenverarbeitung. Aus diesem Grund erscheint wenig verwunderlich, dass keiner der technischen Ansatzpunkte einen expliziten Cloud-Bezug aufweist.

In diesem Zusammenhang muss jedoch die grundsätzliche Frage gestellt werden, inwieweit existierende Standards zur Informationssicherheit im Konflikt mit den Grundprinzipien des Cloud Computing stehen. Insbesondere Anforderungen zur Skalierbarkeit von Cloud-Diensten stellen für viele existierende Sicherheitsstandards eine große Herausforderung dar. So müssen existierende Standard-Sicherheitskomponenten, z.B. Komponenten zur Sicherstellung von Vertraulichkeit & Integrität durch Verschlüsselung, erst ihre Einsatzfähigkeit im Cloud Computing nachweisen.

Auf Grund der skalierbaren Ressourcen eröffnen sich im Cloud Computing auch neuartige Möglichkeiten zur Sicherstellung der Informationssicherheit. Als Beispiel sei hier die Möglichkeit genannt, Daten bei der Speicherung über unterschiedliche Cloud-Dienste zu verteilen. Eine solche Fragmentierung der Daten verhindert, dass ein Angreifer durch Übernahme eines Cloud-Dienstes an die vollständigen Daten bzw. Informationen gelangt. Zertifizierte Standardkomponenten, die eine solche Fragmentierung von Daten vornehmen, könnten künftig einen einfachen, aber wirksamen Schutz vor unerlaubten Datenzugriffen im Cloud Computing darstellen. Weiteres Potenzial zur Adressierung der Informationssicherheit liegt in der Erarbeitung neuer einheitlicher Programmiermodelle, bspw. zur Komposition von Sicherheitsaspekten über die Ebenen (IaaS/PaaS/SaaS) des Cloud Computing hinweg. Im Ergebnis könnten Sicherheitseinstellungen wie Zugriffsrechte, Logging oder Nachweise einheitlich für Cloud-Anwendungen und Cloud-Infrastrukturen verwaltet werden. Darüber hinaus werden Benchmarks & Tests zur faktischen Dokumentation der Informationssicherheit benötigt. Auch hier ist die Anwendbar-

keit existierender Ansätze (bspw. SCAP) im Cloud Computing erst zu bestätigen.

Für Managementstandards bleibt ebenfalls abzuwarten, inwieweit existierende Initiativen (GRC Stack, OCM) die Übertragbarkeit von Managementansätzen (bspw. ITIL, ISO27001) auf das Cloud Computing herstellen können oder ob hier neue Rahmenwerke benötigt werden. Derzeit existieren keine einheitlichen Managementstandards für das Cloud Computing (bspw. Vertragsbedingungen). Vor allem im Hinblick auf Regelungen zur Gewährleistung der Informationssicherheit durch Verträge, versprechen Standards eine Vereinfachung insbesondere für kleine und mittelständische Unternehmen, die keinen kontinuierlichen Rechtsbeistand in Anspruch nehmen können.

### 5.4.5 Datenschutz

Die Anforderungen und Vorgaben für die Standardisierung im Bereich „Datenschutz“ werden stark von lokalen Rahmenbedingungen geprägt.<sup>127</sup> Standards müssen daher flexibel gestaltet sein, um leicht an die unterschiedlichen Vorgaben angepasst werden zu können. Dies gilt für alle Ansatzpunkte zum Datenschutz aus den Bereichen Technik, Management und Recht.

Generell ist zu beobachten, dass keine technischen Cloud-Standards zur Unterstützung des Datenschutzes existieren. Hier könnte bspw. durch standardisierte, technische Komponenten künftig sichergestellt werden, dass Cloud-Anwender auf einen zuverlässigen Datenschutz vertrauen können. In einem ersten Schritt könnte eine Datenschutzkomponente bspw. alle Datenzugriffe zuverlässig aufzeichnen. Diese könnten bei Bedarf vom Nutzer für einen bestimmten Zeitraum eingesehen werden. Der Betrieb solcher Datenschutzkomponenten könnte durch eine unabhängige Schiedsinstanz zertifiziert werden.<sup>128</sup>

Unter den dem Management zuzurechnenden Ansatzpunkten existieren derzeit nur erste Leitfäden, die Anwendungsfälle des Datenschutzes im Cloud Computing beschreiben (bspw. NIST-UC). Speziell für den europäischen und deutschen Rechtsraum fehlen einheitliche Anwendungsfälle, über welche sichergestellt werden kann, dass Anwender von Cloud-Diensten in späteren Schritten Informationen zum vertrauenswürdigen Umgang abrufen können. Diese könnten auch eine Grundlage zur späteren Spezifikation von standardisierten Schnittstellen zum automatisierten Abruf darstellen.

Existierende rechtliche Vorgaben, z.B. die EU-Datenschutzrichtlinie (95/46/EG), finden sich aktuell in Überarbeitung und sollen dabei auch für die Anforderungen des Cloud Computing angepasst werden.<sup>129</sup> Insbesondere die nicht einheitliche Umsetzung der Datenschutzrichtlinie in den EU-

---

<sup>127</sup> Eine ausführliche Diskussion findet sich in Kapitel 6.2.4.

<sup>128</sup> Eine solche Initiative könnte bspw. durch die geplante Stiftung Datenschutz in Deutschland getrieben werden (siehe [http://www.bfdi.bund.de/DE/Oeffentlichkeitsarbeit/Pressemitteilungen/2011/6\\_StiftungDatenschutz.html](http://www.bfdi.bund.de/DE/Oeffentlichkeitsarbeit/Pressemitteilungen/2011/6_StiftungDatenschutz.html)).

<sup>129</sup> Details finden sich in der Diskussion zur EU-Datenschutzrichtlinie in Abschnitt 5.3.1.

Mitgliedstaaten stellt eine Hürde beim Angebot von Cloud-Diensten über Rechtsgebiete hinweg dar. So könnten standardisierte, kohärente Bausteine für die Gestaltung von Vertragsbedingungen einen Beitrag zur Einhaltung der Datenschutzanforderungen innerhalb der EU leisten. Kleine und mittelständische Unternehmen könnten damit auf eine Auswahl von Textmodulen zurückgreifen, um ihre ggfs. länderspezifischen Vertragswerke zu erstellen.

Zur Sicherstellung einer einfachen Überprüfbarkeit der Einhaltung des Datenschutzes durch Cloud-Anwender könnte zudem die Etablierung einer einheitlichen Datenschutzterminologie beitragen. Die Einführung leicht verständlicher Kennzeichnungen von Cloud-Angeboten, die den Datenschutzrichtlinien entsprechen, könnte die Weiterentwicklung leicht verständlicher Zertifikate (z.B. EuroPriSe) künftig beitragen.

### 5.4.6 Interoperabilität

Herausforderungen im Bereich der Interoperabilität stellen überwiegend technische Anforderungen dar, die kaum durch den Betrieb und Einsatz von Cloud-Diensten in unterschiedlichen Rechtsräumen beeinflusst werden.

Die Standardisierung von technischen Ansatzpunkten weist in Summe die größte Reife und potenziell die größte Durchsetzungsfähigkeit auf. So existieren Standards zur Definition von Datei- & Austauschformaten (bspw. OVF), für Programmiermodelle (bspw. HIVE) sowie Protokolle & Schnittstellen (bspw. CDMI, OCCI). Diese zeichnen sich in der Regel durch eine große inhaltliche Tiefe für einen speziellen Problembereich aus (bspw. CDMI für Speicherdienste oder OCCI für Rechendienste). Das Zusammenspiel (Interoperabilität) dieser Standards zum Aufbau von interoperablen Cloud-Diensten ist jedoch bislang nur wenig adressiert und stellt eine Lücke der Standardisierung im Bereich der Standardisierung dar. Erste Bestrebungen zur Sicherstellung der Interoperabilität von Cloud-Standards sind im Rahmen der von SNIA organisierten „cloud plugfests“ zu beobachten (bspw. zwischen OCCI und CDMI).<sup>130</sup> Eine übergeordnete Koordination der Maßnahmen zur Entwicklung eines Cloud-Standards zum integrierten Management von IaaS-, PaaS- und SaaS-Angebote existiert derzeit nicht. Künftige Standardisierung könnte darüber hinaus existierende Benchmarks & Tests um Funktionen zum automatisierten Testen der Interoperabilität erweitern.

Zur Beschreibung von technischen und ökonomischen Diensteeigenschaften stellt die USDL, die im Kontext des Internets der Dienste entwickelt worden ist, einen ersten Ansatzpunkt dar. Die Anwendbarkeit von USDL für Cloud-Dienste, insbesondere die Berücksichtigung von Cloud-spezifischen Eigenschaften, wie z.B. Geschäftsmodelle, ist noch nicht erprobt. Auch der Aufbau von USDL auf der technischen Basis von WSDL kann potenziell eine Hürde für die generelle Anwendbarkeit von USDL im Cloud Computing darstellen,

---

<sup>130</sup> Vgl. hierzu <http://www.snia.org/cloud/cloudplugfest>.

da hier häufig leichtgewichtige, REST-basierte Dienstekommunikation Anwendung findet.

Cloud-Standards zur Unterstützung von Interoperabilität im Bereich des Managements existieren derzeit wenig. Einen ersten Eindruck über Anforderungen in diesem Bereich bietet bspw. NIST-UC. Neben diesem auf die öffentliche Verwaltung beschränkten Beispiel fehlen jedoch Anwendungsfälle, die Interoperabilitätsanforderungen einheitlich für den Einsatz von Cloud-Diensten im Unternehmenskontext vorgeben. Hier sollte insbesondere die Betrachtung ggfs. abweichender Anforderungen in unterschiedlichen Branchen und für variierende Unternehmensgrößen beachtet werden.

Dem Bereich der rechtlichen Ansatzpunkte wird generell nur ein geringer Beitrag zur Sicherstellung von Interoperabilität zugeordnet. Dennoch ist zu beobachten, dass existierende Selbstverpflichtungen (bspw. OCM) nicht die notwendige inhaltliche Tiefe und Verbindlichkeit aufweisen.

### 5.4.7 Portabilität

Die Standardisierung zur Unterstützung der Portabilität von Daten und Diensten weist kaum Spezifik beim Einsatz in unterschiedlichen Rechtsräumen auf. Ähnlich zur Standardisierung der Interoperabilität lässt sich dies mit dem geringen Einfluss des Rechtsrahmens auf diesen Bereich der Standardisierung erklären.

Die technischen Standards für Portabilität verfügen über hohe Reife und ein ausgeprägtes Potenzial für eine künftige Marktakzeptanz. Unter den Standards zu Datei- & Austauschformaten existieren bislang hauptsächlich Dateiformate für den Transport von virtuellen Maschinen (bspw. OVF, CIMSVM). Hingegen ist bspw. der Transport von Daten zwischen unterschiedlichen Cloud-Anbietern ist weniger standardisiert. Hier fehlen bislang Standards, die Vorgaben zur Struktur von Datei- und Austauschformaten vorgeben. Dies bedeutet, dass heute beim Transport von Daten zwischen Cloud-Speicherdiensten ggfs. zeit- und kostenintensive Datentransformationen durchgeführt werden müssen. Auch die Sicherstellung von Interoperabilität durch einheitliche Austauschformate für SaaS-Angebote zwischen unterschiedlichen PaaS-Anbietern ist derzeit noch nicht hinreichend bearbeitet. Auch hier könnte die Portabilität durch einheitliche Datei- und Austauschformate erhöht werden.

Ein vergleichbares Bild zeichnet sich bei Protokollen & Schnittstellen im Bereich der Portabilität. Auch hier weisen Standards zum Transport von virtuellen Maschinen die größte Reife auf. Dedizierte Schnittstellen, die sich exklusiv dem Transport von Datensätzen oder Diensten widmen, konnten im Rahmen der Studie nicht identifiziert werden. Eine erste Initiative in diese Richtung ist Google's Data Liberation Front<sup>131</sup>. Jedoch sind die entwickelten Takeout-Dienste und Schnittstellen nur für Google-Produkte anwendbar. Die Weiter-

---

<sup>131</sup> Siehe <http://www.dataliberation.org/>.

führung dieses Gedankens zu standardisierten „Move-Out“- und „Move-In“-Schnittstellen zeigt einen möglichen Entwicklungsweg für künftige Standards auf.

Ein weiteres Feld für die künftige Standardisierung kann darüber hinaus in der Ergänzung von Benchmarks & Tests um Funktionen zum automatisierten Testen der von Cloud-Anbietern zur Verfügung gestellten Portabilitäts-schnittstellen liegen.

Im Bereich der Managementstandards ist derzeit wenig Aktivität bei der Standardisierung zu beobachten. Die Unterstützung von Portabilität lässt sich generell schwer durch die Standardisierung von bspw. Geschäftsmodellen, Service-Level-Agreements und Management- oder Controlling-Prozesse erreichen. Eine Ausnahme stellt die Vorgabe von standardisierten Vertragsbausteinen zur Zusicherung der Daten- und Dienstportabilität dar. Künftige Standardisierungsvorhaben sollten sich dieser Lücke der aktuellen Standardisierung annehmen.

Existierende Leitfäden zum Cloud Computing (bspw. NIST-UC) beschreiben darüber hinaus erste Anforderungen in Szenarien, die Portabilität von Daten und Diensten erfordern. Analog zum Bereich der Interoperabilität ist auch hier festzustellen, dass solche Leitfäden derzeit nicht in einer ausreichenden Tiefe für Unternehmen, ggfs. unter Berücksichtigung von Branchenspezifika vorliegen.

Rechtliche Vorgaben zur Portabilität existieren aktuell in Form von Selbstverpflichtungen (bspw. OCM). Für die Zukunft bleibt abzuwarten, ob diese eine hinreichende Verbindlichkeit entwickeln können. Falls nötig, könnten ergänzende rechtliche Vorgaben zur Portabilität auftretende Lock-in-Effekte regulieren.

### **5.4.8 Sicherstellung eines funktionierenden Wettbewerbs**

Die Sicherstellung von funktionierenden Märkten für Cloud-Dienste stellt eine übergeordnete Aufgabe von staatlichen oder zwischenstaatlichen Regulatoren dar. Im Ergebnis soll hierdurch ein hinreichender Wettbewerb zwischen Cloud-Anbietern mit geringen Schranken beim Markteintritt ermöglicht werden.<sup>132</sup> Die Standardisierung in diesem Bereich hat sich daher mit den unterschiedlichen Gegebenheiten des vorliegenden Markts auseinanderzusetzen.

Der Beitrag von technischen Standards in diesem Bereich wird als nicht signifikant eingeschätzt. Diese Einschätzung basiert auch auf der vorgenommenen Analyse von Standards, die keinen Bezug zu existierenden, technischen Standards herleiten konnte.

Durch Vorgaben zu Geschäftsmodellen und Service-Level-Agreements, bspw. für Betreiber von Marktplätzen oder Plattformen für Cloud-Dienste, könnte ein Beitrag zur Sicherstellung eines funktionierenden Wettbewerbs erzielt

---

<sup>132</sup> Dies gilt analog auch für den Austritt aus dem Markt.



werden. Jedoch wurden im Rahmen dieser Studie keine diesbezüglichen Initiativen identifiziert.

Das größte Potenzial zur Sicherstellung eines funktionierenden Wettbewerbs im Cloud Computing besitzen allgemein Offenheit, Zertifizierungen oder partizipative Instrumente (z.B. Selbstverpflichtungen, Fördermittel) seitens des Staates (siehe 7.1.3). Notwendige rechtliche Anpassungen oder Vorgaben sollten dies wo nötig ergänzen.

### **5.4.9 Compliance mit geltender Rechtslage**

Die Einhaltung von Gesetzen und unternehmerischen Leitlinien ist Ziel der Compliance. Somit ist offensichtlich, dass Standards in diesem Bereich immer an der geltenden Rechtslage ausgerichtet oder nach deren Vorgaben entwickelt werden müssen.

Existierende Standards, die Compliance betreffen, fallen überwiegend in den Bereich der Managementaspekte. Die Auswirkungen von Cloud-spezifischen Compliance-Anforderungen auf die Standardisierung werden aktuell analysiert (bspw. GRC Stack). Die ersten Ergebnisse deuten jedoch darauf hin, dass die existierende Standards zu Managementprozessen (bspw. ITIL, ISO27001) wohl ausreichend sind. Dieser Eindruck wird auch durch die zunehmende Zertifizierung von Rechenzentren für den Betrieb von Cloud-Diensten nach etablierten Vorgaben (bspw. SSAE 16) gestärkt. Spezielle Cloud-Zertifikate (bspw. EuroCloud-SA) berücksichtigen Aspekte der Compliance in ihren Fragekatalogen ohne diese jedoch detaillierter zu analysieren.

Technische Standards zur Unterstützung von Compliance-Anforderungen im Cloud Computing konnten in der Studie nicht identifiziert werden. Im Kontext von PaaS-Angeboten besteht jedoch die Chance zur Vereinfachung der Aufgaben und Prozesse, die mit Compliance verbunden sind, durch Standardkomponenten. So könnten existierenden Plattform-Architekturen um Komponenten zur Berücksichtigung von länderspezifischen Compliance-Anforderungen erweitert werden. Die dadurch zur Verfügung gestellten Funktionen könnten anschließend von Anbietern beim Betrieb ihrer Cloud-Dienste verwendet werden, um Compliance sicherzustellen.



## 6 Wichtige strategische Trends der Standardisierung im Cloud Computing

### 6.1 Einleitung und Übersicht

Die vorherigen Kapitel 4 und 5 geben einen Überblick über Standardisierungsorganisationen bzw. existierende Vorarbeiten, Standards und Zertifizierungen im Cloud Computing. Die Perspektive dieser Kapitel ist überwiegend auf die Vergangenheit bzw. die unmittelbare Gegenwart gerichtet. Durch die Beschreibung strategischer Trends bei der Standardisierung im Cloud Computing in diesem Kapitel, wird der Blick zusätzlich auf die Zukunft gerichtet.

Der Beschreibung und Auswahl der Trends liegt eine Vielzahl von Quellen zu Grunde, die für diese Studie betrachtet werden (siehe Methodologie in 3.3.3). Bestehende Aktivitäten bei der Standardisierung im Cloud Computing der letzten Jahre werden in Themenbereichen gruppiert. Der Fokus liegt dabei auf Aktivitäten mit starkem, aber nicht notwendigerweise ausschließlichem Bezug zu Deutschland. Solche Themenbereiche, die die größte fortschreitende Eigendynamik auf einen Zeithorizont bis 2015 erwarten lassen, werden herausgegriffen und bilden die sechs Trends, wie sie in diesem Kapitel untersucht werden. Die Trends besitzen alle unmittelbare strategische Relevanz für die Cloud-Standardisierung, da sie einen inhärenten, im Einzelfall aber unterschiedlichen, Bezug zu den Herausforderungen (siehe 3.2.1) im Cloud Computing besitzen.

Die Trends gehen in der Regel aus Entwicklungen im Cloud Computing im Allgemeinen hervor. Der Bezug zur Standardisierung wird aus diesen Entwicklungen abgeleitet, um danach den eigentlichen Trend in der Standardisierung fokussiert zu beschreiben.

Folgende Übersicht fasst die sechs strategischen Trends kurz zusammen, wie sie in den folgenden Kapiteln in größerem Detail beschrieben werden.

**Tabelle 3:** Strategische Trends der Standardisierung im Cloud Computing<sup>133</sup>

<b>Cloud-Standardisierung &amp; staatliche Mitwirkung</b>	<ul style="list-style-type: none"> <li>– Die <b>USA besitzen eine Vorreiterrolle</b> (z.B. <i>NIST Roadmap</i>, „cloud-first“ Grundsatz)</li> <li>– Bei vielen Industrienationen deuten sich <b>ab 2012 zunehmende Bemühungen</b> an, z.B.             <ul style="list-style-type: none"> <li>- Frankreich (z.B. <i>Andromède</i>, Handlungsfeld „Standardisierung“),</li> <li>- Großbritannien (z.B. <i>G-Cloud</i>), Deutschland (z.B. <i>Roadmap</i>),</li> <li>- EU (z.B. <i>ETSI Roadmap</i>, <i>Cloud F&amp;E Projekte</i>) und weitere</li> </ul> </li> </ul>
<b>Cloud-Zertifizierung</b>	<ul style="list-style-type: none"> <li>– <b>Seit 2009 gibt es erste</b>, vergleichsweise noch unreife <b>Cloud-Zertifizierungen</b> für             <ul style="list-style-type: none"> <li>- Standards (z.B. <i>EuroCloud Gütesiegel</i>, <i>EuroPriSe</i>, <i>Cloud Audit</i>),</li> <li>- Experten (z.B. <i>CCSK</i>, <i>IBM certified solution advisor for CC</i>) und</li> <li>- Geschäftspartner (z.B. <i>SAP Certified Provider of Cloud Services</i>)</li> </ul> </li> <li>– Ein <b>hoher Automatisierungsgrad</b> der Auditierung wird <b>angestrebt</b></li> </ul>

<sup>133</sup> Analyse von Booz & Company und FZI.

Offenheit im Cloud Computing	<ul style="list-style-type: none"> <li>– <b>Nachzügler</b> (z.B. AMD, Cisco, Citrix, IBM, VMware, viele KMU) <b>wollen sich zunehmend mit Hilfe offener Standards etablieren</b></li> <li>– <b>Initiativen:</b> DMTF Open Cloud Standards Incubator, Open Cloud Consortium, Open Cloud Manifesto (März 2009), Open Cloud Initiative (seit Juli 2011)</li> <li>– Unterschiedliche Auffassungen zur Offenheit; geringe Beteiligung der Staaten</li> </ul>
Rechtssicherheit für die Cloud	<ul style="list-style-type: none"> <li>– Die bisherigen Cloud-Lösungen garantieren <b>keine Konformität mit geltendem deutschen und europäischen Recht</b> – es bestehen beträchtliche (Haftungs-)Risiken</li> <li>– <b>Verbindliche Standards können Rechtssicherheit schaffen</b></li> <li>– <b>Relevante Rechtsgebiete:</b> Datenschutz, Sicherheits-, Strafprozess-, Verbraucher-, AGB-, Steuer-, Handels-, Urheber-, Privat- und IT-Vertragsrecht</li> </ul>
Cloud-Marktplätze	<ul style="list-style-type: none"> <li>– <b>Die innovative Erweiterung des Cloud Computing</b> um den Marktplatz-Gedanken wird seit 2010 verstärkt aufgegriffen</li> <li>– <b>Standards sind für Flexibilität und Vertrauen</b> im Marktplatz-Ökosystem <b>notwendig</b></li> <li>– IaaS (z.B. Amazon Web Services, Rackspace, Enomaly) wird durch Amazon AWS dominiert; SaaS (z.B. TEXO-Marktplatz, Logistics Mall, Trusted Cloud-Projekte) umfasst auch Lösungen für die Verwaltung</li> </ul>
Governance im Cloud Computing	<ul style="list-style-type: none"> <li>– Es werden <b>erste Standards</b> (z.B. GRC Stack) und Anforderungsdefinitionen (z.B. zu KPIs) zur Governance im Cloud Computing erarbeitet und <b>veröffentlicht</b></li> <li>– Standards werden zur <b>Adressierung der komplexen Anforderungen</b> benötigt</li> <li>– Zunehmender Bedarf an zielgruppenbezogenen, reifen Standards sowie der Einbeziehung existierender Standards (z.B. ITIL, COBIT)</li> </ul>

Der erste Trend (dunkelblau) fügt der Betrachtung eine weitere Perspektive hinzu. Er beschreibt in welcher Form und mit welchem Engagement sich staatliche Akteure bei der Standardisierung im Cloud Computing engagieren.

## 6.2 Strategische Trends im Einzelnen

### 6.2.1 Cloud-Standardisierung und staatliche Mitwirkung

Dieses Kapitel widmet sich der Frage, wie stark und in welcher Form (zwischen-)staatliche Akteure aktuell bei der Standardisierung für das Cloud Computing mitwirken und welche weiteren Maßnahmen geplant sind. Die Betrachtung konzentriert sich stichpunktartig auf solche Staaten und zugehörigen (halb-)öffentlichen Einrichtungen weltweit, bei denen derzeit das größte Bemühen erkennbar ist.

Zurzeit treten vor allem drei wesentliche Formen der Mitwirkung in Erscheinung:

- **Staatliche Förderprogramme** für das Cloud Computing in der Privatwirtschaft im Allgemeinen, die allerdings in der Regel auch immer eine Standardisierung vorbereiten bzw. vorantreiben sollen.
- Existierende oder geplante „**Verwaltungs-Clouds**“, die zwar primär helfen sollen ein fachliches Ziel zu erreichen, aber immer auch Testanwendung sind und die Standardisierung beschleunigen.

- **Standardisierungsroadmaps** für das Cloud Computing, die von staatlicher Seite erarbeitet werden und aus der sich eine Vielzahl unterschiedlicher Maßnahmen ableiten.
- Direkte Mitwirkung bei der **Erarbeitung von Standards** durch (halb-)staatliche Einrichtungen mit dem Ziel öffentliche Anforderungen in die Standardisierung einfließen zu lassen.

Die folgende Betrachtung ist eine Momentaufnahme von Anfang 2012 und basiert auf öffentlich zugänglichen Strategien der Verwaltungen, frei verfügbarem, allgemeinem Informationsmaterial und weltweiten Pressemitteilungen. Die Entwicklung gestaltet sich äußerst dynamisch. Alleine im August / September sind eine Vielzahl weiterer Aktivitäten veröffentlicht worden.

- Der prominenteste staatliche Akteur sind die **USA**, vertreten vor allem durch die NIST und angetrieben durch den „cloud-first“ Grundsatz<sup>134</sup> in der US-Verwaltung. Die wesentlichsten Elemente sind eine Standardisierungsroadmap für die US-Verwaltung und eine Cloud Computing-Referenzarchitektur vom Juli 2011.<sup>135</sup> In der Roadmap werden Prioritäten für die Standardisierung identifiziert, die Empfehlungen bleiben allerdings noch eher generisch ohne Nennung konkreter Verantwortlichkeiten und des angestrebten Zeitrahmens. US-Behörden planen oder betreiben mehrere private Clouds, z.B. NASA Nebula, Defense Information Systems Agency (DISA), Argonne Leadership Computing Facility (ALCF) und weitere<sup>136</sup>.
- Auf **EU-Ebene** sind bereits verschiedenste Aktivitäten mit Bezug zur Standardisierung im Cloud Computing erkennbar, die Ende 2011 zunehmend an Dynamik gewinnen:
  - Im Januar 2010 wurde der Bericht „Future of Cloud Computing“<sup>137</sup> veröffentlicht, der auch die Förderung von Standardisierung und offener Referenzimplementierungen anregt.
  - In der Digitalen Agenda der EU<sup>138</sup> wird empfohlen eine EU-weite Cloud Computing-Strategie zu entwickeln. Die Strategie soll bis 2012 vorliegen und befasst sich in einem ihrer drei Handlungsfelder mit „Research & Standardisierung“. Derzeit finden EU-Konsultationen zum bestmöglichen Einsatz von Cloud Computing in Europa allgemein statt.<sup>139</sup>

---

<sup>134</sup> Der „cloud-first“ Grundsatz verpflichtet US-Behörden vor einer neuen IT-Investitionsentscheidung immer zuerst sichere Cloud Computing-Alternativen zu evaluieren.

<sup>135</sup> <http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/>

<sup>136</sup> Quelle: Cloudbook.net

<sup>137</sup> <http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf>

<sup>138</sup> [http://ec.europa.eu/information\\_society/digital-agenda/](http://ec.europa.eu/information_society/digital-agenda/)

<sup>139</sup> <http://europa.eu/rapid/pressReleasesAction.do?reference=IP%2F11%2F575&format=HTML&aged=1&language=DE&guiLanguage=en>

- Das SIENA<sup>140</sup> Projekt wirkt bei der Definition einer künftigen Standardisierungsroadmap für e-Infrastrukturen mit und hat viele Publikationen mit Orientierungswissen veröffentlicht. SIENA läuft Anfang 2012 aus. Seit Ende 2011 übernimmt auf EU-Ebene verstärkt das ETSI die koordinierende Rolle bei der Cloud-Standardisierung.
- Die EU strebt auch eine Novellierung der Datenschutzregelungen aus dem Jahre 1995 an.<sup>141</sup>
- Das 7. Forschungsrahmenprogramm (FP7), das Wissenschaftsförderprogramm der EU, spielt bei Cloud Computing auf EU-Ebene eine zentrale Rolle. Hier werden wichtige Projekte, wie RESERVOIR<sup>142</sup>, 4CaaS<sup>143</sup>, StratusLab<sup>144</sup>, Venus-C<sup>145</sup>, BonFIRE<sup>146</sup>, Cloud4SOA<sup>147</sup>, CloudTM<sup>148</sup>, Vision Cloud<sup>149</sup> und viele mehr, gefördert, die vielfältige Ansatzpunkte zur Standardisierung bieten.
- **Frankreich** hat im Juni 2010 ein 700 Mio. Euro starkes nationales Förderprogramm für das Cloud Computing bekannt gegeben, das über Staatsanleihen finanziert wird. Davon werden 135 Mio. Euro in „Andromède“ investiert, das als ein Gemeinschaftsprojekt von Verwaltung und Wirtschaft aufgesetzt ist. In der zugehörigen allgemeinen Cloud Computing Roadmap<sup>150</sup> wird Standardisierung und Interoperabilität als ein Handlungsbereich ausgewiesen. L'AFDE, eine Vereinigung französischer Softwarehersteller, ist auf internationaler Ebene in der WG38 der ISO / IEC JTC1 vertreten. AFNOR, das französische „DIN“, zeigt erste Aktivitäten, wie zum Beispiel Workshops.
- In **Großbritannien** kommt der geplanten G-Cloud, einer umfassenden Community-Cloud für die öffentliche Verwaltung, derzeit die größte Bedeutung zu. Deren Einrichtung ist in der „Digital Britain“ Initiative<sup>151</sup> verankert und lässt eine zunehmende Standardisierung erwarten. Getrieben durch die ambitionierten Sparanstrengungen der Regierung, wurde die G-Cloud immer wieder in Frage gestellt. Im September 2011

---

<sup>140</sup> <http://www.sienainitiative.eu>

<sup>141</sup> <http://heise.de/-1131032>

<sup>142</sup> <http://www.reservoir-fp7.eu/>

<sup>143</sup> <http://4caast.morfeo-project.org/>

<sup>144</sup> <http://www.stratuslab.eu/doku.php>

<sup>145</sup> <http://www.venus-c.eu>

<sup>146</sup> <http://www.bonfire-project.com/>

<sup>147</sup> <http://www.cloud4soa.eu/>

<sup>148</sup> <http://www.cloudtm.eu/>

<sup>149</sup> <http://www.visioncloud.eu/>

<sup>150</sup> [http://www.afdel.fr/iso\\_album/extrait\\_livre\\_blanc\\_afdel\\_-\\_cloud\\_computing\\_une\\_feuille\\_de\\_route\\_pour\\_la\\_france.pdf](http://www.afdel.fr/iso_album/extrait_livre_blanc_afdel_-_cloud_computing_une_feuille_de_route_pour_la_france.pdf)

<sup>151</sup> „Digital Britain“, BIS & dcms, Endbericht, Juni 2009.

gab es vermehrt Stimmen aus der Regierung, die sich zur Umsetzung der G-Cloud bekennen.

- In **Japan** wurde auf Initiative des Ministeriums für Inneres und Kommunikation (MIC) in der „Study group on Smart Cloud“ ein Bericht (Mai 2010) erarbeitet, der Standardisierung als wichtigen Erfolgsfaktor für Cloud Computing ausweist. Im ICT Hatoyama Plan aus 2009 wird die Einrichtung der „Kasumigaseki Cloud“ für die japanische Verwaltung bis 2015 gefordert. Japan beteiligt sich beispielsweise an der Förderung von Standards über das Global Inter-Cloud Technology Forum (GICTF).<sup>152</sup>
- Auf **internationaler** Ebene erarbeitet beispielsweise die ITU in der Focus Group Cloud Computing eine Standardisierungsroadmap für Cloud Computing.

Die Standardisierungsanstrengungen befinden sich auf Seiten der Regulatoren weltweit und Anfang 2012 noch überwiegend in einer internen Orientierungs- und Planungsphase. Eine Ausnahme bilden die USA, die ein verhältnismäßig frühzeitiges Engagement im Cloud Computing zeigen und bereits eine Standardisierungsroadmap veröffentlicht haben. Erst in den letzten beiden Jahren haben Cloud Computing-Angebote die technische Reife und ein Potenzial erlangt, das verstärkte Anstrengungen rechtfertigt. Viele andere Staaten innerhalb (z.B. Niederlande, Dänemark oder Schweden) und außerhalb Europas (z.B. Kanada oder Korea) betrachten die Standardisierung im Cloud Computing ebenfalls als zentral und haben Absichtserklärungen veröffentlicht bzw. erste Beiträge in internationalen Gremien geleistet. Die große Herausforderung wird ein international koordiniertes Vorgehen sein, das effiziente Arbeitsteilung ermöglicht. Viele Staaten werden nur im Verbund überhaupt eine Chance besitzen erarbeitete Standards durchzusetzen. Für Deutschland spielt besonders die Abstimmung innerhalb Europas eine wichtige Rolle. Es wird erwartet, dass in den nächsten zwei bis vier Jahren weltweit wesentliche Standardisierungsaktivitäten im Cloud Computing starten werden.

### 6.2.2 Cloud-Zertifizierung

Unter „Cloud-Zertifizierung“ werden im Rahmen dieser Studie alle Zertifizierungsaktivitäten mit Bezug zum Cloud Computing bezeichnet. Eng damit verbunden ist der Themenbereich „Auditierung“. Seit etwa 2009 kann von wirklicher Cloud-Zertifizierung gesprochen werden, als sich folgende drei überwiegend unabhängige Entwicklungsstränge herauszubilden begannen:

- A. **Zertifizierung nach Cloud-Standards:** Die geläufigste Interpretation von Zertifizierung ist die Zertifizierung nach Standards oder sonstigen Vorgaben oder Kriterien.

---

<sup>152</sup> Zusätzlich hat die japanische Zeitschrift NTT Technical Review in 2011 einen Überblick über die Cloud-Standardisierung erstellt. Siehe <https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201106gls.html>



- Zertifizierungen im Cloud Computing sind im Kontext bereits länger **existierender allgemeinerer Zertifizierungsmöglichkeiten** zu sehen. Bestehende Zertifizierungen in der IT-Sicherheit (z.B. IT-Grundschutz-Zertifikat inkl. ISO 27001) trafen auf großen Vertrauensbedarf im Cloud Computing, weshalb diese Zertifizierungen anfänglich die größte Rolle im Cloud Computing gespielt haben. Zunehmend gewinnen auch Zertifizierungen für Datenschutz, Ausfallsicherheit, Compliance (z.B. SSAE-16 / ISAE-3402) und Governance (z.B. GRC Stack, SCAP) an Bedeutung.
- Seit etwa 2010 und mit dem Erscheinen von **Zertifizierungen mit explizitem Cloud Fokus** (EuroCloud Gütesiegel, Trust in Cloud, EuroPriSe) und Auditierungsstandards (z.B. Cloud Audit) für das Cloud Computing erreicht dieser Trend größere Reife.
- Experten der **Deutschen Telekom** fordern im September 2011 eine Zertifizierung für eine „Deutsche Cloud“<sup>153</sup>, die einen Zugriff durch US-Behörden gemäß des „Patriot-Act“ ausschließt.
- **Salesforce.com** wirbt auf ihrem „Vertrauensportal“<sup>154</sup> aktiv mit Zertifikaten, die von Salesforce erworben wurden (SysTrust<sup>155</sup>, VeriSign Secured<sup>156</sup>, TRUSTe<sup>157</sup>, BISGroup für ISO/IEC 27001:2005<sup>158</sup>, SafeHarbor).
- Der **CIO der US-Verwaltung** hat im April 2010 im Rahmen einer Keynote sein Ziel offengelegt Zertifizierungen für Cloud Computing in der gesamten US-Verwaltung in Zukunft aus Effizienzgründen zentral und automatisiert durchführen zu lassen.
- Eine Arbeitsgruppe in diesem Bereich ist **die Cloud Audit Data Federation Working Group (CADF)** der DMTF, die Standards zur Verbreitung von Audit-Informationen erarbeitet, um das Vertrauen in Cloud-Anbieter zu stärken.

B. **Zertifizierung von Cloud-Experten:** Mit zunehmender Reife der Cloud Computing-Industrie steigt der Bedarf an qualifiziertem Personal für diesen Bereich. Als Folge entstehen in der Privatwirtschaft seit 2009 unabhängige (z.B. Certificate of Cloud Security Knowledge der CSA, Cloud Experte von SaaS EcoSystem oder Cloud Experte der Cloud School) und firmenspezifische Zertifizierungen (z.B. IBM certified solution advisor for Cloud Computing) für die Qualifikation als Cloud-Experte. Diese Zertifizierungen besitzen einen engen Bezug

---

<sup>153</sup> <http://www.bloomberg.com/news/2011-09-13/deutsche-telekom-wants-german-cloud-to-shield-data-from-u-s-.html>

<sup>154</sup> <http://trust.salesforce.com/>

<sup>155</sup> <http://www.webtrust.org>

<sup>156</sup> <http://www.verisign.com/ssl/buy-ssl-certificates>

<sup>157</sup> <http://www.truste.com/privacy-program-requirements/>

<sup>158</sup> <http://www.bsigroup.com/en/Assessment-and-certification-services/Client-directory/>



zum ersten Entwicklungsstrang, da sie häufig auf Zertifizierungen von Cloud-Standards basieren.

- C. **Zertifizierung von Cloud-Partnern:** Die zunehmend übliche Auslagerung von Prozessketten der Wertschöpfungsprozesse stellt auch die Cloud Computing-Industrie vor die Herausforderung gleichbleibende Qualität an die Kunden zu gewährleisten. Seit 2010 setzen deshalb insbesondere große internationale IT Anbieter (z.B. SAP, IBM, Microsoft) auf eigene Zertifizierungen von Cloud-Partnern (z.B. SAP Certified Provider of Cloud Services).

Die Cloud-Zertifizierung adressiert neben Informationssicherheit, Datenschutz und Compliance zunehmend andere Herausforderungen, wie Transparenz (z.B. freier Zugang zu Auditierungsinformation), Dienstbereitstellung oder auch Interoperabilität und Portabilität. Gerade in den letzten Bereichen sind allerdings lediglich erste Bemühungen zu erkennen. Cloud-spezifische Standards sind erst im Entstehen bzw. in Planung. Aktuelle Standards besitzen häufig geringe Detaillierung und reflektieren den frühen Entwicklungsstand der Cloud-spezifischen Zertifizierungen. Die Zertifizierung von Cloud-Experten und Cloud-Partnern besitzt indirekten aber mittelfristig wesentlichen Einfluss auf das allgemeine Standardisierungsgeschehen im Cloud Computing, da sie in vielen Fällen eine Neigung zu bevorzugten Cloud-Standards und Lösungen der Zertifizierung besitzen werden, und hat somit ebenfalls großes Potenzial für offene und unabhängige Standards, die den Wettbewerb stärken können.

Der Trend hin zu Cloud-Zertifizierungen gewinnt gerade erst an Schwung, insbesondere im Bereich automatisierter Auditierungen über den gesamten Lebenszyklus. In anderen Bereichen ist das Momentum noch geringer, da Zertifizierungen geeignete Cloud-Standards voraussetzen und diese selbst noch in der Erarbeitung sind. Die Durchsetzungsfähigkeit der Zertifizierungen mit implizitem Bezug zum Cloud Computing ist verhältnismäßig hoch – expliziten Cloud-Zertifizierungen mangelt es durch den oft geringen Reifegrad der zugrundeliegenden Standards noch an Durchsetzungsfähigkeit.

Die Notwendigkeit von Cloud-Zertifizierungen wird absehbar weiter steigen. Aus Sicht etablierter Cloud Computing-Anbieter sind Zertifizierungen ein Mittel, um im Markt weitere Wettbewerbsvorteile zu erlangen. Aus Sicht der Anwender tragen Zertifizierungen und Auditierungsstandards wesentlich zur Vertrauensbildung bei. Die Mitwirkungsmöglichkeiten sind abhängig vom speziellen Cloud-Standard, für den eine Zertifizierung angestrebt wird.

### 6.2.3 Offenheit im Cloud Computing

Seit der Entstehung von Cloud Computing gibt es auch Bestrebungen auf unterschiedlichen Ebenen, um Offenheit im Cloud Computing zu schaffen. Offenheit und Standardisierung sind in diesem Zusammenhang eng verbunden und verfolgen beide die Ziele mehr Wettbewerb, verstärkte Marktteilnahme und verbesserte Markteffizienz im Cloud Computing. Die Ziele von „Open Cloud“ unterscheiden sich dabei von denen von „Open Source“. Die Open

Cloud Initiative betrachtet gemäß ihrer Grundsätze <sup>159</sup> einen offenen Standard im Cloud Computing nur dann als gewährleistet, wenn

- er in allen Details dokumentiert, veröffentlicht und zugänglich ist und das Copyright eine unentgeltliche (Wieder-)Verwendung erlaubt,
- mögliche Patente, auch auf nur Teile des Standards, unwiderrufbar lizenzfrei zur Verfügung stehen,
- Handelsmarken ausschließlich für die nicht-diskriminierende Auszeichnung der Compliance verwendet werden und
- die client- und serverseitige Implementierung gewissenhaft umgesetzt wurde und wahlweise unter einer OSI-bestätigten Lizenz oder als Public Domain freigegeben wurde.

Folgende Organisationen, Vereinigungen und Initiativen besitzen aktuell den größten Einfluss auf offene Standards im Cloud Computing:

- **Open Cloud Initiative (OCI):** OCI ist ein gemeinnütziger Verein in Kalifornien, der offiziell im Juli 2011 mit der Vision angetreten ist, die Idee der „Open Cloud“ durch Standardisierung weltweit voranzutreiben. OCI ist keine Mitgliederorganisation, sondern wird von vertrauenswürdigen erfahrenen Direktoren geleitet, die sich dem Ziel der Offenheit verpflichtet fühlen (z.B. von Cisco, Apache, Deutsche Wolke).
- **Open Cloud Manifesto (OCM):** Im März 2009 haben 30 Firmen (u.a. AMD, Cisco, EMC, Juniper, Novell, SAP, Sun, VMware) unter Führung von IBM das sogenannte OCM (siehe 5.3.1) unterzeichnet, das Offenheit im Cloud Computing fordert. <sup>160</sup> Wichtige Akteure, wie Amazon, Microsoft, Salesforce.com und Google nehmen nicht teil.
- **Open Cloud Consortium (OCC):** OCC (siehe 4.3.8) ist eine Mitgliederorganisation in den USA, die sowohl Privatfirmen (z.B. Citrix, Cisco, Yahoo!, Booz Allen Hamilton) als auch fünf Universitäten und drei US-Behörden umfasst. Fokus sind Forschung u. Referenzimplementierung.
- **DMTF Open Cloud Standards Incubator (OCSI):** OCSI ist eine Arbeitsgruppe der DMTF (siehe 4.3.2), die bis Juli 2010 Spezifikationen und Leitfäden zu Interoperabilität, Architektur und Use Cases verfasst hat. Mitglieder sind AMD, Cisco, Citrix, EMC, HP, IBM, Intel, Microsoft, Novell, Red Hat, Savvis, Sun Microsystems und VMware.

Weitere relevante Arbeitsgruppen sind zum Beispiel die Open Group Cloud Work Group (OGCWG) (siehe 4.3.10), die Open Cloud Computing Interface Working Group (OCCI-WG) und die IETF/OAuth-WG.

Wichtige offene Spezifikationen und Standards sind etwa OVF, OCCI, Cloud Audit, OGF-UC1, OpenID und OAuth.

---

<sup>159</sup> Quellen: <http://www.opencloudinitiative.org/> principles, Heise, Analyse von Booz & FZI.

<sup>160</sup> Der aktuelle Präsident der Open Cloud Initiative Sam Johnston war auch Mitinitiator des Open Cloud Manifesto.

Im Open Source Bereich werden offene Referenzimplementierungen für Cloud Computing wie Open Stack (110 Beteiligte) und Eucalyptus (>80 Partner) vorangetrieben, die ebenfalls eine wichtige Ausgangsbasis für die Entwicklung von Standards darstellen. Bei den beteiligten Firmen handelt es sich um eine Vielzahl internationaler KMUs im Bereich IKT und auch großen IKT-Firmen aus den Reihen der Firmen, die auch in oberen Initiativen aktiv sind. In Deutschland hat die Open Source Business Foundation e.V. (OSBF) kürzlich die Open Cloud Business Initiative (OCBI) gestartet.

Die Analyse liefert folgende Einblicke: Offenheit und offene Standards im Cloud Computing werden vor allem von solchen Akteuren unterstützt, die selber bisher keinen oder nur geringen Zugang zum Cloud Computing-Markt erhalten haben. Hierzu zählen viele KMUs, aber auch große Anbieter, wie AMD, Cisco, Citrix, IBM, VMware oder Open Source Initiativen, wie Apache. Akteure und Initiativen, die Offenheit nicht aus privatwirtschaftlichen Interessen anstreben, sind in der Unterzahl (z.B. Open Cloud Initiative). Insbesondere ist die geringe Beteiligung öffentlicher Einrichtungen auffällig, obwohl die Gremien überdurchschnittlich offen für eine Beteiligung sind. Die Unterstützer von Offenheit im Cloud Computing bilden folglich eine Front gegen etablierte Kräfte, wie Google, Amazon, Apple oder Microsoft, die die größten Marktanteile besitzen und ihre Marktposition durch Offenheit in der Regel bedroht sehen. Auch bei der Standardisierung sind sie den anderen Akteuren voraus. Nichtoffene Ansätze, wie EC2, strahlen heute noch eine deutlich höhere Attraktivität auf Anwender aus als zum Beispiel OVF. Es deutet sich an, dass ohne äußere Einwirkung die etablierten Akteure ihre proprietären Standards durchsetzen werden. Zusätzlich gibt es auch unterschiedliche Auffassungen über Offenheit und deren Ziele, was sich in den unterschiedlichen Mitgliederansätzen von OCI und OCC offenbart (siehe oben). Es besteht das Potenzial auf den wertvollen Referenzimplementierungen und guten ersten Ansatzpunkten, wie der Deutschen Wolke, aufzubauen und offene Standards für das Cloud Computing auch im Interesse der Regelsetzer zu stärken.

### 6.2.4 Rechtssicherheit für die Cloud

Das Thema „Rechtssicherheit in der Cloud“ hat seit 2010 große öffentliche Aufmerksamkeit bei Anbietern, Anwendern, Regelsetzern bzw. in Presse und Fachkreisen erlangt. Insbesondere die großen US-Anbieter bieten zunehmend ausgereifere Cloud Lösungen, mit denen eine größere weltweite Kundschaft erschlossen werden konnte. Das pragmatische Vorgehen dieser Anbieter hat zur Folge, dass die rasante technische Entwicklung einer rechtlichen Untersuchung um Längen voraus ist. Folglich vernachlässigen diese Lösungen bisher in der Regel bestehendes nationales Recht mit allen mittelfristigen Risiken und Unwägbarkeiten für alle Akteure. Cloud Computing entbindet die Nutzer jedoch nicht von bestehenden Rechtsvorschriften, zum Beispiel vom Datenschutz: Der Nutzer, also der Auftraggeber,

- bleibt auch beim Cloud Computing vollständig verantwortlich für die rechtmäßige Datenverarbeitung (§ 11 BDSG),

- ist gesetzlich verpflichtet, den Anbieter sorgfältig auszuwählen (§11 Abs. 2 S.1 BDSG) und
- muss nach Vertragsschluss regelmäßig prüfen, ob der Anbieter die erforderlichen technischen und organisatorischen Maßnahmen einhält.

Erschwerend kommt hinzu, dass die rechtlichen Implikationen von Cloud Computing allgemein komplex sind, in Abhängigkeit der geltenden Rechtsphäre zu beurteilen sind, Besonderheiten je Branche und Anwendungsfall <sup>161</sup> aufweisen sowie in einigen Bereichen noch nicht hinreichend geklärt sind. Einen Beitrag zur Vereinfachung könnte die Neuregelung des Datenschutzes auf EU-Ebene leisten.

Es verwundert nicht, dass einer der wichtigsten potenziellen Cloud Computing-Anwender in Deutschland, nämlich der Mittelstand bzw. KMUs, die bestehende Rechtsunsicherheit als einen der Hauptgründe für die Zurückhaltung beim Cloud Computing angeben.<sup>162</sup> Die Yankee Group berichtet, dass 67% der mittleren und großen Unternehmen Private Clouds bevorzugen, wenn die Vorteile von Cloud Computing realisiert werden sollen. Als einer der wichtigsten Gründe hierfür wird Compliance angegeben. In einigen Anwendungsfällen ist Cloud Computing in der jetzigen Form sogar rechtlich nicht zulässig. Rechtsexperten befürchten allerdings, dass Unternehmen aufgrund geschäftlicher Interessen und durch den Einfluss der Medien die komplexe Rechtslage vernachlässigen könnten.<sup>163</sup>

**Standardisierung** im weiteren Sinn besitzt die zentrale Rolle bei der Schaffung von Rechtssicherheit im Cloud Computing. Nur über eine Vereinheitlichung und Anpassung gesetzlicher Regelungen sowie der Erarbeitung standardisierter Hilfsmitteln (z.B. Verträge, Leitlinien) zur Schaffung von Rechtssicherheit wird sich ein hinreichend rechtskonformes und -sicheres Umfeld für die Nutzer und Anbieter schaffen lassen.

Bei genauerer Betrachtung betreffen die Fragestellungen beim Cloud Computing viele Rechtsbereiche, die jeweils individuell und in Kombination zueinander <sup>164</sup> beantwortet werden müssen. Neben dem Datenschutzrecht sind auch das Sicherheits-, Strafprozess-, Verbraucher-, AGB-, Steuer-, Handels-, Urheber-, Privat- und IT-Vertragsrecht relevant. Als anderweitiges Beispiel

---

<sup>161</sup> Beispiele: Finanzdienstleistungssektor (§ 25 a KWG, GoBS, § 20 ZAG), Telekommunikationsbereich (TKG), Träger von Berufsgeheimnissen (§ 203 StGB: Ärzte, Anwälte, Lebens-, Kranken- oder Unfallversicherer), Anwendungen steuerrelevanter Daten (§§ 146, 147 AO, GDPdU, § 41 EstG).

<sup>162</sup> Siehe z.B. das 10-Punkte-Papier (Dez 2010) der Gesellschaft für Informatik e.V.: <http://www.gi.de/presse/pressearchiv/pressemitteilungen-2010/pressemitteilung-vom-1-dezember-2010.html>.

<sup>163</sup> <http://www.otoxa.com/nc/news/news/cloud-computing-und-rechtssicherheit.html>

<sup>164</sup> Außerdem stellen Cloud-Verträge eine Mischform aus Werk-, Miet- und Leihverträgen dar. Es handelt sich also um eine Matrix, die bei jedem Einzelfall anders aussieht. Aus diesem Grunde können bei solch einem komplexen Thema keine simplifizierten Einheitslösungen angeboten werden.

seien Bilanzierungsrechte zu nennen, die die Vertragsgestaltung im Cloud Computing beeinflussen und bei deren Missachtung die erfolgreiche Jahresabschlussprüfung gefährdet ist.

Gesetzliche Vorgaben sind allerdings nur ein Faktor, der die Rechtssicherheit aus Sicht von Cloud-Nutzern und Anbietern mitbestimmt. Vor allem die Cloud-Nutzer benötigen vertragliche Regelungen, die sicherstellen, dass ihre potenziell sensiblen Daten und Informationen vertraulich behandelt werden, sie Ansprüche aus einer Missachtung geltend machen können und insbesondere die Haftung regeln. Die Cloud-Anbieter ihrerseits befürchten Klagen aus möglichen Datenschutzverletzungen oder hohe Kosten durch individuelle Lösungen für einzelne Staaten. Im Rahmen der EU-Konsultationen zum bestmöglichen Einsatz von Cloud Computing in Europa <sup>165</sup> melden sich beispielsweise Google und Microsoft öffentlich zu Wort und fordern einen harmonisierten EU-Datenschutz.<sup>166</sup> Die EU strebt derzeit eine Novellierung der Datenschutzregeln aus dem Jahre 1995 an (vgl. Kapitel 5.3.1).

Wichtige Initiativen mit Bezug zur Rechtssicherheit sind u.a. die Initiative „Cloud Services Made in Germany“<sup>167</sup>, die Deutsche Wolke<sup>168</sup>, Die Arbeitsgruppe 3 „Contracts and eDiscovery“ der CSA <sup>169</sup>, die Arbeitsgruppe „Privacy and Public Policy (P3)“ von Kantara <sup>170</sup> und eine geplante Arbeitsgruppe zum Datenschutz bei der OMG.

Die Herstellung von Rechtssicherheit im Cloud Computing bedarf einer gesamthafter Sicht und der unterschiedlichsten Mittel, um dem grenzüberschreitenden und besonderen Charakter von Cloud Computing Rechnung zu tragen. Einen Überblick und Lösungsansätze bieten zum Beispiel der Euro-Cloud „Leitfaden Cloud Computing: Recht, Datenschutz & Compliance“ (LRD&C) vom Dezember 2010 <sup>171</sup> oder der BITKOM Leitfaden zu diesem Thema <sup>172</sup>.

Folgende nicht abschließende Auflistung umfasst mögliche Ansatzpunkte in der Standardisierung zur Herstellung von Rechtssicherheit im Cloud Computing:

---

<sup>165</sup> <http://europa.eu/rapid/pressReleasesAction.do?reference=IP%2F11%2F575&format=HTML&aged=1&language=DE&guiLanguage=en>

<sup>166</sup> <http://heise.de/-1341666>

<sup>167</sup> <http://www.cloud-services-made-in-germany.de>

<sup>168</sup> <http://www.deutsche-wolke.de>

<sup>169</sup> <https://cloudsecurityalliance.org/research/working-groups/>

<sup>170</sup> <http://kantarainitiative.org/wordpress/groups/privacy-and-public-policy-work-group/>

<sup>171</sup> <http://www.eurocloud.de/2010/12/02/eurocloud-leitfaden-recht-datenschutz-compliance/>

<sup>172</sup> „Cloud Computing – Was Entscheider wissen müssen. Ein ganzheitlicher Blick über die Technik hinaus. Positionierung, Vertragsrecht, Datenschutz, Informationssicherheit, Compliance Leitfaden.“, [http://www.bitkom.org/files/documents/BITKOM\\_Leitfaden\\_Cloud\\_Computing-Was\\_Entscheider\\_wissen\\_muessen.pdf](http://www.bitkom.org/files/documents/BITKOM_Leitfaden_Cloud_Computing-Was_Entscheider_wissen_muessen.pdf).



- Anpassungen des bestehenden Rechtsrahmens (z.B. Harmonisierung innerhalb der EU, Rahmengesetz für Cloud Computing).
- Zwischenstaatliche Vereinbarungen, wie zum Beispiel Safe Harbor.
- Selbstverpflichtungen der Cloud-Anbieter und rechtskonforme Cloud Computing-Angebote (z.B. Cloud-Anbieter mit Hauptniederlassungen im EU/EWR-Raum, die für Datenschutzverstöße außerhalb der EU haften (Binding Corporate Rules); Zusicherung des Orts der Datenspeicherung und -verarbeitung).
- Leitlinien und Vorlagen zur Vertragsgestaltung / für SLAs (Haftung, Gerichtsstand, Rechtswahl, Schiedsklauseln, Leistungsverrechnung, Leistungsstörungen, Vertragskündigung, Insolvenz des Auftragnehmer, Compliance, Einbindung von Unterauftragnehmer, Kontrollrechte, deutsche Vertragsvorlagen).
- Verschiedenste technische und organisatorische Ansätze als Mittel zur Kontrolle, Compliance und Governance (Risikomanagement, Kontrollsysteme, ITIL, Reporting, automatische Auditierung, firmeninterne Datenschutzorganisation, Firmenrichtlinien etc.).
- Zertifizierung, z.B. für Governance (ISO38500), Informationssicherheit (BSI 100), Datenschutz, Risikomanagement (MaRisk, KontraG), Outsourcing (PS951/SAS70/SSAE16 / ISAE3402), interne Kontrollsysteme (JAP, IDW PS261, 330 / ERS FAIT 1).

Wie unmittelbar aus der Verschiedenartigkeit der Ansatzpunkte ersichtlich wird, kann vollständige Rechtssicherheit auf keinem einfachen Weg erreicht werden, sondern bedarf des Zusammenwirkens sehr unterschiedlicher Maßnahmen und Standardisierungsanstrengungen. Entsprechend stehen die Bemühungen um Rechtssicherheit ebenfalls am Anfang.

Abschließend kann Rechtssicherheit als bisher überwiegend ungelöstes Problemfeld im Cloud Computing betrachtet werden. Die Vielfalt und das Gewicht der noch ungelösten Fragen werden beispielsweise vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein thematisiert<sup>173</sup>. Zwar werden die Forderungen nach Rechtssicherheit in dem Maße stärker werden, wie das Angebot an Cloud Computing-Lösungen zunimmt, entscheidend für einen Erfolg wird aber ein noch stärkeres Engagement für Offenheit durch Unternehmen und Verbände sein. Von staatlicher Seite kann dies durch Koordination oder partizipative Instrumente unterstützt werden.

### 6.2.5 Cloud-Marktplätze

Seit etwa 2010 wird die Idee von Cloud-Marktplätzen verstärkt aufgegriffen und es finden sich zunehmend erste Anbieter und Prototypen von Marktplätzen. Die Idee des Cloud-Marktplatzes geht über die ursprünglich engere Definition von Cloud Computing hinaus und stellt somit eine innovative Erwei-

---

<sup>173</sup> <https://www.datenschutzzentrum.de/cloud-computing/>



terung des Konzepts dar. Sie hat ihren Ursprung in einer Vielzahl von Entwicklungstrends, z.B. Verfügbarkeit von Online-Portalen (z.B. eBay, apps-Marktplätze), Handelsbörsen (XETRA, Strommarkt), Industrialisierung der IT oder IT als Massenware, um nur einige zu nennen. Ohne Cloud Computing und Standardisierung wären Cloud-Marktplätze ebenfalls nicht denkbar.

Aber was sind nun Cloud-Marktplätze? Auf diese Frage erhält man heute noch eine Vielzahl verschiedener Antworten. Im Folgenden wird eine mögliche Definition umrissen, die naturgemäß nur vorläufigen Charakter besitzen kann, da sich dieser Trend voraussichtlich wesentlich weiterentwickeln wird. Ein Cloud-Marktplatz

- ist ein Vermittler von Cloud-Diensten und fokussiert sich auf deren Angebot, Bereitstellung und Abrechnung (nach Zeit oder Last),
- bietet Cloud-Dienste verschiedener Anbieter, die miteinander gemäß des Marktplatzgedankens im Wettbewerb zueinander stehen,
- bietet Leistungen mit Serviceanteil <sup>174</sup>, der in der Regel auf einer pay-per-use Basis abgerechnet wird,
- kann die Möglichkeit vorsehen, verschiedene Cloud-Dienste zu orchestrieren, also zu Mehrwertdiensten zu kombinieren,
- ist ein Angebot an den Nutzer, der über den Cloud-Marktplatz einfachen Zugang zu verschiedenen Cloud-Diensten erhält und
- kann sowohl SaaS, IaaS oder PaaS anbieten, bzw. eine Kombination dieser Arten von Cloud-Diensten.

Aus Sicht des Cloud Computing kann der Marktplatzanbieter entweder gleichzeitig als Cloud-Betreiber auftreten, der die Cloud-Dienste auch betreibt, oder aber als reiner Integrationspunkt im Sinne einer „Wolke von Wolken“. Die Rollenverteilungen können sehr unterschiedlich sein.

Durch die Vielzahl der abgewickelten Services und teilnehmenden Akteure sowie der Notwendigkeit von Flexibilität und Effizienz, ist ein funktionierender Cloud-Marktplatz ohne hochgradige Standardisierung schwer vorstellbar. Auf einem Cloud-Marktplatz kennen sich Anbieter und Nutzer von Cloud-Diensten im Vorhinein nicht. Folglich müssen Anbieter ihre Services generisch, also ohne direkte Vorgaben vom Kunden, entwickeln und insbesondere SLAs festschreiben. Der gesamte Geschäftsablauf sowie die Nutzung von Instanzen müssen vollautomatisch ablaufen. Auf Kundenseite muss vor allem der Bedarf nach Vertraulichkeit erfüllt werden.

Eine rudimentäre Form von Cloud-Marktplätzen, wenn man den Begriff weit fasst, sind z.B. der App Store von Apple oder der Android Market von Google, deren Services auch zunehmend auf Desktop oder Tablet PCs verfügbar sind.

---

<sup>174</sup> Ein Cloud-Marktplatz beschränkt sich folglich nicht auf den reinen Verkauf von Dingen (z.B. eBay).

Die Ausgestaltung und Art der Vorteile der Cloud-Marktplätze sind besonders stark von der Art der Cloud-Dienste, die angeboten werden, abhängig.

IaaS Marktplätze, die Infrastruktur-as-a-Service, also Speicherplatz, Rechenleistung und/oder Laufzeitumgebungen anbieten, besitzen vor allem die Vorteile hoher Skalierbarkeit, hoher Effizienz durch Lastenmanagement und Einfachheit durch Bereitstellung von Massenware („Commoditization“). Beispiele sind u.a. Rackspace<sup>175</sup> oder Enomaly<sup>176</sup>.

SaaS Marktplätze, die interoperable Anwendungen on-demand aus der Cloud anbieten, haben den Reiz, dass die lange angestrebte Industrialisierung der IT, also Wiederverwertbarkeit und Integration von Wertschöpfungsketten auch im Sinne von e-Government, nun in greifbare Nähe rücken. Beispiele sind der TEXO-Marktplatz<sup>177</sup>, CLOUDwerker<sup>178</sup>, die Logistics Mall<sup>179</sup> der Fraunhofer ISST und IML, goBerlin<sup>180</sup> oder Cloud Cycle. Letzteres zeigt, dass Marktplätze eine Möglichkeit darstellen, um dem „One-Stop-Government“ Gedanken noch einen Schritt näher zu kommen.

Data-as-a-Service Marktplätze schaffen neue Verbindungen und Möglichkeiten der automatisierten Analyse bestehender bisher verteilter Datenbanken. Beispiele sind MIA<sup>181</sup> oder SensorCloud<sup>182</sup>.

Human-as-a-Service Marktplätze sind ein Grenzfall und ggf. nicht mehr dem Cloud Computing zuzurechnen, da sie eigentlich den Einkauf von Dienstleistungen ermöglichen, die dann aber von Menschen erbracht werden.

Eine Vielzahl von Standards sind für die Realisierung von Cloud-Marktplätzen notwendig, beispielsweise Standards zu Dienstbeschreibungssprachen, Abrechnungsmodellen, APIs, Datenaustauschformaten, SLAs, Zertifizierung oder Datenschutz. Abhängig von der spezifischen Fragestellung werden auch sehr spezielle Standards notwendig. Der Trend hin zu Cloud-Marktplätzen kann allgemein als vielversprechende Entwicklung gewertet werden, da die Vorteile vielfältig sind und von stärkerem Wettbewerb über größere Effizienz bis zu möglichem Wirtschaftswachstum reichen. Dies unterstreicht die Bedeutung, die der Standardisierung im Cloud Computing allgemein zukommt. Die Offenheit für eine Mitgestaltung ist je nach Serviceart sehr unterschiedlich. Während bei IaaS, derzeit Amazon mit AWS, die Standards dominiert, ist die Verwaltung bei SaaS Marktplätzen mit goBerlin oder dem TEXO-Marktplatz gut positioniert.

---

<sup>175</sup> <http://www.rackspace.com/>

<sup>176</sup> <http://www.enomaly.com/>

<sup>177</sup> <http://internet-of-services.com/index.php?id=277&cmd=infomail&backURL=index.php%3Fid%3D277>

<sup>178</sup> <http://www.trusted-cloud.de/de/845.php>

<sup>179</sup> <http://www.ccl.fraunhofer.de/>

<sup>180</sup> <http://www.trusted-cloud.de/>

<sup>181</sup> <http://www.trusted-cloud.de/de/778.php>

<sup>182</sup> <http://www.trusted-cloud.de/de/774.php>

### 6.2.6 Governance im Cloud Computing

In den letzten drei Jahren wird der Begriff der „Governance“ zunehmend im Zusammenhang mit Cloud Computing verwendet. Seinen inhaltlichen Ursprung hat er in der IT-Governance, die dazu dient die Planung, Entwicklung und den Betrieb der IT an den Unternehmenszielen auszurichten. Die hierfür eingesetzten Mittel sind vielfältig und reichen von der grundsätzlichen Organisation der Unternehmens-IT inkl. Struktur, Rollen und Verantwortlichkeiten über (IT-)Prozesse oder Richtlinien bis zum Controlling mit Steuerungskennzahlen („KPIs“). Die Einführung und Durchsetzung einer Governance ist Aufgabe der Führungs- und Leitungsebenen einer Organisation. Für die Diskussion von Standards einer guten Governance im Cloud Computing („Cloud-Governance“) stellen sich folglich vorab immer drei Fragen:

- Für welche Organisation / Akteur ist die Cloud-Governance gedacht?
- Welche Mittel zur Erreichung einer guten Cloud-Governance sollen eingesetzt werden?
- Welchen Zielen folgt die Cloud-Governance insbesondere in Abgrenzung zur IT-Governance?

Grundsätzlich stellt sich für jeden Akteur, wie beispielsweise Cloud-Anbieter, Cloud-Nutzer oder Regulator, im Cloud-Ökosystem die Herausforderung einer guten Cloud-Governance, wobei deren Ziele variieren. Der Fokus liegt an dieser Stelle vor allem auf der Sicht von Cloud-Betreibern, da diese die zentralste Stelle im Ökosystem innehaben und für diese die größten Bemühungen bei der Standardisierung für eine gute Cloud-Governance erkennbar sind.

Die Mittel zur Erreichung einer guten Cloud-Governance gleichen im Wesentlichen den Ansatzpunkten für die Standardisierung, wie sie im Rahmen dieser Studie in Kapitel 3.2.2 definiert wurden.

In ähnlicher Weise kann man in einer ersten Näherung annehmen, dass die Herausforderungen für das Cloud Computing, wie sie in Kapitel 3.2.1 definiert wurden, den möglichen unspezifischen Zielen einer guten Governance im Cloud Computing im Wesentlichen entsprechen, da es das erklärte Ziel der Unternehmensleitung sein sollte, diese Herausforderungen zu adressieren. Es sei angemerkt, dass die spezifischen Zielsetzungen eines Cloud-Anbieters natürlich sehr verschieden sein und sich insbesondere für öffentliche und privatwirtschaftliche Betreiber unterscheiden können.

Im Folgenden werden beispielhaft wesentliche Standards für gute Cloud-Governance für Cloud-Betreiber angeführt.

- Der prominenteste Standard für gute Governance und mit explizitem Bezug zum Cloud Computing ist der Governance, Risikomanagement und Compliance Stack (GRC Stack, siehe 5.2.3). Das Cloud Trust Protocol (CTP, siehe 5.1.4) und CloudAudit (CA, siehe 5.2.2), die beide Teil des GRC Stacks sind, adressieren vor allem Transparenz und Vertrauensbildung während die Cloud Controls Matrix (CCM, siehe 5.2.3) und der Consensus Assessments Initiative Questionnaire (CAIQ) jeweils Informationssicherheit, Risikomanagement und Datenschutz adressieren.

- Die Open Group stellt in dem Whitepaper „Cloud Computing Key Performance Indicators and Metrics“<sup>183</sup> mögliche KPIs und Kennzahlen vor. Ein wesentlicher Diskussionspunkt ist hierbei, wie Leistung gemessen werden sollte, ob nur in technischen Einheiten oder vor allem in monetären Maßstäben.
- Einige Leitfäden (z.B. Euro Cloud LRD&C) gehen auch explizit auf Compliance, Vertragswesen, SLAs sowie Kontrollrechte und Eskalationsmechanismen ein.

Auch bestehende IT-Governance Standards, die nur einen impliziten Bezug zu Cloud Computing besitzen, kommt eine wesentliche Bedeutung für eine Cloud-Governance zu, da diese in angepasster Form wichtige Herausforderungen an der Schnittstelle von allgemeiner IT und Cloud Computing adressieren. Zu nennen sind hier insbesondere die BSI Grundsicherungsstandards (BSI 100), ITIL oder COBIT der ISACA. Das BSI empfiehlt den Einsatz von ITIL- und COBIT für Cloud Betreiber.<sup>184</sup> Mögliche Vorteile zeigt SERVVIEW auf.<sup>185</sup> Allerdings sei darauf hingewiesen, dass mögliche Cloud-spezifische Zusätze oder Anpassungen für ITIL oder COBIT sinnvoll sein könnten. Häufige Anwendung findet auch der SSAE 16, der Unternehmen dabei unterstützt den Wert und das Risiko einer Auslagerung von Prozessketten zu bewerten, wie es oft implizit beim Cloud Computing der Fall ist.

Standards sind auch im Allgemeinen als Hilfsmittel zur Vereinheitlichung und Steuerbarkeit für gute Governance relevant, weshalb viele weitere Cloud-Standards allgemein Relevanz besitzen. Insbesondere Zertifizierungen besitzen (siehe 6.2.2) eine wichtige Funktion.

Der Trend hin zu Governance-Standards im Cloud Computing liefert bereits einige praktisch verwertbare Ergebnisse (z.B. GRC Stack). Dies trägt dem großen Bedarf nach Governance im Cloud Computing, der durch die anspruchsvollen Beziehungen und die hohe Vernetzung der Akteure im Cloud-Ökosystem entsteht, Rechnung. Allerdings finden die Anforderungen verschiedener Zielgruppen (z.B. Cloud Anbieter vs. Cloud Nutzer) noch nicht in ausgewogener und konsistenter Weise Einzug in bestehende Standards. Gleichzeitig stehen noch viele weitere Detailarbeiten aus, um die Gesamtheit der Problemstellungen konsistent zu adressieren. Die Mitwirkung von Regelsetzern bei Governance-Standards für das Cloud Computing bietet die Chance Anforderungen über einen alternativen Weg zur Festlegung rechtlicher Vorgaben zu verankern. Es kann mit großer Wahrscheinlichkeit davon ausgegangen werden, dass gute Governance für alle Akteure im Cloud Computing steigende Relevanz besitzen wird, da schon alleine die Komplexität im Cloud Computing große Risiken in sich birgt.

---

<sup>183</sup> <http://www.opengroup.org/cloud/whitepapers/ccroi/kpis.htm>

<sup>184</sup> Sicherheitsempfehlungen für Cloud Computing Anbieter (Eckpunkt Papier), BSI, 2011.

<sup>185</sup> ITIL und Cloud Computing: Welchen Mehrwert bietet ITIL mit seinem Service Lifecycle-Ansatz für Cloud Computing (Whitepaper), SERVVIEW, 2009.

## 7 Handlungsempfehlungen zur Standardisierung im Cloud Computing an die Bundesregierung

*Vorbemerkung: Die Empfehlungen in diesem Kapitel sollen eine Diskussionsgrundlage schaffen, um ein koordiniertes und arbeitsteiliges Vorgehen verschiedener Akteure vor allem der öffentlichen Verwaltung und der Wirtschaft zu ermöglichen. Den Handlungsempfehlungen werden zum aktuellen Zeitpunkt bewusst keine Verantwortlichkeiten zugewiesen, so dass sie keinen konkreten Adressaten besitzen.*

In diesem Kapitel werden Handlungsempfehlungen für die Standardisierung im Cloud Computing abgeleitet, die sich aus den Ergebnissen dieser Studie insgesamt ergeben. Standardisierungen sind in der heute vernetzten Welt immer auch auf internationaler Bühne relevant. Dennoch richtet sich diese Studie an deutsche Akteure, die auch über ihre Mitwirkung in europäischen und internationalen Gremien auf entsprechende Standardisierungen einwirken können und sollten. Zentraler Adressat der Handlungsempfehlungen ist die deutsche Bundesregierung. Die überwiegende Mehrheit der Handlungsempfehlungen lassen sich auf EU-Ebene übertragen.

Einführend wird der strategische Handlungsrahmen (Kapitel 7.1.1), in dem eine Standardisierung stattfinden soll, umrissen und die Notwendigkeit eines Handelns begründet (Kapitel 7.1.2). Vor diesem Hintergrund werden Handlungsziele, Handlungsfelder, Zeitrahmen und mögliche Instrumente abgeleitet (Kapitel 7.1.3). Nachfolgend werden die zwei empfohlenen strategischen Handlungsziele bei der Standardisierung und deren Handlungsfelder im Detail beschrieben (Kapitel 7.2, 7.3).

### 7.1 Handlungsrahmen, -begründung und -ziele

#### 7.1.1 Der strategische Handlungsrahmen

Der Handlungsrahmen für eine Standardisierung im Cloud Computing auf europäischer und deutscher Ebene entwickelt sich dynamisch. Für die Bundesregierung stellt sich deshalb die Herausforderung, alle Bemühungen um Standardisierung kontinuierlich an den übergeordneten und sich möglicherweise ändernden Zielsetzungen auszurichten.

Im Folgenden werden die Herausforderungen, die Rolle Deutschlands, Anforderungen der Unternehmen sowie strategische Zielsetzungen und Vorhaben kurz beschrieben. Die Beschreibung fokussiert sich darauf, die Verbindungen zur Standardisierung im Cloud Computing aus der Sicht Deutschlands zum aktuellen Zeitpunkt darzulegen.

**Die Herausforderungen** bei der Standardisierung im Cloud Computing sind grundsätzlich als groß einzuschätzen.

- Die Standardisierung im Cloud Computing betrifft viele verschiedene fachliche Bereiche in teils großer inhaltlicher Tiefe und ist deshalb äußerst komplex.



- Die Verbreitung anwendbarer und genutzter Standards für das Cloud Computing wird durch das Fehlen nationaler Regeln oder deren Harmonisierung sowie unzureichende technische Konvergenz erschwert.
- Bisherige Standardisierungsbemühungen stecken konzeptionell in den Kinderschuhen, da ein Mangel an einheitlichen Definitionen oder Orientierungswissen ein zielorientiertes gemeinsames Handeln behindert.
- Entsprechend engagiert sich aktuell eine Vielzahl verschiedener Einrichtungen und Gremien auf internationaler Ebene, aber überwiegend mit geringer Koordinierung.
- Einige internationale Gremien zeigen großes Engagement, während die überwiegende Mehrheit ihren Fokus nur langsam auf Standards für das Cloud Computing ausrichtet.
- Die Anbieterseite, also insbesondere die großen US-Anbieter, ist wenig an Standardisierung interessiert. Sie etabliert ihre eigenen Industriestandards mit dem Ziel Marktanteile zu sichern oder gar auszuweiten.
- Die Nachfragerseite, vor allem der deutsche Mittelstand, ist durch die Gefahr eines „Lock-Ins“, Rechtsunsicherheit und mangelndem Datenschutz, zurückhaltend bei der Anwendung von Cloud-Lösungen.

**Die Rolle Deutschlands** bei der Standardisierung im Cloud Computing sollte sich aus einer internationalen und europäischen Sicht ableiten.<sup>186</sup>

- *Internationale Ebene:* Wo immer möglich, sollten international breit akzeptierte Anforderungen und Standards im Cloud Computing angestrebt werden.
- *Europäische Ebene:* Für besondere Anforderungen auf europäischer Ebene (z.B. Datenschutz) für die kein internationaler Konsens erreicht werden kann, sollten EU-weite Standards etabliert werden.
- *Nationale/deutsche Ebene:* Auf nationaler Ebene bzw. in Deutschland sollten nur so wenige individuelle Standards etabliert werden wie nötig. Individuelle Anforderungen ergeben sich beispielsweise durch unterschiedliche nationale Rechtsrahmen oder Wirtschaftsstrukturen.

**Die Anforderungen der Unternehmen** wurden unter anderem in 2011 durch Online-Konsultationen der EU-Kommission untersucht, die sich noch in der Phase der Ergebnisauswertung befindet.<sup>187</sup> Erste Anregungen sind:

- Die technische Neutralität von Vorgaben sollte sichergestellt werden.
- Es sollte sich nicht zu frühzeitig auf Standards festgelegt werden.

**Die wichtigsten Vorhaben**, die einen Bezug zur Standardisierung im Cloud Computing und Relevanz für die Bundesregierung haben, finden sich auf europäischer und nationaler Ebene.

---

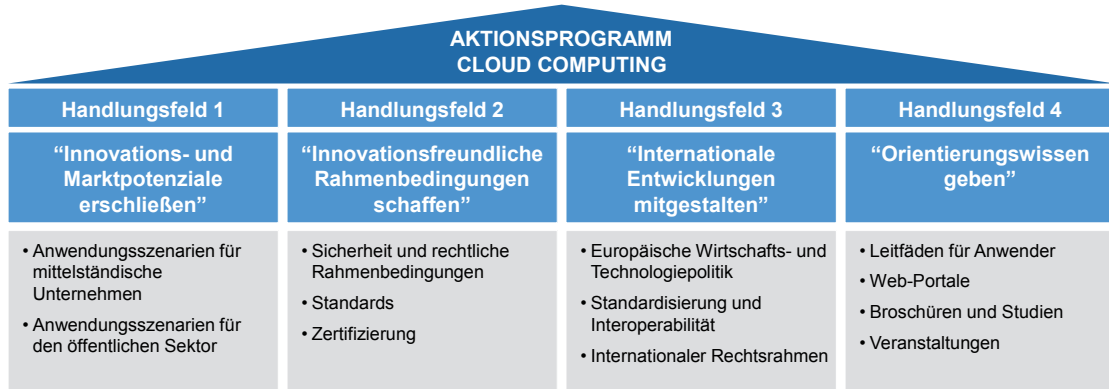
<sup>186</sup> Quelle: Europäische Kommission, Analyse von Booz & Company und FZI.

<sup>187</sup> Quelle: Konsultationen der EU mit der Industrie zu Cloud Computing.



Die wichtigsten strategischen Vorgaben können derzeit aus dem Expertenbericht „The Future of Cloud Computing“<sup>188</sup> für die EU-Kommission, aus den Zielsetzungen des Aktionsprogramms Cloud Computing des BMWi sowie Positionierungen politischer Entscheidungsträger gewonnen werden. Für weitere relevante europäische Vorhaben sei auf die Abhandlungen in Kapitel 6.2 dieser Studie verwiesen.

Der zentralen Bedeutung des Aktionsprogramms Cloud Computing für die Handlungsempfehlungen soll Rechnung getragen werden, indem dessen Handlungsfelder in folgender Abbildung zusammengefasst werden.



**Abbildung 21:** Handlungsfelder des Aktionsprogramms Cloud Computing.<sup>189</sup>

Die Handlungsempfehlungen dieser Studie und einer nachfolgenden Standardisierungs-Roadmap sollten daher – zumindest konzeptionell, bestenfalls aber operativ – eng mit diesen Handlungsfeldern verzahnt werden. Es können folgende Implikationen für die Handlungsempfehlungen in dieser Studie festgehalten werden:

- Neben Anbietern und Anwendern von Cloud Computing aus der Wirtschaft im Allgemeinen, soll insbesondere auch der Mittelstand berücksichtigt werden.
- Die Standardisierung soll im engen Zusammenspiel von Wirtschaft, Wissenschaft und Politik stattfinden. Die Bundesregierung beschränkt sich auf seine Kernaufgaben.
- Der Rechtsrahmen hat viele inhaltliche Bezugspunkte zur Standardisierung (siehe 6.2.4) und kann nicht getrennt betrachtet werden.
- Der Fokus dieser Handlungsempfehlungen berücksichtigt weitere Schwerpunkte des Aktionsprogramms wie Zertifizierung, Sicherheit, offene Standards, rechtliche Rahmenbedingungen oder Orientierungswissen geben.

Hans-Joachim Otto, Parlamentarischer Staatssekretär beim Bundesminister für Wirtschaft und Technologie fordert ein „Cloud Computing - Made and

<sup>188</sup> <http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf>

<sup>189</sup> Quelle: Aktionsprogramm Cloud Computing, BMWi, 2010.

Secured in Germany“.<sup>190 191</sup> Ein solches Markenzeichen soll Vertrauen unter den Marktteilnehmern schaffen und ähnlich wie das weitläufig bekannte „Made in Germany“ dabei helfen, den Export deutscher Cloud-Technologie international und in Europa zu fördern. Die Vision eines solchen Markenzeichens kann vorläufig folgendermaßen umrissen werden:

- Das Markenzeichen soll ein (rechts-)sicheres Cloud Computing gewährleisten, das mit dem deutschen Rechtsrahmen konform ist.
- Das Markenzeichen ist vor allem für Cloud-Lösungen gedacht, die in Deutschland entwickelt werden („Made“) und mit deutscher Sicherheitstechnologie („Secured“) ausgestattet sind.
- Das Markenzeichen soll möglichst mit allen relevanten internationalen und europäischen Standards kompatibel sein und diese lediglich bei spezifischen Anforderungen in Deutschland erweitern.
- Das Markenzeichen ist für die Wirtschaft vorgesehen. „Cloud Computing – Made and Secured in Germany“ ist *keine* Instanz einer Cloud für die öffentliche Verwaltung.<sup>192</sup>
- Das Markenzeichen soll das Modell des freien Marktes widerspiegeln. Beispielsweise muss ein Anbieter seinen Unternehmenssitz nicht in Deutschland haben, noch ist das Markenzeichen ausschließlich für Anwender aus Deutschland gedacht und auch die Datenverarbeitung muss nicht notwendigerweise in Deutschland stattfinden.
- Das Markenzeichen soll ausdrücklich für alle Service-Modelle, also IaaS, SaaS als auch PaaS, geeignet sein.

Abschließend sei angemerkt, dass die Ziele bei der Standardisierung sich immer auch veränderten strategischen Zielvorgaben aus dem Aktionsprogramm Cloud Computing im Allgemeinen anpassen müssen. Beispielsweise gibt es noch Freiheitsgrade, was unter einem „Cloud Computing – Made and Secured in Germany“ genau zu verstehen ist und deren Klärung fällt nicht in den eigentlichen Aufgabenbereich dieser Studie.

### 7.1.2 Die Notwendigkeit ordnungspolitischen Handelns

Ordnungspolitisches Handeln der Bundesregierung muss sich in diesem strategischen Rahmen bewegen. Ihm liegen grundsätzlich folgende Prämissen zu Grunde. Es gilt das Modell des freien Marktes, indem die Marktkräfte zu einem optimalen Punkt des Ausgleichs von Angebot und Nachfrage gelangen. Insofern liegt die Hauptverantwortung für die Standardisierung im Cloud Computing auf Seiten der Wirtschaft. Sie muss durch eine aktivere Rolle bei

---

<sup>190</sup> <http://cloud-practice.de/news/wir-wollen-cloud-computing-made-and-secured-germany-interview-mit-mdb-hans-joachim-otto>

<sup>191</sup> Diese Idee wird auch von anderen Akteuren mit teils variierender Begrifflichkeit aufgegriffen, z.B. durch die Initiative „Cloud Services Made in Germany“. <http://www.cloud-services-made-in-germany.de>.

<sup>192</sup> Beispielsweise ähnlich der G-Cloud in Großbritannien.

der Standardisierung ihre vitalen Interessen im Cloud Computing wirkungsvoll auf dem freien Markt vertreten. Es ist notwendig, dass sich alle Akteursgruppen, wie Anbieter und Anwender, oder große Konzerne und der Mittelstand, so organisieren, dass sie sich auf Augenhöhe begegnen können.

Die Bundesregierung sollte so wenig als möglich in den Markt eingreifen. Ein Eingreifen ist nur dann gerechtfertigt, wenn es Anzeichen für eine mangelnde Wirksamkeit der Marktkräfte gibt. Folglich bedarf ordnungspolitisches Handeln grundsätzlich einer Begründung. Diese lässt sich aus drei Argumentationssträngen herleiten, die sich wiederum auf die empfohlenen Handlungsziele abbilden lassen. Standardisierung ist niemals Selbstzweck, sondern vielmehr ein Mittel zur Erreichung der damit verbundenen Ziele.

### **Begründung I: Durchsetzung des deutschen Rechtsrahmens**

Cloud Computing hat kritische Auswirkungen auf die Durchsetzungsfähigkeit des deutschen Rechtsrahmens (insbesondere Datenschutz, geistiges Eigentum, usw.) und in Folge dessen auf unsere Wirtschaftsstrukturen. Eine regulatorische Nichtbeachtung des Bereichs könnte fatale Folgen für einzelne Personen, Unternehmen oder ganze Wirtschaftszweige haben. Es sei auch auf die detailliertere Abhandlung zur Rechtssicherheit in Kapitel 6.2.4 bzw. der Cloud-Zertifizierung in Kapitel 6.2.2 verwiesen.

Der aktuelle Markt für Cloud Computing wird von US-Anbietern dominiert, die eine Durchsetzung ihrer rechtlichen Vorgaben und zugehörigen Standards (z.B. AGBs) anstreben. Potenziellen Anwendern in Deutschland bleiben deshalb oftmals nur folgende Optionen:

- Nutzung der US-Angebote ohne Anpassungen und bewusstes Eingehen beträchtlicher Rechtsrisiken.
- Aufbau einer privaten Unternehmens-Cloud mit in der Regel geringer Investitionssicherheit.
- Verzicht auf Cloud Computing und Akzeptanz möglicher Einbußen bei der Wettbewerbsfähigkeit.

### **Begründung II: Stärkung des Wettbewerbs**

Eine Aufgabe des deutschen Staats als Regelsetzer ist, das Funktionieren des freien Marktes und den Wettbewerb zu fördern bzw. sicherzustellen. Dies gilt auch für Cloud Computing als Wirtschaftsbereich. In den letzten Jahren lassen sich im Cloud Computing erste Anzeichen für klassische Fälle von Marktversagen beobachten.

- Es gibt Ungleichgewichte bei der Marktmacht der Anbieter. Einzelne US-amerikanische Großunternehmen besitzen de-facto eine Vorrangstellung am Cloud Computing-Markt.
- Es gibt Verzerrungen bei der Informationsverfügbarkeit, die besonders die Kunden der Cloud-Anbieter betreffen. Zu nennen ist beispielsweise unzureichende Transparenz über die Speicherung und Weiterverwendung persönlicher Daten.

- Es lassen sich „Lock-in“ Effekte beobachten. In der Konsequenz ist der Wechsel der Kunden zwischen verschiedenen Cloud-Anbietern nicht oder nur schwer möglich.

Viele große US-Anbieter setzen auf eigene proprietäre Standards und erschweren somit den Marktzugang für andere Anbieter.

### **Begründung III: Potenzial zur Stärkung der deutschen Wirtschaft**

Cloud Computing ist eine Technologie, die verschiedene bestehende und neue Technologiebereiche zu einem stimmigen Konzept kombiniert (siehe 2.3). Das unterstreicht die Bedeutung von Cloud Computing im Allgemeinen und auch für den Wirtschaftsstandort Deutschland. Cloud Computing besitzt das zweifache Potenzial sowohl Effizienz- als auch Innovationsschübe in der deutschen Wirtschaft zu entfalten. Dies gilt für die Anbieter von Cloud-Technologien sowie für Nutzer quer über alle Wirtschaftszweige. Eine wichtige Rolle spielen geeignete Cloud-Standards auch für den deutschen Mittelstand, der knapp 40% aller Umsätze in Deutschland erwirtschaftet.<sup>193</sup> Gerade für diese, im Verhältnis zu den Anbietern, kleinen Anwendern gestaltet sich eine Durchsetzung ihrer Interessen als besonders schwierig. Gleichzeitig besteht bei dieser Zielgruppe großes Effizienz- und Innovationspotenzial durch den Einsatz von Cloud Computing. Cloud Computing nicht gestaltend mit voranzutreiben, würde Deutschland, die deutsche Wirtschaft und den deutschen Mittelstand folglich international mit Wettbewerbsnachteilen behaften.

### **7.1.3 Schlussfolgerung und Ableitung der Handlungsziele**

Grundsätzlich empfiehlt sich folglich angesichts dieser Zusammenhänge ordnungspolitisches Handeln.

Die angeführten Argumente für ordnungspolitisches Handeln beziehen sich im Besonderen auf die Standardisierung, auch wenn sie sich in vielen Fällen aus einer allgemeinen Notwendigkeit ordnungspolitischen Handelns im Cloud Computing herleiten. Standardisierung ist einer der zentralen Hebel, um die Herausforderungen der oben angeführten Rationalen zu adressieren.

**Instrumente<sup>194</sup>:** Es sollten möglichst partizipative Instrumenten eingesetzt werden. Angesichts der Geschwindigkeit der Entwicklungen im Markt erscheint dies geboten, um die Innovationskraft der Firmen positiv zu fördern. Standardisierung ist in dieser Hinsicht empfehlenswert. Dies begründet auch partizipativ-explorative Ansätze, wie das Technologieprogramm Trusted Cloud, in denen die Akteure gemeinsam nach wegweisenden Lösungen su-

---

<sup>193</sup> Institut für Mittelstandsforschung (IfM).

<sup>194</sup> Bisweilen werden ordnungspolitische Steuerungsinstrumente unterteilt in klassische „interventionist instruments“ (d.h. normative Vorgaben wie Gesetze, „Normen“ usw.), „economic instruments“ (insbesondere Förderungen) und „context-oriented instruments“ (d.h. Zertifizierungsverfahren sowie weitere, die eine gewisse Offenheit für die Spezifika der Einzelfälle besitzen, größere Akteurkreise involvieren und einfacher weiterentwickelt werden können); diese Unterscheidung findet sich z.B. bei Holzinger / Knill / Schäfer: Rhetoric or Reality? ‚New Governance‘ in EU Environmental Policy, European Law Journal 12/3, 2006.

chen. Allerdings sollte auch nicht darauf verzichtet werden, da regulierend einzugreifen, wo es erforderlich wird. Schließlich erfordert dies auch ein klares internationales Engagement. Sich nur auf den deutschen Rahmen zu beschränken, führt in der vernetzten IT-Welt ins Abseits.

**Handlungszeitpunkt:** Die Standardisierung im Cloud Computing steht am Anfang (siehe Kapitel 6). Es deuten sich verstärkte Standardisierungsbemühungen sowohl seitens der Industrie als auch der staatlichen Akteure über die nächsten ein bis drei Jahre (2012-2014) an. Ein rasches Handeln ist notwendig, da in diesem Zeitraum entscheidende Standardisierungsentscheidungen im Cloud Computing zu erwarten sind und damit Fakten geschaffen werden. In der gegenwärtigen Frühphase werden die Spielregeln für den Markt von morgen bestimmt. Mit fortschreitender Entwicklung sinken die Einflussmöglichkeiten. Anderenfalls sind ein arbeitsteiliges, effizientes Vorgehen sowie die Berücksichtigung deutscher Anforderungen auf europäischer und internationaler Ebene gefährdet.

**Handlungsziele:** Aus den drei Rationalen für ein ordnungspolitisches Handeln lassen sich zwei wesentliche strategische Hauptziele ableiten. Gleichzeitig lassen sich auf operativer Ebene inhaltliche Empfehlungen für das Technologieprogramm Trusted Cloud ableiten. Folgende Abbildung verdeutlicht den Sinnzusammenhang der drei Handlungsziele, in denen die Bundesregierung positive Impulse für die Standardisierung im Cloud Computing setzen kann.

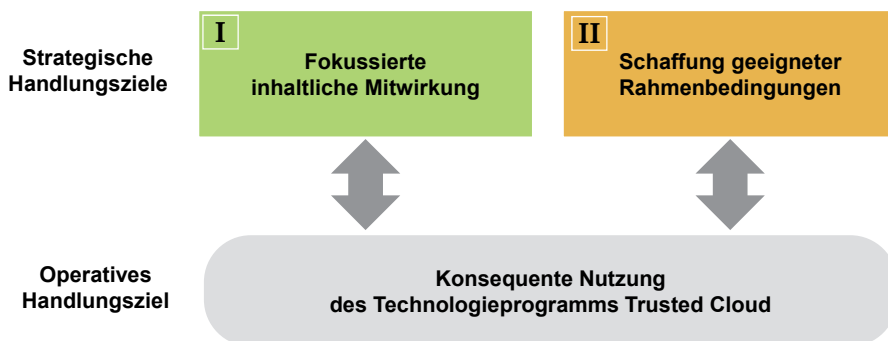


Abbildung 22: Übersicht der Handlungsziele<sup>195</sup>

Es folgt eine kurze Beschreibung der Handlungsziele:

- **Strategisches Handlungsziel I: Fokussierte inhaltliche Mitwirkung**  
Die Bundesregierung sollte in begrenztem Umfang inhaltlich bei der Standardisierung im Cloud Computing mitwirken. Eine solche Mitwirkung muss sich klar auf den übergeordneten Rahmen konzentrieren und sich begründen lassen.
- **Strategisches Handlungsziel II: Schaffung geeigneter Rahmenbedingungen**  
Das zweite strategische Handlungsziel für die Bundesregierung ist die Schaffung geeigneter Rahmenbedingungen für ein zielgerichtetes und koordiniertes Vorgehen aller Akteure in Deutschland bei der Standardi-

<sup>195</sup> Analyse von Booz & Company und FZI

sierung im Cloud Computing. Im Vordergrund sollten möglichst partizipative Instrumente stehen.

- **Operatives Handlungsziel: Konsequente Nutzung des Technologieprogramm Trusted Cloud**

Das dritte Ziel für die Bundesregierung ist die konsequente, zielgerichtete und effektive Nutzung des Technologieprogramms Trusted Cloud für eine Standardisierung im Cloud Computing.

Aus den zwei strategischen Handlungszielen werden 8 Handlungsfelder für den Zeitraum 2012 bis 2015 abgeleitet, die in folgender Übersicht zusammengefasst werden und in den folgenden Kapiteln 7.2 und 7.3 überblicksartig beschrieben werden. Dieses dritte operative Handlungsziel wird in diesem Kapitel nicht weiter vertieft.

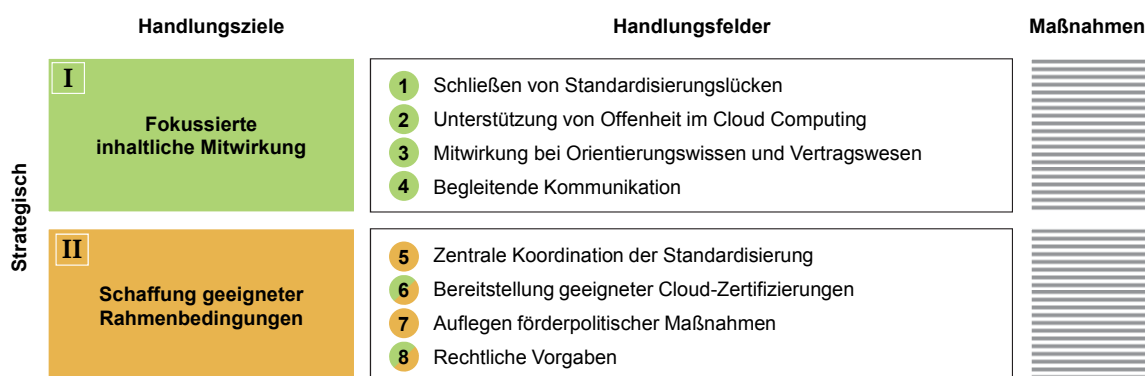


Abbildung 23: Übersicht der Handlungsfelder<sup>196</sup>

## 7.2 Strategisches Handlungsziel I: Fokussierte inhaltliche Mitwirkung

Die Bundesregierung sollte in begrenztem Umfang inhaltlich bei der Standardisierung im Cloud Computing mitwirken. Eine solche Mitwirkung muss sich klar auf den übergeordneten Rahmen konzentrieren und sich wie in Kapitel 7.1.2 ausgeführt begründen lassen. Für Deutschland ist es unerlässlich eine Gesamtsicht über die Standardisierung zu gewinnen. Nur so lassen sich über die nächsten Jahre die geeigneten Schwerpunkte in Deutschland setzen.

Für die Erreichung des ersten Handlungsziels werden vier Handlungsfelder empfohlen: Das Schließen von Standardisierungslücken und eine konsistente Definition der Anforderungen (siehe 7.2.1), die Unterstützung von Offenheit im Cloud Computing (siehe 7.2.2), die Mitwirkung bei Orientierungswissen und Vertragswesen (siehe 7.2.3) und die Durchführung einer begleitenden Kommunikation (siehe 7.2.4).

### 7.2.1 Handlungsfeld 1: Schließen von Standardisierungslücken

Das bestehende Standardisierungsumfeld im Cloud Computing ist heute noch grundsätzlich durch eine fehlende inhaltliche Verknüpfung von

<sup>196</sup> Analyse von Booz & Company und FZI



- überblicksartigen und übergreifenden Anforderungsdefinitionen für das Cloud Computing (z.B. BSI-ESCC, LRD&C) mit
- detaillierten technischen und organisatorischen Standards (z.B. OCCI, ITIL), die für das Cloud Computing geeignet („Cloud-ready“) sind,

gekennzeichnet. Dieser Umstand ist vor allem dem allgemein frühen Entwicklungsstand der Standardisierung im Cloud Computing geschuldet. Umgekehrt eröffnet dies zum jetzigen Zeitpunkt gute Mitgestaltungsmöglichkeiten für die Bundesregierung beim Schließen von Standardisierungslücken.

In diesem Zusammenhang ist es wichtig bestehende Leitfäden und Anforderungsdokumente für das Cloud Computing in Deutschland einheitlich durch eine zentrale Koordination und inhaltliche Unterstützung weiterzuentwickeln. Dies kann die Erarbeitung und Fortschreibung einer zentralen Übersicht von Anforderungsdokumenten öffentlicher und privater Herausgeber ebenso umfassen, wie die Erarbeitung und Fortschreibung einer zentralen Übersicht priorisierter Anforderungen und Lücken.

Eine weitere Möglichkeit besteht darin Standardkataloge für das Cloud Computing auf Basis europäischer und internationaler Katalog aus deutscher Sicht zu ergänzen und kontinuierlich fortzuschreiben. Existierende Bestandsaufnahmen von Standardisierungsaktivitäten umfassen beispielsweise diejenige der IETF<sup>197</sup> oder das „Cloud Standards Wiki“<sup>198</sup>. Auf europäischer Ebene könnte ein solcher Katalog durch die ETSI koordiniert werden. Der Katalog sollte für eine einfache Auffindbarkeit von Standards durch die Nutzer optimiert sein und Empfehlungen zur Verwendung von Standards für die Wirtschaft im Sinne von „Goldstandards“ aussprechen. Die deutsche Verwaltung kann an dieser Stelle eine Vorbildfunktion einnehmen und in ähnlicher Weise, wie mit SAGA („Standards und Architekturen für E-Government-Anwendungen“)<sup>199</sup> für das E-Government, „Goldstandards“ beim Cloud Computing für die deutsche Verwaltung festlegen.

Die Übersicht der Anforderungen, Lücken und Standardkataloge kann gemeinsam mit einer Übersicht geplanter Standardisierungsaktivitäten genutzt werden, um notwendige Standardisierungsaktivitäten zu priorisieren und bei geeigneten Standardisierungsorganisationen zu platzieren.

### 7.2.2 Handlungsfeld 2: Unterstützung von Offenheit im Cloud Computing

Die Schaffung von Offenheit im Cloud Computing ist ein äußerst geeignetes Vorgehen, um bei begrenztem Eingriff in die Marktdynamik übergeordnete Ziele wie Wettbewerb, Transparenz, Vertrauensbildung, Interoperabilität oder die Vermeidung von „Lock-In“-Effekten zu unterstützen. „Offenheit der Plattform und Standardisierung“ wird auch auf Ebene des Aktionspro-

---

<sup>197</sup> <http://tools.ietf.org/id/draft-khasnabish-cloud-sdo-survey-01.txt>

<sup>198</sup> <http://cloud-standards.org>

<sup>199</sup> [http://www.cio.bund.de/DE/Architekturen-und-Standards/SAGA/saga\\_node.html](http://www.cio.bund.de/DE/Architekturen-und-Standards/SAGA/saga_node.html)

gramms Cloud Computing als wichtige Herausforderungen benannt. Gerade in einem Marktumfeld, indem sich deutsche mittelständische Anbieter begrenzter Größe mit großen US-amerikanischen Anbietern konfrontiert sehen, ist Offenheit eine wichtige Voraussetzung, um Wettbewerb zu ermöglichen.

Offenheit im Cloud Computing (siehe auch Kapitel 6.2.3) umfasst die Forderung nach Open Source, offenen Standards und offenen Schnittstellen für das Cloud Computing. Bemühungen um Offenheit in der Vergangenheit und im IKT-Bereich waren in unterschiedlichem Maße erfolgreich. Der entscheidende Erfolgsfaktor für Offenheit im Cloud Computing ist die Akzeptanz offener Lösungen am Markt. Alle Bemühungen müssen sich an diesem Kriterium messen lassen. Bei ausbleibendem Erfolg sind bestehende Maßnahmen erneut zu evaluieren und auch striktere Maßnahmen in Erwägung zu ziehen. Bis heute ist es beispielsweise der EU-Kommission trotz erheblichem Druck nicht gelungen wichtige Protokolle der Microsoft-Serveranwendungen offenzulegen.<sup>200</sup> Zum jetzigen Zeitpunkt wird

- eine Mitwirkung bei Standardisierungsgremien, die offene Standards vorantreiben (siehe 6.2.3),
- die Bewerbung offener Standards und vor allem
- das Setzen von Anreizen für die Verwendung offener Standards

empfohlen. Während die beiden erst genannten Punkte im Rahmen anderer empfohlener Handlungsfelder (siehe 7.3.1 und 7.3.2) adressiert werden können, ist für den letztgenannten ein eigenständiges Handeln erforderlich.

Die Schaffung rechtlicher und finanzieller Anreize für den Einsatz von offenen Standards und Open Source im Cloud Computing kann in verschiedener Weise erfolgen. Beispielsweise können offene Standards für ein Gütesiegel für das Cloud Computing (vgl. Kapitel 7.3.2) gefordert werden oder im Rahmen von Goldstandards empfohlen werden. Ebenso wäre es denkbar, ein Gütesiegel für die Verwendung offener Standards im Cloud Computing als Voraussetzung für die Teilnahme an Ausschreibungen der öffentlichen Hand zu fordern. Sollten sich Anzeichen für ein Marktversagen im Cloud Computing erhärten, können auch steuerliche Vergünstigungen als weitreichende Maßnahme in Erwägung gezogen werden.

### **7.2.3 Handlungsfeld 3: Mitwirkung bei Orientierungswissen und Vertragswesen**

Die Rolle der Bundesregierung bei der Standardisierung im Cloud Computing sollte sich im Wesentlichen auf die übergeordnete, koordinierende und regelsetzende Mitwirkung beschränken. Die eigentliche inhaltliche Erarbeitung von Standards für das Cloud Computing ist Aufgabe der Wirtschaft und Wissenschaft. An der Schnittstelle der Rolle von öffentlicher Hand und derjenigen der Wirtschaft gibt es die Bereiche des Orientierungswissens und Ver-

---

<sup>200</sup> <http://www.heise.de/newsticker/meldung/Microsoft-kommt-EU-entgegen-und-lizenziert-Quellcode-fuer-Windows-Server-Update-169054.html>

tragswesens, die ebenfalls eine wesentliche, teils inhaltliche, Mitwirkung durch den Gesetzgeber verlangen.

Die wesentliche Mitwirkung bei der Erarbeitung von Orientierungswissen ermöglicht dem Staat erst die transparente und fundierte inhaltliche Kommunikation seiner Richtlinien, Anforderungen und Definition des Cloud Computing an Cloud-Anbieter, Cloud-Anwender oder Standardisierungsgremien. Dies erscheint insbesondere erforderlich, da das Standardisierungsumfeld im Cloud Computing bisher geringe Konsistenz und hohe Komplexität aufweist.

Die Standardisierung im Bereich des Vertragswesens sollte weiterhin maßgeblich durch die Wirtschaft vorangetrieben werden. Naturgemäß besitzt das Vertragswesen aber einen engen Bezug zu den rechtlichen Vorgaben, so dass an dieser Schnittstelle eine enge Koordination empfohlen wird. Als Beispiel seien die Allgemeinen Geschäftsbedingungen (AGB) angeführt, die in §§ 305–310 BGB<sup>201</sup> (ehemals AGB-Gesetz) ein rechtliches Gegenstück besitzen, in dem rechtliche Anforderungen verbindlich festgeschrieben sind. Für Cloud Computing besteht bisher weder eine Vorgabe seitens der Verwaltung noch ein Konsens zwischen Wirtschaft und Staat, welche Bereiche im Vertragswesen rechtlich verankert werden und welche nicht (vgl. Kapitel 6.2.4).

Entsprechend sollte die Bundesregierung bei der Erarbeitung und Bereitstellung von Orientierungswissen für das Cloud Computing mitwirken. In einer Voruntersuchung können die Arbeiten geplant und priorisiert werden, die nachfolgend durch eine zentrale Stelle (z.B. im DIN) koordiniert und bei Standardisierungsorganisationen platziert werden können. Mögliche Ansatzpunkte bei der Erarbeitung von Orientierungswissen sind etwa die Übernahme bzw. Erweiterung existierender Definitionen zu Cloud Computing für Deutschland (vgl. Terminologie in Future of Cloud Computing<sup>202</sup>, NIST Definition<sup>203</sup>) oder die Mitwirkung bei der Definition von Use Cases für Deutschland (z.B. für Mittelstand). Weiteres Orientierungswissen in Form von Definitionen, Leitfäden, Online-Portalen, Broschüren oder Studien ist sinnvoll.

Eine Untersuchung zum rechtlichen Rahmen für ein Vertragswesen im Cloud Computing kann Empfehlungen erarbeiten. Mögliche Empfehlungen sind etwa die Einführung allgemeiner Vertragsbedingungen für das Cloud Computing (d.h. Einbeziehung aller Aspekte, wie Abrechnung, Sicherheit, Qualitätssicherung, Überwachung der SLA, Transparenz, Datenschutz etc.), Vorgaben zur Sprache der Vereinbarungen (z.B. Deutsch) oder Kriterien für die Gültigkeit von vertraglichen Regelungen.

---

<sup>201</sup> <http://www.gesetze-im-internet.de/bgb/BJNR001950896.html#BJNR001950896BJNG023401377>

<sup>202</sup> <http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf>

<sup>203</sup> <http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf>

#### 7.2.4 Handlungsfeld 4: Begleitende Kommunikation

Der Wissensstand über Cloud Computing ist in Deutschland im Allgemeinen noch sehr unterschiedlich ausgeprägt und in einigen Bereichen gering. Dies ist nicht als ungewöhnlich zu betrachten, sondern spiegelt die unterschiedliche Verwendung des Begriffs und die Komplexität des Themas wieder. Für den Bereich der Standardisierung im Cloud Computing besteht ein eigenständiger Bedarf für eine Kommunikation, die eigene spezielle Anforderungen besitzt.

Ein Schwerpunkt der Kommunikation liegt auf allen Beteiligten, die an der Standardisierung im Cloud Computing auf deutscher Ebene beteiligt sind oder Anforderungen einbringen sollten. Eine besondere Bedeutung besitzt die Ausgewogenheit bei der Kommunikation als auch bei der Berücksichtigung von Anforderungen verschiedener Akteursgruppen innerhalb Deutschlands. Es ist wichtig, dass große Firmen, der Mittelstand, Endkunden sowie Anbieter und Anwender als Akteursgruppen auf gleicher Augenhöhe agieren können. Während große Firmen ihre Interessen bei der Cloud-Standardisierung bereits stärker in Industrieverbänden/-konsortien vertreten, besteht beispielsweise beim deutschen Mittelstand oder den Anwendern noch Potenzial.

Insofern ist das Vorhandensein geeigneter Gremien eine Voraussetzung für die wirkungsvolle Kommunikation. Die Bildung von Arbeitsgruppen zum Cloud Computing und dessen Standardisierung bei mittelständischen Vereinigungen wie dem Bundesverband mittelständische Wirtschaft (BVMW) oder dem Bundesverband IT-Mittelstand (BITMi e.V.) wird empfohlen. Mittelfristig kann die Einrichtung einer deutschen Spiegeleinrichtung ähnlich dem Cloud Standards Customer Council<sup>204</sup> angeregt werden, das die Interessen der deutschen Endkunden durch Mitwirkung bei Anforderungen und Anwendungsfällen vertritt. Zusätzlich sollten insbesondere auch öffentliche Einrichtungen (z.B. BSI), Industrieverbände und Normungsorganisationen in Deutschland einbezogen werden. Den zweiten Schwerpunkt bildet die Kommunikation mit wichtigen europäischen (z.B. bei der ETSI, EuroCloud), internationalen (z.B. ITU) und weiteren nationalen (z.B. aus den USA, Frankreich) Standardisierungsorganisationen.

Für eine gezielte Kommunikation ist die Durchführung von Informationsreihen & -kampagnen für alle Akteursgruppen in Deutschland sinnvoll, um den Wissensstand zu vergrößern und die Meinungsbildung zu fördern. Alle Kommunikationsmaßnahmen sollten auf Basis einheitlichen Orientierungswissens und Informationsmaterials durchgeführt werden. Zusätzlich können Konsultationen in kleineren Expertengruppen auf internationaler, europäischer und deutscher Ebene durchgeführt werden, um das Verständnis der unterschiedlichen Anforderungen und des weiteren Vorgehens zu schärfen.

Ergänzend ist auch die Durchführung von Online-Konsultationen zur Cloud-Standardisierung in Deutschland, die für alle Akteure offen stehen, möglich.

---

<sup>204</sup> <http://www.cloud-council.org>

Deren Ziel ist die Schaffung von Transparenz hinsichtlich der speziellen tatsächlichen Bedarfe und Anforderungen in Deutschland (vgl. auch EU-Konsultationen<sup>205</sup>).

### **7.3 Strategisches Handlungsziel II: Schaffung geeigneter Rahmenbedingungen**

Das zweite strategische Handlungsziel für die Bundesregierung sollte die Schaffung geeigneter Rahmenbedingungen für ein zielgerichtetes und koordiniertes Vorgehen bei der Cloud-Standardisierung in Deutschland sein. Im Vordergrund sollten möglichst partizipative Instrumente stehen. In diesem Kontext wird insbesondere die Einführung von vertrauensbildenden Zertifizierungen für das Cloud Computing in Deutschland empfohlen. Weitere Möglichkeiten sind beispielsweise Selbstverpflichtungen der Cloud Computing-Branche oder Fördermechanismen.

Für die Erreichung des zweiten Handlungsziels werden vier Handlungsfelder empfohlen: Zentrale Koordination der Standardisierung (7.3.1), Bereitstellung geeigneter Cloud-Zertifizierungen (7.3.2), Auflegen förderpolitischer Maßnahmen (7.3.3) und das Anpassen rechtlicher Vorgaben (7.3.4).

#### **7.3.1 Handlungsfeld 5: Zentrale Koordination der Standardisierung**

Es muss Aufgabe des deutschen Staates sein, die gesamtwirtschaftlichen und -gesellschaftlichen Interessen bei der Standardisierung im Cloud Computing aus einer deutschlandweiten Perspektive zu wahren. Dies umfasst neben den Interessen der Wirtschaft und der öffentlichen Verwaltung auch den Schutz der Endnutzer, also ebenso der Bürger als Anwender von Cloud-Technologie. Diese Aufgabe kann nur erfüllt werden, wenn die Bundesregierung die zentrale Koordination bei der Cloud-Standardisierung in Deutschland sicherstellt. Einer zentralen koordinierenden Stelle für das Cloud Computing in Deutschland, die kontinuierlich Wissen aufbaut und auch für die Standardisierung zuständig ist, kommt dabei eine wichtige Rolle zu. Ein möglicher Kandidat für die Einrichtung einer solchen Stelle ist das DIN.

Des Weiteren sollte eine Standardisierungsroadmap für das Cloud Computing in Deutschland erarbeitet werden. Sie kann die zeitliche und inhaltliche Planung unter Benennung von Verantwortlichkeiten detaillieren und unter anderem Ergebnisse und Empfehlungen dieser Studie operationalisieren. Für das zeitliche Vorgehen ist zu berücksichtigen, dass im ersten Schritt die Standardisierung in laufenden Forschungsprojekten vorangetrieben werden sollte. Im zweiten Schritt ist die Formung von Anwender-/Industriekonsortien für solche Standards denkbar, die für Deutschland größtes Gewicht besitzen, um diese im dritten Schritt in bestehenden Standardisierungsgremien einzubringen. Grundsätzlich ist eine enge europäische und internationale Abstimmung notwendig.

---

<sup>205</sup> <http://europa.eu/rapid/pressReleasesAction.do?reference=IP%2F11%2F575&format=HTML&aged=1&language=DE&guiLanguage=en>



Ein weiteres Hilfsmittel stellen Standardisierungsstrategien für die Wirtschaft im Cloud Computing dar, die in einer Voruntersuchung auf ihre Wirksamkeit und Potenziale bewertet werden können. Mögliche konkrete Aspekte von Strategien sind eine Verzahnung von Standardisierung und Wirtschaftsförderung von Cloud Computing (z.B. Netzwerk Cloud Computing) oder die Einrichtung von Normenkartellen bzw. Bildung von Patentpools.

Eine zentrale Koordination ist auf die Mitwirkung wichtiger Akteure bei der Standardisierung angewiesen. Beispielsweise kann diskutiert werden, ob das Bundesamt für Sicherheit in der Informationstechnik (BSI) das Cloud Computing bei den IT Grundsicherungs-Standards berücksichtigen sollte, ob das DIN dem Cloud Computing größere Bedeutung im Normenausschuss "Informationstechnik und Anwendungen" (NIA) zuweisen sollte oder ob die Bundesnetzagentur sich verstärkt mit der ITU-T Focus Group on Cloud Computing koordinieren sollte. Weitere Akteure werden unter 7.2.4 erwähnt.

### **7.3.2 Handlungsfeld 6: Bereitstellung geeigneter Cloud-Zertifizierungen**

Heute verfügbare Zertifizierungen für das Cloud Computing (z.B. EuroCloud Star Audit SaaS) besitzen noch keine ausreichende Vertrauenswirkung. Eine ausführliche Betrachtung hierzu findet sich in Kapitel 6.2.2. Aus regulatorischer Sicht sollten Zertifizierungen aber als ordnungspolitisches, weiches aber wirkungsvolles Instrument eine Schlüsselrolle einnehmen, um Vertrauen in das Cloud Computing in Deutschland zu schaffen. Zertifizierungen können auch einen Beitrag zur Schaffung von Wettbewerb leisten.

Die Erarbeitung von Zertifizierungen sollte als eine langfristige Aufgabe betrachtet werden. Kurzfristige Lösungsansätze erscheinen als nicht erfolgsversprechend. Vielmehr setzt eine ausreichende Zertifizierung für das Cloud Computing eine Vielzahl anderer Standards voraus, nach denen zertifiziert werden soll. Diese sind in weiten Teilen noch nicht in ausreichender Qualität und Tiefe verfügbar. Gleichzeitig muss Zertifizierung auch rechtliche Vorgaben berücksichtigen. Wichtig erscheint auch eine starke Mitwirkung der öffentlichen Hand bei der Erarbeitung von Zertifizierungen, so dass alle notwendigen Anforderungen einfließen werden und das nötige Vertrauen geschaffen werden kann.

Erfolgreiche Zertifizierungen sind folglich zugleich große Herausforderung als auch vielversprechendes Instrument. Als nächster Schritt kann eine Voruntersuchung durchgeführt werden, die mögliche Optionen für Cloud Computing-Zertifizierungen in Deutschland erarbeitet und als inhaltliche Entscheidungsgrundlage dient. Als Leitgedanke kann ein „Cloud Computing – Made and Secured in Germany“ (siehe 7.1) dienen. Eine Zertifizierung sollte, wo immer möglich, europäische, internationale und bestehende Standards einbeziehen. Eine Voruntersuchung kann auch Zeitpläne und Entwicklungsstufen der empfohlenen Zertifizierungen in Abhängigkeit von der erwarteten Verfügbarkeit notwendiger Standards erarbeiten. Mögliche Freiheitsgrade für Zertifizierungsoptionen sind etwa die Anzahl und Art von Zertifizierungen (z.B. nach Standards, von Experten oder von Geschäftspartnern), die Beteili-



gung privater Einrichtungen, der angestrebte Automatisierungsgrad oder die Rollenverteilung möglicher Mitwirkender.

Die Erarbeitung von Zertifikaten für das Cloud Computing sollte durch eine zentrale Stelle koordiniert werden, um Lösungen zu ermöglichen, die eine ausgewogene Gesamtkonzeption der Zertifizierungen sicherstellen und sich nicht ausschließlich auf einzelne Bereiche (z.B. Sicherheit) beschränken. Wichtige Einrichtungen sind beispielsweise das Bundesamt für Sicherheit in der Informationstechnik (BSI), die Datenschutzzentren der Länder oder die Bundesnetzagentur (BNetzA). Als akkreditierte Zertifizierungspartner sind etwa das BSI, der TÜV, die TÜV-IT, Cert-IT, BITMi oder ähnliche denkbar.<sup>206</sup>

### 7.3.3 Handlungsfeld 7: Auflegen förderpolitischer Maßnahmen

In Deutschland bilden das Aktionsprogramm Cloud Computing des BMWi und insbesondere auch das Technologieprogramm Trusted Cloud des BMWi über die nächsten Jahre das Kernelement der förderpolitischen Maßnahmen für die Wirtschaft. In diesem Gesamtrahmen wird auch implizit die Standardisierung im Cloud Computing gefördert. Zusätzlich sind weitere, flankierende, förderpolitische Maßnahmen denkbar, die direkt Potenziale bei der Standardisierung adressieren. Auf europäischer Ebene können analog laufende Forschungs- und Entwicklungsprojekte im Cloud Computing durch zusätzliche Standardisierungsmaßnahmen unterstützt werden.

Es erscheint sinnvoll die Arbeitsergebnisse laufender Projekte auf ihr Potenzial für die Standardisierung für das Cloud Computing zu bewerten und ggf. ausgewählte, kritische Leutturnprojekte mit großem Standardisierungspotenzial weiter zu unterstützen. Eine andere Form der Unterstützung ist die Bereitstellung von Testumgebungen (z.B. Testbeds, Plugfests) zur Prüfung von Arbeitsergebnissen auf deren Interoperabilität und Kompatibilität. Die Tests prüfen folglich potenzielle Standards auf deren Einsatztauglichkeit und fördern frühzeitig die Akzeptanz künftiger Standards. Es können auch direkt ausgewählte Standardisierungsarbeiten in Projekten unterstützt werden. Auch der Verzicht auf weitere Förderungen ist eine valide Option, falls die Standardisierungspotenziale als nicht hinreichend betrachtet werden.

Als weitere Möglichkeit kann ein Netzwerkmanagement für Cloud Computing beispielsweise auf Landesebene im Rahmen der Wirtschaftsförderung (z.B. als ein Netzwerk bei Bayern Innovativ) oder auf Bundesebene (z.B. ec-net) angeregt und koordiniert werden.

Für ein Cloud Computing innerhalb der öffentlichen Verwaltung engagiert sich unter anderem das Bundesministerium für Inneres (BMI) bei folgenden drei Aktionsbereichen: (1) Sicherheit bei Cloud Computing, (2) Cloud-Einsatz in der (Bundes-)Verwaltung und Standardisierung bei Cloud Computing und (3) Rechtliche Rahmenbedingungen beim Cloud Computing.

---

<sup>206</sup> Die Auswahl erhebt keinen Anspruch auf Vollständigkeit.

### 7.3.4 Handlungsfeld 8: Rechtliche Vorgaben

Cloud Computing ist ein umfassendes Technologiekonzept, das viele fachliche, technische und organisatorische Bereiche berührt und deshalb bei einer detaillierten Betrachtung eine Wechselwirkung zu vielen rechtlichen Vorgaben besitzt.<sup>207</sup> In einigen Bereichen steht die Verträglichkeit des Rechtsrahmens mit Cloud Computing in Frage. Andererseits sind möglicherweise zusätzliche rechtliche Vorgaben für das Cloud Computing notwendig. Der betroffene rechtliche Rahmen geht weit über den Bereich des Datenschutzes hinaus und ist zusätzlich in einem europäischen Kontext zu betrachten. Kapitel 6.2.4 („Rechtssicherheit“) diskutiert weitere inhaltliche Details.

In diesem Zusammenhang erscheint eine Bestandsaufnahme und umfassenden Prüfung bestehenden Rechts auf dessen Verträglichkeit und Hinlänglichkeit für Cloud Computing ratsam. Auf dieser Basis können rechtlicher Vorgaben für das Cloud Computing als Anpassung bestehender oder Erlass neuer rechtlicher Vorgaben erarbeitet werden. Es sollte geprüft werden, inwieweit rechtliche Vorgaben in einem Rahmengesetz für Cloud Computing geregelt werden können. Zusätzlich ist eine rechtliche Verankerung von Anreizen (siehe 7.2.2) möglich. Eine wichtige Alternative zu rechtlichen Regelungen sind Selbstverpflichtungen der Wirtschaft, falls diese als erfolgsversprechend beurteilt werden. Eine wichtige Abhängigkeit von neuen Regelungen besteht zu den Datenschutzregelungen auf EU-Ebene, die sich aktuell in der Überarbeitung befinden.

Der öffentlichen Verwaltung kommt selbst eine Vorbildfunktion ein. Es kann geprüft werden, inwieweit eine Richtlinie ähnlich dem „cloud-first“ Grundsatz der US-Verwaltung auch in Deutschland anwendbar ist.

---

<sup>207</sup> Zu rechtlichen Vorgaben im Sinne dieser Studie zählen Vorschriften, Recht, zwischenstaatliche Abkommen, Richtlinien, aber auch branchenspezifische Kodizes und Selbstregulierungsmaßnahmen.

## Anhang

### **Anhang A: Vorarbeiten, Standards und Zertifizierungen mit Bezug zum Cloud Computing**

In der Studie wurde eine umfassende Recherche des Normungs- und Standardisierungsumfelds durchgeführt. Folgender Anhang listet alle Vorarbeiten, Standards und Zertifizierungen, die in diesem Rahmen betrachtet wurden (siehe 3.3.2). Jeder Standard wird kurz unter Angabe der in dieser Studie verwendeten Abkürzung, des Namens, seines regionalen Fokus (International (Int.), Europa (EU), Deutschland (DE), USA (US)) sowie seinem Bezug zum Cloud Computing (explizit oder implizit) genannt.

Akb.	Name	Region	Cloud-Bezug
2301	<u>Draft Guide for Cloud Portability and Interoperability Profiles</u>	Int.	Explizit
2302	<u>Draft Standard for Intercloud Interoperability and Federation</u>	Int.	Explizit
2002/16/EG	<u>2002/16/EG ("EU-Standardvertragsklauseln", Controller-to-Processor)</u>	EU	Implizit
95/46/EG	<u>EU-Richtlinie 95/46/EG ("Datenschutzrichtlinie")</u>	EU	Implizit
AO	<u>Abgabenordnung</u>	DE	Implizit
BDSG	<u>Bundesdatenschutzgesetz (BDSG)</u>	DE	Implizit
BSI 100	<u>IT Grundschutz - BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS)</u>	DE	Implizit
BSI 100	<u>IT-Grundschutz - BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise</u>	DE	Implizit
BSI 100	<u>IT Grundschutz - BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz</u>	DE	Implizit
BSI 100	<u>IT-Grundschutz - BSI-Standard 100-4: Notfallmanagement</u>	DE	Implizit
BSI-ESCC	<u>BSI Eckpunktepapier Sicherheitsempfehlungen für Cloud Comp. Anbieter</u>	DE	Explizit
CA	<u>Automated Audit, Assertion, Assessment, and Assurance API</u>	Int.	Explizit
CAdES	<u>Cryptographic Message Syntax Advanced Electronic Signatures</u>	EU	Implizit
CAIQ	<u>Consensus Assessments Initiative Questionnaire</u>	Int.	Explizit
CCI	<u>Common Criteria for Information Technology Security Evaluation</u>	Int.	Implizit
CCM	<u>Cloud Controls Matrix</u>	Int.	Explizit
CCRA	<u>Cloud Computing Reference Architecture</u>	Int.	Explizit
CCUCDG-1	<u>Cloud Computing Use Cases</u>	Int.	Explizit
CCUCDG-2	<u>Moving to the Cloud</u>	Int.	Explizit
CDMI	<u>Cloud Data Management Interface</u>	Int.	Explizit
CExperte1	<u>Cloud Experte - SaaS EcoSystem</u>	DE	Explizit
CExperte2	<u>Cloud Experte - CloudSchool</u>	Int.	Explizit
CIM	<u>Common Interface Model (CIM) infrastructure specification</u>	Int.	Implizit
CIMSVM	<u>CIM System Virtualization Model</u>	Int.	Implizit
OCCST	<u>Open Crowded Cloud Service Taxonomy</u>	Int.	Explizit
COA	<u>Collaboration Oriented Architecture</u>	Int.	Implizit
COBIT	<u>COBIT Framework for IT Governance and Control</u>	Int.	Implizit

Akb.	Name	Region	Cloud-Bezug
CSA1	<u>Security Guidance for Critical Areas of Focus in CC</u>	Int.	Explizit
CTP	<u>Cloud Trust Protocol</u>	Int.	Explizit
DataLF	<u>Google's Data Liberation Front</u>	US	Implizit
DMTF-1	<u>Architecture for Managing Clouds (White Paper)</u>	Int.	Explizit
DMTF-UC1	<u>Interoperable Clouds</u>	Int.	Explizit
DMTF-UC2	<u>Use Cases and Interactions for Managing Clouds (White Paper)</u>	Int.	Explizit
DNS	<u>Domain Name System</u>	Int.	Implizit
DSGdL	<u>Datenschutzgesetze der Länder</u>	DE	Implizit
EC2 - AMI	<u>Amazon Machine Image</u>	Int.	Explizit
EC2 - API	<u>Amazon Elastic Compute Cloud</u>	US	Explizit
EMI	<u>Eucalyptus Machine Image</u>	Int.	Explizit
EuroCloud-SA	<u>EuroCloud Star Audit ("Gütesiegel für die Cloud")</u>	EU	Explizit
EuroPriSe	<u>The European Privacy Seal for IT Products and IT-Based Services</u>	EU	Implizit
FIPS 140-201	<u>FIPS 140-2: Security Requirements for Cryptographic Modules</u>	US	Implizit
FIPS 140-201	<u>FIPS 180-3: Secure Hash Standard (SHS)</u>	US	Implizit
FIPS 140-201	<u>FIPS 181: Automated Password Generator (APG)</u>	US	Implizit
FIPS 140-201	<u>FIPS 185: Escrowed Encryption Standard (EES)</u>	US	Implizit
FIPS 140-201	<u>FIPS 186-3: Digital Signature Standard (DSS)</u>	US	Implizit
FIPS 140-201	<u>FIPS 188: Standard Security Label for Information Transfe</u>	US	Implizit
FIPS 140-201	<u>FIPS 190: Guideline for the Use of Advanced Authentication Technology Alternatives</u>	US	Implizit
FIPS 140-201	<u>FIPS 196: Entity Authentication Using Public Key Cryptography</u>	US	Implizit
FIPS 140-201	<u>FIPS 197: Advanced Encryption Standard (AES)</u>	US	Implizit
FIPS 140-201	<u>FIPS 198-1: The Keyed-Hash Message Authentication Code (HMAC)</u>	US	Implizit
FIPS 140-201	<u>FIPS 199: Standards for Security Categorization of Federal In-</u> <u>formation and Information Systems</u>	US	Implizit
FIPS 140-201	<u>FIPS 200: Minimum Security Requirements for Federal Infor-</u> <u>mation and Information Systems</u>	US	Implizit
FIPS 140-201	<u>FIPS 201: Personal Identity Verification (PIV) of Federal Em-</u> <u>ployees and Contractors</u>	US	Implizit
FTP	<u>File Transfer Protocol</u>	Int.	Implizit
GICTF-1	<u>Use Cases and Functional Requirements for Inter-Cloud Com-</u> <u>puting</u>	Int.	Explizit
GRC Stack	<u>Governance, Risk Management and Compliance (GRC) Stack</u>	Int.	Explizit
GridFTP	<u>GridFTP: Protocol Extensions to FTP for the Grid</u>	Int.	Implizit
HGB	<u>Handelsgesetzbuch</u>	DE	Implizit
HIVE	<u>Apache Hive</u>	Int.	Explizit
HTML	<u>HyperText Markup Language</u>	Int.	Implizit
HTOP	<u>An HMAC-Based One-Time Password Algorithm</u>	Int.	Implizit
HTTP	<u>Hypertext Transfer Protocol</u>	Int.	Implizit
IBM-UC1	<u>The Transformation of Education through State Education</u> <u>Clouds</u>	US	Explizit
IBM-UC2	<u>IBM Study: Midsize Businesses Increasing IT Budgets; Investing</u> <u>in Analytics and Cloud Computing</u>	US	Explizit

Akb.	Name	Region	Cloud-Bezug
ISO/IEC 24762	<u>Guidelines for ICT DR Services [based on SS507]</u>	Int.	Implizit
ISO/IEC 27001	<u>IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen</u>	Int.	Implizit
ISO/IEC 27002	<u>IT-Sicherheitsverfahren - Leitfaden für das Informationssicherheits-Management</u>	Int.	Implizit
ISO-SOA	<u>General Technical Principles of Service Oriented Architecture</u>	Int.	Implizit
ITIL	<u>Information Technology Infrastructure Library</u>	UK	Implizit
JAQL	<u>Query Language for JavaScript(r) Object Notation</u>	Int.	Explizit
JSDL	<u>Job Submission Definition Language</u>	Int.	Implizit
JSON	<u>JavaScript Object Notation</u>	Int.	Implizit
keyprov	<u>Provisioning of Symmetric Keys</u>	Int.	Implizit
KMIP	<u>Key Management Interoperability Protocol</u>	Int.	Implizit
LRD&C	<u>EuroCloud Leitfaden Recht, Datenschutz &amp; Compliance</u>	DE	Explizit
Malstone Benchmark	<u>Malstone Benchmark</u>	Int.	Implizit
NIST-UC1	<u>NIST Cloud Computing Use Cases</u>	US	Explizit
OAuth	<u>Open Authorization Protocol</u>	Int.	Implizit
OCCI	<u>Open Cloud Computing Interface</u>	Int.	Explizit
OCM	<u>Open Cloud Manifesto</u>	Int.	Explizit
OCRA	<u>OATH Challenge-Response Algorithms</u>	Int.	Implizit
OGF-UC1	<u>Open Cloud Computing Interface - Use cases and requirements for a Cloud API</u>	Int.	Explizit
OpenID-Auth	<u>OpenID Authentication</u>	Int.	Implizit
OSGi	<u>OSGi Service Platform</u>	Int.	Implizit
OSIMM	<u>The Open Group Service Integration Maturity Model</u>	Int.	Implizit
OVF	<u>Open Virtualization Format</u>	Int.	Implizit
PAdES	<u>Advanced Electronic Signatures for Portable Document Format (PDF) documents</u>	EU	Implizit
PCI-DSS	<u>PCI Data Security Standard</u>	Int.	Implizit
PIG	<u>Apache Pig</u>	Int.	Explizit
PKCS	<u>Public-key cryptography standards</u>	Int.	Implizit
PKI	<u>X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile (RFC3820)</u>	Int.	Implizit
REST	<u>REpresentational State Transfer</u>	K.A.	Implizit
S3	<u>Amazon Simple Storage Service</u>	US	Explizit
Safe Harbor	<u>US-EU Safe Harbor Datenschutzvereinbarung</u>	EU	Implizit
SAGA	<u>Standards und Architekturen für E-Government</u>	DE	Implizit
SAML	<u>Security Assertion Markup Language</u>	Int.	Implizit
SAP-1	<u>KPI-Based Process Modelling</u>	DE	Implizit
SAS 70	<u>Statement on Auditing Standards Nr. 70</u>	US	Implizit
SCAP	<u>Security Content Automation Protocol</u>	US	Implizit
SDF	<u>Service Delivery Framework</u>	DE	Implizit
SML	<u>Service Modeling Language</u>	Int.	Implizit
SMTP	<u>Simple Mail Transfer Protocol</u>	Int.	Implizit

Akb.	Name	Region	Cloud-Bezug
SNIA-CSUC	<u>SNIA Cloud Storage Use Cases</u>	Int.	Explizit
SOAP	<u>Simple Object Access Protocol</u>	Int.	Implizit
Sogeti-UC1	<u>Seize the Cloud: A Manager's Guide to Success with Cloud Computing</u>	US	Explizit
SP 800	<u>NIST Special Publication (SP) 800-53 Recommended Security Controls for Federal Information Systems</u>	Int.	Implizit
SPML	<u>Service Provisioning Markup Language</u>	Int.	Implizit
SS 507	<u>Singapore Standard for Information and communications technology disaster recovery services</u>	Nat.	Implizit
SSAE16	<u>Statement on Standards for Attestation Engagements No. 16</u>	Int.	Implizit
SSL/TLS	<u>Secure Sockets Layer / Transport Layer Security</u>	Int.	Implizit
StGB	<u>Strafgesetzbuch</u>	DE	Implizit
TCG	<u>Trusted Computing Standards</u>	Int.	Explizit
TCP/IP	<u>The Internet Protocol Suite</u>	Int.	Implizit
TEXO GF	<u>The TEXO Governance Framework</u>	DE	Implizit
TIA-942	<u>TIA Telecommunications Infrastructure Standard for Data Centers</u>	Int.	Implizit
TKG	<u>Telekommunikationsgesetz</u>	DE	Implizit
TM-eTOM	<u>Framework: Business Process Framework (eTOM)</u>	Int.	Implizit
TM-IFS	<u>Framework: Integration Framework Suite</u>	Int.	Implizit
TM-INT	<u>Framework: Interfaces</u>	Int.	Implizit
TM-SID	<u>Framework: Information Framework (SID)</u>	Int.	Implizit
TM-TAM	<u>Framework: Application Framework (TAM)</u>	Int.	Implizit
TOG-UC1	<u>Strengthening your Business Case for Using Cloud (White Paper)</u>	Int.	Explizit
TOG-UC2	<u>Building Return on Investment from Cloud Computing (White Paper)</u>	Int.	Explizit
TOG-UC3	<u>Business Adoption Strategies in "Cloud Buyers' Decision Tree" (White Paper)</u>	Int.	Explizit
TOTP	<u>Time-Based One-Time Password Algorithm</u>	Int.	Implizit
TR 102 030	<u>Provision of harmonized Trust-service status information</u>	EU	Implizit
Trust in Cloud	<u>Trust in Cloud</u>	DE	Explizit
TS 101 456	<u>Policy requirements for certification authorities issuing public key certificates</u>	EU	Implizit
UR	<u>Usage Record</u>	Int.	Implizit
USDL	<u>Unified Service Description Language</u>	DE	Implizit
WADL	<u>Web Application Description Language</u>	Int.	Implizit
WAPBP	<u>Web Application Privacy Best Practices</u>	Int.	Implizit
WBEM	<u>Web-Based Enterprise Management</u>	Int.	Implizit
WS-*	<u>Web Service Federation Language (WS-Federation)</u>	Int.	Implizit
WS-*	<u>Web Services Addressing (WS-Addressing)</u>	Int.	Implizit
WS-*	<u>Web Services Agreement Specification (WS-Agreement)</u>	Int.	Implizit
WS-*	<u>Web Services Description Language (WSDL)</u>	Int.	Implizit
WS-*	<u>Web Services Interoperability Basic Profile 2.0, 1.2 and 1.1</u>	Int.	Implizit
WS-*	<u>Web Services Interoperability Basic Security Profile 1.1 and 1.0</u>	Int.	Implizit
WS-*	<u>Web Services Policy (WS-Policy)</u>	Int.	Implizit



Akb.	Name	Region	Cloud-Bezug
WS-*	<u>Web Services Reliable Exchange (WS-RX)</u>	Int.	Implizit
WS-*	<u>Web Services Resource Access (WS-RA)</u>	Int.	Implizit
WS-*	<u>Web Services Resource Framework</u>	Int.	Implizit
WS-*	<u>Web Services Secure Exchange (WS-SX)</u>	Int.	Implizit
WS-*	<u>Web Services Security (WSS)</u>	Int.	Implizit
WS-*	<u>Web Services Transaction (WS-TX)</u>	Int.	Implizit
WS-*	<u>WS-I Attachments Profile</u>	Int.	Implizit
WS-*	<u>WS-I Simple SOAP Binding Profile</u>	Int.	Implizit
X.1520	<u>Common vulnerabilities and exposures</u>	Int.	Implizit
X.1521	<u>Common vulnerability scoring system</u>	Int.	Implizit
XACML	<u>eXtensible Access Control Markup Language</u>	Int.	Implizit
XAdES	<u>XML Advanced Electronic Signatures</u>	EU	Implizit
XBRL	<u>eXtensible Business Reporting Language</u>	Int.	Implizit
XDR	<u>eXternal Data Representation</u>	US	Implizit
XML	<u>Extensible Markup Language</u>	Int.	Implizit
XMLDSig	<u>XML signature</u>	Int.	Implizit
XMLENCL	<u>XML Encryption Syntax and Processing</u>	Int.	Implizit
XPath	<u>XML Path Language v1.0 and v2.0</u>	Int.	Implizit
YCSB	<u>Yahoo! Cloud Serving Benchmark</u>	Int.	Explizit

## Anhang B: Standardisierungsorganisationen

In der Studie wurde eine Vielzahl von Organisationen, die sich bei der Standardisierung engagieren, recherchiert („Standardisierungsorganisationen“, siehe 3.1.1). Folgende Übersicht listet eine Auswahl der betrachteten Organisationen (siehe 3.3.1). Jeder Akteur wird kurz unter Angabe der in dieser Studie verwendeten Abkürzung, des Namens, seines regionalen Fokus (International (Int.), Europa (EU), Deutschland (DE), USA (US), Frankreich (FR), Japan (JP), Kanada (CA)) sowie seines identifizierten Branchenschwerpunkts (Allgemein, Cloud Computing (CC), IKT, Sonstige) benannt.

Abk.	Name	Region	Branche
AF-NOR	<u>Association française de normalisation</u>	FR	Allgemein
AICPA	<u>American Institute of Certified Public Accountants</u>	US	Sonstige
ANSI	<u>American National Standards Institute</u>	US	Allgemein
ARTS	<u>Association for Retail Technology Standards</u>	US	Sonstige
BDI	<u>Bundesverband der Deutschen Industrie</u>	DE	Allgemein
BITKOM	<u>Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.</u>	DE	IKT
BSI	<u>British Standards Institution</u>	UK	Allgemein
CCIF	<u>Cloud Computing Interoperability Forum</u>	Int.	CC
CCUCDG	<u>Cloud Computing Use Cases Discussion Group</u>	Int.	CC
CEN	<u>Europäisches Komitee für Normung</u>	EU	Allgemein
CIO-Circle	<u>CIO-Circle</u>	DE	IKT
CIOColloquium	<u>CIOColloquium</u>	DE	IKT
CSA	<u>Cloud Security Alliance</u>	Int.	CC
CSSC	<u>Cloud Standards Customer Council</u>	Int.	CC
DIN	<u>DIN Deutsches Institut für Normung e. V.</u>	DE	Allgemein
DKE	<u>Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE</u>	De	Allgemein

Abk.	Name	Region	Branche
DMTF	<u>Distributed Management Task Force</u>	Int.	IKT
EGI	<u>European Grid Infrastructure</u>	EU	IKT
ETSI	<u>European Telecommunications Standards Institute</u>	EU	IKT
EuroCloud	<u>EuroCloud Europe</u>	EU	CC
Euro-Cloud-DE	<u>EuroCloud Deutschland eco e. V.</u>	DE	CC
FACC	<u>Fraunhofer Allianz Cloud Computing</u>	DE	CC
GICTF	<u>Global Inter-Cloud Technology Forum</u>	Int.	CC
IEEE	<u>Institute of Electrical and Electronics Engineers</u>	Int.	Tech.
IETF	<u>Internet Engineering Task Force</u>	Int.	IKT
IGE	<u>Initiative for Globus in Europe</u>	EU	IKT
INCITS	<u>Int. Committee for Information Technology Standards</u>	Int.	IKT
IRTF	<u>Internet Research Task Force</u>	Int.	IKT
ISACA	<u>Information Systems Audit and Control Association</u>	Int.	IKT
ISO	<u>Int. Standards Organization</u>	Int.	Allgemein
ITU	<u>International Telecommunications Union</u>	Int.	IKT
JISC	<u>Japanese Industrial Standards Committee</u>	JP	Allgemein
Kantara	<u>Kantara Initiative (Liberty Alliance)</u>	Int.	IKT
NESSI	<u>Networked European Software and Services Initiative</u>	EU	IKT
NIST	<u>National Standards and Technology Institute</u>	US	Allgemein
OASIS	<u>Organization for the Advancement of Structured Information Standards</u>	Int.	IKT
OCC	<u>Open Cloud Consortium</u>	Int.	CC
ODCA	<u>Open Data Center Alliance</u>	Int.	IKT
OGF	<u>Open Grid Forum</u>	Int.	IKT
OMG	<u>Object Management Group</u>	Int.	Technologie
Open Group	<u>The Open Group</u>	Int.	IKT
OSBF	<u>Open Source Business Foundation</u>	Int.	IKT
PCI	<u>PCI Security Standards Council</u>	Int.	IKT
SCC	<u>Standards Council of Canada</u>	CA	Allgemein
SNIA	<u>Storage Networking Industry Association</u>	Int.	IKT
TM Forum	<u>TM Forum</u>	Int.	IKT
VDE	<u>VDE Verband der Elektrotechnik Elektronik Informationstechnik e.V.</u>	DE	IKT
W3C	<u>World Wide Web Consortium</u>	Int.	IKT
WS-I	<u>Web Services Interoperability Organization</u>	Int.	IKT



---

## Impressum

Das Normungs- und Standardisierungsumfeld von Cloud Computing – Eine Untersuchung aus europäischer und deutscher Sicht unter Einbeziehung des Technologieprogramms „Trusted Cloud“

Eine Studie im Auftrag des Bundesministeriums für Wirtschaft und Technologie.

Studienerstellung durch Booz & Company in Kooperation mit dem FZI Forschungszentrum Informatik.

Gesamtverantwortung: Dr. Rainer Bernnat (Booz),  
Dr. Wolfgang Zink (Booz)

Leitung Projektteam: Dr. Nicolai Bieber (Booz)

Projektteam: Joachim Strach (Booz),  
Robin Fischer (FZI)

Wissenschaftliche Begleitung: Prof. Dr.-Ing. Stefan Tai (FZI)

Booz & Company GmbH  
Anna-Louisa-Karsch-Straße 2  
D-10178 Berlin

FZI Forschungszentrum Informatik  
Friedrichstraße 60  
10117 Berlin

---