Bundesministerium
für Wirtschaft
und Technologie

WIRTSCHAFT.
WACHSTUM.
WOHLSTAND.

CLOUD
Computing

Das Normungs- und Standardisierungsumfeld von Cloud Computing

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

Kurzfassung

Impressum

Herausgeber
Bundesministerium für Wirtschaft
und Technologie (BMWi)
Öffentlichkeitsarbeit
11019 Berlin
www.bmwi.de

Redaktion
Eine Studie im Auftrag des Bundesministeriums für Wirtschaft und Technologie

Erstellung 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, Berlin
FZI Forschungszentrum Informatik, Berlin

Stand
Februar 2012

Druck
Hansa Print Service GmbH, München

Gestaltung und Produktion
PRpetuum GmbH, München

Das Bundesministerium für Wirtschaft und Technologie ist mit dem audit berufundfamilie® für seine familienfreundliche Personalpolitik ausgezeichnet worden. Das Zertifikat wird von der berufundfamilie gGmbH, einer Initiative der Gemeinnützigen Hertie-Stiftung, verliehen.

Diese Broschüre ist Teil der Öffentlichkeitsarbeit des Bundesministeriums für Wirtschaft und Technologie. Sie wird kostenlos abgegeben und ist nicht zum Verkauf bestimmt. Nicht zulässig ist die Verteilung auf Wahlveranstaltungen und an Informationsständen der Parteien sowie das Einlegen, Aufdrucken oder Aufkleben von Informationen oder Werbemitteln.

Inhalt

Die Langfassung der Studie steht als Download unter www.trusted-cloud.de zur Verfügung.

1. Zusammenfassung und Ausblick

Das Standardisierungsumfeld ist heterogen

Das Normungs- und Standardisierungsumfeld im Cloud Computing ist erst im Entstehen begriffen. Es gewinnt jedoch zunehmend an Eigendynamik. Diese Studie ist somit zwangsläufig eine erste Momentaufnahme.[1] 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 ungeeignete nationale Regeln oder deren Harmonisierung sowie unzureichende technische Konvergenz erschwert.

Die USA sind Vorreiter

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. Eine Vorreiterrolle unter den Standardisierungsgremien hat das NIST der US-Verwaltung, das als erstes Gremium eine Standardisierungsroadmap für das Cloud Computing erarbeitet hat. Einige internationale Gremien zeigen ebenfalls großes Engagement, während die überwiegende Mehrheit ihren Fokus nur langsam auf Standards für das Cloud Computing ausrichtet. Auf europäischer Ebene besitzen das ETSI und EuroCloud den größten 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 Mitwirkung. Viele führende Industriestaaten befinden sich im Jahr 2012 hinsichtlich Cloud Computing und seiner Standardisierung in der Orientierungs- und Planungsphase.

Erste Standards etablieren sich

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. Attraktivität strahlen auch erste Standardisierungsansätze wie OCCI, OVF, Open Stack oder CDMI aus, die alle einen expliziten Bezug zum Cloud Computing aufweisen. Die Standardisierungslücken und Weiterentwicklungsmöglichkeiten sind allgemein groß. Es gibt eine recht unübersichtliche Menge teils ähnlicher oder unreifer Standards mit unklarer Relevanz am Markt. Das Potenzial einer Vielzahl etablierter Standards für andere Bereiche und Branchen, die in angepasster Form für das Cloud Computing wichtig werden, wird nur langsam erschlossen (bspw. OAuth, SCAP, WS-* oder USDL). Managementstandards, wie der GRC Stack, sind äußerst rar.

Die Herausforderungen sind breit gefächert

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.

1 Während der sechsmonatigen Studienerstellung gab es eine Vielzahl neuer Veröffentlichungen, die nicht alle berücksichtigt werden konnten (z. B. TOSCA, http://www.oasis-open.org/committees/tosca/).

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 wichtige Standardisierungsentscheidungen im Cloud Computing zu erwarten sind.

Das Handlungswirken seitens der Politik sollte auf möglichst partizipative Instrumente setzen und sich auf zwei Ziele konzentrieren: Die Unterstützung bei der inhaltlichen Orientierung und die Schaffung geeigneter grundsätzlicher Rahmenbedingungen. Wichtige Handlungsfelder sind Zertifizierungen, Orientierungswissen, Rechtsverträglichkeit, zentrale Koordination, begleitende Kommunikation – und auch die Schaffung notwendiger rechtlicher Vorgaben. Eine Marke „Cloud Computing – Made and Secured in Germany“[2] könnte hierfür ebenso einen Ansatzpunkt darstellen, wie eine Standardisierungsroadmap für Deutschland.

2 „Wir wollen Cloud Computing made and secured in Germany“ – Interview mit MdB Hans-Joachim Otto, http://cloud-practice.de/news/wir-wollen-cloud-computing-made-and-secured-germany-interview-mit-mdb-hans-joachim-otto.

2. Einleitung

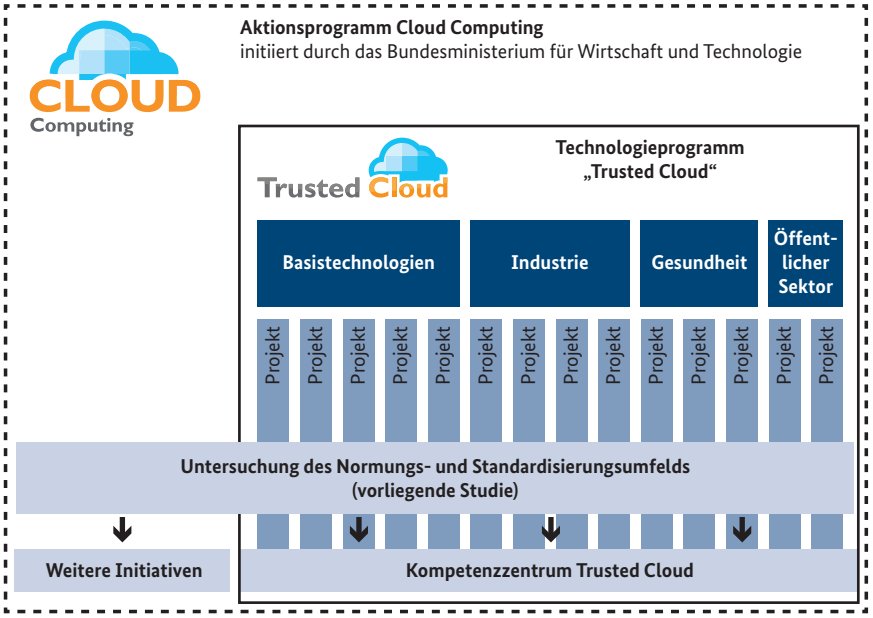
Ausgangssituation und Zielsetzung der Studie

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. Diese Studie ist in den Kontext des „Aktionsprogramms Cloud Computing“ eingebettet (siehe Abbildung 1). Das Aktionsprogramm wurde vom BMWi initiiert und wird von einer Allianz aus Wirtschaft, Wissenschaft und Politik getragen. Ein Teil des Aktionsprogramms 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.

Vor diesem Hintergrund ist die erste Zielsetzung der vorliegenden Studie, 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 Standards auch auf Vorarbeiten zur Standardisierung sowie Zertifizierungen (vgl. Kap. 3). Das größte Gewicht liegt auf der Betrachtung technischer Standards. Die weitere Untersuchung von Standards für das Management entspricht dem breit gefassten Anspruch der Studie. Zusätzlich werden wichtige 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.[3] Die Studie soll einen strategischen Aktionsrahmen und ordnungspolitische Handlungsempfehlungen erarbeiten und damit die Grundlage für eine deutsche Roadmap zur Standardisierung im Cloud Computing schaffen.

Abbildung 1: Einordnung der vorliegenden Studie



Quelle: BMWi, Analyse von Booz & Company und FZI

3 Die Ergebnisse der projektspezifischen Analyse und die daraus abgeleiteten Handlungsempfehlungen stehen nur den jeweils betreffenden Trusted Cloud-Projekten zur Verfügung.

Vorgehen und Aufbau der Studie

Die Studie ist in die beiden Teile „Überblick Normen und Standards im Cloud Computing“ und „Analyse der Trusted Cloud Projekte“ gegliedert. Beide sind eng miteinander verwoben (siehe Abbildung 2). Für die allgemeine Beschreibung des Normungs- und Standardisierungsumfeldes war deshalb die Rückkopplung mit den Trusted Cloud-Projekten wichtig, um die Praxistauglichkeit zu schärfen. Intensive Sekundärrecherchen wurden zudem durch Interviews mit einer Reihe von Experten abgerundet.

Ein Kernstück des übergreifenden Analyserasters bildet die Taxonomie für Standards im Cloud Computing (siehe Kap. 3).

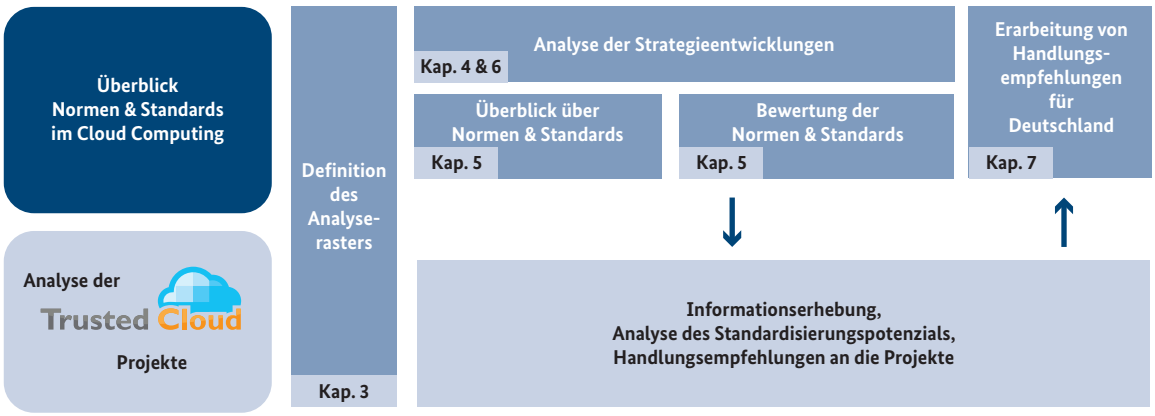
Vorab werden die Strategieentwicklungen ausgewählter Organisationen untersucht („Standardisierungsorganisationen“, siehe Kap. 4), die sich bei der Cloud-Standardisierung engagieren und ein Mindestmaß an Partizipationsmöglichkeit bieten.

Auf dieser Basis wird ein Überblick über relevante Standards, Zertifizierungen sowie Vorarbeiten gegeben. Zudem werden ausgewählte Standards bewertet und Weiterentwicklungsmöglichkeiten sowie Lücken identifiziert (siehe Kap. 5).

Mit Blick auf die Zukunft werden im Anschluss daran maßgebliche strategische Trends (siehe Kap. 6) bei der Standardisierung im Cloud Computing beschrieben.

Abschließend werden aus den Gesamtergebnissen Handlungsempfehlungen für die Cloud-Standardisierung für die deutsche Bundesregierung abgeleitet (siehe Kap. 7).

Abbildung 2: Vorgehen und Aufbau der Studie



Quelle: Booz & Company und FZI

3. Taxonomie für Standards im Cloud Computing

Begriffe im Cloud Computing und auch bei dessen Standardisierung werden häufig uneinheitlich verwendet. Deshalb definiert die vorliegende Studie für die Untersuchung des Normungs- und Standardisierungsumfelds eine konsistente Taxonomie. Sie ermöglicht ein zielgerichtetes Vorgehen, eine strukturierte Betrachtung und die begriffliche Eindeutigkeit bei Beschreibung und Bewertung. So werden Standards zum einen anhand der Herausforderungen im Cloud Computing kategorisiert, die sie adressieren („Wofür?“). Zum anderen werden Standards anhand ihrer Ansatzpunkte für die Standardisierung („Wodurch?“) unterschieden.

Neun Herausforderungen

Auf Basis von Literaturstudien wurden neun besonders relevante Herausforderungen im Cloud Computing identifiziert (siehe Abbildung 3), die sowohl die Perspektiven von Anbietern und Anwendern sowie überge-

Abbildung 3: Detaillierung der Herausforderungen im Cloud Computing (1. & 2. Ebene)

1	Effizienz der **Dienstebereitstellung**
a	Nutzung von Entwicklungstools & -komponenten
b	Aufbau skalierbarer Architekturen
c	Ressourcenmanagement & Flexibilität
d	Verfügbarkeit der Dienste
2	Effektivität der **Dienstenutzung und -steuerung**
a	Vertragsgestaltung inkl. Haftungsfragen
b	Steuerung der Dienste durch den Anwender
c	Governance- und Eskalationsmechanismen
3	**Transparenz** der Leistungserbringung und Abrechnung
a	Abrechnung inkl. Lizenzmanagement
b	Qualitätssicherung & Überwachung SLA
c	Art und Ort der Datenverarbeitung

4	**Informationsicherheit**
a	Identitäts- & Rechtemanagement
b	Vertraulichkeit & Integrität
c	Zugriffsschutz, Logging, Abwehr von Angriffen
d	Nachweis & Zertifizierung
5	**Datenschutz**
6	**Interoperabiltität**
a	Migration in die/aus der Cloud
b	Integrationsfähigkeit in on-Premise IT
c	Cloud-Föderation
7	**Portabiltität** zwischen Anbietern
a	Dienst-Portabilität
b	Daten-Portabilität
8	Sicherstellung eines funktionierenden **Wettbewerbs**
9	Compliance mit geltender **Rechtslage**

Quelle: Analyse von Booz & Company und FZI

Abbildung 4: Ansatzpunkte der Standardisierung im Cloud Computing

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, ...*
	Leitfäden, Audit, etc.	*BSI Eckpunktepapier, NIST UC, EuroCloud LRD&C*
Recht	Rechtliche Vorgaben	*EU Datenschutzrichtlinie, BDSG , Safe Harbor*
	Selbstverpflichtungen	*Open Cloud Manifesto, ...*
	Unternehmensrichtlinien	*Interne Policies, ...*

Quelle: Analyse von Booz & Company und FZI

ordnete Interessen abdecken. Die Herausforderungen gelten allgemein für das Cloud Computing und bilden gleichzeitig die Grundlage für die Identifikation der Herausforderungen in der Standardisierung. Sie werden auf einer zweiten Ebene noch einmal in 19 weitere Unterkategorien untergliedert.

14 Ansatzpunkte

Gemäß des breiten Studienfokus (vgl. Kap. 2.1) und im Zuge der Recherchen zu Standards wurden 14 verschiedene Ansatzpunkte in den Bereichen Technik, Management und Recht identifiziert (siehe Abbildung 4). Sie dienen zur fachlichen Strukturierung des Normungs- und Standardisierungsumfelds im Cloud Computing.

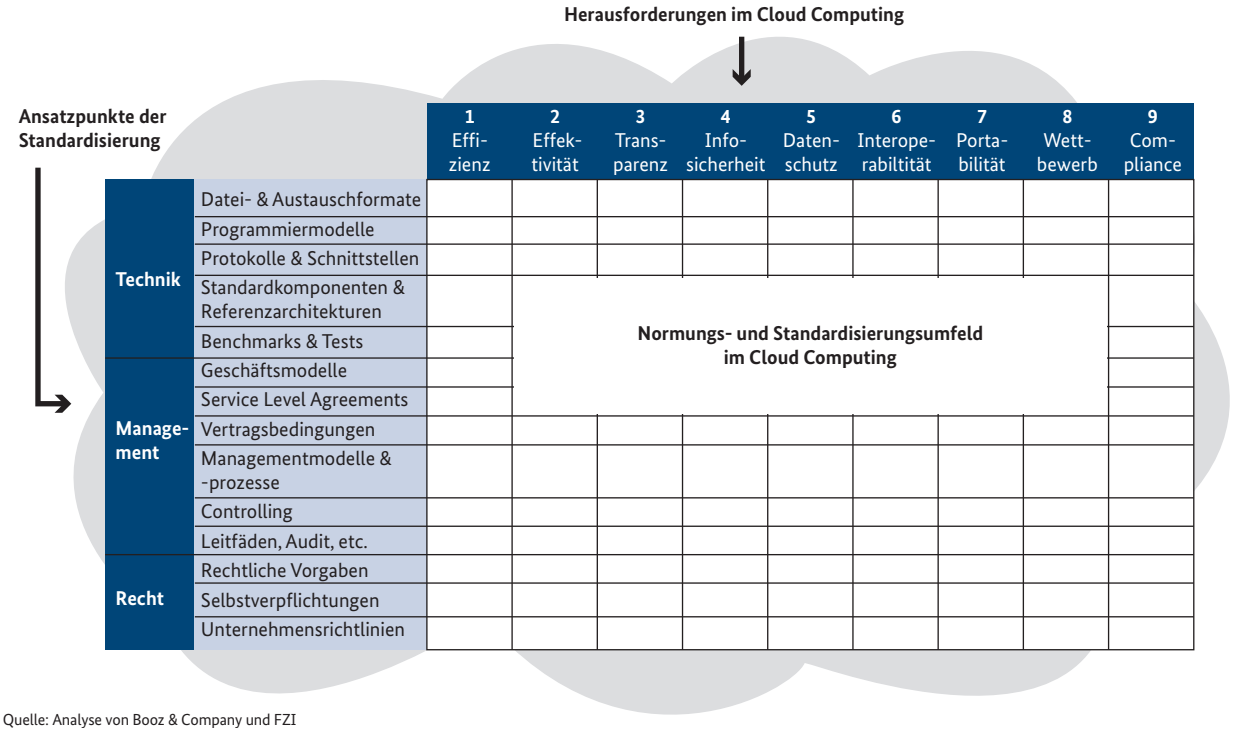
Die Einordnungsmatrix

Die Taxonomie betrachtet die Standardisierung aus zwei Perspektiven und spannt so einen Raum zur Einordnung der Standards im Cloud Computing auf („Einordnungsmatrix“, siehe Abbildung 5).

Der Begriff „Standard“

Zusätzlich wird der Begriff „Standard“ differenziert nach Formalisierungsgrad und Verbindlichkeitswirkung betrachtet. Es werden Vorarbeiten wie Orientierungswissen, (Referenz-) Implementierungen oder Spezifikationen, sowie Industriestandards, Standards und Normen unterschieden. Zertifizierungen liegen orthogonal zu diesem Begriffsverständnis.

Abbildung 5: Taxonomie als Normungs- und Standardisierungsumfeld im Cloud Computing



Quelle: Analyse von Booz & Company und FZI

4. Standardisierungsorganisationen im Cloud Computing

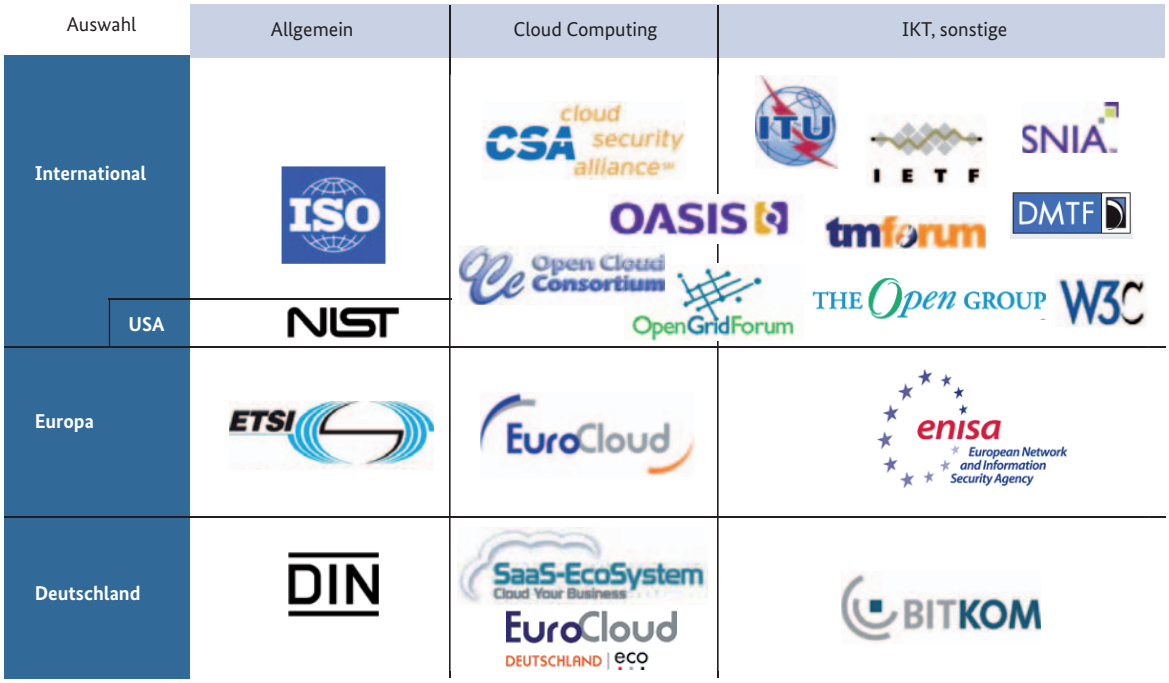
Es existiert eine Vielzahl verschiedener Akteure im Normungs- und Standardisierungsumfeld von Cloud Computing. Die Studie skizziert die wichtigsten Organisationen, die sich durch ein Mindestmaß an Engagement bei der Standardisierung im Cloud Computing und ein Mindestmaß an Partizipationsmöglichkeiten 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 privatwirtschaftliche Unternehmen sind nicht im Fokus. Bei Letzteren bestehen keine regulären Mitwirkungsmöglichkeiten für Außenstehende.

19 wichtige Standardisierungs-Organisationen

Abbildung 6 zeigt überblicksartig die 19 bedeutenden Organisationen sortiert nach ihrem thematischen und regionalen Fokus. Die USA nimmt mit der NIST eine Vorreiterrolle bei der Cloud-Standardisierung ein. 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 paneuropäischer Unternehmensverband der Anbieter von Cloud Computing mit großem Einfluss. In Deutschland unternehmen das DIN, der BITKOM und das BSI erste Schritte bei der Anforderungsdefinition. Abbildung 7 beschreibt in Stichpunkten das Engagement der 19 Organisationen bei der Standardisierung im Cloud Computing.

Abbildung 6: Wichtige Standardisierungsorganisationen im Cloud Computing



Quelle: Analyse von Booz & Company und FZI

Weitere Organisationen

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

Deutschland: DKE, Bundesnetzagentur, BSI, BVMW, BITMi, BDI.

Andere Länder: Cloud Computing Forum (CCF) in Korea, Global Inter-Cloud Technology Forum (GICTF) und die Cloud Operations and Security Arbeitsgruppe in Japan, China Communications Standards Association (CCSA).

Europa: EGI, NESSI, ENISA, CEN.

International: Cloud Computing Interoperability Forum (CCIF), Open Cloud Consortium (OCC), Object Management Group (OMG), Cloud Standards Customer Council (CSCC), Open Data Center Alliance (ODCA).

Abbildung 7: Engagement der Standardisierungsorganisationen im Cloud Computing

Fokus		Organisation	Standardisierungsengagement im Cloud Computing (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, MalStone 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; Gremienübersicht
	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-*)
	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
	IKT	TM-F (TM Forum)	Anpassungen von Frameworx 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 Encyption, XML Digital Signature oder SOAP)
USA		NIST (National Institute of Standards and Technology)	Cloud Computing Standardisierungsroadmap, Referenzarchitekturen, Taxonomie, Use Cases, Orientierungswissen, Koordination
Europa	CC	EuroCloud	Umfangreicher Leitfaden zu Recht, Datenschutz und Compliance, EuroCloud Star Audit („SaaS-Gütesiegel“)
	IKT	ETSI (Europäisches Institut für Telekommunikationsnormen)	Standards, Lückenanalyse und Testsysteme zu Interoperabilität, Anforderungen, Use Cases, Koordination, Standardisierungsroadmap
	IKT	ENISA (Europäischen Agentur für Netz- und Informationssicherheit)	Cloud Computing – SME Survey, Cloud Computing Information Assurance Framework, Cloud Computing Risk Assessment
DE	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, Telekommunik. &	Leitfaden des Arbeitskreis „Cloud Computing & Outsourcing“, Betreiber von Cloud-Practice.de (z. B. vertragliche Regelungen, Use Cases)

Quelle: Organisationen, Analyse von Booz & Company und FZI

5. Relevante Standards im Cloud-Umfeld

Die Analyse des Standardisierungsumfeldes soll einen Überblick über existierende Normen, Standards, Vorgaben, Zertifizierungen und Vorarbeiten im Cloud Computing schaffen und diese in den Kontext des Technologieprogramms Trusted Cloud einordnen. Offene Bereiche („White Spots"), in denen ein gestalterischer Beitrag zur Weiterentwicklung und Etablierung von Standards in Deutschland und darüber hinaus geleistet werden kann, sollen identifiziert werden. Anbieter, Anwender und Intermediäre von Cloud-Diensten sind in ihrer Geschäftstätigkeit einer Vielzahl von Standards ausgesetzt. 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 zu Cloud Computing aufweisen. Fallweise Berücksichtigung erfahren Standards mit wichtigem implizitem Bezug zu Cloud Computing (z. B. Web Service Standards).

Abbildung 8: Übersicht der 20 „Cloud-Standards"

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

Quelle: Analyse von Booz & Company und FZI

20 „Cloud-Standards“

Es wurden 20 prototypische Standards, Vorgaben, Zertifizierungen bzw. Vorarbeiten („Cloud-Standards“) ausgewählt. Diese werden im Detail untersucht und bewertet sowie mit weiteren ca. 35 ähnlichen Standards verglichen (siehe Abbildung 8). Mit dieser Vorgehensweise soll der Überblick allgemeingültig, übersichtlich und gleichzeitig möglichst umfassend und konkret gestaltet werden.

Bei der Auswahl und Bewertung der 20 Cloud-Standards handelt es sich um eine Momentaufnahme von Anfang 2012. Auf Grund der hohen Dynamik ist die Aktualität der Darstellung kritisch zu berücksichtigen.

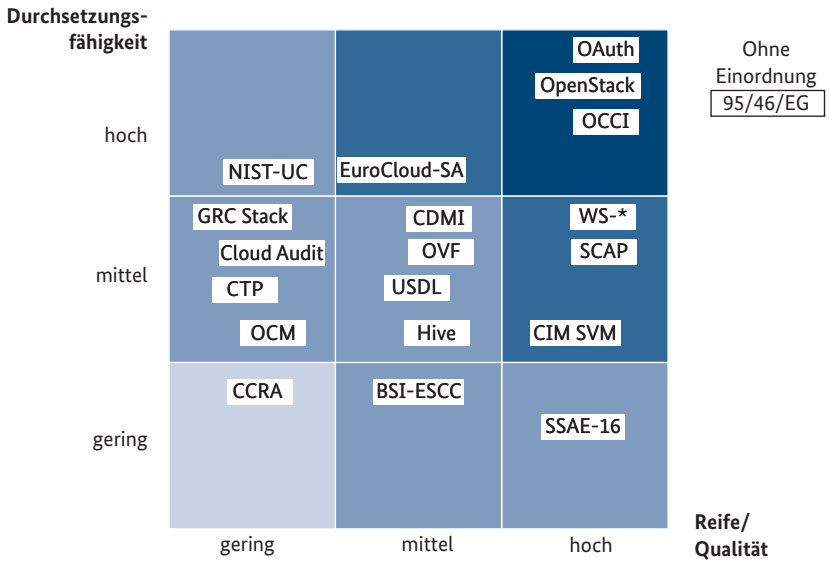
Die 20 Cloud-Standards besitzen nach Möglichkeit Vorbildcharakter, decken die Bereiche Technik, Management und Recht ab und finden größte Beachtung in Fachkreisen. Kein branchenspezifischer Standard besaß genug allgemeine Strahlkraft, um in die engere Auswahl zu gelangen.

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 Bewertungsergebnisse für die Standards (siehe Abbildung 9) spiegeln 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!“). Lücken im Normungs- und Standardisierungsumfeld wurden unter Einbeziehung der Gesamtstudienergebnisse und existierender Lückenanalysen (z. B. NIST) identifiziert. Abbildung 10 illustriert das Vorgehen von der Einordnung der bewerteten 20 Standards in das Umfeld (Schritt 1) über die Potenzialanalyse im Umfeld (Schritt 2) bis zur Bewertung der Lücken (Schritt 3).

Abbildung 9: Bewertung der 20 „Cloud-Standards“



Quelle: Analyse von Booz & Company und FZI

Standardisierungslücken im Cloud-Umfeld

Die Lücken spiegeln den frühen Stand der Standardisierung im Cloud Computing wider. Viele existierende Standards, die nur einen impliziten Bezug zum Cloud Computing besitzen, bilden eine solide Basis. 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.

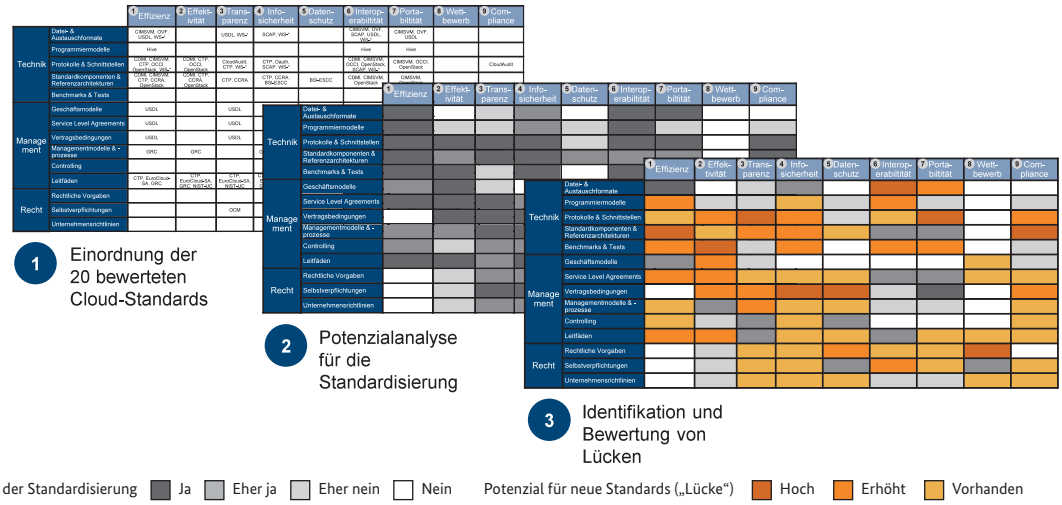
Das Zusammenspiel des Rechtsrahmens und der Standardisierung im Cloud Computing ist vielschichtig und wird bislang überwiegend auf Datenschutz reduziert. Auf europäischer und deutscher Ebene ist die Klärung des grundsätzlichen strategischen regulatorischen Vorgehens notwendig.

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.

Abbildung 10: Vorgehen bei der Identifikation von Cloud-Standardisierungslücken



Quelle: Analyse von Booz & Company und FZI

6. Wichtige strategische Trends bei der Standardisierung im Cloud Computing

Mit der Beschreibung strategischer Trends bei der Standardisierung im Cloud Computing wird der Blick zusätzlich auf die Zukunft gerichtet. 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. Alle Trends besitzen unmittelbare strategische Relevanz für die Cloud-Standardisierung, da sie einen inhärenten Bezug zu den Herausforderungen im Cloud Computing aufweisen (siehe Kap. 3).

Sechs Strategische Trends

Sechs strategische Trends wurden ohne Anspruch auf Ausschließlichkeit identifiziert. Sie sind in Abbildung 11 zusammengefasst. Der erste Trend (dunkelblau) fügt der Betrachtung eine themenübergreifende Perspektive hinzu. Er analysiert allgemein die Aktivitäten staatlicher Akteure bei der Standardisierung im Cloud Computing.

Abbildung 11: Strategische Trends bei der Standardisierung im Cloud Computing

Cloud Standardisierung und staatliche Mitwirkung	→ Die **USA besitzen eine Vorreiterrolle** (z. B. NIST Roadmap, „cloud-first" Grundsatz[4]) → Bei vielen Industrienationen deuten sich **ab 2012 zunehmende Bemühungen** an, z. B. – Frankreich *(z. B. Andromède und Handlungsfeld „Standardisierung")*, – Großbritannien *(z. B. G-Cloud)*, Deutschland *(z. B. Roadmap, Trusted Cloud)*, – EU *(z. B. ETSI Cloud-Standardisierungsroadmap, Cloud F&E Projekte)* und weitere
Cloud Zertifizierung	→ **Seit 2009 gibt es erste**, vergleichsweise noch unreife **Cloud-Zertifizierungen** für – Standards *(z. B. EuroCloud Gütesiegel, Trust in Cloud, EuroPriSe, Cloud Audit)*, – Experten *(z. B. „Cloud Experte", CCSK, IBM certified solution advisor for CC)* und – Geschäftspartner *(z. B. SAP Certified Provider of Cloud Services)* → Es wird ein **hoher Automatisierungsgrad** bei der Auditierung **angestrebt**
Offenheit im Cloud Computing	→ **Nachzügle**r *(z. B. AMD, Cisco, Citrix, IBM, VMware, viele KMU)* **wollen sich zunehmend mit Hilfe offener Standards etablieren** → Initiativen: DMTF Open Cloud Standards Incubator, Open Cloud Consortium, Open Cloud Manifesto (März 2009), Open Cloud Initiative (seit Juli 2011) → Unterschiedliche Auffassungen zur Offenheit; geringe Beteiligung der Staaten
Rechtssicherheit für die Cloud	→ Die bisherigen Cloud-Lösungen garantieren **keine Konformität mit geltendem deutschen und europäischen Recht** – es bestehen beträchtliche (Haftungs-)Risiken → **Verbindliche Standards können Rechtssicherheit schaffen** → R**elevante Rechtsgebiete:** Datenschutz, Sicherheits-, Strafprozess-, Verbraucher-, AGB-, Steuer-, Handels-, Urheber-, Privat- und IT-Vertragsrecht
Cloud Marktplätze	→ **Die innovative Erweiterung des Cloud Computing** um den Marktplatz-Gedanken wird seit 2010 verstärkt aufgegriffen → **Standards sind für Flexibilität und Vertrauen** im Marktplatz-Ökosystem **notwendig** → 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
Governance im Cloud Computing	→ Es werden **erste Standards** *(z. B. GRC Stack)* und Anforderungsdefinitionen *(z. B. zu KPIs)* zur Governance im Cloud Computing erarbeitet und **veröffentlicht** → Standards werden zur **Adressierung der komplexen Anforderungen** benötigt → Zunehmender Bedarf an zielgruppenbezogenen, reifen Standards sowie der Einbeziehung von existierenden Standards mit impliziter Bezug *(z. B. ITIL, COBIT)*

Quelle: Analyse von Booz & Company und FZI

4 Der „cloud-first" Grundsatz verpflichtet US-Behörden vor einer neuen IT-Investitionsentscheidung immer zuerst sichere Cloud Computing-Alternativen zu evaluieren.

7. Handlungsempfehlungen für die Standardisierung im Cloud Computing

Aus den Gesamtergebnissen der Studie werden Handlungsempfehlungen für die Standardisierung im Cloud Computing an die Bundesregierung abgeleitet, die sich weitgehend auf die EU übertragen lassen.

Die Empfehlungen sind in enger Verzahnung mit bestehenden Handlungsfeldern 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 bilde das Aktionsprogramm Cloud Computing, das Technologieprogramm Trusted Cloud und die angestrebte Marke „Cloud Computing – Made and Secured in Germany“ den entscheidenden Rahmen.

Wirtschaft und Staat sind aufgefordert zu handeln

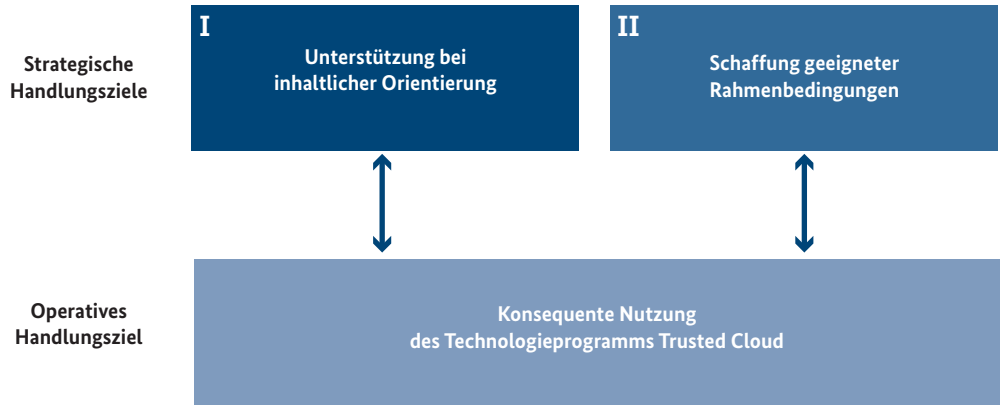
Die deutsche Wirtschaft trägt die Hauptverantwortung, durch eine aktivere Rolle bei der Standardisierung ihre vitalen Interessen im Cloud Computing wirkungsvoll zu vertreten. Es ist notwendig, dass sich alle Akteursgruppen, wie Anbieter, Anwender, große Konzerne und Mittelstand auf Augenhöhe begegnen.

Es gilt das Modell des freien Marktes, in den so wenig wie nötig eingegriffen werden sollte. Dennoch ist zugleich auch ordnungspolitisches Handeln entscheidend, denn damit kann einem möglichen Marktversagen frühzeitig begegnet werden. Cloud Computing sollte auch kein Gebiet mit unklarer Rechtslage sein. Dafür birgt es zu viele Wachstumschancen und ist für die Wirtschaft von zu großer Bedeutung.

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.

Zwei strategische Handlungsziele stehen im Vordergrund (siehe Abbildung 12). Zusätzlich gilt es, auf operativer Ebene das Technologieprogramm Trusted Cloud konsequent für die Standardisierung zu nutzen.

Abbildung 12: Übersicht der Handlungsziele



Quelle: Analyse von Booz & Company und FZI

Strategisches Handlungsziel I:

Der Staat sollte bei der inhaltlichen Orientierung unterstützen. Der Schwerpunkt liegt auf der Anforderungsdefinition und Schaffung von Orientierungswissen. Die eigentliche Standardisierung ist Aufgabe der Wirtschaft.

Strategisches Handlungsziel II:

Um ein koordiniertes, zielgerichtetes und erfolgreiches Vorgehen aller Akteure bei der Standardisierung zu ermöglichen, sollten geeignete Rahmenbedingungen bei der Standardisierung geschaffen werden. Das Handlungswirken sollte auf möglichst partizipative Instrumente setzen.

Zu den Handlungszielen wurden acht Handlungsfelder identifiziert, für die jeweils konkrete Maßnahmen empfohlen werden (siehe Abbildung 13).

1 – Schliessen von Standardisierungslücken

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 im Cloud Computing sollte durch das Setzen von Anreizen gefördert werden. Standards sollten auf Offenheit geprüft werden.

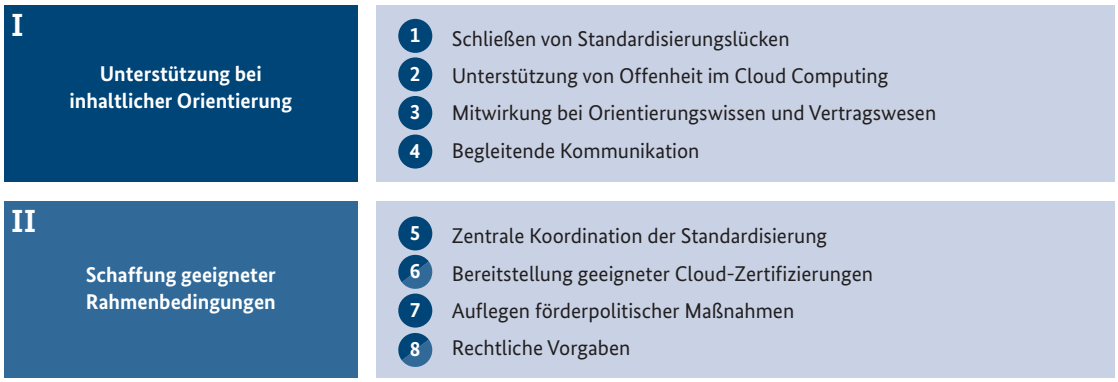
3 – Mitwirkung bei Orientierungswissen und Vertragswesen

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 Standardisierung im Cloud Computing zu stärken.

Abbildung 13: Übersicht der acht Handlungsfelder



Quelle: Analyse von Booz & Company und FZI

5 – Zentrale Koordination der Standardisierung

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 wie das Technologieprogramm Trusted Cloud auf Bundesebene 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.

www.bmwi.de