Federal Ministry
of Economics
and Technology

BUSINESS.
GROWTH.
PROSPERITY.

CLOUD
Computing

The Standardisation Environment for Cloud Computing

An analysis from the European and German point of view, including the 'Trusted Cloud Technology Programme'

Short version

Imprint

Publisher
Federal Ministry of Economics and Technology (BMWi)
Public Relations
11019 Berlin
www.bmwi.de

Editorial department
Study commissioned by the Federal Ministry of Economics and Technology

Produced by Booz & Company in co-operation with the FZI Forschungszentrum Informatik

Overall responsibility
Dr. Rainer Bernnat (Booz),
Dr. Wolfgang Zink (Booz)

Head of project team
Dr. Nicolai Bieber (Booz)

Project team
Joachim Strach (Booz),
Robin Fischer (FZI)

Academic support
Prof. Dr.-Ing. Stefan Tai (FZI)
Booz & Company GmbH, Berlin
FZI Forschungszentrum Informatik, Berlin

Last Revised
February 2012

Print
Hansa Print Service GmbH, Munich

Design and production
PRpetuum GmbH, Munich

The Federal Ministry of Economics and Technology has been awarded the berufundfamilie® audit certificate for its family-friendly HR policy. The certificate is granted by berufundfamilie gGmbH, an initiative of the Hertie Foundation.

Contents

The long version of the study in German is available for download under www.trusted-cloud.de

1. Summary and outlook

The standardisation environment is heterogeneous

The standardisation environment for cloud computing is only just starting to develop. However, it is picking up speed. So this study is inevitably an initial snapshot.[1] Existing work on standardisation has yet to pass the concept stage, since a lack of common definitions or orientational knowledge has impeded joint and targeted progress. The widespread deployment of genuinely useful and usable standards for cloud computing is hindered by a lack of suitable national rules, of harmonisation, and of technical convergence.

The USA is leading the way

Thanks to the market power of their proprietary industry standards, established US providers are exerting the greatest influence on standardisation in cloud computing. In the second tier, there are consortia aiming to have open standards as a market entry strategy. A pioneering role amongst the standardisation bodies is being played by the NIST of the US administration: it was the first body to draw up a standardisation roadmap for cloud computing. Some international bodies are also very much involved, but the overwhelming majority are being slow to focus on standards for cloud computing. At European level, ETSI and EuroCloud are the most influential bodies. In Germany, the DIN, BITKOM and the BSI are taking first steps towards the definition of the specifications. Major future commercial users of cloud computing, and SMEs in particular, are failing to play a sufficient part in the process. Many leading industrial nations are currently at the stage of orientation and planning in the field of cloud computing and cloud standardisation.

First standards becoming accepted

Much work is currently being done on preparations, e. g. orientational knowledge, specifications or reference implementations. Proprietary, commercial solutions in particular are widespread, and are currently emerging as the industry standard. Initial standardisation attempts like OCCI, OVF, Open Stack or CDMI, all of which make explicit reference to cloud computing, are also proving attractive. Generally, there are large gaps in standardisation and there is great potential for development. There is a confusing plethora of standards, some of them similar, some of them underdeveloped, and their degree of market relevance is sometimes unclear. The potential contained in a large number of established standards for other fields and sectors, which in an adapted form are becoming important for cloud computing, is only being developed slowly (e.g. OAuth, SCAP, WS-* or USDL). Management standards, like GRC-Stack, are extremely rare.

A diverse range of challenges

There is a need for a holistic approach and a co-ordinated definition of the aims in the field of cloud standardisation. As far as possible, this should be co-ordinated at international, European and German level. The main aim should be to close the gaps in the interest of functioning and fair competition. For example, there are many challenges in terms of interoperability, portability, enhanced transparency, legal certainty (e.g. with regard to data privacy), information security and governance, or – more fundamentally – in terms of openness to more competition.

The industry and the state are both called on to act

The chief responsibility lies with the German business community, which needs to play a more active part in standardisation in order to assert its key interests in the field of cloud computing. At the same time, there is a need for a policy response by government, since this is the only way to prevent possible market failure at an early stage. Cloud computing should not be a field where the legal situation is unclear or even completely open: it simply offers too many opportunities for growth if the right framework is in place. Rapid action is needed since major decisions on cloud standardisation are likely to be seen by 2014.

1 In the course of the six months in which the study was produced, a lot of new publications appeared, not all of which could be taken into account (e. g. TOSCA, http://www.oasis-open.org/committees/tosca/).

The work of policy-makers should aim to use instruments that are as participation-based as possible, and should focus on two objectives: contributions in terms of content guidance, and the establishment of an appropriate policy environment. Key fields of action include certification, orientational knowledge, compatibility with the law, central co-ordination, supporting communication – and the establishment of the necessary rules and regulations. A brand called "Cloud Computing – Made and Secured in Germany"[2] could provide a starting point for this, as could a standardisation roadmap for Germany.

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

2. Introduction

Current situation and aims of the study

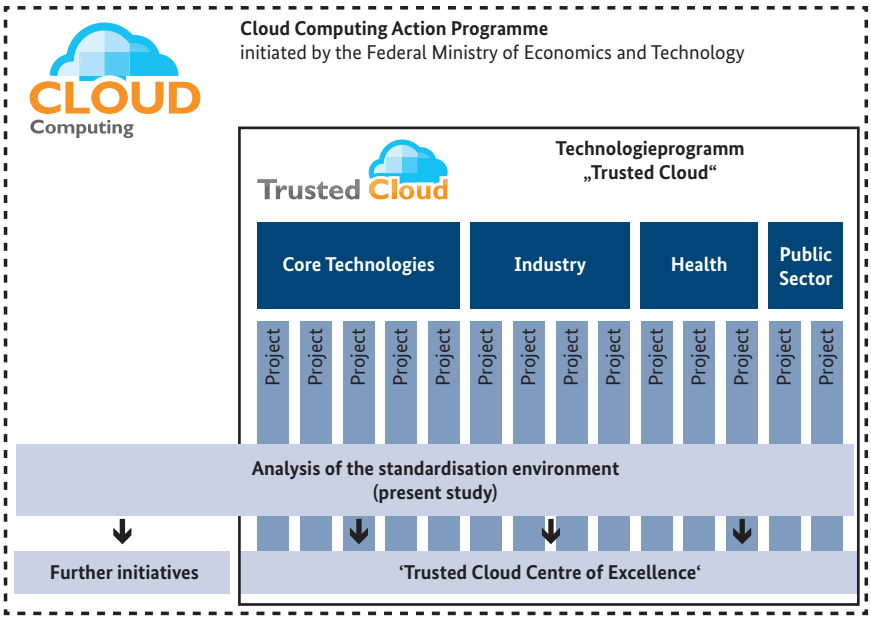
In spring 2011, the Federal Ministry of Economics and Technology (BMWi) commissioned Booz & Company to undertake the study "Standardisation in cloud computing" in co-operation with the FZI. This study is embedded in the context of the Cloud Computing Action Programme (cf. Figure 1). The Action Programme was launched by the BMWi and is being driven by an alliance of the industry, academia and government. The Action Programme includes the BMWi's Trusted Cloud Technology Programme, which aims to promote research and development activities for efficient and innovative cloud infrastructures and secure and trustworthy cloud-based services.

In view of this, the first objective of this study is to provide an overview of the present standardisation situation. The German perspective is included as part of the overall analysis at European and international level. In addition to standards, the study also looks at preparatory work for standardisation and at certification (cf. Chapter 3). The main focus is on technical standards. The additional coverage of management standards is in line with the study's broad approach. It also considers key legal factors.

The study's second aim is to make recommendations for the 14 selected Trusted Cloud projects regarding the potential and the problems of standardisation in the period up to early 2015.[3]

The study aims to draw up a framework for strategic action and policy recommendations, thereby creating a foundation for a German roadmap for cloud standardisation.

Figure 1: The setting for this study



Source: BMWi, Analyse von Booz & Company und FZI

3 The findings of the project-specific analyses and the recommendations for action derived from them are available only to the relevant Trusted Cloud projects.

Approach and structure of the study

The study is divided into two parts: "Overview of standards in cloud computing" and "Analysis of Trusted Cloud projects". The two sections are closely interlinked (cf. Figure 2). In order to enhance the emphasis on the practical nature of the work, the interlinkage with the Trusted Cloud projects played an important role in the general description of the standardisation environment. Intensive secondary research was also undertaken via interviews with a number of experts, including partners of the 14 Trusted Cloud projects.

The taxonomy of standards in cloud computing (cf. Chapter 3) formed a core element of the overarching analytical framework.

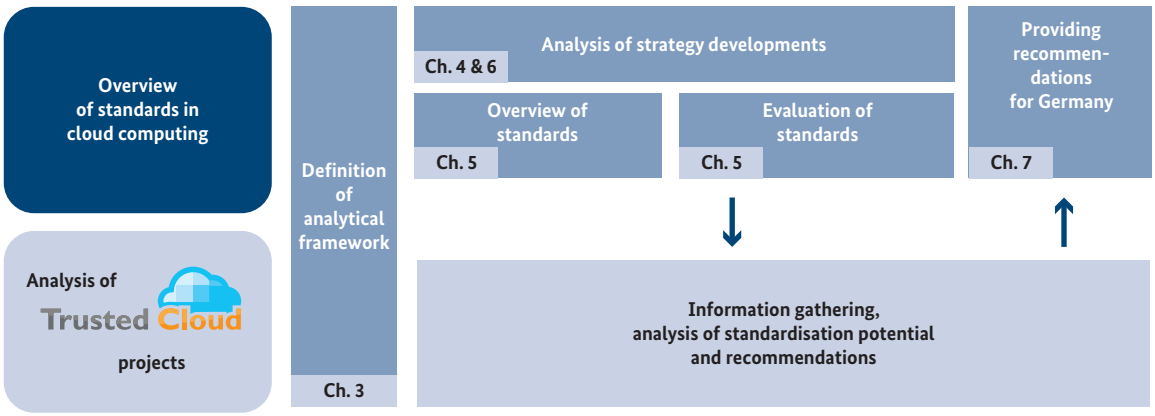
First, the study looks at developments in the strategy of selected organisations ("Standardisation organisations" – cf. Chapter 4) involved in cloud standardisation which offer a minimum degree of opportunities for participation.

On this basis the study produces an overview of relevant standards, certifications and preparatory work. Furthermore, selected standards are assessed and possibilities for further development and gaps are identified (cf. Chapter 5).

With a view to the future, major strategic trends in cloud standardisation are then described (cf. Chapter 6).

Finally, recommendations for action on cloud standardisation by the German Government are derived from the overall findings (cf. Chapter 7).

Figure 2: Approach and structure of the study



Source: Booz & Company und FZI

3. Taxonomy of standards in cloud computing

Terms are often used inconsistently in cloud computing and mean different things to different people, even in efforts to standardise the terminology as such. For this reason, this study puts a significant emphasis on the definition of a consistent taxonomy for its analysis of the standardisation environment.

This enables a targeted approach, a structured view and a clear use of terminology in the description and evaluation. First, standards are classified in terms of the challenges they address in cloud computing ("Why?"). Second, standards are distinguished on the basis of their approach ("How?").

Nine challenges

Working from the literature, nine especially relevant challenges in cloud computing were identified (cf. Figure 3) which cover both the perspectives of providers

Figure 3: Details of the challenges in cloud computing (1st and 2nd levels)

1	Efficiency of **service provisioning**
a	Usage of development tools & components
b	Creation of scalable architectures
c	Resource management & flexibility
d	Availability of services
2	Effectiveness of **service usage and control**
a	Contracts incl. questions of liability
b	Control of services by users
c	Governance/escalation mechanisms
3	**Transparency** of service delivery and billing
a	Billing incl. license management
b	Quality assurance and monitoring SLA
c	Type and location of data processing
4	**Information security**
a	Identity & rights management
b	Privacy & integrity
c	Access control, logging, attack prevention
d	Verification & certification
5	**Data privacy**
6	**Interoperability**
a	Migration in the/out of the Cloud
b	Ability to integrate into on-premise IT
c	Cloud federation
7	**Portability** between providers
a	Service portability
b	Data portability
8	Ensuring fair **competition** in the market
9	**Compliance** with regulatory requirements

Source: Analyse von Booz & Company und FZI

Figure 4: Fields of standardisation in cloud computing

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

Source: Analyse von Booz & Company und FZI

and users and overarching interests. The challenges apply to cloud computing in general and also form the basis for the identification of the challenges posed by standardisation. At a second level, they are subdivided again into 19 further subcategories.

14 fields of standardisation

In line with the broad focus of the study (cf. Chapter 2) and in the course of the research on standards, 14 different fields of standardisation were identified in the areas of technology, management and law (cf. Figure 4). They serve to structure the substance of the standardisation environment in cloud computing.

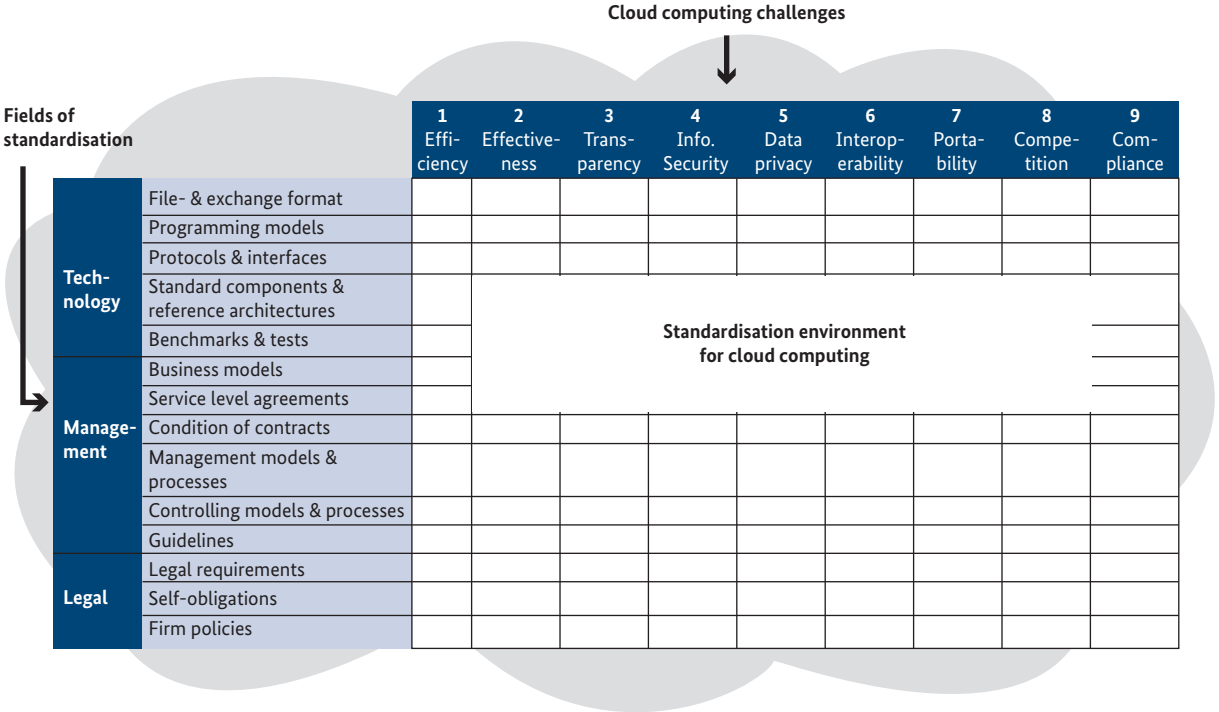
The classification matrix

The taxonomy views standardisation from two perspectives and thus spans a space within which to classify the cloud standards (cf. the Classification Matrix in Figure 5).

The term “standard”

Also, the term “standard” is differentiated in terms of how formal and binding the standard is. A distinction is drawn between preparatory work like orientational knowledge, (reference) implementations or specifications, and industry standards, standards and technical standards. Certifications are orthogonal to this understanding of terms.

Figure 5: Taxonomy as a standardisation environment in cloud computing



Source: Analyse von Booz & Company und FZI

4. Standardisation organisations in cloud computing

There are a large number of different players in the field of cloud standardisation. The study sketches out the leading organisations which are characterised by at least a minimum of involvement in cloud standardisation and offer at least a minimum degree of possibilities to participate (here termed “standardisation organisations”).

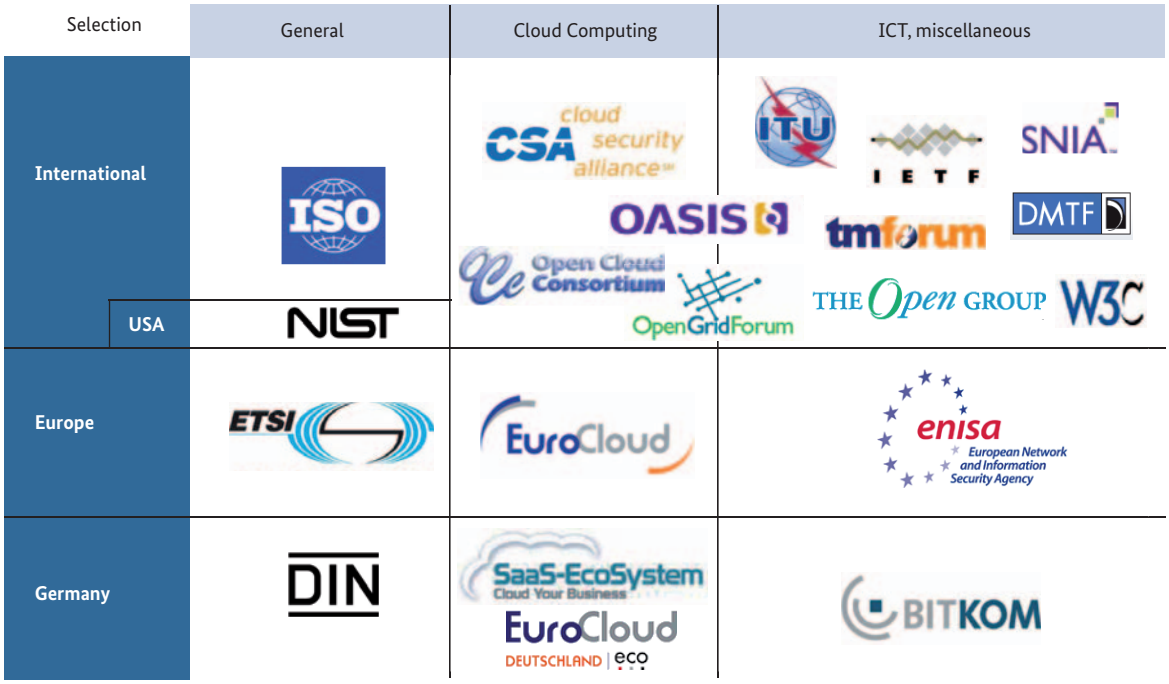
The selection is based on initial research covering more than 150 different institutions. In line with the goal of the study, the focus is on standardisation organisations, standard development organisations, interest groups, consortia and public institutions.
A common feature of all of these is that they have bodies promoting standards or preparatory work with an implicit or explicit reference to cloud computing. The focus does not include research institutions or private-sector companies. In the latter case, outsiders are not normally able to participate in decision-making processes.

19 leading standardisation organisations

Figure 6 gives an overview of the 19 leading organisations, classified by their thematic and regional focus. The USA (NIST) is playing a pioneering role in cloud standardisation.

Some international standardisation bodies are also very much involved, but the overwhelming majority are being slow to focus on standards for cloud computing. At European level, ETSI will serve as a co-ordinator. EuroCloud is a highly influential, pan-European association of cloud computing providers. In Germany, the DIN, BITKOM and the BSI are taking first steps towards the definition of the specifications. Figure 7 provides brief notes on the involvement of the 19 organisations in cloud standardisation.

Figure 6: Leading standardisation organisations in cloud computing



Sources: Analyse von Booz & Company und FZI

Other organisations

In addition to the organisations looked at here, there are others which have yet to display clear involvement or which do not offer any opportunities to participate. Some of them are likely to play a greater role in future:

Germany: German Commission for Electrical, Electronic & Information Technologies (DKE), Federal Network Agency, Federal Office for Information Security (BSI), German Association for Small and Medium-sized Businesses (BVMW), Federal Association of SMEs in IT (BITMi), Federation of German Industries (BDI).

Other countries: Cloud Computing Forum (CCF) in Korea, Global Inter-Cloud Technology Forum (GICTF) and the Cloud Operations and Security Working Group in Japan, China Communications Standards Association (CCSA).

Europe: 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).

Figure 7: Involvement of the standardisation organisations in cloud computing

		Organisation	Involvement in standardisation in cloud computing (examples)
International	General	**ISO (International Organization for Standardization)**	OSIMM, OVF, SOA, orientational knowledge, specifications and co-ordination of cloud standardisation (e.g. in JTC 1/SC 38)
	CC	**CSA (Cloud Security Alliance)**	Best practices, orientational knowledge and standards in the field of security for cloud computing (e. g. GRC-Stack)
	CC	**OCC (Open Cloud Consortium)**	Cloud infrastructure – infrastructure for research purposes, cloud computing test environments, reference implementations, MalStone Benchmark
	ICT	**DMTF (Distributed Management Task Force)**	OVF, System Virtualization Management Standards (VMAN), management data model
	ICT	**IETF (Internet Engineering Task Force)**	Internet protocols and standards, such as FTP, HTTP/HTTPS, TCP/IP, X.509 Certificates, PKI or OAuth; overview of responsible bodies
	ICT	**ITU (International Telecommunication Union)**	Cloud definition, ecosystem, use cases specifications and architecture, security in CC, cloud infrastructure, analysis of gaps, action plan
	ICT	**OASIS (Organization for the Advancement of Structured Information Standards)**	Concepts, use cases and gaps in cloud identity (in IDCloud), many implicitly relevant standards (e.g. SAML, ODF, SOA, WS-*)
	ICT	**OGF (Open Grid Forum)**	Open Cloud Computing Interface (OCCI) or GridFTP
	ICT	**SNIA (Storage Networking Industry Association)**	Cloud Data Management Interface (CDMI), Storage Management Initiative Specification (SMI-S), eXtensible Access Method (XAM)
	ICT	**TOG (The Open Group)**	Standards to integrate cloud computing into existing corporate architectures, e.g. Cloud Computing Reference Architecture (CCRA)
	ICT	**TM-F (TM Forum)**	Adaption of Frameworx for CC, Cloud Billing, Cloud SLA Mgmt., Cloud Security & Risk, Cloud Business Process Framework
	ICT	**W3C (World Wide Web Consortium)**	USDL Incubator, general web standards (e.g. HTML, XML, CSS, WSDL, XML Encyption, XML Digital Signature or SOAP)
USA		**NIST (National Institute of Standards and Technology)**	Cloud Computing Standardisation Roadmap, reference architectures, taxonomy, use cases, orientational knowledge, co-ordination
Europe	CC	**EuroCloud**	Comprehensive guidelines on law, data privacy and compliance, EuroCloud Star Audit (“SaaS quality mark”)
	ICT	**ETSI (European Telecommunications Standards Institute)**	Standards, analysis of gaps and testing systems for interoperability, specifications, use cases, co-ordination, standardisation roadmap
	ICT	**ENISA (European Network and Information Security Agency)**	Cloud Computing – SME Survey, Cloud Computing Information Assurance Framework, Cloud Computing Risk Assessment
Germany	General	**DIN (Deutsches Institut für Normung)**	Bodies following work of ISO JTC 1/SC 38 in NIA-01-38 “Distributed application platforms and services”
	CC	**SaaS-ES (SaaS-EcoSystem)**	“Trust in Cloud” certificate for SaaS and cloud solutions, “Cloud Expert” certificate
	ICT	**BITKOM** (Federal Association for Information Tech, Telecommunications and New Media)	Guidelines of “Cloud Computing & Outsourcing” working group, operator of Cloud-Practice.de (e.g. contractual rules, use cases)

Source: Organisationen, Analyse von Booz & Company und FZI

5. Relevant standards in the cloud environment

The analysis of the standardisation environment aims to provide an overview of existing standards, requirements, certification and preparatory work in cloud computing and to place them in the context of the Trusted Cloud Technology Programme. The aim is also to identify "white spots" in which a substantive contribution can be made towards the further development and establishment of standards in Germany and beyond. Providers, users and intermediaries of cloud services are exposed to a wide variety of standards in their business activities. 160 standards were identified and analysed in the course of intensive secondary and primary research. The focus is on cross-sectoral standards which make explicit reference to cloud computing.

Standards with a significant implicit reference to cloud computing (e. g. web service standards) are included on a case-by-case basis.

Figure 8: Overview of the 20 "cloud standards"

		Standards, certifications, rules and preparatory work	Similar	Initiator
Technology	CC	**CCRA (Cloud Computing Reference Architecture):** reference architecture for cloud services	Reference architectures of NIST or BSI	TOG
	CC	**CDMI (Cloud Data Management Interface):** API for data access in IaaS, DaaS scenarios	XAM, iSCSI, NFS, WebDAV	SNIA
	CC	**Cloud Audit (Automated Audit, Assertion, Assessment, and Assurance API):** API for access to audit information	SCAP	CSA
	CC	**CTP (Cloud Trust Protocol):** uniform techniques and nomenclature to boost transparency	SCAP, OCRL	CSA
	CC	**OCCI (Open Cloud Computing Interface):** API for cloud management (especially IaaS)	DeltaCloud, Libcloud, APIs von EC2, Rackspace, Eucalyptus, vCloud etc.	OGF
	CC	**OpenStack (OpenStack Cloud Software):** framework for the building of cloud infrastructures	OpenNebula, Nimbus (interfaces: CMDI, OCCI, OVF)	(Various)
	ICT	**CIMSVM (CIM System Virtualization Model):** object model and interfaces for virtual systems & components	–	DMTF
	ICT	**Hive (Apache Hive):** programming model for data requests	JAQL, PIG	Apache
	ICT	**OAuth (Web Authorization Protocol):** protocol and interface for identity management	OpenID, WS Federation, SAML	IETF
	ICT	**OVF (Open Virtualization Format):** file format for virtual machines	AMI, EMI	DMTF, ANSI, ISO
	ICT	**SCAP (Security Content Automation Protocol):** protocol and interface to download security content	CloudAudit	NIST
	ICT	**USDL (Unified Service Description Language):** description language for virtual services	WSDL, UDDI, WADL, OWL-S, SNN, WSMO, e3Value, PAS1018 etc.	W3C
	ICT	**WS-* (Web Service Standards):** specifications and standards for web services	WSDL, WS Policy, WS Agreement, WS Security, etc.	OASIS, OGF, W3C
Management	CC	**BSI-ESCC (basic security recommendations for cloud computing providers):** guidelines	Other specfication documents	BSI
	CC	**EuroCloud-SA (EuroCloud Star Audit):** certificate for providers of cloud services	EuroPriSe, TiC	EuroCloud
	CC	**GRC-Stack (Governance, Risk Management and Compliance Stack):** framework for risk assessment of cloud providers	CloudAudit, CCM, CAIQ, CTP	CSA
	CC	**NIST-UC (Cloud Computing Use Cases):** guidelines for applications in cloud computing with a focus on US agencies	Use Cases of OGF or DMTF	NIST
	General	**SSAE-16 (Statement on Standards for Attestation Engagements No. 16):** certificate for providers of cloud services	CobiT, BSI-100, ISAE 3402, ITIL, SAS 70, IDW PS 330/951/FAIT1	AICPA
Law	CC	**OCM (Open Cloud Manifesto):** voluntary commitment to openness for cloud providers	–	(Various)
	General	**95/46/EC (EU Directive 95/46/EC "Data Protection directive"):** EU data protection rules	Federal Data Protection Act, Länder data protection acts, Safe Harbor	EU

Source: Analyse von Booz & Company und FZI

20 “cloud standards”

20 prototypical standards, requirements, certifications and examples of preparatory work (“cloud standards”) were selected. These were examined and evaluated in detail and compared with some 35 similar standards (cf. Figure 8). This approach aims to make the overview both generally valid and easy to grasp, whilst also being as comprehensive and specific as possible.

The selection and evaluation of the 20 cloud standards is a snapshot from the beginning of 2012. In view of the pace of developments, a critical view needs to be taken of how up-to-date the snapshot is.

The 20 prototypical cloud standards serve as models, cover the fields of technology, management and law, and are greatly respected by experts. None of the sector-specific standards had enough general impact to be included on the shortlist.

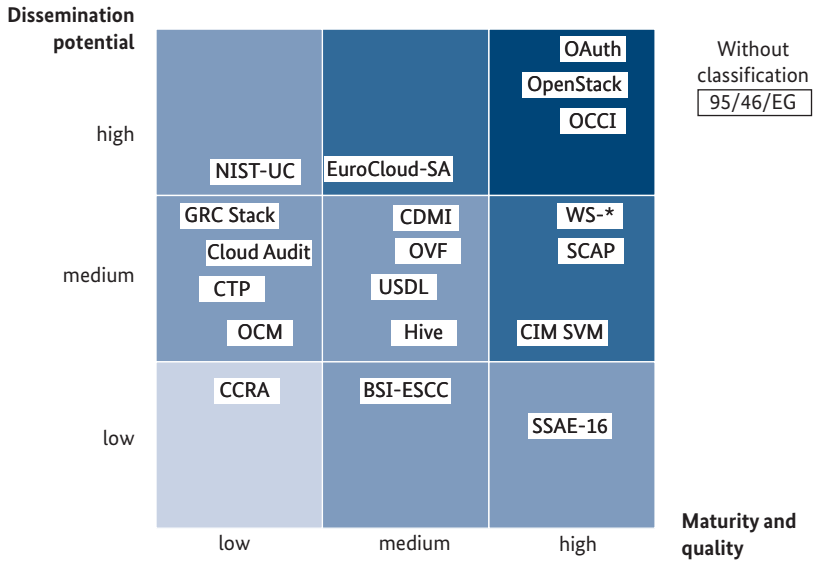
The vast majority of the standards are of international relevance. Some of them have a (slight) European or national reference (e.g. BSI-ESCC, USDL, NIST-UC, EuroCloud-SA, 95/46/EC).

The findings of the evaluation of the standards (cf. Figure 9) reflect the early developmental stage of cloud computing. Standards which already existed before cloud computing tend to be more mature (e.g. SCAP, WS-*, OAuth, CIMSVM, SSAE-16) than those drafted specifically for cloud computing. On the other hand, standards which make explicit reference to cloud computing generally exert greater influence than those which make implicit reference.

Effective use should be made of standards which are already widespread and mature (“Use!”). Those which are less widespread should be promoted (“Promote!”) and those which are at a developmental stage should be contributed to (“Contribute!)”.

Gaps in the standardisation environment were identified; this process included the overall study results and existing analyses of gaps (e.g. NIST). Figure 10 illustrates the approach, from the classification of the 20 standards in the environment (step 1) to the analysis of potential in the environment (step 2) and the evaluation of the gaps (step 3).

Figure 9: Evaluation of the 20 “cloud standards”



Source: Analyse von Booz & Company und FZI

Gaps in standardisation in the cloud environment

The gaps reflect the fact that cloud standardisation has still to mature. A solid basis is formed by many existing standards which only make implicit reference to cloud computing. However, they still need to be adapted to cloud computing. Many new standards, being developed specifically for cloud computing, lack sufficient maturity. In certain areas, a total lack of standards can be seen.

The majority of the standardisation activities are focused on challenges like information security, efficiency, interoperability or portability, and mainly take a technology-driven approach. There is further need for IT standards, for example for standard components, reference architectures, benchmarks, tests, or protocols and interfaces.

The largest gaps exist in the field of management standards. There are no, or only inadequately comprehensive, standards for business models, service quality agreements, management models and processes, auditing and contractual rules. It would also be feasible to have standardised, binding corporate rules (BCRs) for cloud providers on data privacy on the basis of voluntary commitments.

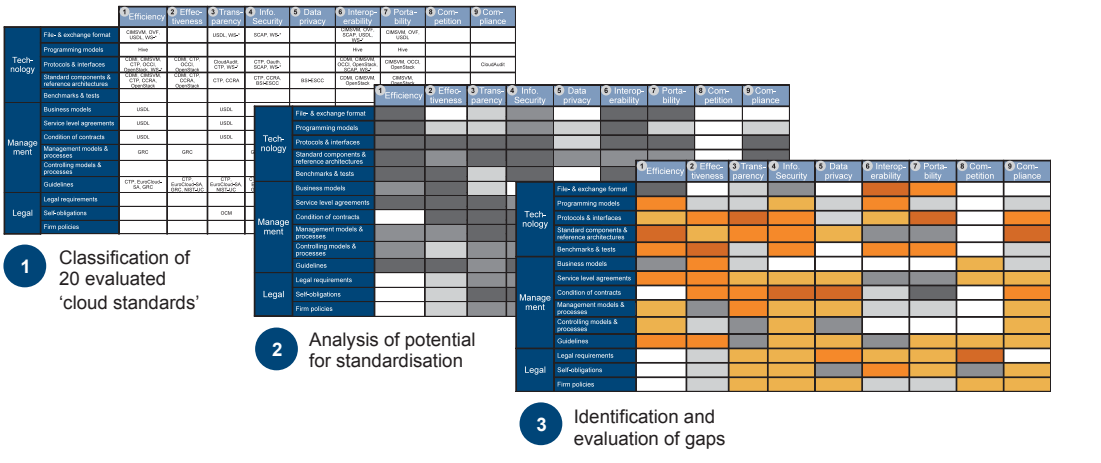
The interplay between the legal framework and standardisation in cloud computing occurs at many different levels, but has so far largely been reduced to the field of data privacy. There is a need to clarify the fundamental strategic regulatory approach at European and German level.

Standardisation potential in Germany

The main challenges for Germany and Europe lie in the field of interoperability, data privacy, legal certainty and competition. The top priority should be the establishment of a cloud certification system, e. g. a quality mark like “Cloud Computing – Made and Secured in Germany”. For this to happen, it will be necessary to verify compliance with the law, and to provide orientational knowledge.

The Trusted Cloud Technology Programme contains further potential for standardisation, e.g. in terms of security architectures, secure operator platforms, solutions for data privacy and transparency, identity management, cloud service descriptions, and protocols and interfaces.

Figure 10: Identification procedure for gaps in cloud standardisation



Source: Analyse von Booz & Company und FZI

6. Important strategic trends

The description of strategic trends in cloud standardisation shifts the focus to the future. To provide a basis from which to work, various activities of recent years were grouped in thematic areas. The probable development of those thematic areas which look likely to be most dynamic in the period up to 2015 is studied. The focus is placed on trends with a strong relationship to Europe or Germany. All of the trends are of direct strategic relevance to cloud standardisation, since they contain an inherent reference to cloud computing (cf. Chapter 3).

Six strategic trends

Six strategic trends were identified, without any claim that this list is exhaustive. They are summarised in Figure 11. The first trend (dark blue) adds an interdisciplinary perspective to this approach. It provides a general analysis of the activities of government stakeholders in cloud computing.

Figure 11: Strategic trends in standardisation in cloud computing

Cloud standardisation and government involvement	→ **The USA plays a pioneering role** *(e.g. NIST roadmap, "cloud first" principle[4])* → Many industrial countries are showing signs of **greater effort from 2012**, e.g. – France *(e.g. Andromède and "Standardisation" field of action)*, – UK *(e.g. G-Cloud)*, Germany *(e.g. Roadmap, Trusted Cloud)*, – EU *(e.g. ETSI Cloud Standardisation Roadmap, Cloud R&D projects)* etc.
Cloud certification	→ **Since 2009** there have been the **first**, comparatively immature **cloud certifications** for – standards *(e.g. EuroCloud quality seal, Trust in Cloud, EuroPriSe, Cloud Audit)*, – experts *(e.g. "cloud expert", CCSK, IBM certified solution advisor for CC)* and – business partners *(e.g. SAP Certified Provider of Cloud Services)* → A **high degree of automation** in auditing is **desired**
Openness in cloud computing	→ Those **lagging behind** *(e.g. AMD, Cisco, Citrix, IBM, VMware, many SMEs)* **want to increasingly become established with the aid of open standards** → **Initiatives:** DMTF Open Cloud Standards Incubator, Open Cloud Consortium, Open Cloud Manifesto (March 2009), Open Cloud Initiative (since July 2011) → Divergent views on openness; little government involvement
Regulatory clarity for the cloud	→ The existing cloud solutions **do not guarantee compliance with current German and European law** – there are considerable (liability) risks → **Binding standards can create regulatory clarity** → **Relevant areas of law:** data privacy, security, criminal procedure, consumer, commercial, tax, copyright, private and IT contracts
Cloud marketplaces	→ The i**nnovative expansion of cloud computing** to include the marketplace concept has been increasingly taken up since 2010 → Standards are **needed for flexibility and trust** in the marketplace ecosystem → IaaS *(e.g. Amazon Web Services, Rackspace, Enomaly)* is dominated by Amazon AWS; SaaS *(e.g. TEXO-Marketplace, Logistics Mall, Trusted Cloud projects)* also includes management solutions
Governance in cloud computing	→ **Initial standards** *(e.g. GRC-Stack)* and definitions of specifications *(e.g. on KPIs)* for governance in cloud computing are being drafted and **published** → Standards are needed to **address the complex requirements** → Increasing need for mature standards oriented to target groups and for the inclusion of existing standards with an implicit reference *(e.g. ITIL, COBIT)*

Source: Analyse von Booz & Company und FZI

4 The "cloud first" principle requires US agencies always to evaluate secure cloud computing alternatives prior to any new IT investment decision (cf. www.cio.gov/documents/federal-cloud-computing-strategy.pdf).

7. Recommendations for action

Recommendations for action by the Federal Government on standardisation in cloud computing are derived from the overall findings of the study; these recommendations largely apply to the EU as well.

The recommendations should be viewed in close connection with existing fields of action. At EU level, these are primarily the European Commission's planned cloud strategy, the expert report "The Future of Cloud Computing", and the ongoing R&D projects on cloud computing in the context of FP7. In Germany, the context for this work is provided by the Cloud Computing Action Programme, the Trusted Cloud Technology Programme, and the envisaged "Cloud Computing – Made and Secured in Germany" mark.

The industry and the state are both called on to act

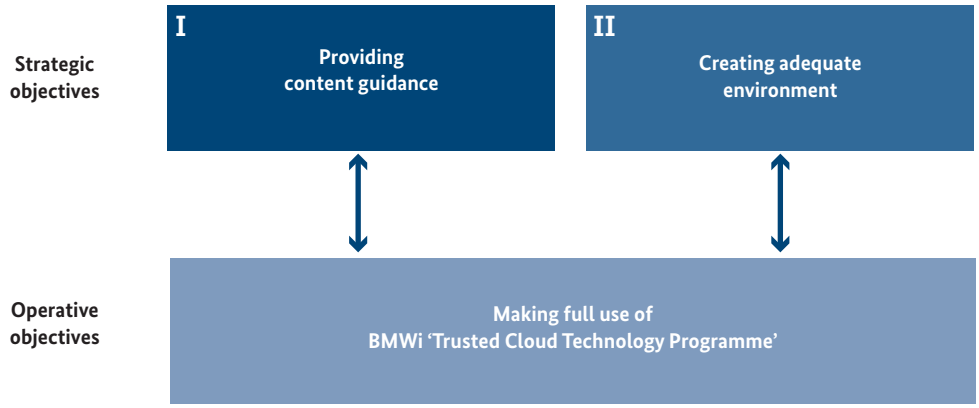
The chief responsibility lies with the German business community, which needs to play a more active part in standardisation in order to assert its key interests in the field of cloud computing. It is necessary for all the groups of stakeholders, such as providers, users, large companies and smaller businesses, to come together as equals.

The model should be the free market with as little intervention as possible. Nevertheless, there is still a need for a policy response by government, since this can prevent possible market failure at an early stage. Cloud computing should not be a field where the law is unclear: quite simply, it offers too many opportunities for growth and its commercial importance is too great.

Rapid action is needed since crucial decisions on cloud standardisation are likely to be seen by 2014, meaning that the future course will have been determined by then. The rules of the game for tomorrow's market are now being defined at this early stage. As developments progress, the possibilities to influence them will diminish.

The emphasis is on two strategic objectives (cf. Figure 12). In addition, it is vital to make thorough use at operational level of the Trusted Cloud Technology Programme for the purposes of standardisation.

Figure 12: Overview of the objectives



Quelle: Analyse von Booz & Company und FZI

Strategic objective I:

The state should provide support in terms of content guidance. The focus is on the definition of requirements and the creation of orientational knowledge. The industry is responsible for the actual standardisation.

Strategic objective II:

In order to make it possible for all the stakeholders to take a co-ordinated and targeted approach to stand Eight fields of action were identified in terms of the objectives, and specific measures are recommended for each of these (cf. Figure 13).

1 – Closing gaps in standardisation

The priority should be on gaps in standardisation, and public-sector requirements should be clearly stated. Existing standards should be catalogued (e. g. similar to an e-government SAGA).

2 – Support for Openess in cloud computing

Incentives should be put in place to promote the openness of standards in cloud computing. Standards should be scrutinised in terms of how open they are.

3 – Paticipation on orientational knowledge an contract law

Orientational knowledge and the pillars for it should be defined and drawn up in order to avoid duplication of work. Standards for contracts should be defined separately from the legal framework.

4 – Supporting documentation

Standardisation activities, orientational knowledge and support services should be communicated to all stakeholders via public relations activities, in order to raise awareness of standardisation in cloud computing.

Figure 13: Overview of the eight fields of action

Source: Analyse von Booz & Company und FZI

5 – Central co-ordination of standardisation

Standardisation must be co-ordinated centrally in Germany, separately from national, European and international levels of administration, and involving all the stakeholders (e. g. standardisation roadmap).

6 – Provision of appropriate certifications

The “Cloud Computing – Made and Secured in Germany” brand should be underpinned by appropriate certifications in cloud computing.

7 – Providing policy backing

Thorough use should be made of existing support measures like the Trusted Cloud Technology Programme for standardisation purposes.

8 – Legislation

The current legal framework should be thoroughly screened for its appropriateness and its implications for cloud computing, so that needs for legislation can be ascertained.

www.bmwi.de