D3.1 - STANDARDS, NORMALIZATION AND CERTIFICATIONS ASSOCIATED

VERSION 1.0

CLOUD FOR EUROPE

FP7- 610650

DUE DATE: 30/03/2014

DELIVERY DATE: 01/05/2014

AUTHOR:
M. Draoli (Agid), H. Leitold (A-SIT),
F.J.M. van Dam (MINEZ), J. Colpaert (FEDICT)

PARTNERS CONTRIBUTED:
AGID, A-SIT, ESPAP, CGC, BSI, MINEZ,

DISSEMINATION LEVEL:*
PU

NATURE OF THE DELIVERABLE:** R

INTERNAL REVIEWERS:
Roger Dean (EEMA), Linda Strick (Fraunhofer)

* PU = Public, CO = Confidential

** R = Report, P = Prototype, D = Demonstrator, O = Other

VERSIONING

Version	Date	Name, Organization
01	22.01.2014	Agid, CCG
02	28.032014	AGID, MINEZ, BSI, ESPAP, TUBITAK, MINHAP, FEDICT
03	11.04.2014	Agid, ESPAP, MINEZ, CCG, UPORTO
04	30.04.2014	AGID,
1.0	01.05.2014	Fraunhofer

EXECUTIVE SUMMARY

The main objective of the Work Package 3 (WP3) "Gap Analysis" of the Cloud for Europe project is to determine the position and perception of the European public sector about Cloud Computing and the vendor's Cloud services offering. More specifically, WP3 should identify the gaps between the current market offering and the requirements of European Public Administrations in terms of cloud services. The identification of the main gaps to be addressed enables a more effective selection and evaluation of the research and development services to be procured by the Cloud for Europe PCP.

With this document we recognised the need of analysing not only specific technical or functional gaps, but the gap between the existing ecosystem of IT services and a future Cloud ecosystem where the strategic objectives of the European Commission, of the Member Coutries and of each actor playing a role in that scenario could be fulfilled. The document identifies a methodology to reach this goal and defines the way these gaps will be represented as the final output of the workpackage.

According to the Description of Work, the core sections of the document report on the state of the art in the field of cloud architectures, cloud standards and certification. For this purpose, the results of the Cloud Standards Coordination (CSC) initiative and of the CERT-SIG have been taken in account. As a result, the document summarizes the state of work of fifteen relevant standardization bodies and the characteristics of main certification schemas.

In the framework of the Workpackage 4, the document can be used as a reference for the identification of the technical constraints of the solutions to be provided.

In the remainder of the workpackage 3, the document is a first step towards a clear identification of key gaps to be addressed by the project.

TABLE OF CONTENTS

LIST OF FIGURES

1 INTRODUCTION

1.1 SCOPE AND GOALS OF THE DELIVERABLE

The declared main objectives of the Cloud for Europe project are to remove the obstacles for Cloud adoption and to harmonize the requirements from different public organisations beyond national borders. The main objective of the Work Package 3 (WP3) is to determine the position and perception of the European public sector about Cloud Computing and the vendor's Cloud services offering. The scope of WP3 includes the assessment of the state of the art in the national and international context of Cloud Computing in public administrations, including research in the area, projects and initiatives, commercial solution and services, cross-border e-government services, procurement models and standards used in public sector and for specific public sector application domains.

In the context of the project, the output of the WP3 aims to be a relevant and useful contribution to the assessment and selection of the PCP services to be procured, task that is performed in the WP4. That means several Cloud services shall be identified so that implementing and piloting solutions to challenge the gaps between current market offerings and next future public administration requirements.

In order to satisfy the timeline of the project and in particular the milestone of the tender release, this concrete objective has to be reached running in parallel the activities of WP3 and WP4 in parallel. As a consequence, the two Workpackages have continuously exchanged preliminary partial results and information, also through shared meetings. This allowed focusing the work of the WP3 on what would be really useful for the WP4 and the project as a whole.

The declared objective of the WP3 is the analysis of the gap between the current market offering and the requirements of European Public Administrations in terms of cloud services.

After the first period of work, we understood the need of going beyond the declared objective. First of all, we recognized the existence of complex interrelation between the actors aging in a cloud system. So, we felt the need of analysing not just specific technical or functional gaps, but the **gap between the existing ecosystem of IT services and a future**

Cloud ecosystem where the strategic objectives of the European Commission, of the Member Coutries and of each actor playing a role in that scenario have been fulfilled.

In the context of the project, we intend as **IT service ecosystem** the complex of a community of customers, business and institutional autonomous entities that work together to enable IT services. It comprehends autonomous organizations that behave like service providers, service consumers, organizations having both the consumer and provider behaviours (intermediators, brokers ...) and finally organization with special roles, as developers. In the existing scenario, most of the IT services are provided as outsourcing services or as on premise services; cloud services have a lower market share.

Government, intended in a broad sense, including central and local adnministrations, schools, hospitals ... is a subset of the actors in the IT service ecosystem.

In the framework described above, we can identify some **measurable objectives** of the Cloud for Europe project:

- the growth of the market share of Cloud services with respect to other legacy forms of IT service provisioning;
- the growth of the value of Cloud services involving government (in any role, provider, consumer or other);
- the growth of the value of Cloud services involving government and another party established in a different Country (cross border cloud service).

In this framework, the goal of the WorkPackage 3 of the project can be better focused on the identification of the barriers that more affect the pursuit of the three objectives mentioned above.

1.2 METHODOLOGY AND ORGANIZATION OF THE DELIVERABLES

According to the Definition of Work, three documents have to be delivered in the framework of the Workpackage three activities. The Deliverables are described as in the following:

- **Deliverable D3.1: Standards, Normalization and Certifications Associated** (this document). It compiles and summarizes all specific technical information like a glossary of terms and concepts, the state-of-the-art of Cloud Computing technology and services at European and international level from the technical perspective. It will describe the technical requirements requested by the different administrations and public bodies to the suppliers, good practices and methodologies followed for the adoption of the Cloud Computing model in the European Public Administrations, technical recommendations, standards and certifications. It will deepen into the technical requirements of cross-border eGovernment Services. It will describe European and international experience of successful implementations of Cloud-based solutions from the technical point of view.

- **Deliverable D3.2 Public Sector Study.** This deliverable includes information of the European public sector from the organizational and functional perspective; it will describe the level of knowledge of Cloud Computing and degree of implementation and acceptance of the Cloud model in the public sector, the economic costs associatedwith the implementation of the model, the model of decision followed to carry out the adoption of the service, equirements requested to suppliers, risk analysis carried out, means of monitoring the quality of the service, reasons that have influenced not to adopt the model. It will describe key benefits for organizations that have adopted Cloud Computing, challenges experienced by Public bodies after the Cloud Services implementation, degree of satisfaction of the entities with the services provided by the vendors, next steps of the entities and possible future implementation of Cloud models.

- **Deliverable D3.3 Study of Market vendors offering and Public Administrations requirements.** The deliverable deepens into the matching between offering and demand; will describe the type of vendors that are providing Cloud services to European public administrations, where are they orienting Cloud Computing in the coming years, and how it affects administrations and European government agencies. From the other side, it will describe the type of Cloud services requested by European public administrations and will

profile a Standard Service Catalogue required by European public administrations including a gap analysis with the current vendor's portfolio.

In the context of the project, the Deliverbales aims to be a relevant and useful contribution to the assessment and selection of the PCP services to be procured, task that is performed in the WP4. Since WP3 and WP4 are running in parallel, specific needs of the Workpackage 4 have been driving the studies conducted in WP3:

- There is a need of avoiding superposition among the three deliverables. For sake of clarity, the decision is the three deliverables will respectively afford the analysis mainly from the point of view of technology, of government and of the market vendors.
- The scope of interest of the WP3, as defined in the DoW, is quite broad. There is the need of focusing on what is really useful for the definition of the objectives of the PCP. For this purpose we recognize the need of defining a **"target" vision of the Cloud 4 Europe Project.** This vision, that will drive the study, can be represented as **an ecosystem of IT services** that could deriive by the policies and strategies for the development of Cloud in Europe as established by the Europen Commission and Member Countries.
- There is the need of evaluating the impact of a solution to an identified gap on the global scale of the ecosystem. This is to assure that a good local solution would not have a negative side effect on the equilibrium of the ecosystem (as an obvious example, a good solution for government could be unacceptable for the market).
- In the framework of the target IT service ecosystem, a good way of describing gaps is by means **of key use cases,** especially if put in relation with the main phases of the Cloud Services life-cycle [103]. The goal is the identification of significant use cases to overcome existing barriers.
- The target ecosystem and the identification of key use cases lead to the identification of technological, organizational, legal **key areas of interest or specific cloud services** to be addressed with the instrument of PCP.
- The definition of the target vision, use cases, key areas and cloud services is an iterative process and a continuous contribution for the identification of the PCP objective. Accordingly, each of the three Deliverable will contain a contribution to the refinement of the identified objectives, with D3.3 giving the final view.

A second point regards the possibility of using existing resources without "reinventing the wheel". Significant contributions to the analysis of global, European and national Cloud ecosystems are public available as a result of studies, market analysis, academic research performed in the last few years. As a whole, they represent a relevant knowledge base for the WP3 work. For this reason, the first activity has been the constitution of a **document repository** for the benefit of WP3 and of the project as a whole.

1.3 THE C4E DOCUMENT AND KNOWLEDGE REPOSITORY

The first part of the work has been conducted mainly as a desktop research on the existing literature. For that purpose, we have collected relevant documents coming from studies, market analysis, academic research performed by market analysts, government agencies, private companies, academic centres, standardization bodies. For sake of completeness, the collection comprehends also relevant press releases, slide presentations of recognized experts in the Cloud sector.

The collection of documents has been organised in a document repository made available to all the members of the project through the on line collaboration system of the Project coordinator. The document repository has been organised in the following sections:

- Policy, strategies and vision: documents regarding political addresses and implementation strategies at the global and European level. It also comprehends attempts of envisioning the future Cloud ecosystems.
- Use cases: documents describing existing and foreseen cases of use of Cloud services. It comprehends both high level (business) use cases and more specific use cases in vertical areas as monitoring, control, identification.
- Reference architectures and standards: documents, mainly coming from standardization bodies, describing cloud reference architectures and the status of the art in the standardizadion of cloud technologies.
- Cloud certification and security: technical documents about the key areas of cloud certification and security
- Cloud EU funded projects: relevant documents coming from European funded projects. It includes relevant public deliverables of research and development projects
- Companies and market sectors: position papers and market studies produced by global companies acting in the cloud market

- Market offering: portfolios of cloud services offered by relevant companies in the market

The description of each collected document has been enriched by ad hoc metadata, including keywords, a summary description and an evaluation of the relevance the document has for the purpose of the Workpackage 3.

The collected documents are indexed by the internal search engine. This enables complex and focused search of the documents on the basis of specific needs.

1.4 PRELIMINARY IDENTIFICATION OF KEY AREAS

In this section we describe a preliminary result of the key areas where the gaps are concentrated, as they can be desumed by the existing literature. The final identification of the gaps will be described in the final deliverable D3.3. This preliminary identification is needed in order to focus the effort of the Workpacage and of the project as a whole since the beginning.

1.4.1 *ORGANISATIONAL ISSUES*

Organisational issues exist where the characteristics of cloud services deployment gives challenges compared to traditional data processing center or outsourcing models. The challenges posed on the organisations by the introduction of the Cloud paradigm are in the mainstream through the outsourcing of IT services.

Cloud computing in some sense can be defined as the ultimate expression of outsourcing, "where a customer contracts out computing resources and, depending on the specific model, also business data that is processed and stored by the cloud provider. With cloud computing, organizations can have on-demand self-service for computing capabilities, such as server time and network storage when needed." This is perceived as a threat to the level of autonomy of each organisation:

- **Autonomy of the Information system vs centralization / resource pooling / centralization:** it regards the risk perceived by the organization to lose autonomy in the management of its own information system
- **IT department vs business departments:** the delivery of cloud services is perceived to be much easier than traditional IT services. This create an internal competition

between IT departments and business departments, that are attempted to become more independent

- **Consumer side contracts vs provider side contracts:** Procurement issues arise from current procurement law not matching "take-it or leave-it" paradigm of cloud contracts.

1.4.2 *LEGAL ISSUES*

Legal Issues exist where particularities of cloud service deployment gives challenges compared to traditional data processing center or outsourcing models (mainly addressing public cloud, some applicable to private cloud). According to the recent Commission public consultation on cloud computing, the legal regime was unclear to respondents in 90 % of cases. There is general confusion among stakeholders regarding rights and responsibilities in cross-border cloud computing situations, in particular with regard to matters relating to liability and jurisdiction. Coupled with the fragmentation of the internal market, this calls for further harmonisation of laws across the Member States, in particular by eliminating gaps and weaknesses in applicable EU legislation, notably the Unfair Commercial Practices Directive and the Unfair Contract Terms Directive in terms of consumer protection, and the E-Commerce Directive when it comes to exemptions from private copy levies [112].

Main legal issues can be summarized as follows:

- Data location restrictions refer to explicit or legal requirements to keep data on site or within national borders.
- Data protection is the major barrier when processing personal data. It is a question of control, as well as can lead to data location restriction (e.g. not allowing transfer outside the EU/EEA). To mitigate data protection challenges, data is frequently required to stay in European data centres (European clouds) or to stay under the jurisdiction of a European Country. Doing so may be economically viable: European clouds would not be the cheapest, but the added cost can be offset by a data protection/security benefit.
- Data ownership: the citizen is the legal owner of his/her data and has control over who can access them.
- Lawful access has two dimensions – ensuring that data gets accessible like on court order, at the same time not having data seized by foreign authorities on the grounds of physical location of data.

- Enforcement issues arise where a public authority cannot exercise rights like supervision or seizing outside their territory. If no mutual assistance is defined (like with the draft Data Protection Regulation), this can be a barrier.

1.4.3 *TECHNICAL ISSUES*

Technical Issues to a large extend derive from compliance requirements, like implementing legal requirements or exercising controls and responsibility for mission-critical data and processes:

- Security can be argued as a horizontal concern that origins from passing control to a provider. While the same applies to conventional outsourcing, the highly standardized nature of Cloud paradigms give less flexibility on technical or contractual solutions.
- Data and service portability is related to avoiding vendor lock-ins, as well as to business continuity if there are outages. While technologies exist for IaaS, it is less mature for PaaS and hardly seen for SaaS.
- Non-Repudiation of transactions in the cloud. Hence it is important, that an uninterrupted and verifiable logging system (e.g., with hash trees or chain signatures) and node authentication is assured. The non-repudiation relates to all parties within the transaction processes – the cloud providers, the service providers and the customers.
- Auditability mechanism of the whole cloud system should be established for standardized audit trails.
- Expandability and Scalability of the cloud system and the services within. The cloud system has to improve both, to facilitate the service provider in respect of release upgrades and in operational scalability.
- Difficulties combining cloud services from different vendors (interoperability issue)
- Complexity when moving from one vendor to the other (portability)
- Service composition in multi-cloud environments that raises the issues of a proper Management of Service Level agreements in multi-cloud environments.

1.5 DOCUMENT STRUCTURE

The document is structured as follows:

- Chapter 1 Introduction describes the scope and the goals of the deliverables and the methodology used to pursue those goals.
- Chapter 2 is a Glossary of relevant terms
- Chapter 3 "A vision of cross bordering clouds for European public services" establishes a high level framework as a reference for the rest of the study
- Chapter 4 "Cloud Computing Architectures and Technologies" describes the state of the art in the definition of Cloud and Cloud computing architectures
- Chapter 5 "Standardization and Certification" describes the state of the art in the field of Cloud Certification. Annex 1 provides the list of standards for cloud computing produced by main SDOs listed above in this section.
- Chapter 6 "Hitting the target of the C4E vision" is a preliminary report of how Member States are affording the migration to Cloud computing. The second part of the chapter first abstract concrete use cases and gives a description of three common business models, further relevant high level use cases are identified which group thematically similar use cases together
- Finally, conclusions are drawn.

2 GLOSSARY OF TERMS AND CONCEPTS

Terms and concepts in cloud computing environments are often used inconsistently and mean different things to different people, even in efforts to standardize the terminology as such. For this reason, this section puts a significant emphasis on the definition of a consistent terms and concepts of cloud computing. The NIST Institute of Standards and Technology Cloud Computing definition [1] is widely accepted as a valuable contribution toward providing a clear understanding of cloud computing technologies and cloud services, being the cloud computing definition most used for ICT industry. For this reason we will adopt NIST Cloud Computing references to characterize the terms and concepts of cloud computing.

The NIST (U.S. National Institute of Standards and Technology) Cloud Computing definition [1] is widely accepted as a valuable contribution toward providing a clear understanding of cloud computing technologies and cloud services, being the cloud computing definition most used for ICT industry. For this reason C4E adopt the NIST definitions and to characterize the terms and concepts of cloud computing.

A	

B	

C	
Community cloud	The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises
Cloud Consumer	A person or organization that maintains a business relationship with, and uses service from, Cloud Providers.
Cloud Provider	A person, organization, or entity responsible for making a

	service available to interested parties.
Cloud Auditor	A party that can conduct independent assessment of cloud services, information system operations, performance and security of the cloud implementation.
Cloud Broker	An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between Cloud Providers and Cloud Consumers.
Cloud Carrier	An intermediary that provides connectivity and transport of cloud services from Cloud Providers to Cloud Consumers.
Cloud Service Management	Cloud Service Management includes all the service-related functions that are necessary for the management and operations of those services required by or proposed to customers.
D	
Data Portability	The ability to transfer data from one system to another without being required to recreate or reenter data descriptions or to modify significantly the application being transported.
G	
Government	We intend as "government" in a broad sense, not only government agencies and other units of the (typically centralized) executive branch, but also other publicly funded institutions, including for public schools, hospitals, and similar entities established within the framework of public law and funding.
H	
Hybrid cloud	The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)
I	
Infrastructure-as-a-Service (IaaS)	The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating

	systems and applications.
Interoperability	The capability to communicate, execute programs, or transfer data among various functional units under specified conditions
M	
Monitoring and Reporting	Discover and monitor the virtual resources, monitor cloud operations and events, and generate performance reports.
Metering	Provide a metering capability at some level of abstraction appropriate to the type of service (e.g, storage, processing, bandwidth, and active user accounts)
P	
Platform-as-a-Service (PaaS)	The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.
Privacy-Impact Audit	Systematic evaluation of a cloud system by measuring how well it conforms to a set of established privacy-impact criteria.
Performance Audit	Systematic evaluation of a cloud system by measuring how well it conforms to a set of established performance criteria.
Portability	The ability to transfer data from one system to another without being required to recreate or reenter data descriptions or to modify significantly the application being transported
Provisioning/Configuration	process of preparing and equipping a cloud to allow it to provide (new) services to its users
Private cloud	The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises
Public cloud	The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider". A public cloud variant is what most consumers are familiar with when they are using for example Google mail, Dropbox or the iCloud services of Apple

R	
Resource Abstraction and Control Layer	Entails software elements, such as hypervisor, virtual machines, virtual data storage, and supporting software components, used to realize the infrastructure upon which a cloud service can be established.
Rapid provisioning	Automatically deploying cloud system based on the requested service/resources/capabilities
Resource change	adjust configuration/resource assignment for repairs, upgrades, and joining new nodes into the cloud
S	
Service Orchestration	refers to the arrangement, coordination and management of cloud infrastructure to provide different cloud services to meet IT and business requirements
Service Provision	A Cloud Broker in the act of providing a Cloud Service
Service Consumption	A Cloud Broker in the act of using a Cloud Service.
Security Audit	Systematic evaluation of a cloud system by measuring how well it conforms to a set of established security criteria.
Software-as-a-Service (SaaS)	The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure.
W	

X
Y
X

3 A VISION OF CROSS BORDERING CLOUDS FOR EUROPEAN PUBLIC SERVICES

This chapter aims to sketch a reference scenario for the Cloud for Europe Project. The reference scenario should be represented in the form a future Cloud ecosystem where the strategic objectives of the European Commission, of the Member Coutries and of each actor playing a role in that scenario have been fulfilled. The description of this vision will be finalised in the deliverable D3.3, as a way to represent the gaps between the current situation and a future desirable scenario.

3.1 EU STRATEGY FOR THE ADOPTION OF CLOUD COMPUTING

This chapter resumes the key point of the European strategy for the development of Cloud compunting in the European Union.

3.1.1 *UNLEASHING THE POTENTIAL OF CLOUD COMPUTING IN EUROPE*

The Commission promotes the rapid adoption of cloud computing in all sectors of the economy in order to boost productivity.

In September 2012, the European Commission adopted a strategy for "Unleashing the Potential of Cloud Computing in Europe" (European Commission, 2012). The strategy outlines actions to deliver a net gain of 2.5 million new European jobs, and an annual boost of €160 billion to the European Union GDP (around 1%), by 2020. The goal of EU strategy is increase the use of cloud solutions and services across European Union public and private sector, and to stimulate the active adoption of cloud computing by providing a climate of certainty and trust. This strategy is the result of an analysis of the overall policy, regulatory and technology landscapes and of a wide consultation with stakeholders, to identify ways to maximise the potential offered by the cloud.

The Commission would like to see a broad participation by relevant stakeholders in implementing these actions.

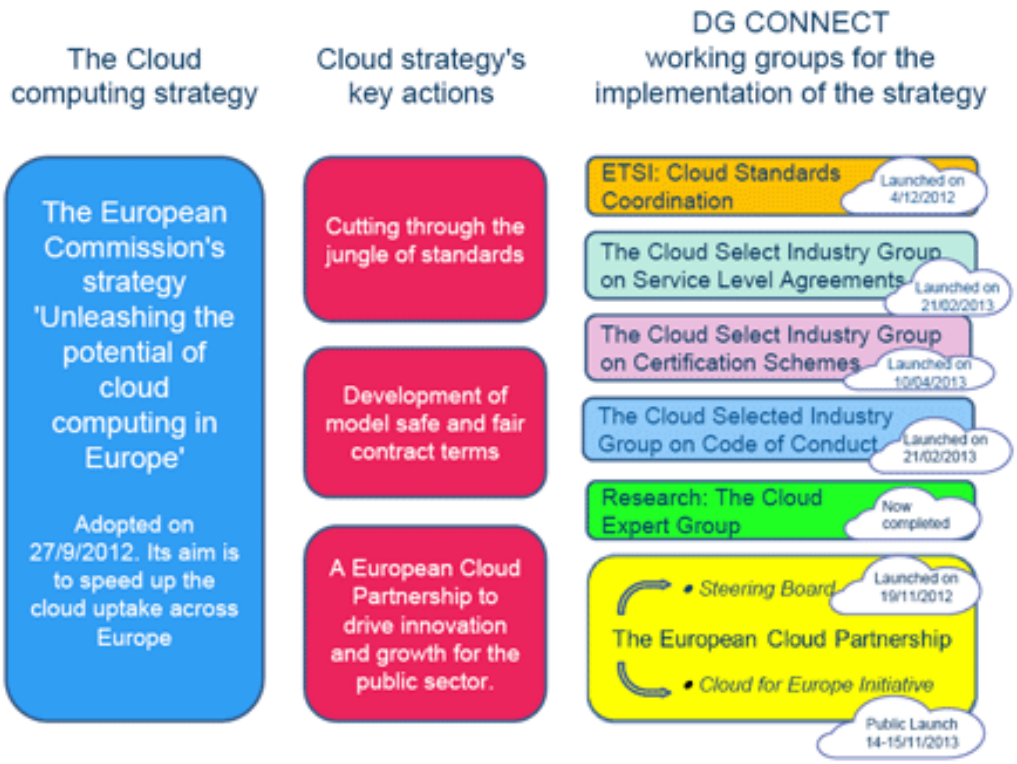


Figure 1 European Cloud Computing Strategy; key actions and working groups

The Cloud computing Strategy includes three key actions:

SAFE AND FAIR CONTRACT TERMS AND CONDITIONS

The Commission's proposal for a Regulation on a Common European Sales Law addresses many of the obstacles stemming from diverging national sales law rules by providing contractual parties with a uniform set of rules. The proposal includes rules adapted to the supply of "digital content" that cover some aspects of cloud computing.

The aim of the cloud computing strategy is to develop model contract terms that would regulate issues not covered by the Common European Sales Law. On 26th february 2014 The European Parliament voted in favour of introducing an optional pan-EU contract law designed to improve cross-border digital sales for both businesses and consumers. The Common European Sales Law (CESL) would give trading parties the option of doing business within a new, additional legal framework, rather than within the national laws of the states in which they operate. Models of contract terms are specific of cloud services such as:

- data preservation after termination of the contract,
- data disclosure and integrity,
- data location and transfer,
- ownership of the data,
- direct and indirect liability change of service by cloud providers and subcontracting.

Specific reccomendations have been issued by the Commission, as the Communication „Against lock-in: building open ICT systems by making better use of standards in public procurement" and the Decision on "standard contractual clauses for the transfer of personal data to processors established in third countries" [510].

Identifying and disseminating best practices in respect of model contract terms will accelerate the take-up of cloud computing by increasing the trust of prospective consumers. This is needed not only for consumers and small firms, who are offered take-it-or-leave-it contracts, but also for **service level agreements** between larger corporations and public authorities.

Cloud users should furthermore be able to evaluate any cloud service offer on the basis of standardised procedures regarding the security and warranties provided by the service, so-called Service Level Agreements (SLA).

CUTTING THROUGH THE JUNGLE OF STANDARDS

Cutting through the jungle of technical standards so that cloud users enjoy interoperability, data portability and reversibility is one of the aims of the strategy. Necessary standards have been identified in 2013 by ETSI

The Commission has stated aim is to introduce new, pan-European certification schemes for cloud computing, including data protection, by 2014. These certification schemes will address data protection, especially data portability, and focus on increased transparency of cloud service providers' security practices. The Commission is working to support ENISA and other relevant bodies to assist the development of these EU-wide voluntary certification schemes and establish a list of such schemes by 2014.

INITIATIVE FOR A EUROPEAN CLOUD PARTNERSHIP

The European Cloud Partnership (ECP) consist of high level procurement officers from European public bodies and key players from IT and telecom industry. The European Cloud Partnership (ECP) brings together industry and the public sector to work on common procurement requirements for cloud computing in an open and fully transparent way.

The ECP Steering Board provided advice to the Commission on strategic options to turn cloud computing into an engine for sustainable economic growth, innovation and cost-efficient public and private services.

The public sector has a key role to play in shaping the cloud computing market. But with the public sector market fragmented, its requirements have little impact, services integration is low and citizens do not get the best value for money.

The ECP aimes at driving the first steps towards better public procurement of cloud services in Europe, based on common definitions of requirements and possibly eventually going as far as joint procurement across borders. Pooling public requirements could bring higher efficiency and common sectoral requirements (e.g. eHealth, social care, assisted living, eGovernment services) would reduce costs and enable interoperability. The private sector would also benefit from higher quality services, more competition, rapid standardisation and better interoperability and market opportunities for high-tech SMEs.

The ECP Steering Board is composed of high-level representatives of the IT and telecom industry and decision makers from governmental IT policy making and chaired by Toomas Hendrik Ilves, President of Estonia. The Steering Board held its first meeting on November 19 2012.

The ECP research activities are aiming at helping Europe's public authorities procure cloud products and services, so as to build trust in European cloud computing. These activities were supported by an initial budget of €10million under the EU's Research Programme, which set up the Cloud for Europe project. In addition, the EU's new Horizon 2020 programme will also provide €22million of support for the development of cloud computing services in public sector innovation under the 2015 work package.

3.1.2 *TRUSTED CLOUD EUROPE*

"Establishing a Trusted Cloud Europe" was prepared by the European Cloud Partnership (ECP) to propose options on how to help public & private organisations in Europe buy and sell cloud services in a safe & trusted environment.

The document represents an important step in the execution of the cloud computing strategy. It is the result of a collaborative process in which participants of public administrations, cloud businesses, and data protection advocates have joined forces through the European Cloud Partnership, and have worked together to establish a roadmap for European leadership in the cloud.

The Steering Board recognizes that access to cloud services in Europe is currently hampered by a number of uncertainties and challenges, which vary from use case to use case. Depending on the type of data, type of service, and need for enforcement, adoption of the cloud may be impeded by legal, technical, operational or economic barriers. Barriers vary from use case to use case, and include legal issues, operational concerns, and technological challenges.

The document proposes the concept of the Trusted Cloud Europe: **a framework to support the definition of common cloud best practices, linking them to use cases, and applying them in practice.**

Trusted Cloud Europe supports a single market for cloud services, generating benefits for all European stakeholders:

• On the demand side, European cloud users (citizens, businesses – including SMEs – and public administrations) will be able to choose and use cloud services with confidence, knowing that they adhere to European legal norms and international standards, and that data in such clouds is secure;

• On the supply side, cloud providers will be able provide their cloud services to European customers, without hindrance from national regulatory barriers.

These goals can be reached by establishing a **shared understanding** of regulatory and legal norms, and security and **trust**, common to cloud users and to cloud service providers, and how these can be tied to specific use cases. These solutions should be based on best practices, favouring internationally recognized norms and standards wherever possible to ensure a global perspective that cloud computing inherently requires.

3.2 R&D CLOUD PROJECTS AND INITIATIVES FOR THE PUBLIC SECTOR

This chapter provides a short summary for R&D cloud projects and initiatives with relevance for the public sector. The summaries do not go deep into project specific details and are based on public available information. It is an indicative listing without claiming completeness but covers the most important topics and directions. An in depth analysis of the status of research and innovation projects funded by public organisation will be in Deliverable D3.2.

3.2.1 *OPEN-DAI*

CIP funded project

Duration: February 2012 – September 2014

Partners: 11 partners from Italy, Spain, Sweden and Turkey

The Open-DAI (Opening Data Architectures and Infrastructures of European Public Administrations) project aims to make data and platforms available to cloud-enabled public sector services to decrease the hurdle of implementing new cloud-enabled services for public administrations, companies or citizens. The goals as described by the project itself [56]:

Innovation, business opportunities and digital services are the three goals that drive Open-DAI. All Consortium partners work together:

- *to open up a large part of the Public Administrations' (PAs') databases to a wide audience of potential users through an open data hub in order to correlate data and to implement new digital public services;*
- *to evolve the PAs' information systems towards an open model and Service Oriented Architecture (SOA) in order to overhaul the monolithic and closed models and to facilitate software maintenance of existing silos;*
- *to host the PA's services into a scalable cloud infrastructure in order to meet the evolving needs.*

3.2.2 *ARTIST*

FP7 funded project

Duration: October 2012 – September 2015

Partners: 9 partners across Europe

One main reason which hinders the take-off of cloud computing in the public sector is the migration of existing services to cloud-enabled services. This may raise a huge amount of costs. ARTIST is a migration service which takes care of the transformation of legacy application to cloud applications and achieves saving rates of up to 50%. The service uses model driven engineering techniques and is separated in the following phases (as described on the project website [62]):

- ***Pre-migration phase:*** *Evaluate the feasibility of the migration through a technical and business analysis, providing potential costs and effort required to carry out migration.*
- ***Migration Phase:*** *Create a plan for migration steps. analyse and model the non-cloud software, transform the non-cloud software models to modernized models*
- ***Post migration phase:*** *Validate functionality of the migrated app and test that it has same behaviour as in original. Certify reliability and quality of the service provider.*
- ***Evolution:*** *Maintenance activities of the application after migration to the target environment, such as software updates or cloud provider changes if necessary.*

3.2.3 *SUCRE*

FP7 funded project

Duration: October 2012 – September 2014

Partners: Seven partners across Europe from the academia sector and industry

SUCRE addresses the interoperability issue of cloud related services. The key objective is

[…]the consolidation of the European Cloud Computing and Open Source communities by creating a critical mass of stakeholders who will work together on promoting the use of Open Source in Cloud Computing.[61]

The project basically focuses on two main use cases: Open Clouds for Public Sector applications and Open Clouds for the Health Care Provisioning Industry.

The outcome of the project will include: Cloud and Open Source Magazine, Recommendation reports, young researchers' forum and workshops.

3.2.4 *G-CLOUD*

The G-Cloud is an UK Government initiative to ease the procurement process of public sector bodies. The initiative contains a framework agreement with the suppliers, so that public administrations can purchase services from the G-Cloud *Cloudstore* without issuing a full tender. The G-Cloud strategy is defined as follows [57]:

- *achieve large, cross government economies of scale;*
- *deliver ICT systems that are flexible and responsive to demand in order to support government policies and strategies;*
- *take advantage of new technologies in order to deliver faster business benefits and reduce cost;*
- *meet environmental and sustainability targets;*
- *allow government to procure in a way that encourages a dynamic and responsive supplier marketplace and supports emerging suppliers.*

3.2.5 *DEUTSCHE WOLKE*

Deutsche Wolke is an Open-Source initiative to establish a federal cloud infrastructure in Germany. The initiative focuses on the requirements and needs of German companies and fills the gap concerning local tailored cloud solutions. According to the project website the service was developed targeting the following objectives [

- *Safety*
    - *Server and data are located exclusively in Germany and underlie the country's strong data security regulations.*
    - *Cloud data is protected from access by third parties as well as their ability to further process this data.*

- *Transparency*
    - *Unique assignability of data in the cloud: If necessary, data can be entirely extracted from or permanently deleted from the cloud. The path of data with the cloud can always be traced.*
- *Reliability*
    - *The main focus will be a high-performing Cloud-Infrastructure which responds dynamically to changing customer-needs.*

3.2.6 *HELIXNEBULA*

FP7 funded project

Duration: October 2012 – September 2014

Partners: 10 partners across Europe from academia sector and industry

Helix Nebula – the Science Cloud is an initiative to support and provide European IT-intense research organizations with cloud computing resources. The project was launched and is supported by three major research institutions: CERN, the European Space Agency (ESA) and the European Molecular Biology Laboratory (EMBL). The initiative is not limited to research organizations, it is also open for other stakeholders' needs: governments, businesses and citizens.

As described by the project team the strategic plan is as follows [59]:

- *Establish multi-tenant, multi-provider cloud infrastructure*
- *Identify and adopt policies for trust, security and privacy*
- *Create governance structure*
- *Define funding schemes.*

3.2.7 *OpenNebula*

Open Nebula is a project which aims to provide solutions to manage clouds and virtualized datacenters. It combines existing solutions and targets open, flexible, extensible solutions.

The core objectives of Open Nebula are [60]:

- ***Openness*** *of the processes and the technology*
- ***Excellence*** *for being a project of the highest quality in every aspect of its operations*
- ***Cooperation*** *with open-source efforts and research projects to advance cloud computing*
- ***Innovation*** *in new technologies and methods to address needs of large-scale cloud deployments*

3.2.8 CLOUD SOFTWARE PROGRAM

The Cloud Software Program project is a Finnish initiative driven by the public sector, in cooperation with leading ICT companies and pioneers to improve the competitive position of Finnish cloud software providers in the global market.

The project has developed a Strategic Research Agenda that provides focal points on future Cloud research. It suggests that, from the business viewpoint, the focus of research in the coming years should be in supporting a change towards smaller, leaner and more competitive ecosystems, as well as growing the emerging ecosystems around mid-size enterprises. Also, the report indicates a continuing need in ecosystem assessment and similar activities. The project recommends focusing on shortening the idea-to-business cycle in the Cloud domain, developing ecosystems, and focusing on superior user experience to provide edge in the future Cloud markets. The project has also produced several papers on revenue models in Cloud Computing. This is a very important and often neglected area that will directly benefit startup creation with readily available business model suggestions. [63]

3.2.9 ITALIAN PUBLIC SYSTEM OF CONNECTION AND COOPERATION

According to the BSA Global Cloud Computing Scoreboard [64] Italy is one of the leading countries regarding cloud applications and services in Europe. Regarding the use of Cloud Computing in public administrations Italy has a modern electronic signature law and therefore can provide faster and more secure eGovernment services to the citizens. Further, several Italian public administrations show a high interest towards cloud computing and providing services.

3.3 CLOUD MARKET IN EUROPE

This chapter provides a short summary of the status of the Cloud market, with a specific view on the European market. An in depth analysis will be in Deliverable D3.3.

3.3.1 *CLOUD MARKET PLAYERS – CLOUD FOCUSSED VS. CLASSICAL IT*

In contrast to the USA landscape, European computing/datacenter infrastructures are fragmented and split up among multiple cloud providers (principally SME with the exception of the telecommunication industry). Although most big multinational IT companies are active in the market, the size of their cloud operations is limited, and their services are often run from non-dedicated colocation datacenters. Most of these companies do not focus on their public cloud (virtual private cloud) offerings, but position themselves rather as private cloud builders for a large enterprise or government market.

Only a few companies are building large scale public clouds platforms that serve as the base for their VPC offerings (Amazon, Microsoft, …).The majority of mainstream large IT companies build their (often private/community) cloud offerings with enterprise solutions (typically based on VMware cloud technology).

Due to the small scale of the cloud operations of the more classical IT companies, the available network bandwidth and free compute and storage capacity are limited, forcing them to ask their customer's a pre-notice of sometimes weeks or months for a moderate grow in resources.

On the positive side, these companies can have their datacentre(s) (often using colocation) in the country of the customer, which may relief some legal concerns. The security of the co-location approach may be questionable however.

Some private cloud builder can build and operate the private/community cloud infrastructure on customer premises.

Due to the different market approach, it is rather unlikely that the same player will be successful as a builder of private/community clouds and as public cloud operator.

3.3.2 *COMMUNITY/PRIVATE CLOUD VS VIRTUAL PRIVATE CLOUD IN A PUBLIC CLOUD.*

As enterprise and government applications require a multi-tiered application protection infrastructure, we expect that the classical 'public cloud' (individual machines more or less directly connected to the Internet) will disappear in favour of the Virtual Private Cloud (VPC) approach, where compute power and storage are combined with (multi-tier) virtual network services. Whenever we speak about public cloud in this section, we are talking about a VPC in a public cloud.

3.3.3 *CERTIFICATIONS AND QUALITY ASSURANCE*

Even though their cloud operations are rather small, a lot of IT companies can provide the necessary security credentials. Most players have achieved ISO27001 certification, some of them also provide SSAE16 or SOC2 type 2 reports for their cloud operations. Not many IaaS players are offering PCI DSS2 certified services (they often claim that this is more application related, but PCI DSS also imposes a number of controls on the infrastructure layer). Certifications schema will be detiled described in the following.

A verification of the scope of the certification or third party report is absolutely needed as some of the providers only have certification for the low level operations of the datacentre premises.

3.3.4 *TECHNOLOGY*

The few large scale public cloud operators have built their own cloud foundation and orchestration software platform (Amazon, Microsoft).

Most other IaaS cloud players (including big multinational IT companies) build their cloud offerings with either VMware or Openstack technology. This approach may not scale as well as. Early adopters of Openstack have been hindered by the ongoing evolution of the platform, and it is unlikely that the situation will clear up soon.

The cloud platform war is probably not over, and newcomers may take over a significant part of the market (mainly because there are not that many dependencies on the cloud platform choice).

3.3.5 *RESILIENCE*

- The big public cloud operators build clusters of datacenters (2 or 3 sites) that are close enough to each other for a active-active load distribution, and far enough from each other for surviving a small disaster.
- The smaller cloud operators may only have single datacenters in a limited number of regions.
- In an IaaS approach, the cloud user is often responsible for distributing the load over a couple of locations where the CSP is present. The CSP must provide the necessary inter-site communication and load-balancing tools. Most providers with clustered datacenters offer these tools.
- Active-active load balancing over multiple locations is attractive because it guarantees that the resources are available and tested. In active-passive scenario's, on must be sure that the compute capacity is available and the services are tested when the disaster occurs.

3.3.6 *STANDARD TERMS AND CONDITIONS*

The standard terms and conditions of most cloud providers are still protecting the point of view of the cloud operator. Enterprise and government customers must painfully re-negotiate these terms and conditions, a process that may destroy the advantages of a cloud approach. Example clauses found in most standard T&C's:

- The cloud customer is not allowed to perform vulnerability scans on his cloud applications. It is clear that the CSP needs to protect the infrastructure and other customers, but the clauses are so general that they need to be painfully renegotiated
- The CSP may interrupt the service immediately if it believes that the customer is violating some laws or policies.

There is an urgent need for common terms and conditions defined from the cloud consumer point of view, with a good understanding of the cloud provider's

3.3.7 *STANDARD SERVICE LEVEL AGREEMENT*

Although the SLA's offered by some providers may be good enough, the penalty level is by far not sufficient to reflect the damage caused by an outage. Furthermore, the guarantees against data loss are often vague or inexistent. To even worse, there is no consistent way to compare the data loss protection level offered by different CSP's.

Some CSP's will offer different service levels (e.g. silver, gold, platinum) in which features are combined together. This tiering does not always correspond to the customer's needs and may make the solution unattractive.

3.3.8 *PORTABILITY ACROSS CLOUD PROVIDERS*

In general, today it is unlikely that a Virtual Machine containing on application can be easily ported to another cloud provider, except if both cloud providers are using the same technology. The recommended approach today is to use scripting tools like chef, puppet, and vagrant, to build and customize the VM instances from a standard reference image.

Although there are some initiatives to describe the network structure and firewalling rules in a platform-independent way (e.g. OASIS TOSCA), today's CSP's do not support this kind of portability. The customer must therefore automate the creation of the network structure or recreate the structure manually for each CSP.

The use of a cloud broker may overcome the portability problems mentioned above, but most cloud brokers are proprietary solutions and the customer might become locked-in with the cloud broker instead of the cloud provider.

The cloud user can decide not to use the load balancing and firewalling features offered by the cloud provider, but instead implement the functions in a portable virtual appliance. This approach can also simplify the move from one provider to another. The approach also enhances security because the cloud provider has no view on the actual network flows anymore.

3.4 THE C4E VISION OF CLOUD IN EUROPE 2020

In the next few years, technology developments and innovations will run much faster than organisation and governments could do in order to exploit the benefits. Nevertheless, some specific actions can be put in place in order to reduce this gap.

3.4.1 *THE SERVICE IMPERATIVE*

The global vision of C4E embraces the definition of Servicification, aka Everything-as-a-Service, according to the perspective on the future of cloud in Europe of NESSI initiative [607] which states: "The availability of software-based services, accessible over the Internet by means of simple-to-use Application Programming Interfaces (APIs), allow for third parties to quickly innovate new solutions on top of such services. A simple example is the speed of innovation on top of available Cloud-based storage services such as Dropbox and Box.net which both have grown an amazing ecosystem of applications around their basic services and managed to boost innovation through third-parties".

3.4.2 *THE SERVICE COMPOSITION IMPERATIVE*

Heterogeneity is a crucial point for the development of a wide European cloud market. In contrast to the USA landscape, European computing/datacenter infrastructures are fragmented and split up among multiple cloud providers (principally SME with the exception of the telecommunication industry). The European Commission is persuaded that rather than brute-forcing an European inroad by just copying the US approach verbatim, is better to adopt a strategy that leverages the strength of the European telecommunication sector to enter into the cloud market as an infrastructure/platform provider, and investments into dealing with the heterogeneity and segmentation of the European infrastructure.

In the next few years the trend through data center consolidation will go on: data centers will grow in size to thousands of square meters each. Nevertheless, small and less robust data centers will continue to exist, especially in the Public administrations. Focusing on the cloud market, we can envision that public clouds lead today, but hybrid will probably lead in the next future

In our vision, the future Information system of a Public administration established in a given country M could be modeled as as a composition of services provided by different economic operators:

- services of public cloud providers established in in Country M or abroad
- services of private clouds, owned by the government of Country M acting as a cloud provider
- services of private clouds owned by Public administrations, acting as cloud providers, established in other Countries
- services provided on premise (just legacy or as a consequence of a critical decision)

On the provider's side, the market offering of a **Cloud provider** established in a given Country M could be modeled as a composition of**:**

- services provided on premise,
- services of cloud providers established in Country M,
- services of cloud providers established abroad or big global cloud providers

As a conclusion, in our vision future public information systems could be developed as seamless, easy, dynamic, adaptable, flexible integration of mainly already available service components, with a limited need of developing ad hoc IT components.

3.4.3 *THE POINT OF VIEW OF THE PUBLIC SECTOR*

On the standpoint of the public sector, the vision of the C4E 2020 focuses on several points, namely, policy and security aspects, usability and interface features or macro integrated customization capacities.

Regarding security, we can affirm, with a high degree of certitude, that all cloud based services will offer a high level standard security offer, like efficient real time data tracking to locate geographically where the client data is hosted, with all the information regarding the technical information of the facilities, with an overview of the security systems, physical and virtual ones, and with information regarding the owner of the datacenter and the contractual relations with the service provider.

The encryption will be the rule in the context of data storage and transfer, optimally before any transfer, to avoid data uncovering during its transmission. We will have different levels of encryption, more or less strong, depending on the frequency of access data needs or

depending on the data privacy level. That is, there shall be established different and strict encryption profiles for the public sector requirements.

Services will be grouped by areas or activity profiles such as education, health, local government, defense, with its own specific level of security policies and associated deployable services, in order to make it easier for government entities to procure the set of services that best fits your activity. In other words, the offer shall be projected through an integrated range of services targeted to a particular area.

The interoperability and the portability will be the key evolution of cloud technology. In the next five years, cloud will evolve in order to develop and adopt standards to guarantee an adequate compatibility in the way to provide an effective portability between different suppliers. It will be easy, secure and simple to switch between cloud providers without any loss of structure or data integrity.

The standardization will extend to the management interface of services and the approach to procure services in a way that will make less technical, more transparent and more users friendly the acquisition and the administration of cloud services and resources.

This need will surely create a new market level, between the client and the provider, which can be assured by the provider itself, by an independent dedicated broker or by a governmental (national or European level) entity. We can call it a sort of portal which will above, provide the services, management and handling tools and, below, typifies and aggregate the market offer.

It will also ensure compliance with all requirements leading to ensure full interoperability between platforms.

The public sector yearns for an assumed implementation of a European cloud safe zone involving only players capable to ensure that all data will be handled and stored in European territory and that the communications circuits will be restricted to that territory.

For last, the creation of a European cloud observatory or authority will be mandatory in the next few years, in order to certify the providers and to audit and monitor compliance with the established requirements.

3.4.4 *THE POINT OF VIEW OF THE MARKET/INDUSTRY*

Concerning the industry point of view, we foresee substantial changes in the business model and the companies' structure.

We anticipate a shift of the traditional hegemony of the big traditional players for smaller companies or national or international partnerships for SMEs with local implementation, by their own or in partnership arrangements with other SMEs or with big companies.

The characteristic European disposition for security and the traditional trusty impetus for national companies will change the rules the US based big players are trying to implement in Europe, in their approach of deploy only highly typified services, using large centralized data centers without taking into account local or regional specificities.

The preference for local players with local implementation and physical structures will force the introduction of a different approach in order to involve a better physical and cultural similarity between the client and his supplier, capable to produce bonds of trust between them and enhance the ability to adapt the services to his specific necessities.

This approach will also be forced by the specifics of the applicable legal frameworks of each country.

Taking into account that the relevant players, in particular European players, yearn for the implementation of clear and concrete rules governing the sector, in the next few years, and considering the work that has been developed by the European Commission in this path, we will assist at the consolidation of standards and at the creation of a certification system for solutions and providers of cloud services.

This system of standardization and certification will be Europe-wide and will be managed by an independent and autonomous organization with responsibilities in development of standards, creation and management of a system of certification – for solutions and providers – and for monitoring the accordance of their activity with the enforceable rules and requirements.

These initiatives will bring transparency, accuracy, reliability and healthiness to the sector as well as promote its fast development and the mass adoption of cloud based services in the public sector and beyond.

4 CLOUD COMPUTING ARCHITECTURES AND TECHNOLOGIES

4.1 GOALS AND PRINCIPLES OF CLOUD COMPUTING

The rapid growth of cloud has meant that large numbers of independent vendors, of all sizes, have sprung up since cloud began, all vying for competitive difference, in an environment so new it is unregulated. Several attributes of cloud computing motivate organizations to adopt cloud computing [3] :

- **Availability:** Users have access to data and applications from around the globe;
- **Collaboration:** Organizations see the cloud as a way for members to work simultaneously on common data and information;
- **Elasticity:** Organizations can request, use, and release as many resources as needed based on changing needs;
- **Lower infrastructure costs:** The pay-per-use model allows an organization to pay only for the resources that it needs with no minimal investment in physical resources (i.e., to move from fixed costs to variable costs). The organization incurs no infrastructure-maintenance or upgrade costs for these resources;
- **Reliability:** Cloud providers have much more robust reliability mechanisms for supporting service-level agreements (SLAs) than those that a single organization could cost-effectively provide. However, it is important to note that organizations often view reliability as a barrier because cloud providers tend to rely on commodity hardware that is known to fail;
- **Risk reduction:** Organizations can use the cloud to test ideas and concepts before making major investments in technology;
- **Scalability:** Organizations have access to many resources that scale based on user demand;

Cloud Computing is viewed as a term used to describe the delivering of ICT servives over the Internet. The NIST definition [1] is widely accepted as a valuable contribution toward providing a clear understanding of cloud computing technologies and cloud services, being

the cloud computing definition most used for ICT industry. For this reason we adopt NIST Cloud Computing references to characterize the terms and concepts of cloud computing.

NIST defines Cloud Computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g, networks, servers, storage, applications, and services), that can be rapidly provisioned and released with minimal management effort or service provider interaction. The essential characteristics of cloud computing include [1]:

- **On-demand self-service**: Single users can gain access to the relevant computing services automatically. This implies that consumers can easily obtain cloud services without human interaction. They can consume resources as they need and only what they need. They do not need to involve management or an IT organization.
- **Broad network access**: The services are available over a network (usually the internet), and can be accessed in a standardized way regardless of the platform being used. Broad network access is needed for obtaining and using cloud services and additional services through standard mechanisms. A side note here is that a recent study of Federal Ministry of Economics and Technology of Germany concluded that standardization of cloud computing is only just starting to develop (Federal Ministry of Economics and Technology, 2012).
- **Resource pooling, multi-tenancy**: The service provider serves multiple clients, where the different physical or virtual resources are allocated and reallocated in a fluctuating manner, based on the clients demand. This implies that physical and virtual computing resources (like storage, processing power, memory) are pooled and shared my multiple consumers.
- **Rapid elasticity**: the ability of cloud capabilities to rapidly scale up and down, depending on the needs of the customer at that moment. Services can be flexibly provided and returned, usually automatically, to scale rapidly and proportionately with demand. To the consumer, the resources available appear to be unlimited and can be requested "in any quantity, at any time".
- **Measured service**: The use of cloud services can be measured and monitored, providing transparency optimizing resource use. ***The automat***ic ***nature of on-dem****and self-service* and *resource-pooling allow monit*oring*, controlling an*d reporting of resource usage. Cloud services can therefore be sold on a pay-per-use basis, on a level of abstraction appropriate to the type of service (e.g. storage, processing, bandwidth, and active user accounts).

The different type of Cloud environments (i.e., software, infrastructures, platforms, services, etc.) are represented in a specific deployment models, typically defined as:

- **Public Cloud** - The cloud infrastructure is for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
- **Private Cloud** - The cloud infrastructure is for exclusive use by a single organization comprising multiple consumers. It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
- **Hybrid Cloud** - The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., load balancing between clouds).
- **Community Cloud** - The cloud infrastructure is for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g. mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

The cloud environment consists of three main types of services structured in three layers, namely:

- **Software-as-a-Service (SaaS)** - This layer provides applications as a service for the end users, considering the hosting layer, where companies host applications for the users.
- **Platform-as-a-Service (PaaS)** - At this level, developers can design, build, and test applications that run on the IaaS. This layer offers the same environment as the traditional software development environment. the opportunity of providing new applications for the Cloud and distributed through SaaS can make this layer a very attractive layer for developers
- **Infrastructure-as-a-Service (IaaS) -** This is considered the foundation of the cloud computing that provide hardware products and related services, such as processing, servers, storage devices, database management, and all other hardware related services offered as a service to the end user.

Some key organizational concerns can act as barriers to the adoption of cloud computing [3]:

- **Interoperability** - The cloud-computing community has not yet defined a universal set of standards or interfaces, resulting in a significant risk of vendor lock-in as well as problems with portability of data
- **Latency** - All access to the cloud occurs through a network (or the internet in the case of public clouds), introducing latency into every communication between the user and the environment.
- **Legal issues** - Because cloud vendors tend to locate server farms and data centers where it is cheaper to operate them, some cloud-computing users have concerns about jurisdiction, data protection, fair information practices, and international data transfer.
- **Platform or language constraints** - Some cloud environments provide support for specific platforms and languages only.
- **Security** - The key concern is data privacy; in most cases, organizations do not have control of or know where cloud providers store their data. Security is about Confidenciality; Integrity and Availabiliy. Privacy is also considered part of Security. For every aspect there are concerns.

The challenges relating to cloud computing highlight the need to consider data and systems protection in the context of logical as well as physical boundaries. Major security objectives for cloud computing are the following:

- Protect data from unauthorized access, disclosure and modification;
- Prevent unauthorized access to cloud computing resources;
- Ensure isolation;
- Ensure service availability;
- Ensure effective governance, control and compliance processes are in place;
- Ensure appropriate security provisions for cloud applications;
- Ensure security of cloud connections and networks;
- Enforce privacy policies;
- Ensure incident prevention, detection and response.

Key issues that need to be addressed when assessing security standards for cloud computing are:

- Cross-border legal issues, including variations in data protection regulations;
- Conflict of interest between cloud customers and national security of the hosting country;
- Visibility and transparency;

- Assurance and trust;
- Certification, audit and testing;
- Identity and Access Management;
- Provider use of the services of other providers;
- Virtualization and multi-tenancy risks;
- Data location control;
- Secure data deletion and the exit process;

The lack of standards resulting from growth of cloud now threatens the future of cloud. Without them, there are areas of cloud that cannot progress to the quality required for widespread adoption. Current international security standards, such as the ISO/IEC 27000 series, are already widely used by global cloud providers, and increasingly used by smaller providers.

New standards and certification schemes, including clouds-pecific ones, are also being developed and brought into use, with the explicit intent of encouraging and further illuminating good practice by providers, in a form that is comprehensible to current and potential future cloud consumers.

The underlying cause of many of the risks and challenges associated with cloud computing is that the cloud service customer passes over responsibility for data and for applications to the cloud service provider and the provider has an environment in which resources are shared (the multitenant model). Typical risks and challenges concern [4]:

- Availability of services and/or data;
- Lack of data classification mechanisms;
- Integrity of services and/or data;
- Confidentiality concerns;
- Regulatory Compliance;
- Repudiability and lack of forensic capability;
- Loss of control of services and/or data;
- Responsibility ambiguity;
- Lack of liability of providers in case of security incidents;
- Cost and difficulty of migration to the cloud (legacy software, etc.;
- Vendor lock-in.

4.2 FUNCTIONAL AND NON-FUNCTION REQUIREMENTS

Functional requirements are defined as technical functionalities which relate to a business process. Non-functional requiements represent qualities or properties of a system, and not necessarily specific technological requirements. The most often referred non-functional requirements for Cloud Computing are described as follows:

- Elasticity
- Scalability
- Availability
- Accessibility
- Reliability
- Security
- Resilience
- Response time
- Uptime
- Fault Tolerance
- Performance
- Interoperability
- Usability
- Non-Repudiation

Reference architectures support the detailed design of cloud solutions contributing to the fulfillment of functional and non-functional requirements.

Cloud Computing has emerged to offer products and services that are delivered via the Internet and consumed in real time by a growing array of client devices, that are dynamically scalable and to provide virtualized resources. Cloud products and services must be assure characteristics, such as virtualization, pay-per-service, based on grid infrastructure, failover, recoverability, reconfigurability, resource management, scalability, data integrity, service customization, elasticity, services and service level agreements, performance, availability and open standards that are required for any Cloud infrastructure to offer.

Cloud Services and applications should designed from the user perspective and enable the collect of non-functional requirements to map onto the functional requirements. Functional requirements, specifies a function that a cloud product or cloud service (i.e., software) must be capable of performing. Non-functional requirements represent qualities or properties of a system, and not necessarily specific technological requirements.

4.2.1 CLOUD FUNCTIONAL REQUIREMENTS

Cloud providers have to understand such requirements and offer methods to acquire the necessary infrastructure to fulfill the users' expectations. Cloud infrastructures are the main focus of cloud computing and should have functionalities that assure cloud infrastructures capabilities to support cloud services and users expectations. Physical resources, such as compute, storage, network and other hardware resources, as well as software assets, compose cloud infrastructures. ITU-T[5] describes in [6][7] the main functional requirements of cloud computing which are related with the main resources provides by cloud infrastructure, namely:

COMPUTE RESOURCES

Compute resources are used to provide essential capabilities for cloud services and to support other system capabilities such as resource abstraction and control, management, security and monitoring.

The basic unit of allocation and scheduling of compute resources is a computing machine. Computing machine can be physical or virtual. The capability of a computing machine is typically expressed in terms of hardware configuration, availability, scalability, manageability and energy consumption.

- Computing machine requirements - include the hardware resource virtualization, and to support horizontal scalability (e.g., enable adding more computing machines) and vertical scalability (e.g., adding more resources with a computing machine). It is recommended to use power optimization solutions to reduce energy consumption.
- Virtual Machines (VMs) Requirements - include providing of virtualized and isolated computing environment for each Operation System (OS). Requirements for VMs include the virtualization of CPU, memory, Network Interface, and the duplication of VMs, Dynamic migration of VM's, Management automation. It is required to support migration of virtual machines between different physical computing machines.
- Software Resources Provision Requirements - The software resources include the software for building cloud infrastructure resource pools, and the software in support of service implementation. It is recommended Automated Provision and Deployment (e.g., resources should be automatically provisioned and deployed to target devices or platforms without operator intervention) of Cloud Services and a Unifed Software

Resource Management (e.g., capabilities for licence information registration, allocation, recovery, expiration notification and metering).

NETWORK RESOURCES

Typically, there are several types of networks involved in cloud computing services delivery and composition. ITU-T defines a generic model for cloud infrastructure described as follows:

a) Intra-datacentre network - The network connecting local cloud infrastructures, such as the datacentre local area network used to connect servers, storage arrays and L4-L7 devices (e.g., firewalls, load balancers, application acceleration devices).
b) Access and core transport network: The network used by CSCs to access and consume cloud services deployed by the CSP.
c) Inter-datacentre network: The network interconnecting remote cloud infrastructures. These infrastructures may be owned by the same or different CSPs.

General Requirements for Network Resources apply to the network resources of the access and core transport networks, intra-datacentre networks, and the inter-datacentre networks.

- Network Resources (e.g., bandwidth, number of ports, network addresses) are required to be scalable, ensure services performance and availability in order to support SLA objectives. It is important that network resources can to adapt dynamically the traffic generated by cloud services and support IPV4 and IPv6 addressing.
- Access and core transport network - need to support the delivery of cloud services in an optimal way in terms of performance, scalability and agility (e.g., through network programmability).
- Intra-Datacenter Network should provide elastic addressing and multi-paths for multi-tenant users and appropriate means to cope with flexible network address space demands. It is recommended to support different security and QoS policies, dynamic migration, traffic monitoring, and the establishment of a logical network among VMs. Need support public IP address and private IP address mapping, and dynamic DNS, static DNS and network services (e.g., firewall, load balancer, VPNs services) for multi-tenant users.
- Inter-Datacenter Network is recommended to support scalability to match the demand level of public and private clouds, to be resilient to failures and to any topology changes, to deal with VMs network addresses overlapping, and to support different logical networks.

STORAGE RESOURCES

Requirements for storage resources include storage space, storage interface, storage management, store availability, and data de-duplication. Storage Space is required to support dynamic storage space expansion. The storage interfaces resources are required to support either block storage interfaces or file system interfaces, to support object storage accessed via web service data path interfaces, to support structured data-sharing access interfaces, and can optionally support multiple types of interfaces.

- Storage Management is required to provide the capabilities for user authentication and authorization and capabilities for storage resources; to provide basic configuration capabilities, including storage domain configuration, file system namespace configuration, storage resources configuration and local file system configuration; to provide performance monitoring and statistics (e.g., disk I/O speed, disk space usage, CPU utilization, memory utilization, job completion), to support alert capabilities, to provide replication, archive and retention capabilities;
- The storage availability requirements include the monitoring of data failure, the providing of data backup and data recovery, and data verification capabilities, to support access through legitimate channels without time constraints, as well as the geographical constraints, to support data synchronization to keep data consistency.
- The data de-duplication is a method of reducing storage usage by eliminating redundant data. The data de-duplication can save resources of storage space and network bandwidth to transfer data.

ABSTRACTION AND CONTROL RESOURCES

Abstraction and control resources allow a CSP to access physical resources through software abstraction. It also provides composition, coordination, monitoring and scheduling of compute, storage, and network resources, and is responsible for controlling the interactions between resource pools and cloud services; the creation, modification, customization and release of abstracted resources; the monitoring of all physical and virtual resources; detection resources failures.

4.2.2 CLOUD NON-FUNCTIONAL REQUIREMENTS

Cloud computing non-functional requirements can be associated to operational, security and privacy, and legal factors [8].

CLOUD OPERATIONAL REQUIREMENTS

Operational requirements related to concerns towards the operation of cloud computing include:

- **Performance** - Performance in cloud computing is related to multiple aspects such as the capacities of the access networks which itself may depend on the geographical location or the accessing devices. Network latency may be a significant hurdle. Performance is also depended on the architecture of the application that is hosted in the cloud. In particular, it depends on the intensity of the backend data transfer between the front end and the cloud. A related consideration is therefore that application architectures may need to be fundamentally re-designed to deliver optimal performance when hosted in a cloud. A final limitation factor for several operational factors is the delivery over a network (usually the Internet) since the performance, availability, and reliability of the network limits the service level guarantees that can be provided by the individual cloud services.
- **Availability -** Availability in cloud computing means that cloud services should be available 24h/day for users. Service redundancy is a common characteristic of this requirement. Is mostly achieved through service redundancy (e.g., via replication or mirroring of data and computation) across multiple physical locations.
- **Reliability -** Whereas availability is mostly concerned with the prevention of disruption of the access to cloud resources, reliability is concerned with other, mostly more business severe forms of disruption, such as loss of data or of execution in progress.
- **Scalability -** Scalability refers to the capability of clouds to scale the permanent access to cloud resources according to the demand (e.g., to meet the needs of a growing business).
- **Elasticity** - is the flexibility of clouds to adapt the allocation of temporary resources – in either direction - in order to guarantee agreed service levels (e.g., an agreed maximum response time.
- **Portability & Lock-In -** Portability refers to the possibility to transfer an application or data from one cloud to another. This is typically linked to a concern about lock-in into the services of one provider. Commodity services using standard service interfaces may reduce lock-in. Non-standard management and interfaces increase lock-in. A particular concern is the incompatibility of data formats that may prevent customers from changing cloud service providers.

- **Standardization -** Standardization is closely linked to the issue of portability and lock-in is the question on the use of standards in clouds, typically with a requirement for open standards. Such standards may relate to areas as virtual image formats, cloud management APIs or data formats.
- **Cloud Management Capabilities** - The user can have only limited insights and access to the cloud environment. However, infrastructure clouds differ in the management capabilities they offer towards their users and the transparency that is connected to this.
- **Response time -** This requirement describes how much time it takes from the moment a user sends a request to the system, until a complete response is provided. This requirement describes how much time it takes from the moment a user sends a request to the system, until a complete response is provided.
- **Uptime -** The total time the service is available. It may be expressed as a percentage. When considering this requirement, it is necessary to take into account the provider's own uptime.
- **Fault Tolerance -** One of the system's properties is how it can withstand errors, either hardware or software-based. In the case of cloud, non-software errors can be generated either at the physical or the virtual machines hosting the service. While the first case is usually out of the developer's control, virtual machine faults can be handled by different means, for example by spawning new instances, or having backup VMs to respond to failures.
- **Interoperability -** Cloud services can interact with other local services within the Cloud, with remote services that are in the enterprise space, or with remote services in other Clouds. The evolving trend is that Cloud interaction is getting really global. Aspects such as Cloud service interoperability, composition, and collaboration are increasingly relevant and nearer to reality.

CLOUD SECURITY AND PRIVACY REQUIREMENTS

Security and privacy requirements are related to concerns on cloud computing user perspective such as issues on data protection, isolation breach or insider fraud.

- **Loss of governance** - The loss of governance is a typical general concern associated with cloud computing. It is linked to the transfer of management for critical data and computation to a cloud provider. It is further linked to the limitation in cloud

management capabilities and transparency from the view of the user. Cloud providers today often follow a one-size-fits-all approach where standard governance is provided and no tailoring to individual customers is done.

- **Isolation failure** - Apart from dedicated private clouds, infrastructure clouds typically serve multiple tenants at the same time. Due to the use of virtualization technology, clouds can achieve an efficient use of hardware resources and load balancing. This includes the possibility that one machine hosts multiple virtual machines and potentially data and computation from different tenants. Isolation failure addresses the general concern about data leakage or intrusion in between different tenant application environment hosted on the same cloud.
- **Insider Fraud** - Whereas isolation failure mainly addresses intrusion on the technical level (e.g., by malware at the virtualization layer), insider fraud addresses the risk that arises from the access of cloud administrators. Cloud administrators need on the one hand the necessary access rights to fulfill their duties, but they need also be prevented from accessing critical data or introducing harmful software to the applications hosted in the cloud. This may be intentional or unintentional (e.g., via malware carried on a memory stick).
- **Management Interface Compromise -** The management interfaces that allow for automated external management of capabilities of the cloud like starting or migrating a virtual machine are generally accessible via the Internet. This also offers additional intrusion possibilities.
- **Insecure or Incomplete Data Deletion** - Data deletion is necessary pre-requisite to keep confidentiality and data security requirements. However it is not always done complete and in way that would not allow experts to restore data. While secure disposal of storage is one concern, another important concern is reliable cleansing of storage resources (memory, disk, etc.) once they are released by one tenant.
- **Confidentiality** - Confidentiality relates to the accessibility of information. This needs to be restricted to authorized persons. In clouds this is typically related also to the risk of insider fraud.
- **Data protection** - Protecting data can go beyond the limitation of access and in sensitive cases (e.g., be achieved via data encryption in the cloud). However, such solutions may include new related risk areas such as the management of keys. Also, the data encryption in the cloud has a number of disadvantages as to performance and limitation of computations on the data.
- **Resilience** - Resilience is a wider security concern that addresses the capability of the cloud to counter unforeseen threats and maintain availability even in critical security

situations. Cloud resilience is on the one hand related to the redundancy and replication mechanisms as described under availability. On the other hand, it may introduce new mechanisms like integrity check of results received from replicated computation in different cloud locations.

LEGAL AND COMPLIANCE REQUIREMENTS

Legal and Compliance Factors addresses legal and compliance related concerns, including:

- **Compliance** - Compliance includes all aspects of confirming to regulations. This duty applies to the cloud user and owner of the data and applications hosted in the cloud. Cloud computing creates particular new questions in this context such as compliance in the context of cross-border cloud computing.
- **Liability** - Liability is one aspect of the *Terms of Use* and addresses the question of liability relations in a cloud business (e.g., relate to the consequences of data loss or data leakage).
- **Accountability** - Accountability is often linked to the notion of trust. It is also closely related to the concept of transparency. In general, accountability is linked to more formalized ways of assessing the practices of the cloud provider from an organizational down to a technical level. There is also a related research debate about trusted computing and strong accountability that implies a close interplay between machine-readable policies, monitoring and enforcement mechanisms.
- **Transparency** - Transparency is related to the question of how transparent the provisioning of cloud services is organized and what monitoring and auditing is allowed to be initiated and performed by the cloud user.
- **SLA's** - This includes defining the process of managing and monitoring the capacity, data protection, data privacy, operational integrity, vulnerability management, business continuity, disaster recovery, identity management, and ownership of intellectual properties. Similarly, *Operation Level Agreement* (OLA) requirements too have to be discussed threadbare and signed.

4.3 CLOUD REFERENCE ARCHITECTURES, MODELS AND FRAMEWORKS

Cloud computing architecture is used as a guideline to understand the whole process including actor roles inside a cloud computing environment. Currently, there is only a few cloud computing architecture that can be used as a reference for building a cloud computing solutions.

This section describes na overview of the cloud computing reference architecture developed by NIST, IBM, ORACLE, DMTF and ITU.

4.3.1 NIST CLOUD ARCHITECTURE

NIST has developed a logical extension of their cloud definition by the development of NIST CCRA [9] (Figure 1). This generic high-level conceptual model constitutes an effective tool for discussing cloud requirements, structure and operation. It defines a set of actors, activities and functions and it can be used in development process to design cloud computing architecture. The NIST CCRA serves several objectives, including the analysis of standards [10] for security, interoperability, and portability of data.

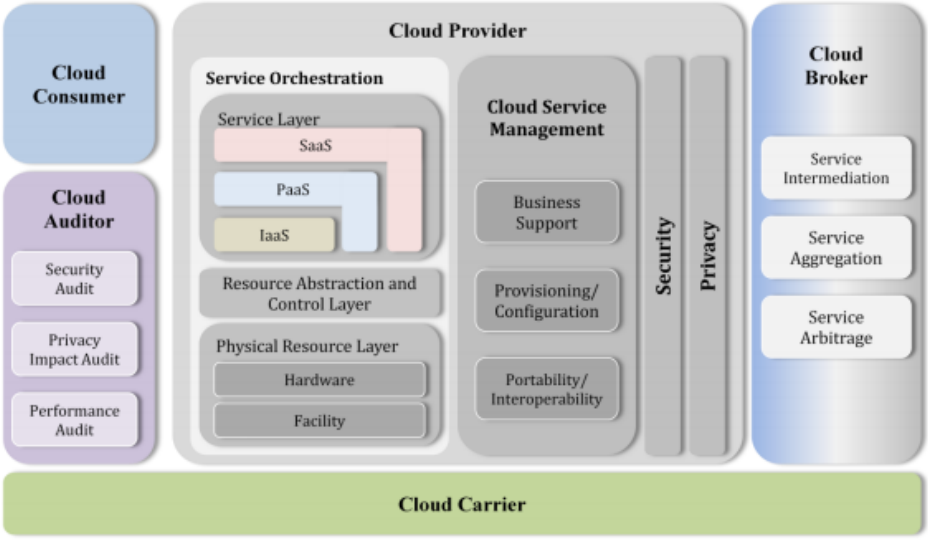


Figure 1: NIST Conceptual Reference Model for Cloud Computing [2]

It outlines five major parties involved in a cloud ecosystem namely cloud consumer, cloud provider, cloud auditor, cloud broker and cloud carrier.

Service Orchestration refers to the composition of system components to support the Cloud Providers activities in arrangement, coordination and management of computing resources in order to provide cloud services to Cloud Consumers.

- Service layer: Define interfaces for cloud services access through service interfaces of each the three service models IaaS, PaaS and SaaS.
- Resource abstraction and control layer: composed by components that enables the management of computational resources (i.e., virtual machines (VM's), operation systems, databases and processing capacity) of physical layer through software abstractions. The control layer is composed by components that ensures the the resource pooling, access control, and service monitoring.
- Physical Layer: includes all infrastructure resources (i.e., CPU, memory, routers, firewalls, connectivity and network interfaces, data storage) and facility resources (cooling, power and communications). These resources are usually associated to data center services.

The Service Layers are also responsible for the overall management of the cloud by the cloud service management (CSM), characterized by their three components (Figure 2):

- Business Support: consists of all business related services with the clients and supporting process, such as customer management, Contract management, inventory management, accounting and billing, reporting, auditing, pricing, and rating.
- Provisioning and Configuration: handles all aspects of provisioning, resource changing, monitoring and reporting, metering and SLA management.
- Portability and Interoperability: supports the migration of services and data between clouds, moving data or applications across multiple clouds and communication between or among multiple clouds. Cloud providers should provide mechanisms to support data portability, service interoperability, and system portability.

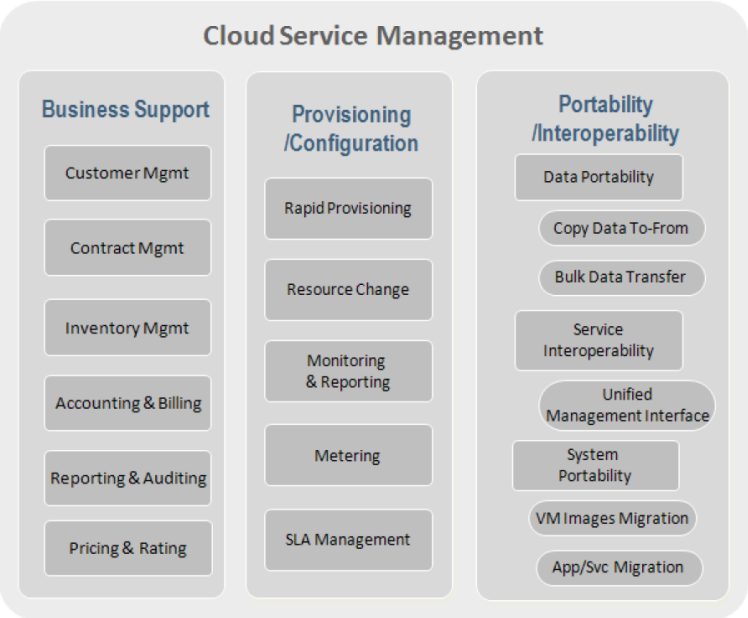


Figure 2: Cloud Service Management [2]

The Security and Privacy aspects of the cloud cut across all architecture layers and is important to assure requirements such as authentication, authorization, availability, confidentiality, identity management, integrity, audit, security monitoring, incident response, and security policy management, and protect users data information and in the cloud.

4.3.2 IBM CLOUD ARCHITECTURE

The IBM Cloud Computing Reference Architecture (CCRA) [11][12] (Figure 3), defines the fundamental cloud architectural elements, three main roles - Cloud Service Consumer, Cloud Service Provider and Cloud Service Creator, governance policies tailored for the environment or organization and detailed documentation of all the most important cloud components. This architecture provides the guidelines for creating a cloud environment, specifications for the physical components of a cloud implementation (network, compute, storage, and virtualization) and for the software components required to run operational and business management processes. Includes use cases, non-functional requirements, components, operations, security, performance and scalability, resiliency, consumability considerations, cloud service creation guidance and much more.

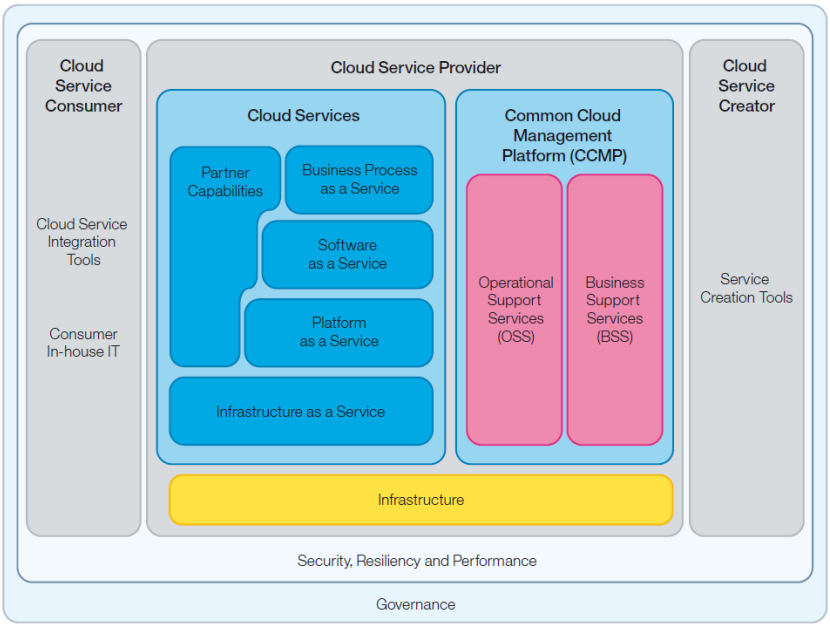


Figure 3: IBM High-level Cloud Reference Architecture [5]

SECURITY AND RESILIENCY

IBM's reference architecture specifications incorporate proven security and reliability technologies as well as simplified security management and enforcement. IBM security surrounding clouds focuses on developing trusted virtual domains, authentication, isolation management, policy and integrity management, and access control (Figure 4)

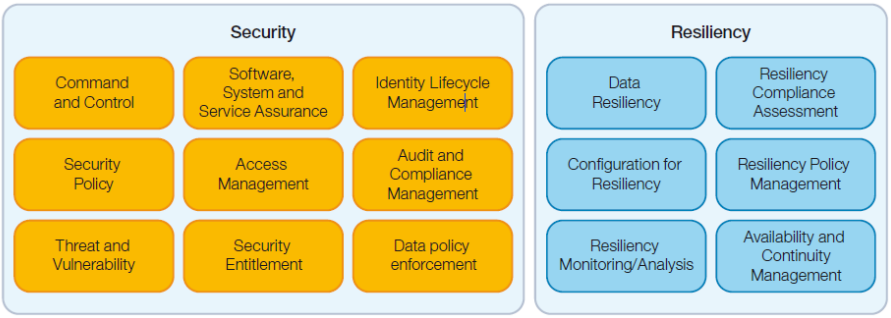


Figure 4: IBM CCRA Security Components [5]

The key security focus areas for the cloud services layer include: (1) Federated identity, authorization and entitlements; (2) Audit and compliance reporting; (3) Intrusion detection and prevention; (4) Secure separation of subscriber domains; (5) Secure integration with existing enterprise security infrastructure.

CLOUD MANAGEMENT

The core components of this architecture are mainly cloud services, a Common Cloud Management Platform (CCMP)[12] that integrates the operational and business management of all layers of the cloud environment, including the CCMP itself. The CCMP exposes a set of management services for the delivery and management of cloud services of service models (IaaS, PaaS, SaaS) and business process services (any business process delivered through the cloud service model). The CCMP is comprised of two modules:

- Operational support services (OSS): defines the set of systems management services that may be exploited by cloud service developers. This services encountered in traditionally managed data centers, such as monitoring and event management, provisioning, incident and problem management;
- Business support services (BSS) - defines the capabilities required to enable the business management of one or more specific managed cloud services, such as account management, service billing, order management.

These modules are decomposed into components and sub-components or functions required for creating a CCMP implementation that represents services of CCMP. Figure 5 depicts the sub-components of IBM CCMP layer and respectively service modules for OSS e BSS

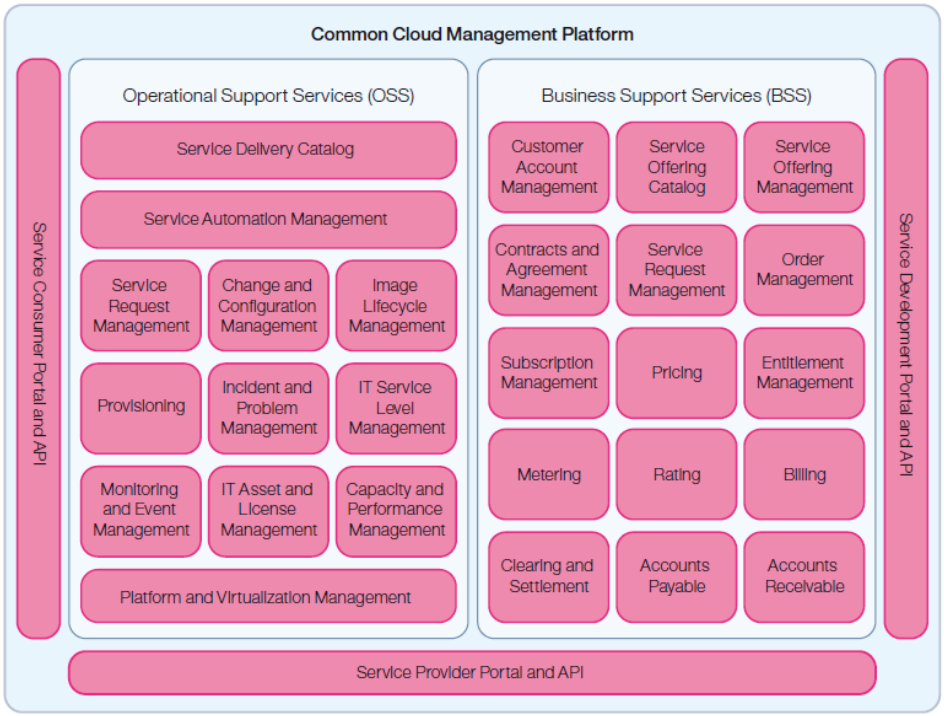


Figure 5: IBM Common Cloud Management Platform Modules [5]

IBM participates in several cloud standards initiatives within various standards development organizations across the spectrum of cloud service models IaaS, PaaS and SaaS, all of which work toward improvements in cloud interoperability and security.

4.3.3 ORACLE CLOUD ARCHITECTURE

The Oracle Cloud reference Architecture [13] (Figure 6) is largely centers on "the Cloud", which refers to the capabilities, resources and services that work together to provide IaaS, PaaS, and SaaS services to developers, end users and application owners. The cloud actors are described as Cloud Consumers (represents all types of users of Cloud capabilities), Cloud Brokers (represent a special class of both Cloud provider and consumer) and Cloud Provider (the provider of cloud services).

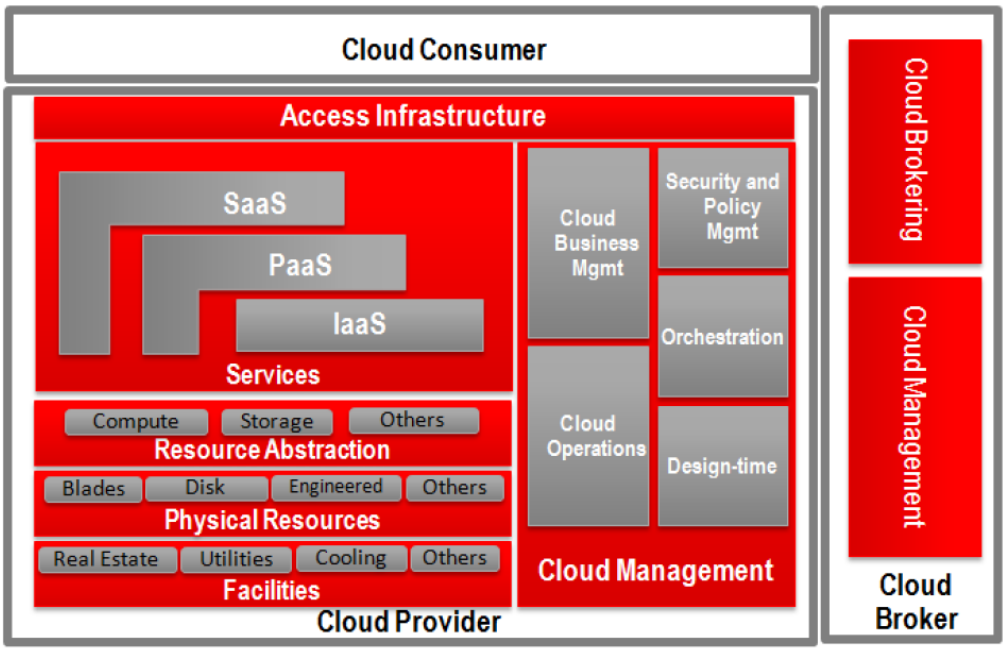


Figure 6: Oracle Cloud Computing Reference Architecture [6]

- Access layer: enables end users, developers, and application owners access to the service layers (and hosted Cloud applications) as well as the Cloud management interface
- Cloud management layer: exposes the Cloud logic needed to design, provision, and manage Cloud services for developers and application owners. It also provides the control plane for the Cloud operator to manage the underlying Cloud infrastructure. Oracle envisions five major areas of concern within the Cloud management layer:

1) Business management, which covers the business management aspects of the Cloud);
2) Operations - supports the runtime capabilities for the Cloud infrastructure;
3) Security and policy management - support the security and policy management requirements of the Cloud infrastructure;
4) Design-time - supports the model management and design-time tools;
5) Orchestration - provides the capabilities for orchestrating the key.

- Management layer: sits between the access and resource layers to mediate all communications. Communication from the access layer cannot talk directly to the resources.
- Services Layer: services layer contains the deployable entities built from the Cloud's Infrastructure, Platform, and/or Software services
- Resources Layer: Resource layer aggregate and manage physical and virtual resources.

4.3.4 DMTF CLOUD ARCHITECTURE

The DMTF Reference Architecture (Figure 7) for managing cloud represents the conceptual Cloud Service Reference Architecture which describes key components and the interrelationships among these components [14]. Key Components includes:

- Actors (Cloud Service Provider, Cloud Service Consumer and Cloud Service Developer);
- Interfaces (i.e., Service Catalog, Security manager and Service manager, that are exchanged over the functional interfaces);
- Data artifacts (describes the semantic content and the specific format (i.e., service requests, SLAs, contracts, service templates, service offerings, and images.);
- Profiles (include normative specializations or extensions of the interfaces and artifacts, or combinations of them).

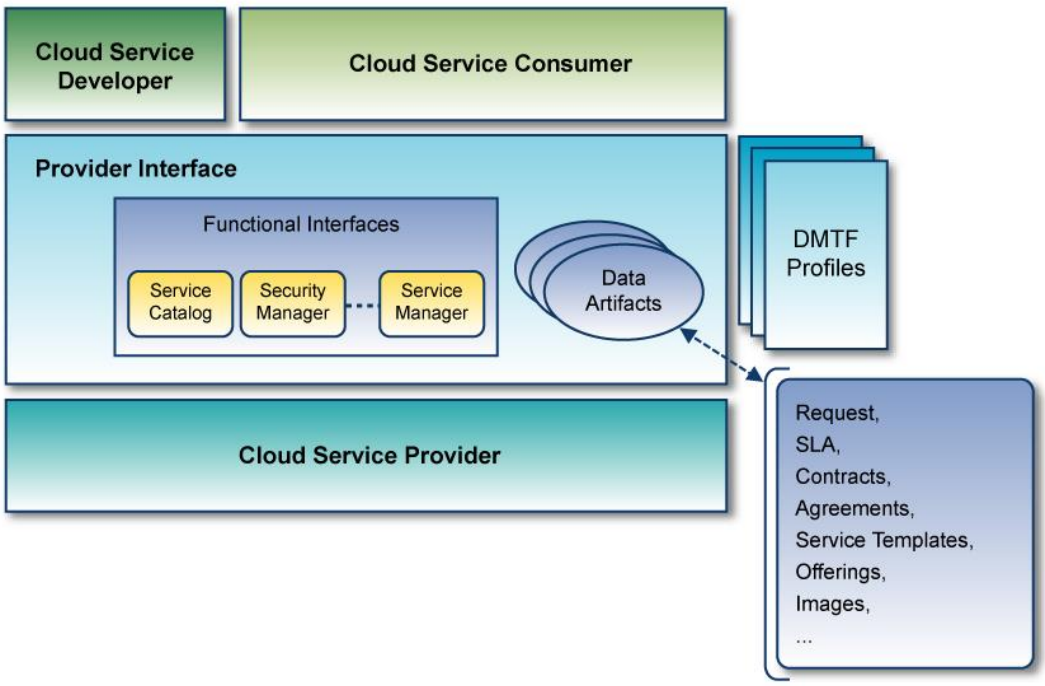


Figure 7: DMTF Cloud Service Reference Architecture[14]

4.3.5 ITU CLOUD REFERENCE ARCHITECTURE

ITU Cloud Reference Architecture defines the functional requirements and reference architecture of cloud computing, which includes the functional architecture, functional layers and blocks.

ITU defines Cloud Computing actors as:

- Cloud Service Partner (CSP)
- Cloud Service Provider (CSP)
- Cloud Service User (CSU)
- Inter-cloud Service Broker (ISB)

Figure 8 shows the major functional blocks of the ITU cloud computing reference architecture. It is recognized that cloud service providers will decide which functional blocks are appropriate to their business, and how the chosen functional blocks are implemented.

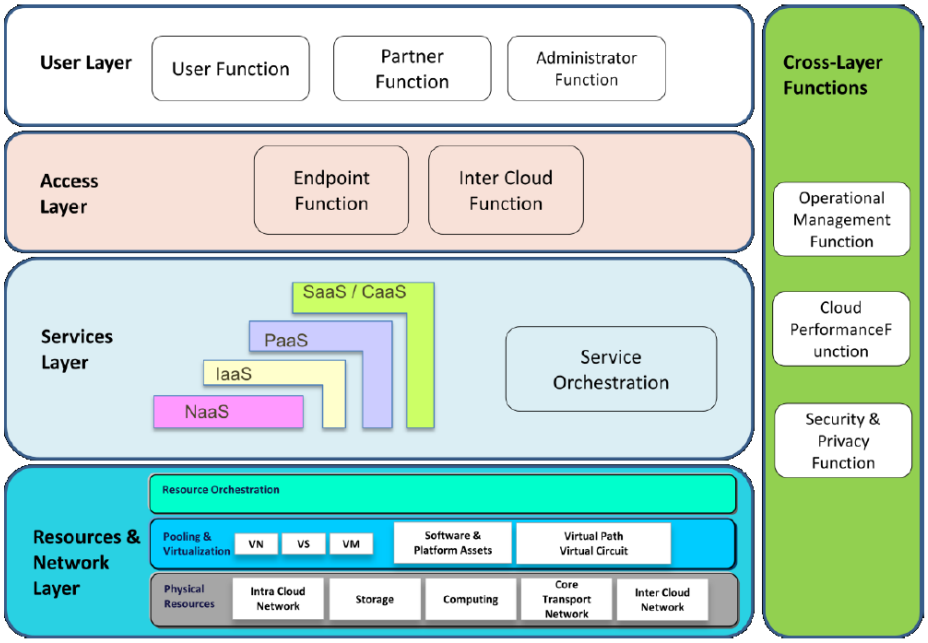


Figure 8: ITU Cloud Computing Reference Architecture [15]

This CCRA is composed into the following layers:

- **User Layer** - The user layer includes the User function (supports a CSU to access and consume cloud services), Partner function (enables the CSP relationship with CSP), and Administrator function (supports the enterprise administrator to manage and administrate cloud resources and services within business processes).
- **Access Layer** - The access layer includes the endpoint function (controls cloud traffic and improves cloud service delivery) and Inter-cloud function (CSPs inter-cloud connections to enable the ubiquitously offer of Cloud services offered by CSPs on a global basis.
- **Services layer** - The services layer includes the service orchestration (is the process of deploying and managing "cloud services"), and Cloud services (provides the cloud services categories and any composition of these services).
- **Resources and network layer -** The services layer includes the service Resource Orchestration (support the management, monitoring, and scheduling of computing, storage and network resources and the resource orchestration), Pooling and Virtualization (pooling and virtualization of physical resources), and Physical Resources (computing, storage, and network resources fundamental to providing cloud services).

- **Cross-layer functions -** The cross-layer functions include Security and privacy (security related controls to mitigate the potential threats in cloud computing environments), Cloud Performance (to aggregate cloud network information, service routing, SLAs), Cloud Auditing (collects audit events, logging and reporting information) and Cloud Operational Management.

4.4 INTERCLOUD AND BROKER MECHANISMS

4.4.1 *INTERCLOUD ENVIRONMENTS*

Intercloud is a term which refers to the interconnectivity of cloud data centers. The first approach of cloud resource provisioning is to host services on a single cloud provider, this cloud provider hosts the service in a specific data center (if multiple are available) and, more important, on a (mostly) vendor-specific architecture. This imposes several challenges for the customer:

- **Cloud provider unavailability** can lead to service downtimes, without the possibility to transfer the service to another provider.
- **Vendor-lock-in**: The cloud provider may have proprietary programming interfaces which are only valid on this single infrastructure

According to [66] the benefits of Intercloud environments for clients are:

- **Diverse geographic locations**: Enables the customer to have fine grained control of where specific resources are positioned. Large vendors already have cloud computing centers all around the world, but it is not likely to happen that any provider will have capacity located in all countries around the world.
- **Better application resilience**: In case of a provider outage the services of customers who rely on a single data center will not work anymore. Designing applications to be multi-data-center ready solves this issue partially, at least for providers with multiple data centers around the world. Further, the Intercloud mechanism also refers to the cooperation of multiple cloud providers in different data centers. This also acts as insurance, in case providers are shut down for some reasons.
- **Avoidance of vendor-lock-in**: One outcome of using Intercloud mechanisms is that vendor-lock-in is avoided and data or services can be transmitted between providers freely.

The above mentioned advantages in Intercloud environments mainly apply to customers, but there are also strong arguments for Cloud providers to be part of an Intercloud environment:

- **Expandability**: For customers the provider has an infinite number of resources, but of course even large cloud providers have their limits. Intercloud environments enable small and large cloud providers to absorb computing load spikes by offloading services to other providers.
- **SLAs**: The Cloud providers are able to issue stricter SLAs, because they have the ability to offload their computation to other cloud providers in case of operation outages.

4.4.2 *BROKER MECHANISM*

The broker mechanism is on a higher abstraction layer than Intercloud mechanism, it does not deal with raw computation units, but with services and applications.

Brokering is an essential element of service-oriented architectures and utility resource sharing. Brokers act as intermediaries that match client needs with provider services by aggregating information about multiple providers and client requests. As cloud services are evolving and get more complex it may be too complex for customers to manage the services integration. The customer may instead contact a cloud broker who provides the service for the customer and manages the relationship between the cloud provider and the customer. Figure 9 shows a typical Cloud Broker use case scenario.

Figure 9: Usage Scenario for Cloud Brokers

According to Gartner [65] a cloud broker can provide services in one of the following three categories:

- **Cloud Service Intermediation**: An intermediation broker provides services which are directly dependent on other services and enhance the service functionality delivered

to the customer. The intermediation broker providers could also manage pricing and billing.

- **Cloud Service Aggregation**: Aggregation broker providers combine multiple services to one or multiple new services to be used by the customer. This moves complexity regarding service integration, process integrity or intermediation from the end-user to the broker. The broker takes care of data security aspects of the communication of the services.
- **Cloud Service Arbitrage**: The Cloud Service Arbitrage broker provider is similar to the Cloud Service Aggregation broker provider, but has the difference that the aggregated services are not fixed, they are chosen in a dynamic way. An example for Cloud Service Arbitrage is a cloud service providing access to multiple e-mail services.

4.4.3 *PROJECT: BROKER@CLOUD*

Broker@Cloud [67] is an EU FP7 funded project which aims to provide an advanced intermediary cloud service broker.

> *The goal of the Broker@Cloud project is to develop a framework that will equip cloud service intermediaries with advanced methods and mechanisms for continuous quality assurance and optimization of software-based cloud services. The framework will allow enterprise cloud service brokers to monitor the obligations of providers towards consumers, as well as to detect opportunities for optimizing service consumption. [68]*

The outcome of the project is (as illustrated in Figure 10):

- Create a set of methods and tools to create a platform-neutral description of cloud services to facilitate continuous quality assurance and optimization.
- Create a set of methods and mechanisms to help enterprise cloud service brokers to perform governance and continuous quality control.
- Create a set of methods and mechanisms to enable continuous cloud service failure prevention and recovery through proactive and reactive failure detection.
- Create a set of methods and mechanisms to enable continuous optimization of consumed cloud services.
- Validation of the results.

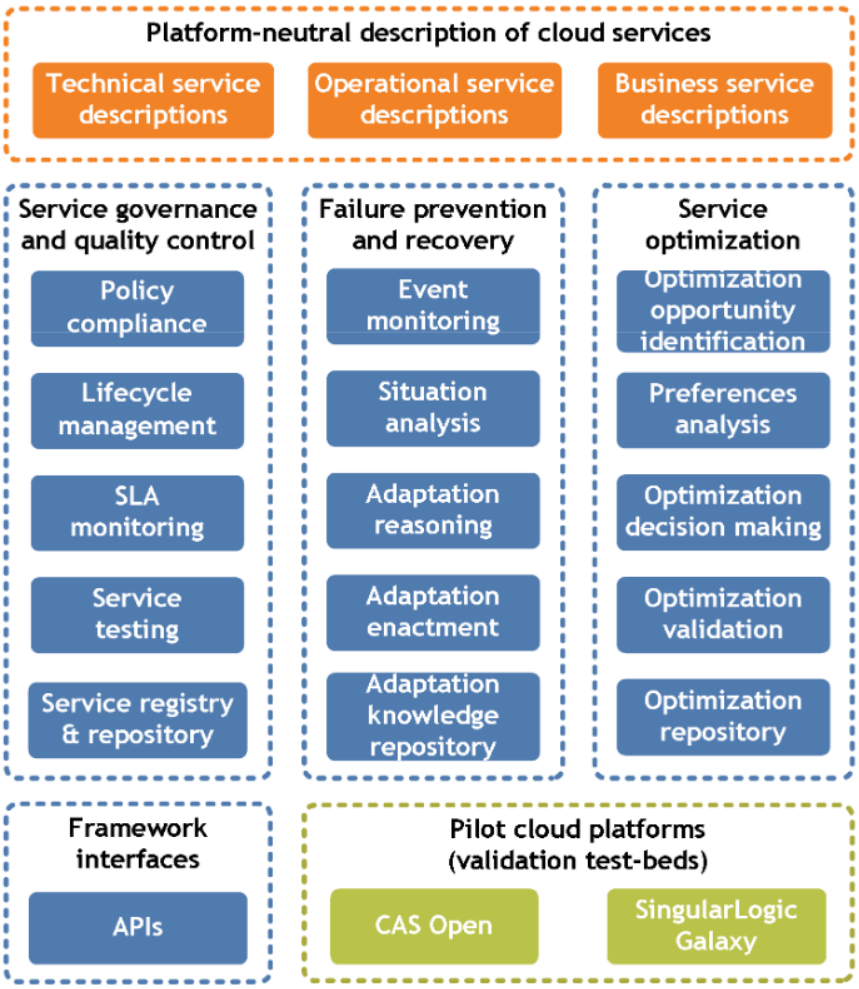


Figure 10: Broker@Cloud outcome [68]

4.5 KEY TECHNOLOGIES AND APPLICATIONS FOR CLOUD

Cloud Computing technology evolved from other similar technologies and still overlaps in functionality and design. Grid computing is/was a term that was invented in the mid-1990s, to provide computing resources on demand, as electronic power grids provide energy on demand. Applying a different scale and viewing it on a different abstraction layer, cloud computing uses grid computing as a basis and augments its functionality with various aspects. But the key enabling technologies described in this chapter are very similar and got adapted over the years.

4.5.1 *VIRTUALIZATION*

Virtualization generally refers to the abstraction of physical resources to logical resources. It enables (together with other technologies) flexibility, increases server efficiency, saves costs and therefore makes the business more valuable. And therefore is one of the key enablers of cloud computing.

Server virtualization was the first and most important steps towards cloud computing. Before virtualization techniques were used, there usually was a one-application-per-server deployment scenario. Virtualization enables the operator of a data center to deploy multiple virtual servers on a single physical server, without the knowledge of the applications on the virtualized servers. This brings a high boost on server utilization, which was at about 20 percent average before virtualization and therefore helps the operators to save costs and efficiently use all of its available resources.

Besides processing power/processors the virtualization also takes place for all kinds of hardware like data storage, network resources and connectivity, and so on. Using virtualization on its own does not provide key features like flexibility at the scale of cloud computing. To unleash the flexibility as provided by current cloud computing environments a Distributed Resource Scheduler (DRS) is required which aggregates resources from multiple servers and provides them in a resource pool on demand. On top of this approach, the cloud computing paradigms IaaS, PaaS and SaaS are built.

4.5.2 *MASS DISTRIBUTED STORAGE*

Cloud computing providers make available huge loads of storage space, required by cloud computing enabled applications. For this purpose the classic distributed storage model is adopted, and extended by adding redundancy. Data is spread around different data centers, at different geo-locations to increase data redundancy and therefore increase the reliability of the service.

A typical distributed file system implementation used in cloud computing data centers is the Hadoop Distributed File System (HDFS) developed by the Hadoop Apache team:

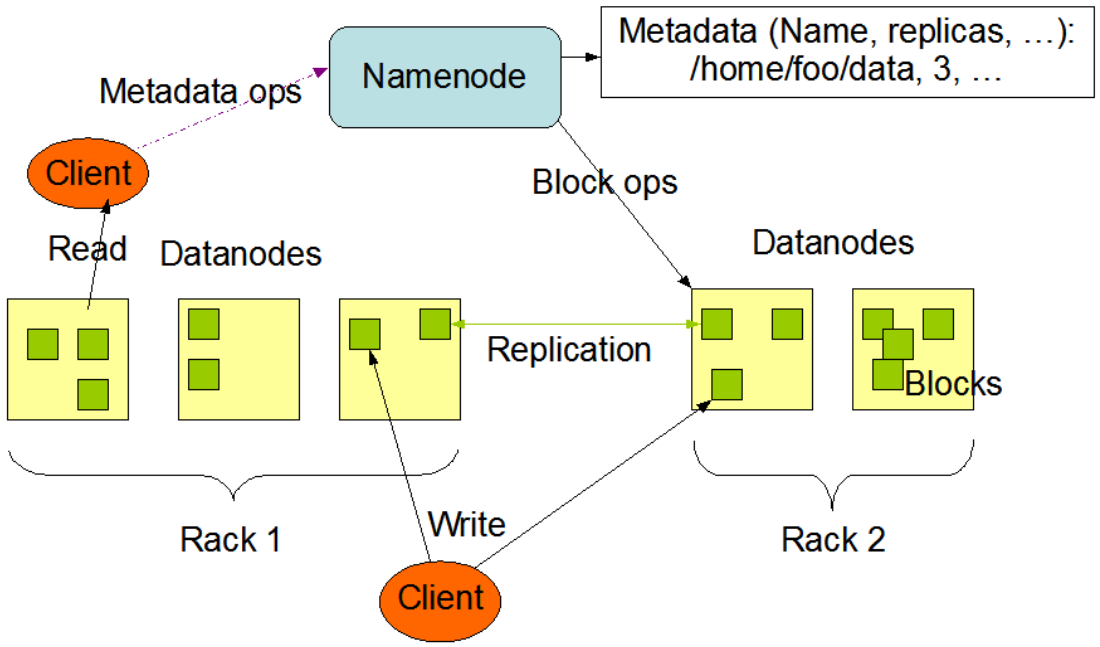


Figure 11: HDFS architecture overview [69]

HDFS is able to run on common hardware, and is, in contrast to other existing distributed file systems highly fault tolerant. HDFS follows a master-slave principle where a master node has multiple slave (or worker) nodes attached where the data (split into blocks) gets saved redundantly. HDFS provides, among others, several mechanisms to ensure high availability like failover nodes, multiple storage nodes and automatic resynchronization of failed nodes [69].

This type of storage is comparable to a file system, so without additions it is only meant to manage storage on block level and not for managing structured data like databases.

4.5.3 *PARALLEL PROGRAMMING MODEL*

A key enabler for cloud computing is the capability to make parallel programming available transparently to user. *MapReduce* is one system developed by Google, which is used (or at least acts as a paradigm) to other implementing parties. The system is used to process large amounts of data on massively distributed systems (see 4.5.2) with a large number of nodes in parallel. In a simplified view, using the *MapReduce* approach a task is divided into smaller subtasks and distributed along the worker grid, also called the *Map*-phase. Then a master node collects the results and assembles the primarily requested data (*Reduce*-phase).

With using this approach together with massively scaling data storage, it is possible to build applications operating on a huge amount of data completely transparent to the user.

4.5.4 *DATA MANAGEMENT*

Beside the storage of large amounts of unstructured data (see chapter 4.5.2), cloud computing services also need to process and analyze a large amount of structured data. The data storage mostly is based on the *Mass Distributed Storage* service, but needs additional functionality to satisfy the needs of cloud enabled applications processing masses of data. There are basically two reference solutions available when talking about big data:

Googles Bigtable is a solution not available to the public but used by many Google services, a paper has been published which describes the architecture of *Bigtable* [70]. The system better describes as a multi-dimensional sparse set and is not related to relational databases. It is designed to scale into petabytes and to hundreds or thousands of participating machines.

Apache HBase in contrast is an open source project, modeled after *Googles Bigtable* approach on top of Hadoop and HDFS. It provides a comparable distributed data storage with similar features.

Many other implementations of other vendors exist. All of them are similar and have the goal to process large amounts of structured data in a minimum of time, transparent to the user.

5 STANDARDIZATION AND CERTIFICATION

5.1 CLOUD STANDARDIZATION

Standards Development Organizations (SDOs) are already available specific Cloud Computing Standards to support of many functions and requirements for cloud computing. The analysis of the standardization activities aims to provide an overview of existing work in cloud computing standardization. The analysis of the standardization environment aims to provide an overview of existing standards, requirements, certification and preparatory work in cloud computing and to place it in the context of C4E project.

- Main SDOs that are working in cloud standards developmentAlliance for Telecommunications Industry Solutions (ATIS)[16]
- Cloud Security Alliance (CSA)[17]
- CSMIC (Cloud Services Measurement Initiative Consortium)[18]
- Distributed Management Task Force (DMTF)[19]
- ETSI (European Telecommunications Standards Institute)[20]
- IEEE (Institute for Electrical and Electronics Engineers) [21]
- International Standards Organization (ISO)[22]
- IEC (International Electrotechnical Commission)[23]
- ITU (International Telecommunications Union) [6]
- NIST(National Institute of Standards and Technology) [24]
- Organization for the Advancement of Structured Information Standards (OASIS)[25]
- Open Data Center Alliance: The Open Data Center Alliance (ODCA) [26]
- Open Grid Forum: The Open Grid Forum (OGF)[27]
- Storage Networking Industry Association (SNIA)[28]
- Telecommunications Industry Association (TIA)[29]

The NIST Cloud Computing Standards Roadmap Working Group (CCSRWG) [9] has compiled an inventory of standards relevant to Cloud Computing[29], in order to assist the NIST Cloud Computing Standards Roadmap[9] for Interoperability, Portability, Security, Performance, Service Agreements, Monitoring and Accessibility for the IaaS, Paas and SaaS service models.

European Comission proposed to ETSI to coordinate with ICT stakeholders that work in the cloud standards ecosystems and devise standards roadmaps to support the development of EU policy in critical areas such as security, interoperability, data portability and reversibility. ETSI had launched the Cloud Standards Coordination (CSC) initiative to develop cloud standardization roadmap in cloud standardization that covers areas such interoperability, security and privacy and SLAs (Service Level Agreements). The cloud standards roadmaps developed by NIST and ETSI cover the main areas of Cloud Computing standardization and were reported in NIST Roadmap Standards [9] and ETSI Cloud Standards Coordination Report [2].

Annex 1 provides the list of standards for cloud computing produced by main SDOs listed above in this section.

5.2 CLOUD CERTIFICATION: FRAMEWORKS, MODELS AND SCHEMES

This section identifies and systemies certification schemes for cloud computing services, including studies, standards and certification schemes that were developed to cloud computing contexts.

In the context of the European strategy for Cloud Computing [2], the EU has created the Cloud Select Industry Group (C-SIG), composed by industry experts, and a set of working groups, included on cloud certification designated as CERT-SIG to working on cloud certification schemes in the context of the EU cloud computing strategy. This working group has produced a Cloud Computing Certifications Schemes List (CCSL), which were listed by ENISA in [31], that includes the following main standards:

- ISO 27001[32]
- ISO 20000 [33]
- ITIL (Information technology Infrastructure Library)[34]
- CSA Open Certification Framework (OCF)[35]
- Eurocloud Star Audit [36]
- Leet Security Rating Guide
- COBIT [37]

5.2.1 IT GOVERNANCE, MANAGEMENT AND SECURITY

EU organizations (public sector or private sector) have to take attention to performance, predictability and accountability in the governance and management of cloud services and related IT resources. Governance is related to the application of policies for using services and defining the principles and rules that determine how an organization should behave. Many of the principles of IT Governance and IT Management best practices are relevant to cloud environment because it provides guidelines that support the service management and business strategy.

Best practices such as COBIT, ISO 20000, ITIL, ISO 38500, and ISO 27001 are being used around the world as a common frameworks and standards for IT operations. Those frameworks can be used into cloud certification scheme to evaluate the capacity of organizations, including public and private companies, to provide cloud services according to the best practices.

COBIT (Control Objectives for Information and related Technology) [37] is one of ISACA [38]. COBIT 5 is the latest edition of ISACA's globally accepted framework, providing an end-to-end business view of the governance of enterprise IT that reflects the central role of information and technology in creating value for organizations. The principles, practices, analytical tools and models found in COBIT 5 embody thought leadership and guidance from business, IT and governance experts around the world.

ISO/IEC 20000 is a Service Management System (SMS) Standard [39]. It specifies requirements for the service provider to plan, establish, implement, operate, monitor, review, maintain and improve an SMS. The requirements include the design, transition, delivery and improvement of services to fulfill agreed service requirements. The current version of ISO/IEC 20000 is ISO/IEC 20000:2011[39].

ITIL (IT Infrastructure Library) [34] [40]provides a guidance for IT Service Management [41]. It provides a framework for the governance of IT, the service wrap, and focuses on the continual measurement and improvement of the quality of IT service delivered, from both a business and a customer perspective. It is organized around the service lifecycle that include the Service Strategy, Service Design, Service Transition, Service Operation, and Continual Service Improvement. Some of key benefits of use ITIL by organizations include the increase of customer satisfaction, the improvement of service availability, financial savings and resource management, time to market for new products and services and optimized risk. ITIL

provides the foundation for quality IT service management and is aligned with various international quality standards.

The ISO/IEC 38500:2008 [42] is a standard for Corporate Governance of Information Technology [5]. This standard provides a framework for effective governance of IT to assist those at the highest level of organizations to understand and fulfill their legal, regulatory, and ethical obligations in respect of their organizations use of IT. This standard is applicable to organizations from all sizes, including public and private companies, government entities, and not-for-profit organizations. This standard provides guiding principles for directors of organizations on the effective, efficient, and acceptable use of Information Technology (IT) within their organizations.

ISO/IEC 27001 [39] is a security certification standard published by the ISO and the IEC. This standard was developed to provide a model for establishing, implementing, operating, monitoring, and maintaining an information security management system. It is widely recognized as the highest security standard in the industry for examining the efficacy of an organizations overall security posture, providing requirements for establishing, implementing, maintaining and continuously improving an Information Security Management System (ISMS). ISO 27001:2013 [40] is the actual version of this standard.

5.2.2 CLOUD SECURITY ALLIANCE (CSA) CERTIFICATION FRAMEWORK

Cloud Security Alliance (CSA) [35] is leading by a broad coalition of industry practitioners, corporations, associations and other key stakeholders with the mission to promotes the use of security assurance best practices within cloud computing.

The Security, Trust and Assurance Registry (STAR) is an initiative form CSA that improving transparency and assurance in the cloud and provides a accessible registry that documents the security controls provided by various cloud computing offerings and provides guidance to users that want to contract cloud services from cloud providers. According STAR, the 13 domains to address cloud computing security are:

- Cloud Computing Architectural Framework
- Governance and Enterprise Risk Management
- Legal and Electronic Discovery
- Compliance and Audit
- Information Lifecycle Management
- Portability and Interoperability

- Traditional Security, Business Continuity, and Disaster Recovery
- Data Center Operations
- Incident Response, Notification, and Remediation
- Application Security
- Encryption and Key Management
- Identity and Access Management
- Virtualization

STAR is based on a multilayered structure defined by the Open Certification Framework Working Group that has developed the CSA Open Certification Framework (CSA-OCF) [43] for cloud providers certification according to the Cloud Security Alliance's industry leading security guidance and control objectives. This framework is structured on the following three levels of trust:

- Level 1: STAR Self-Assessment - Submission of Consensus Assessments Initiative Questionnaire (CAIQ) [44] and report and CSA Cloud Control Matrix [45] to indicate the cloud provider compliance with CSA best practices;
- Level 2: STAR Certification by third party assessment;
- Level 2: STAR Attestation by third party assessment;
- Level 3: Continuous Monitoring Based Certification;

Each level of trust provides an incremental level of visibility and transparency into the operations of the cloud service provider and a higher level of assurance to the cloud consumer.

5.2.3 SAS 70 AUDITS STANDARD

The Statement on Auditing Standards (SAS) No. 70 [46] is a set of auditing standards to measure handling of sensitive data developed by American Institute of Certified Public Accountants (AICPA)[47] which provides guidance to service auditors when assessing the internal control of a service organization and issuing a service auditor's report. Also provides guidance to auditors of financial statements of an entity that uses one or more service organizations. Service Organizations within almost every conceivable industry can be viewed as potential candidates for SAS Audit:

- Claims processing centers
- Trust/benefit plan administrators
- Data centers and co-locations

- Application service providers
- Payroll processors,
- Internet service providers

Many of these standards are recognized as globally accepted best practices approaches

5.2.4 OPEN DATACENTER ALLIANCE MODEL

The Open Data Center Alliance (ODCA) [48] is an independent organization that coordinate the development of standards for cloud computing. ODCA has adopted a usage model-centric approach in defining and sharing its prioritized requirements with standards organizations and solutions providers.

The usage models define IT requirements for cloud adoption and an ODCA Vision for Cloud Computing. These enable the federation, agility and efficiency across cloud computing while identifying the specific innovations in Secure Federation, Automation, Common Management and Policy and Solution Transparency required for widespread adoption of cloud services.

ODCA usage models [49] cover:

- Provider Security Assurance and Security Monitoring - address IT's greatest challenge for cloud adoption by proposing standard security levels for cloud services and compliance.
- Service Catalog and Standard Units of Measurement for IaaS - enable feature, price and performance comparisons across private and public clouds for increased transparency and easier IT decision-making.
- Virtual Machine Interoperability and IO Controls - address the technical foundation required for federated cloud interoperability and improved quality of service.
- Regulation and Carbon Footprint Values - outline expectations for cloud services to ensure compliance to government and corporate reporting requirements and outline a means for services to be CO2 aware for subscribers.

The Open Data Center Usage Models [50] are based on the following assumptions and principles. Each Usage Model defined by the Alliance has this paradigm as its base [51]:

1) Alliance members, principally medium and large enterprise IT organizations, will deploy and operate applications in multiple cloud infrastructure environments.
2) Cloud consumer will choose a unique mix of solutions from a Cloud-Provider(s) based on a unique set of business and technical requirements.

3) Cloud providers create cloud infrastructure environments for cloud consumers; they will do so by designing, building and operating those environments using standard, open and interoperable building blocks and interfaces in adherence with the principles outlined in the Alliance's initial publication of Usage Models and the Open Data Center Vision Statement.

5.2.5 EUROCLOUD STAR AUDIT CERTIFICATION PROGRAM

Eurocloud [52] developed the certification *Eurocloud Stard Audit to SaaS* [36] offers for cloud computing to help potential customers make informed decisions by the development of this certification program that gives a certificate that is a meaningful selection tool for the users.This certification program has the objective to build trust in cloud services in the provider and use side.

The EuroCloud SaaS Star Audit is suitable for any company operating a dedicated SaaS application. The audit aims to establish a high level of security and transparency for users and providers alike. The audit starts with the providers general profile, carries on with contract and compliance including data privacy protection, general security, operation and infrastructure, operation processes and goes as far as application and implementation.

The services providers that want to be a certification by EuroCloud Star Audit for SaaS process encompass the following categories:

- Provider profile
- Contract and compliance
- Security
- Infrastructure operation
- Application
- Implementation

Providers can earn one to five stars by way of point system and established set of minimum criteria. The core issues are legal aspects, reliable provision of technology services as well as data protection, data security and compliance with fundamental quality standards for operation processes and application format.

Eurocloud Star Audit Family is composed by:

- EuroCloud Star Audit SaaS - certifies SaaS Provider with 1 to 5 stars;
- Eurocloud Star Audit SaaS Ready - certifies DC-Provider with 4 to 5stars;

- EuroCloud Star Audit SaaS App - allows SaaS Provider to certify with 4 to 5 stars;
- eco/Eurocloud Datacenter Audit Certification [52] - certified cloud provider datacenter.

5.2.6 LEET SECURITY RATING GUIDE

Leet security [53] is a rating agency in the field of ITC services. Rating system [54]created by leet security is a security labelling mechanism based on five levels from A to E (being A the best case) which are assigned to three dimensions of security for each service rated: confidentiality, integrity and availability (CIA).

It is important to highlight that ratings are not assigned to vendors, as a whole; on the contrary, a rating is analysed for each of the services provided (in the same way, a vendor chooses which services wants to be rated, i.e., not all the services provided by a vendor must have a rating).

The rating system assigns every cloud service with a label, depending on the security measures it implements, the general conditions of the vendor and the resilience mechanisms in place. These labels provide information about the three dimensions of security because users requirements could be completely different in each and the label has to provide enough information for users to make better decisions on what service to buy (if they want to consider information security in their decision). So, when potential customers look for a cloud service, it should be easy for them to look at its security label and know which service offers the security conditions that fit their needs. The rating scope includes all the systems connected and not completely segregated for the systems directly involved in the service provision. Systems consist of people, processes and technology, like servers, applications and network components, including virtualized components.

Criteria analyzed by the rating methodology are divided into the following (14) chapters:

- Information security Management Program
- Systems Operation
- Personnel Security
- Facility Security
- hird-party processing
- Resilience
- Compliance
- Malware protection

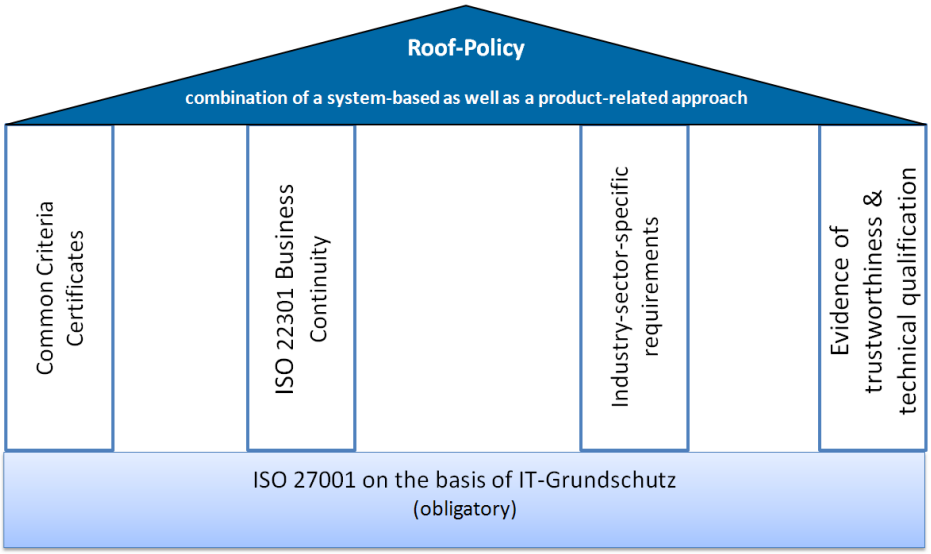
- Network controls
- Monitoring Access control
- Secure development
- Incident handling
- Cryptography

5.2.7 *BSI CLOUD CERTIFICATION APPROACH*

From a high level point of view, a cloud consists of software and hardware parts which are connected in a complex way. To get a valid security statement about such systems BSI [57] considers primary two points:

(1) Security statements about the processes within a complex system as well as
(2) Security statements about the robustness of the used products.

Hence a certification should combine a system-based as well as a product-related approach. The following figure visualizes the composition of different well known certification schemes.



The roof-policy (a Technical Guideline[1]) consolidates different accepted certificates in a Cloud Certification bundle. The bundle consists of a obligatory part, the system-based approach (ISO 27001 on the basis of IT-Grundschutz [40]) as well as product-related certificates for security critical parts on the basis of Common Criteria (e.g. hypervisors, operating systems, networking equipment, etc.). IT-Grundschutz uses a holistic approach to this process.

[1] This document is currently under development with input from a running pilot certification.

Through proper application of well-proven technical, organizational, personnel, and infrastructural safeguards, a security level is reached that is suitable and adequate to protect business-related information having normal protection requirements. IT-Gundschutz already includes five modules for cloud computing (Cloud-Management, Cloud Storage, Web Services, Virtualisation, Web Applications).

The IT-Grundschutz Certificate or a self-declaration offers companies and agencies the possibility of making transparent their efforts regarding IT security. BSI has defined three variants of the IT-Grundschutz qualification: the IT-Grundschutz Certificate and the self-declarations "IT-Grundschutz entry level" and "IT-Grundschutz higher level".

Issue of the IT-Grundschutz Certificate is based on an audit carried out by an external auditor licensed with the BSI. The outcome of the audit is an audit report which is submitted to the certification authority that decides on the issue of IT-Grundschutz Certificates. The baseline set of criteria on which the procedure is based is the latest version of the BSI's IT-Grundschutz Manual. The "Audit Scheme for Auditors" describes the audit procedure followed, the audit report, the decision and issue of the IT-Grundschutz Certificate.

Additional voluntary certificates from the domain of Business Continuity, industry-sector-specific requirements and evidences like statements about technical qualification etc. can be included. The modular approach allows different levels of trust which are currently under development.

5.2.8 US FEDERAL GOVERNMENT FEDRAMP PROGRAM

The US Federal Government created the Federal Risk and Authorization Management Program (FedRAMP) to provide a standardized approach to security assessment, authorization and continuous monitoring for cloud products and services [55]. According to the FedRAMP program, all Cloud Service Providers (CSP's) who would like to provide products or services to Federal Government departments and agencies have to be authorized by Third Party Assessment Organizations (3PAO's) which are themselves accredited by the FedRAMP program.

The FedRAMP program authorization and accreditation procedures follow the Federal Information Security Management Act (FISMA) and uses the *"NIST SP 800-53 R3 controls for low and moderate impact systems"* and adds some more controls specific to the requirements of cloud computing.

All federal agencies running cloud services and deployments at moderate and low impact level must meet the requirements of FedRAMP and services that began before June 2012 have until June 2014 to become compliant. Private cloud deployments for single agencies and implemented entirely in federal facilities are exempted.

The FedRAMP web site provides a list of Iaas, PaaS and SaaS services that meet FedRAMP requirements and are authorized to be used by federal agencies. The web site also provides a list of accredited 3PAO's that can be used by CSP's to receive authorization.

6 HITTING THE TARGET OF THE C4E VISION

This chapter contains a preliminary description of how the goals of the C4E project could be afforded, starting from the analysis of existing literature. It describes the types of approach (policies and strategies) of Member Countries to the deployment of Cloud computing in public sector, migration strategies and concrete actions.

The second part of the chapter first abstract concrete use cases and gives a description of three common business models, further relevant high level use cases are identified which group thematically similar use cases together.

6.1 COUNTRY SPECIFIC STRATEGIES

A good synthesis of the Governments approach to cloud is in [410]. That studies show as Government – mostly implicitly – have taken on several different roles with respect to their approaches to cloud computing. Although these categories have overlapping characteristics, one can analytically distinguish among six basic (or ideal-type) hig-level roles:

- Governments as Users – governments are adopting cloud computing services to take advantage of its costs savings and innovative features
- Governments as Regulators – acting through their legislative, judicial, regulatory branches, governments regulate to implement policy through the rule of law
- Governments as Coordinators – governments coordinate public and private initiatives, through standard setting processes, and by facilitating the sharing of information between private and public stakeholders
- Governments as Promoters – governments actively promoting the cloud industry by endorsement, funding, and incubation programs
- Governments as Researchers – governments conducting or funding research on technical or societal issues related to cloud computing
- Governments as Service Providers – governments providing cloud services for use by other government agencies or the public.

Pragmatically and more explicitely, governments adopt concrete strategies to fulfil concrete objectives. Some States have chosen, according to their social, economic and cultural characteristics, the path of cloud computing before the "European Cloud Computing Strategy", sponsored by the European Commission since 2012 for "unleashing the potential of cloud computing in Europe". Deliverable D3.2 will go in depth in the analysis of per Country strategies. Just as example, we resume in the following the strategies of four contries participating to the C4E project:

- **Portugal** government addressed its cloud strategy to reduce public sector costs and stimulate economic growth (based on its public spending review plan to reduction debt-to-GDP ratio).
- **The Dutch way** is characterized by attention to citizens' personal data with the aims to build a safe cloud infrastructure that will encourages the use of cloud computing on a larger scale.
- **Spanish Government** adapted a cloud strategy to its regionalism system, with the aims to fill its "digital divide" between central and local administrations using a private network of high speed called SARA.
- Finally, newcomer in April 2014, is the **Slovenian long term strategy** document on Cloud Computing, contained in the mission statement: "*Cloud Computing in Slovenia is a base for economic growth*". This document exposes three different goals for the implementation of Cloud Computing and three clouds deployment models to enable privacy friendly and legally compliant cloud services.

Each Country, as a concrete result of its own specific strategy, is promoting and implementing concrete actions. The recent study performed by Technopolis [403] clearly identifies three different approaches:

- **Procurement and Marketplace.** It's an emerging model for cloud focused on procurement. It generally relies on a procurement framework to allow easier purchase of cloud solutions and on a marketplace (like Apple App Store). This model is already operational in the UK (with G-Cloud and the CloudStore), which is clearly seen by other Member States as the flagship initiative, and is in development in the Netherlands and in Portugal. Some other Member States have also considered this approach. The idea with that model is to focus on cost savings and improvement of the local economy through a better involvement of local cloud suppliers. The general philosophy is to turn to the market for achieving more cost savings, through external providers' applications and even infrastructure (public cloud is indeed the main model). Efficiency is achieved through standardized processes and procedures

with pan-governmental accreditations and is easier to monitor in terms of actual adoption and savings targets.

- **Resource Pooling:** The second major emerging model involves resource pooling across administrations through a common central infrastructure and/or platform. This model is already operational in Spain with numerous applications around the Sara Network and is currently in deployment in France (DILA, pilot), Belgium (Fedict) and the Netherlands (also an adopter of the first model). The main idea is to get the infrastructure right first around a private cloud, allowing for more potential developments for critical or sensitive applications. But, in reality, initiatives focus so far on IaaS solutions rather than applications.
- **Standalone applications.** This model involves isolated standalone applications developed by Ministries on their own. There is no real central coordination in this model (even when a central policy does exist). In most of the cases, the effort is concentrated on the cloudification of existing applications (especially for horizontal solutions). Those applications may be already quite advanced in terms of features, implying often advanced requirements and need for back-up systems. The cloud adoption for these applications is clearly driven by cost savings objectives.

Of course, the implementation of these strategies follows phased approach. First build an internal private (or community) cloud. And when business continuity, security, dataprotection of public cloud suppliers is at a sufficient level, move to using public cloud services.

6.2 MIGRATING TO THE CLOUD: STRATEGIES AND REQUIREMENTS

Migration to the cloud may pose a challenge for organizations, as it requires planned, coordinated and multidisciplinary approach. In this section we will review the state of the art in standards, recommendations and literature. The papers reviewed include the studies accomplished for several European governments and notable recommendations issued by other countries or international and expert standardization bodies. The general recommendations and requirements for cloud migration are presented in the following six sections, which correspond to the top-level groups identified in the literature.

6.2.1 *DETERMINING ECONOMIC IMPACT*

Cost reductions and optimizations are identified as one of the cloud adoption drivers. However, often it is not easy to evaluate and estimate their exact effect on the performances of the organization and furthermore of all involved stakeholders.

For such an evaluation the impact horizon can be identified on two levels. The first one is related to macro environment, which includes the entities directly and indirectly involved in the organization's sphere, going up to national or even international level, trying to consider all the effects of internetworked relationships between organizations and aggregate added value and developments brought in by cloud transition.

Analysis of the impacts of macro environment has been subject of study performed for Spanish government [78]. The study provided models for calculation of impact of cloud transition on Gross Domestic Product (GDP) development, demonstrating the process of valuation of influence on aggregate employment and public finance.

More tangible impact of cloud migration for individual organizations may be identified within organization boundaries – its evaluation should be a starting point in every organizational planning. At that level, the approximate outcome of the service migration might be assessed by using quantitative models. These models are usually based on the analysis and comparison of different investment alternatives and options, involving the metrics such as TCO (Total Cost of Ownership), ROI (Return of Investment) as well as IRR (Internal Rate of Return) or CoC (Cash-on-Cash Return). The metrics are to be considered from the perspective of capital, operational and opportunity costs.

These methodologies and approaches on quantitative measuring of expected cloud adoption benefits vary based on the target group or specific application. Many of those methodologies focus on specific area or category only. Usually the vendors and system integrators offer their framework and tools to assist in this task. Examples of these are solutions from Microsoft, VMware and HP [90], [93], [73].

Vendor neutral cost assessment approaches such as [74] consider different costs types, indirect costs and take into account possible losses. Their models include also the process-related costs, such as strategic decision and cloud selection making, system failure and the costs related to back-sourcing and discarding.

The benefits quantification should take into account the broader application type of the use case. Further it might require special domain related view and metrics, as demonstrated in

[75], which describes the framework for assessing economic impact of cloud adoption and use for research application. The study performed by ONTSI and Deloitte in Spain [78] focused on specific microeconomic definitions and provided various use cases, templates and measures to facilitate the cost and benefit assessment of cloud adoption for public administrations. Based on various examples they demonstrated the method to connect objectives, principles and results, showing how to derive and quantify specific measures for each desired outcome.

The recommendations for public institutions, based on research conducted for Italian government by DigitPA group suggest that, regardless of the cost calculation model being applied, the time horizon for cost-benefit consideration should be based on medium to long-term appraisal. This is essential in order to avoid the risks of an analysis influenced by the costs of migration expected in the early stages of a cloud computing project, as well to consider the costs that are absent in projects that maintain unchanged processes, applications and technologies [76].

Finally, the requirement presented in [77] stresses the necessity to have defined and implemented cloud service metrics, which role is to facilitate constant comparisons, provide monitoring capabilities and help to increase understanding of application costs and its units of standard metrics. The economic estimation of the cloud adoption should not be taken only in the preparation phase of migration. Based on NIST requirements, these metrics and even the cost-estimating model alone should be the subject of reevaluation and revision in the function of time. It is furthermore advised to reassess the metrics periodically and compare them with previous expectations and desired outcomes. The costs and benefits should not be reconsidered only internally, but the market state, technology advancements and new services and product portfolios should be taken into account in updated execution cycles.

6.2.2 *PLANNING TO CHANGE*

As the systems, standards and landscape are evolving, it might be crucial to follow an agile, flexible approach in the process of cloud migration. It is, therefore, not only suggested to rely on phase-based planning, implementation and service deployment, but to structure the migration process on that way that it includes and presumes the possibility for repetitive executions and iterative improvements of the services.

In its vision of G-Cloud for Italy, Microsoft suggested such dynamic approach [82], by recommending initial mapping (setup) and constant reassessment (refresh) of demand by institutions. According to their recommendation, the planning should be both user and

service oriented, requiring the constant reevaluation of the possibilities and search for new opportunities. The vision presented by Microsoft is based on contractual system that is flexible enough to enable bidirectional information flow and live adoption to the new realities and potentials resulting from new technologies, architectures, applications or service models.

Recommendations by *NIST Technical Considerations for US Government Cloud* similarly include the context awareness notion as mentioned in *Requirement 5* [77]. It points out that it is required to understand the value and benefits of cross-agency demand aggregation, functionality integration and collaboration, which may derive new opportunities and leverage synergistic and networking effects. Other requirements mention cloud service metrics and imperative to define them and apply iteratively during the course of process execution. That way it would be possible to obtain the performances overview of service costs and categories of metrics, reassess and reevaluate them in the function of time. Such approach might also provide new metrics, which might be applied to get even more detailed insights.

6.2.3 *STRUCTURING ASSESSMENT PROCESS AND DECISION MAKING*

Not all applications, processes or services within organization might be perfect candidates for migration to the cloud, nor they could have equal priority or would provide similar business value or effects, once migrated. Furthermore, the impact of their migration might vary according to the overall phase and institutional readiness for the cloud. The whole cloud transition process might involve diverse transition stages, each one reflexing particular maturity level and its impact on interconnected landscape. Therefore, the selection of the services or assets to be moved to the cloud, as well as their respective priorities and impacts, are the subject of the previous planning and strategic decision.

The importance of decision making process has gained specific attention and as such was included in US Federal Cloud Computing Strategy. Decision Framework for Cloud Adoption [79] was further reviewed in NIST Technical Considerations for US Government Cloud [77]. The framework defines three important stages both for the cases of moving or creating applications for the cloud, as following:

- Selecting service to move to a cloud
- Provisioning cloud services effectively
- Managing services rather than assets

For the selection of services to be moved, considered as important are not only the particular organisation's readiness, but also the overall readiness of the government, network infrastructure and market state, as well as technical and data prerequisites.

The framework further urges organisations to perform mind-set or paradigm shift: the attention of all parties involved should be re-focused to services, rather than assets, which should be actively monitored and periodically re-evaluated. Finally, in the document provided is the mapping of *USG Cloud Computing Technology Roadmap*, whereas all ten requirements originating from the roadmap [80] were expanded and integrated into decision making process.

6.2.4 *FOLLOWING GOOD PRACTICES*

In its study of operational government cloud infrastructures [81], ENISA identified three main categories of recommended best practice approaches, as follows:

- A governmental cloud catalogue
- Consolidation of existing clouds
- Building national cloud infrastructure based on open source

Based on this study, it is recommended the governments to take the step to eliminate the drawbacks that are keeping the public bodies from going into the cloud by establishing cloud catalogue. The catalogue based approach should represent an intermediary solution for contract enforcement and security accreditation, assuming that the providers and services included in the catalogue conform to the compliance of baseline set of security requirements and other measurements and metrics. The public institutions therefore are suggested to, where possible, stick to the services offered through intermediary, standardized and preapproved solution, structured and accessible through the form of governmental cloud catalogue.

Furthermore ENISA suggests basing the cloud solutions on open source stack, identifying the main advantages of such approach:

- Greater scalability level
- Service is open to everyone
- Customer lock-in mitigated
- Low administration costs

- Innovation capacity based on low costs and wide potential network of innovators and integrators
- Streamlined data law compliancy

In the same document ENISA suggested ten recommendations, applicable at the various levels of authorities. In the context of particular organizations the most applicable are the following grouped recommendations:

- Business sustainability model
- Addressing "*loss of control*" and "*locality*" issues
- National and EU law compliance
- Application of common SLA frameworks and certifications

Similarly, the good practice for public authorities identified in study for Spanish government [78] is to perform migration process progressively and carry it in controlled transition processes. It has been advised to begin with the IT process or component that is not critical and that allows for the development of a pilot process. The next recommendation from the same document suggests to study the market and analyse existing solutions prior to the cloud migration, in order to evaluate the real capacity of providers to respond to the cloud technology demands. After the project is executed and migration done, the staff in the public organisation should be allocated to the functioning system, being previously trained in management and monitoring of service level agreements and in the performances of service audits.

In the phase of solution selection and contract negotiation, [76] identifies the following actions:

- The use of standardized framework for the evaluation of suppliers. The check lists can be partitioned into domains that have the goal of understanding whether and how supplier can meet the requirements of a user of cloud services.
- The compliance of the terms should be constantly monitored during the execution phase and compared with the user requirements and contractual terms.

For such purpose the public administrations can apply frameworks such as *Information Assurance Framework* [89] and *Security and resilience in governmental clouds* [85] – both by ENISA, as well *as Cloud Control Matrix Security* [91] by CSA.

6.2.5 *CONTRACTUALISATION AND LEGAL ASPECTS*

Applying the traditional patterns of legislation on the context of cloud raises new questions and issues as it stretches through different organisation boundaries, and very often can include cross-country collaboration and data transfer. The cloud market is still young market and not all services are defined and mature to entirely face the various customer or service types and cover majority of the cases for each market, customer or jurisdiction. Consequently is the responsibility to ensure proper legal conformance of the service contract and define the quality levels of obtained service proportionally higher and more demanding for public authorities.

Study done for Italian government [84] emphasizes the importance of proper contractualisation, which presumes defining the clear and unambiguous responsibilities and service level expectations. As the potential problems with higher significance and occurrence they mention issues such as inadequacy of contracts, inability to negotiate contract terms, the complications related to governing laws and jurisdictions as well as failures to comply with privacy legislations. Further noted are possible loss of governance, lock-in on various levels and reflections of legal action on other customers.

Additionally identified by [86] and [87] are the following categories of issues:

- Providers offer one-sided contracts, containing provider-friendly terms and little or no opportunity to negotiate or change
- There are no accepted standards for contract terms or service levels for non-routine undertakings
- Products and services are offered 'as-is', without any representations and warranties
- Sole responsibility for adequate security, data protection and backups are imposed on customer
- Providers tend to disclaim all liability for direct or consequential damages
- On-line forms are often incorporated, which are subject to unilateral change or even deletion
- Providers retain universal right to suspend service or terminate contract
- Many contracts are lacking clear descriptions of responsibility attributable to the provider

Some of the issues arise from the fact that many cloud providers are newcomers, with little outsourcing or software licencing experience, highly dependent on third party software and

platform providers and therefore unable to flow down the requested contractual commitments.

From that point it is necessary for the public administrations planning to migrate to the cloud to identify, case by case, what types of data are intended to be transferred to the cloud and define the respective expectations, obligations and responsibilities, enforcing their clear reflection in the cloud contracts.

For the purpose of data protection [76] recommends designation of specific *Privacy Level Agreement* (PLA), which should define levels and warranties related to the protection and security of personal data by the cloud provider. It could tightly define the mode of data encryption and its control by public administration, restrictions on transfer of the data, traceability of actions on data and related responsibilities. Further it could state the guarantees of portability and policies of persistence and retention.

In the terms of *Service Level Agreements* (SLA) and related penalties, the exact nature of monitoring metrics, penalties as well as the parties and processes used to estimate the level of obligation fulfilment of these commitments should be thoroughly analysed. In some cases providers define themselves as solely responsible side to assess level of fulfilment of the contract. In other cases providers define additional risks separately from SLA, excluding some objective circumstances from it and thus objectively and effectively changing its scope.

The sole existence of SLA and related penalties should be taken in the risk assessment and not accepted per se without detailed consideration. Some providers offer SLA penalties in financial terms which pose symbolic fines in regards to the possible loses done on customer side. Such points should be clearly identified by public authorities as they might provide only incorrect information or expectation on service availability or quality level.

One of the approaches used to bootstrap legal analysis is methodology offered in [85], which starts by analysing the following questions:

- Which services identified in the scenario is the Public authority (PA) considering migrating to the cloud?
- Are there specific laws or regulations that apply to the services and what are the relevant duties or obligations imposed upon the PA (eg. data retention, data protection, interoperability, medical file management, disclosure to authorities)?
- What is the nature of the data or information that would be processed with these services?

- What are the specific legal provisions that apply to the types of data or information that will be processed and what are the relevant duties or obligations imposed upon the PA (such as data protection, intellectual property, confidentiality, security)?
- What is the data or information flow (internal and external) during the operation of these services?
- Who are the subjects (natural and/or legal persons) involved in the operation of the services and what are their roles (responsibilities, duties, obligations, and liabilities)?

Other perspective on possible legal risks is given in [86] in which ENISA provides detailed descriptions and templates for assessment of legal risks and preparation of possible mitigations.

6.2.6 *RISK ASSESSMENT AND SECURITY*

Risk assessment is one of the crucial steps necessary to be evaluated prior to the cloud migration. It may stretch in various aspects, such as legal, organisational, financial, technical, and especially privacy and security related.

One of approaches to perform risk assessment defined in [84] starts from the question "*What kind of damage would be created if …* ". Their methodology applied to answer, in broad terms, the requirements of confidentiality, integrity and availability. For each asset or service concerned it considers the following set of question:

What kind of damage would be created if [84]:

- The valuable asset becomes publicly available?
- The employee of service provider has access to valuable asset?
- The process or functions are fraudulently manipulated by an attacker outside?
- The process or function did not provide the expected results?
- Information or data are modified in unauthorized manner?
- The valuable asset is not available for a given period of time?

The publication of Rosado et. al [92] provides the broader analysis of security related issues and migration processes, providing the overview on diverse approaches performed to migrate to the cloud, such as migration of legacy applications, migration of services and their reuse and integration.

The both [92] and [86], beside the risks, mention also the benefits and namely security benefits arising from the cloud migration, which might positively impact the overall services,

their quality, reliability and availability. With that uncovered are also perspectives which were not available with the legacy deployments, such as usage of multiple locations, integration of edge networks, improved timeliness of response to incidents or threat management.

In study from ENISA [86] it is explicitly demonstrated how security can be used as a market differentiator, by providing rapid and smart scaling of the resources and standardized interfaces for managed security services. In such scenario the audit and SLA may enforce better overall risk management and awareness.

The studies by ENISA [85] and [86] further provide risk assessment framework based on use-case scenarios and impact assessment risks, which may be applied by public authorities in the process of risk management. On the other side [77] defined the list of high-priority security requirements, identifying four areas of security assessment. The first one relates to improving the situational understanding in cloud security context, which takes into account the cloud service model perspective, security architectures, the implications of cloud deployment and broadens understanding of shared security responsibilities.

Under the area of process oriented requirements NIST Technical Recommendations [77] advised several crucial processes to be taken, such as cloud audit assurance, log management and privacy guidelines, followed by assessment of providers' trustworthiness, business continuity and disaster recovery. Other areas covered by their recommendations include challenging risk-mitigations and definition of focused technical requirements.

Recommendations by the Agency for Digital Italy (former DigitPA) study [76] emphasized the importance of portability and interoperability between different clouds, and recommendation to use proper auditing, incident reporting and response facilities. The identification of the chain of responsibility and providence service resilience models were also included as recommendation by the Agency for Digital Italy.

6.3 KEY USE CASE SCENARIOS FOR THE FUTURE OF CLOUD SERVICES IN PUBLIC SECTOR

6.3.1 *BUSINESS MODELS*

Regarding Public Administrations, three main use case models, differing in cross-border relevance and usage scenario can be identified [71]:

- *Government to Citizen:* The Government to Citizen Communication models the interaction between governments and citizens. The information transfer may take place in the citizen country, but may also take place in foreign European countries to i.e. use services provided by European governments. Government to Citizen Relationships cover: electronic applications, notifications, eParticipiation, eCollaboration, access to open data, tax return or complain/concern management [71].

Figure 12: Government to Citizen

- *Government to Business:* The Government to Business communication models the interaction between governments and the commercial business sector to provide business related information to ease the realization of business processes. Government to Business relationships may cover: electronic procurement, notifications and access to open data. [71] Because the communication may also take place across country borders services using this model also need to tackle cross-border issues.

Figure 13: Government to Business

- *Government to Government:* The Government to Government communication models the interaction between governmental organization in one country and also cross-border. The relationships may cover: electronic support for federated, cross-governmental process, shared repositories or information systems. [71]

Figure 14: Government to Government

All use-cases have in common that very sensitive and personal information is processed, therefore data protection and data security is inherently important for all services.

6.3.2 HIGH LEVEL USE CASES

This section introduces high level use cases for cloud computing relevant for the public sector. Each high level use case contains a single detailed use case representing the family of use cases best. The scope of this document is to only describe the problem which can be solved using cloud computing, an aimed solution description is not part of the scope.

- *Assure Quality - Audit Service:* Governmental services operate on sensitive, personal and confident data. It is inherently important that services operate as they are designed and data remains protected and secure and service operation is not influenced by provider outages.

  The use case representing this family best is *"Independent third party assurance"*:
  Actors: Provider, Partner
  An independent third party assurance to guarantee sustainability will contribute to build trust among governmental organizations / public bodies using cloud services.
  In line with recommendation 2 of the report "Good Practice Guide for securely deploying Governmental Clouds" (ENISA, 2013), and based on use case 108 of the Cloud Standards Coordination report (ETSI, 2013), the idea is to establish a kind of active and proactive independent escrow service by a third party. This party should assure a seamless takeover of the cloud operations that provider A executes for a governmental organization to cloud provider B. This should therefore include the (functionality of the) software, the users' data and the current state of transactions. This service should meet reliability, security and privacy requirements of governmental organizations using this service. [72]

- *Operate Service – Manage:* One reason for considering migration to the cloud is that the availability is increased because the services are not hosted "in-house", but the

operator also gives away a lot of control. This involves the establishment of strict service level agreements between the Customer (Public Administration) and the cloud provider. This use case family tackles with use cases concerning end-to-end quality, uptime guarantee, service continuity and disaster recoveries. This closely works together with technologies like intercloud communication and broker mechanisms.

One detailed use case of this family is "Burst Capacity":
Actors: Provider, Partner
A system or service runs in a defined "source" location, to overcome bursts it uses intercloud mechanisms to absorb bursts by utilizing alternate locations or cloud environments such as a shared or public cloud (target) to obtain additional resources. This happens transparent to the user, the service remains up and the operation is not disturbed in any way. It requires license flexibility, and sufficient network and security controls. Further it may also be possible to react pro-active to avoid high bursts by providing location aware load balancing.

- *Operate Service – Migrate:* Migration always concerns two aspects (a) migration of existing legacy applications to cloud environments and (b) migration of existing cloud applications from one provider to another. Migrating existing legacy applications is a very time consuming task and is one of the main reasons why public administrations chose to not deploy to the cloud. After the migration is performed it is inherently important that services can be moved between cloud providers seamlessly and vendor lock-in is avoided. This massively eases disaster recovery or migration on provider bankruptcy.

  To underline the importance of interoperability and avoid vendor lock-in the use case "Changing Cloud Vendors" is described here:
  Actors: Provider
  An organization using cloud services decides to switch cloud providers or work with additional providers. To perform the migration seamlessly it is inherently important that all participating cloud providers work on the same basis of interfaces and interaction possibilities.

- *Operate Service – Monitor:* Monitoring is an important component of every system/environment. Concerning cloud computing, monitoring is more challenging than in classical IT deployments because the customer may request reports

concerning single services, but the cloud provider may spread the operation of the service across different data centers and may need to collect the required data. The situation even gets more complex if hybrid-cloud deployments are used, where the customer needs to monitor internal resources (private cloud) but also relies on external monitoring services from external cloud providers (public cloud). In fact, customers migrating services to cloud need monitor solutions which observe cloud applications alongside with internal IT systems.

The core use case in this family is "Monitoring & management of deployed software":
Actors: Provider, Partner
Monitor the health of infrastructure & perform capacity planning for future needs. A service has been configured and is in operation. Certain conditions or runtime operational events have been identified or detected that are significant enough to demand immediate notification of the condition or event to the service customer. An example is the detection of an intrusion or an unexpected configuration change.

- *Operate Service - Provision/Configure/Administer:* This use case family tackles with the provision, configuration and administration of existing or new cloud nodes. It needs to be suitable to use existing virtual machine images or create new ones. One of the main advantages of cloud computing compared to classical IT system is that flexibility is inherently increased, flexibility involves that new resources (e.g. in the form of new computing nodes, deployed automatically) are provisioned on demand and paid-by-use. This approach includes that currently unused resources are freed to decrease costs.

  One use case in this family is the "Deploy Machine Image" use case:
  Actors: Customer
  The cloud consumer wishes to create a new instance of a "machine" (a logical instance of one or more CPUs connected to local memory and, optionally, local data storage) with software loaded from a machine image.

- *Operate Service – Terminate:* This use case family contains (a) use cases for service contract termination and (b) use cases for cloud contract termination:
  Terminating cloud contract:
  Actors*:* PaaS customers; developers, SaaS providers; solution provider

An organization (cloud service customer) obtaining a cloud service from a cloud service provider directly or via a cloud service partner (a broker) would like to terminate its contract. There can be many reasons for doing so, for example the organization would like to change cloud service provider of partner or wants to move to a non-cloud environment. The use case is focusing on the terms and conditions that should be in a SLA, and the enforceability of those terms and conditions to do so.

- *Prepare & Procure Service:* This class of use cases refers to all use cases/services described in the service catalogue. For details on the services to be procured refer to Service Catalogue defined in Deliverable D4.1.

- *Setup Cloud Service:* This class of use cases refers to services providing reusable components or templates which can be used/purchased by customers and deployed.

7 CONCLUSIONS

This deliverable is a contribution to the definition of the research and development services to be procured by the Cloud for Europe PCP process. Most of the contributions are on the technical side, and specifically regard Cloud computing reference architectures, standardization and certification. Chapter 4 and 5 give an exhaustive view of the status of the art in these fields.

On the other side, the deliverable is also a first step of the Workpackage 3 towards a clear identification of key gaps to be addressed by the project. It identifies a methodology to reach this goal and defines the way these gaps will be represented: mainly through the definition of a target scenario (target ecosystem) and the description of key use cases that can be implemented in that scenario. Deliverable D3.2 and D3.3 will give specific contributions to reach this goal, respectively as the result of the analysis of the government position and of the market position.

8 REFERENCES

The following references contain information that may be valuable to the reader of this Report, and provide additional information about topics covered within this Report.

[1] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," NIST, Special Publication 800-145, 2011.

[2] E. Commission, C. From, T. H. E. Commission, T. O. The, T. H. E. Council, T. H. E. E. Economic, T. H. E. Committee, and O. F. The, "Unleashing the Potential of Cloud Computing in Europe," 2012.

[3] G. A. Lewis, "The Role of Standards in Cloud- Computing Interoperability," no. October, 2012.

[4] V. Ersion, "Cloud Standards Coordination Final Report November 2013," no. November, 2013.

[5] ITU, "TU-T Study Group 13 - Future networks including cloud computing, mobile and next-generation networks." [Online]. Available: http://www.itu.int/en/ITU-T/about/groups/Pages/sg13.aspx.

[6] N. Networks and C. Computing, "ITU-T," 2013.

[8] B. R. Analysis, "D1.3.1," 2011.

[9] F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, and D. Leaf, "NIST Cloud Computing Reference Architecture Recommendations of the National Institute of Standards and."

[10] NIST, "NIST Cloud Computing Standards Roadmap," Jul. 2013.

[11] T. Leadership and W. Paper, "Getting cloud computing right," no. April, 2011.

[12] "IBM Cloud Computing Reference Architecture," vol. 3, no. 1, p. 2012, 2012.

[13] A. Oracle, W. Paper, O. Enterprise, and T. Solutions, "Cloud Reference Architecture," no. November, 2012.

[14] W. Paper, O. Cloud, and S. Incubator, "Interoperable Clouds A White Paper from the Open Cloud Standards Incubator," pp. 1–21, 2009.

[15] F. G. C. Tr, "FG Cloud TR," vol. 0, 2012.

[16] ATIS, "Telecommunications Industry Solutions (ATIS)." [Online]. Available: http://www.atis.org/.

[17] "Cloud Security Alliance (CSA)." [Online]. Available: https://cloudsecurityalliance.org/.

[18] "Cloud Services Measurement Initiative Consortium (CSMIC)." .

[19] "Distributed Management Task Force (DMTF)." [Online]. Available: http://www.dmtf.org/.

[20] "European Telecommunications Standards Institute (ETSI)." [Online]. Available: http://www.etsi.org/.

[21] IEEE, "IEEE (Institute for Electrical and Electronics Engineers)." [Online]. Available: http://www.ieee.org/.

[22] "International Standards Organization (ISO)." [Online]. Available: http://www.iso.org/.

[23] "International Electrotechnical Commission (IEC)." [Online]. Available: http://www.iec.ch/.

[24] NIST, "NIST (U.S National Institute of Standards and Technology)." [Online]. Available: http://www.nist.gov/.

[25] "Organization for the Advancement of Structured Information Standards: (OASIS)."

[26] "Open Data Center Alliance: The Open Data Center Alliance (ODCA)." [Online]. Available: http://www.opendatacenteralliance.org/.

[27] "Open Grid Forum: The Open Grid Forum (OGF)." [Online]. Available: http://www.ogf.org/dokuwiki/doku.php.

[28] "Storage Networking Industry Association (SNIA)." [Online]. Available: http://www.snia.org.

[29] "Telecommunications Industry Association (TIA)." [Online]. Available: http://www.tiaonline.org.

[30] NIST, "NIST Inventory of Standards Relevant to Cloud Computing." [Online]. Available: http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/StandardsInventory.

[31] M. A. C. Dekker and D. Liveri, "Certification in the EU Cloud Strategy," no. November, pp. 1–43, 2014.

[32] ISO, "INTERNATIONAL STANDARD ISO / IEC 27001 Information technology — Security techniques — Information security management systems — Requirements," vol. 2013, 2013.

[33] ISO, "ISO 20000 Certification."

[34] ITIL, "Information Technology Infrastructure Library (ITIL)." [Online]. Available: http://www.itil.org/.

[35] CSA, "Cloud Security Alliance (CSA)." [Online]. Available: https://cloudsecurityalliance.org/.

[36] E. Star and A. Certificate, "Software as a Service," 2011.

[37] "Leet security, 'Rating guide.'"[Online]. Available: http://www.leetsecurity.com/rating-guide.

[38] P. Copy and R. C. Young, *A Business Framework for the Governance and Management of Enterprise IT*. .

[39] O. Data and A. L. L. R. Reserved, "Open Data Center Alliance USAGE MODELS:," 2011.

[40] "BSI - IT-Grundschutz Certification Approach."

[41] "FedRAMP." [Online]. Available: http://cloud.cio.gov/fedramp.

[42] ISACA, "ISACA." [Online]. Available: http://www.isaca.org/.

[43] I. Standard, "INTERNATIONAL STANDARD ISO / IEC 20000," vol. 2005, 2005.

[44] V. Arraj, C. Process, and P. Llc, "ITIL ®: the basics," no. July, 2013.

[45] ITIL, "ITIL ® Service Management Practices V3 Qualifications Scheme Contents."

[46] I. Standard, "INTERNATIONAL STANDARD ISO / IEC 38500," 2008.

[47] V. Statement, "Open Certification Framework," no. August, 2013.

[48] CSA, "Consensus Assessment Questions (Cloud-Specific Control Assessment)." [Online]. Available: https://downloads.cloudsecurityalliance.org/initiatives/cai/CSA-CAI-Question-Set-v1-1.xlsx.

[49] CSA, "CSA CLOUD CONTROLS MATRIX VERSION 3.0." [Online]. Available: https://downloads.cloudsecurityalliance.org/initiatives/ccm/CSA_CCM_v3.0.xlsx.

[50] C. G. Nickell and C. Denyer, "An Introduction to SAS 70 Audits," vol. 20, no. 70, pp. 58–69, 2007.

[51] AICPA, "American Institute of Certified Public Accountants (AICPA)." [Online]. Available: http://www.aicpa.org/.

[52] O. D. Alliance, "Open Data Center Alliance." [Online]. Available: http://www.opendatacenteralliance.org/.

[53] ODCA, "Open Data Center Alliance Usage Models." [Online]. Available: http://www.opendatacenteralliance.org/ourwork/usagemodels#securefederation.

[54] Eurocloud, "EuroCloud." [Online]. Available: http://www.eurocloud.org/.

[55] D. C. Stars, D. S. Audit, P. Datacenter, and S. Audit, "Level of Performance Datacenter Star Audit," 2010.

[56] "Leet Security." [Online]. Available: http://www.leetsecurity.com.

[57] "Bundesamt für Sicherheit in der Informationstechnik (BSI)." [Online]. Available: https://www.bsi.bund.de/EN/Home/home_node.html.

[73] HP CloudSystem TCO Calculator, http://www8.hp.com/us/en/cloudsystem-matrix/tco-calculator.html

[74] B. Martens et al: Costing of Cloud Computing Services: A Total Cost of Ownership Approach, 2012 45th Hawaii International Conference on System Sciences

[75] Cloud Computing Economics: An evidence-based approach for Research Applications. e-InfraNet WP3 Deliverable

[76] Cloud Computing and Public Administration – Recommendations and Proposals. DigitPA, June 2012

[77] Technical Considerations for USG Cloud Computing Deployment Decisions, NIST Draft, October 2011

[78] El Estudio Cloud Computing. Retos y Oportunidades. May 2012.

[79] V. Kundra. Federal Computing Strategy. February 2011.

[80] US Government Cloud Computing Technology Roadmap Volume I, November 2011

[81] Good Practice Guide for securely deploying Governmental Clouds, ENISA, 2013

[82] G-Cloud: un'opportunità per la Pubblica Amministrazione e per il Paese. Microsoft. February 2013

[83] Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services. Queen Mary University of London, School of Law. 2010.

[84] Cloud Security: una sfida per il futuro. Ministry of Economy and Finance, Italy. 2011.

[85] Security & Resilience in Governmental Clouds. Making an informed decision. ENISA. 2011.

[86] Cloud Computing: Benefits, risks and recommendations for information security. ENISA. December 2012.

[87] Four Risky Issues When Contracting for Cloud Services. Gartner. 2011.

[88] Contracting for Cloud Computing Services — Clear Skies or Stormy Weather? AAC America - Association for Corporate Counsel. June 2012.

[89] Cloud Computing Information Assurance Framework. ENISA. 2009.

[90] VMWare ROI TCO Calculator http://roitco.vmware.com/vmw/Content/VMware_ROI_TCO_Calculator_Guide.pdf

[91] Cloud Controls Matrix. Cloud Security Alliance. September 2013.

[92] D. Rosado et al. Security Analysis in the Migration to Cloud Environments. Future Internet 2012.

[93] Microsoft Integrated Virtualization ROI Tool, https://www.microsoft.com/canada/virtualization/why/roi/default.mspx

[103] "European Cloud Computing Strategy: public sector adoption, key action, state of the play and Cloud for Europe" Ken Ducatel DG-Connect, slide presentation October 30, 2013.

[112] "Opinion of the Committe on Legal Affairs on Unleashing the potential of cloud computing in Europe", 23 septembre 2013

[401] "Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Up-take", SMART 2011/0045, D4 - Final Report, International Data Corporation (IDC), July 13, 2012.

[402] "Towards a good practice guide for securely deploying Governmental Clouds", European Union Agency for Network and Information Security (ENISA), November 15, 2013.

[403] "Analysis of cloud best pratices and pilots for the public sector", Study Report, Technopolis Group, September 20, 2013.

[404] "Analysis of cloud best pratices and pilots for the public sector", Appendix C to the Study Report – Country reports, Technopolis Group, September 20, 2013.

[405] "The Future of Cloud Computing", Opportunities For Eropean Cloud Computing Beyond 2010, European Commission – Information Society and Media, Expert Group Report, Public Version 1.0, Rapporteur for this Report: Lutz Schubert [USTUTT-HLRS], Editors: Keith Jeffery [ERCIM], Burkhard Neidecker-Lutz [SAP Research], January 26, 2010.

[407] "The Economics of Cloud Computing", Federico Etro – IUP Journal of Managerial Economics, May2011, Vol. 9 Issue 2, p7-22. 16p.

[408] "SIIA Comments: EU Public Consultation on Cloud Computing", Software & Information Industry Association (SIIA), August, 2011.

[409] "BSA Global Cloud Computing Scorecard: A Clear Path to Progress", BSA – The Software Alliance, 2013.

[410] "Governments and Cloud Computing: Roles, Approaches, and Policy Considerations", The Berkman Center for Internet & Society at Harvard University, Urs Gasser and David R. O'Brien, Research Publication No. 2014-6, March 17, 2014.

[503] "Advances in Clouds: Research in Future Cloud Computing", European Commission, Expert Group Report, Public version 1.0, Editors: Lutz Schubert [USTUTT-HLRS] – Keith Jeffery [STFC], January, 2011.

[504] "A Roadmap for Advanced Cloud Technologies under H2020: Recomendations by the Cloud Expert Group", European Commission – Digital Agenda for Europe, Editors: Lutz

Schubert [USTUTT-HLRS], Keith Jeffery [ERCIM], Burkhard Neidecker-Lutz [SAP], December, 2012.

[505] "Cloud for Science and public authorities: Final Report – A study for the European Commision, DG Communications Networks, Content & Technology", European Commission – Digital Agenda for Europe, study carried out for the European Commission by International Data Corporation (IDC) and Trust-IT Services Ltd, July 18, 2013.

[506] "US Government Cloud Computing - Technology Roadmap - Volume 1 – Release 1.0 (Draft) – High-Priority Requirements to Further USG Agency Cloud Computing Adoption", National Istitute of Standars and Technology – US Department of Commerce, November, 2011.

[507] "Cloud Computing in the public sector: rapid international stocktaking", Neil Robinson, Rebecca Schindler, Jonathan Cave and Janice Pedersen, Prepared for the Netherland's Ministry of Internal Affairs and Kingdom Relation (BZK), August, 2010.

[508] "The Future of Cloud Computing: 3RD Annual Survey 2013", North Bridge Future of Cloud Computing Survey in Partnership with GigaOM Research, 2013.

[509] "COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: Against lock-in: building open ICT systems by making better use of standards in public procurement", European Commision, COM(2013) 455 final, Brussels 25.6.2013.

[510] "EUROPEAN COMMISION DECISION: on standard contractual clauses for the transfert of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, 12.2.2010.

[701] "Cloud Computing Use Cases: White Paper – Version 4.0", produced by Cloud Computing Use Case Discussion Group, July 2, 2010.

[702] "Identity in the Cloud Use Cases – Version 1.0", Organization for the Advancement of Structured Information Standards (OASIS), May 8, 2012.

[703] "Identity in the Cloud Gap Analysis – Version 1.0", Organization for the Advancement of Structured Information Standards (OASIS), November 25, 2013.

[705] "Uses Cases and Interactions for Managing Clouds: A White Paper from the Open Cloud Standards Incubator – Version: 1.0.0", Distribuited Management Task Force (DMTF), June 8, 2010.

[706] "Cloud Computing Use Cases – Version 1.0", Cloud Standards Customer Council, October, 2011.

9 ANNEX 1 - CLOUD COMPUTING STANDARDS LIST

SDO	**Standard Reference**	**Title**	**Date**	**Available online**
ATIS	ATIS-0200003	CDN Interconnection Use Case Specification and High Level Requirements	Jun-11	http://www.atis.org/docstore/product.aspx?id=25633
ATIS	ATIS-0200004	CDN Interconnection Use Cases and Requirements for Multicast-Based Content Distribution	Jan-12	http://www.atis.org/docstore/product.aspx?id=26078
ATIS	ATIS-0200005	Cloud Framework for Telepresence Service	Fev-12	http://www.atis.org/docstore/product.aspx?id=26079
ATIS	ATIS-0200006	Virtual Desktop Requirements	Mai-12	http://www.atis.org/docstore/product.aspx?id=26147
ATIS	ATIS-0200008	Trusted Information Exchange (TIE)	Out-12	http://www.atis.org/docstore/product.aspx?id=26798
ATIS	ATIS-0200009	Cloud Service Lifecycle Checklist	Nov-12	http://www.atis.org/docstore/product.aspx?id=27854
ATIS	ATIS-0200010	CDN Interconnection Use Cases and Requirements in a Multi-Party Federation Environment	Dez-12	http://www.atis.org/docstore/product.aspx?id=27860
ATIS	ATIS-I-0000001	Format of ATIS Namespace	Jul-11	http://www.atis.org/docstore/product.aspx?id=25634
ATIS	ATIS-I-0000002	ATIS XML Schema Development Guidelines	Jul-11	http://www.atis.org/docstore/product.aspx?id=25638
CSA	CCM 3.0	Cloud Control Matrix	Set-13	https://cloudsecurityalliance.org/research/ccm/
CSA	CTP	Cloud Trust Protocol	Jul-05	https://docs.google.com/file/d/0Bx7isS-1a6NwUVZjbTVzZTladTg/edit?pli=1 https://cloudsecurityalliance.org/research/ctp/
CSA	PLA	Privacy Level Agreement	Fev-13	https://cloudsecurityalliance.org/research/pla/
CSA	TCI	Reference Architecture - Trusted Cloud Initiative	Fev-13	https://cloudsecurityalliance.org/research/tci/
CSA	OCF	Open Certification Framework	Nov-12	https://cloudsecurityalliance.org/research/ocf/
CSMIC	SMI Framework 2	Service Measurement Index - measures for Cloud Services	Jul-05	http://csmic.org/resources/
DMTF	DSP0243	Open Virtualization Format Specification V2	Ago-13	http://dmtf.org/sites/default/files/standards/documents/DSP0243_2.0.1.pdf
DMTF	DSP0262	Cloud Audit Data Federation (CADF) - Data Format and Interface Definitions Specification	Fev-14	http://dmtf.org/sites/default/files/standards/documents/DSP0262_1.0.0c.pdf
DMTF	DSP0263	Cloud Infrastructure Management Interface (CIMI) Model and RESTful HTTP-based Protocol	Out-13	http://dmtf.org/sites/default/files/standards/documents/DSP0263_1.1.0.pdf
DMTF	DSP0264	Cloud Infrastructure Management Interface - Common Information Model (CIMI-CIM)	Jan-13	http://dmtf.org/sites/default/files/standards/documents/DSP0264_1.0.0.pdf
DMTF	DSP2027	Cloud Infrastructure Management Interface (CIMI) Primer	Out-12	http://dmtf.org/sites/default/files/standards/documents/DSP2027_1.0.1.pdf

DMTF	DSP8009	Cloud Infrastructure Management Interface (CIMI) XML Schema	Fev-14	http://schemas.dmtf.org/cimi/1/dsp8009_1.1.0a.xsd
DMTF	DSP-IS0301	Software Identification and Entitlement Usage Metrics	Mai-12	http://www.dmtf.org/sites/default/files/standards/documents/DSP-IS0301_1.0.0.pdf
DMTF	OVF	Open Virtualization Format (OVF), OVF 1.0	Dez-10	http://www.dmtf.org/sites/default/files/standards/documents/DSP0243_1.1.0.pdf
ETSI	ETSI TR 102 997	CLOUD: Initial analysis of standardization requirements for Cloud services	Abr-10	http://docbox.etsi.org/CLOUD/Open/TR_102997v111_Standardization_Rqmts_for_Cloud_services.pdf
ETSI	ETSI TR 103 125	CLOUD: SLAs for Cloud services	Nov-12	http://www.etsi.org/deliver/etsi_tr/103100_103199/103125/01.01.01_60/tr_103125v010101p.pdf
ETSI	ETSI TR 103 126	CLOUD: Cloud private-sector user recommendations	Nov-12	http://www.etsi.org/deliver/etsi_tr/103100_103199/103126/01.01.01_60/tr_103126v010101p.pdf
ETSI	ETSI TS 103 142	CLOUD: Test Descriptions for Cloud Interoperability	Abr-13	http://www.etsi.org/deliver/etsi_ts/103100_103199/103142/01.01.01_60/ts_103142v010101p.pdf
ETSI	TS 103 142	Test Descriptions for Cloud Interoperability	Abr-13	http://www.etsi.org/deliver/etsi_ts/103100_103199/103142/01.01.01_60/ts_103142v010101p.pdf
FI-WARE	n/a	SLAware: Service Level Agreements Specification	Mai-12	https://forge.fi-ware.eu/docman/view.php/7/2920/SLAware+%28public+May+2012%29.pdf
IEEE	IEEE P2301	Draft Guide for Cloud Portability and Interoperability Profiles (CPIP)	n/a	https://standards.ieee.org/develop/project/2301.html
IEEE	IEEE P2302	Draft Standard for Intercloud Interoperability and Federation (SIIF)	Jan-12	https://www.oasis-open.org/committees/download.php/46205/p2302-12-0002-00-DRFT-intercloud-p2302-draft-0-2.pdf
ISO	ISO 9241-171	2008, Ergonomics of human-system interaction - Part 171: Guidance on software accessibility	Jan-12	http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39080
ISO	ISO 9241-20:2008	Ergonomics of human-system interaction - Part 20: Accessibility guidelines for information, communication technology (ICT) equipment and services	Jun-11	http://www.iso.org/iso/catalogue_detail.htm?csnumber=40727
ISO	ISO/PAS 22399:2007	Societal security - Guideline for incident preparedness and operational continuity management	Nov-13	http://www.iso.org/iso/catalogue_detail?csnumber=50295
ISO/IEC	ISO/IEC 17203	Information Technology - Open Virtualization Format (OVF)	Dez-11	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=59388
ISO/IEC	ISO/IEC 17788	Cloud Computing Overview and Vocabulary	Jun-14	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=60544
ISO/IEC	ISO/IEC 17789	Cloud Computing Reference Architecture	Jun-14	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=60545
ISO/IEC	ISO/IEC 17826	Cloud Data Management Interface (same as SNIA CDMI)	Nov-12	http://www.iso.org/iso/catalogue_detail.htm?csnumber=60617
ISO/IEC	ISO/IEC 18180	Information technology - Specification for the Extensible Configuration Checklist Description Format (XCCDF) Version 1.2 (NIST IR 7275)	Jun-13	http://webstore.iec.ch/preview/info_isoiec18180%7Bed1.0%7Den.pdf
ISO/IEC	ISO/IEC 19086	Cloud computing - SLA framework and terminology	Nov-13	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=63902
ISO/IEC	ISO/IEC 1st WD 27036-4	Information technology - Security techniques - Information security for supplier relationships - Part 4: Guidelines for security of cloud services	Abr-13	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=59689
ISO/IEC	ISO/IEC 20000-1	Service management system requirements	Abr-11	http://www.iso.org/iso/catalogue_detail?csnumber=51986

ISO/IEC	ISO/IEC 24751-1:2008	Information technology -- Individualized adaptability and accessibility in e-learning, education and training -- Part 1: Framework and reference model	Jan-13	http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=41521
ISO/IEC	ISO/IEC 27001	Information security management systems – Requirements	Out-08	http://www.iso.org/iso/catalogue_detail?csnumber=42103
ISO/IEC	ISO/IEC 27002	Code of practice for information security controls	Abr-08	http://www.iso.org/iso/catalogue_detail?csnumber=50297
ISO/IEC	ISO/IEC 27002	ISO/IEC 27002:2013 Information technology - Security techniques -- Code of practice for information security controls	Set-13	http://www.iso.org/iso/catalogue_detail?csnumber=54533
ISO/IEC	ISO/IEC 27017	Guidelines on Information security controls for the use of cloud computing services based on ISO/IEC 27002	Mar-14	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43757
ISO/IEC	ISO/IEC 27018	Code of practice for data protection controls for public cloud computing services	Jan-14	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=61498
ISO/IEC	ISO/IEC 27036-4	Information security for supplier relationships - Part 4: Guidelines for security of cloud services	Abr-13	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=59689
ISO/IEC	ISO/IEC WD 27035-1	Information technology - Security techniques - Information security incident management - Part 1: Principles of incident management	Mar-13	http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=60803
ISO/IEC	ISO/IEC WD 27035-3	Information technology - Security techniques -- Information security incident management -- Part 3: Guidelines for CSIRT operations	Mar-13	http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=62072
ISO/IEC	ISO/IEC WD 27039	Information technology -- Security techniques -- Selection, deployment and operations of intrusion detection systems	Out-13	http://www.iso.org/iso/catalogue_detail.htm?csnumber=56889
ISO/IEC	ISO/IEC WD TS 27017	Information technology - Security techniques -- Information security management - Guidelines on information security controls for the use of cloud computing services based on ISO/IEC 27002	Mar-14	http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43757
ISO/IEC	ISO/IEC 29115	Information technology - Security techniques - Entity authentication assurance framework	Mar-13	http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=45138
ISO/IEC 29115	ISO/IEC 9594-8:2008	Information technology - Open Systems Interconnection -- The Directory: Public-key and attribute certificate frameworks	Fev-14	http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=53372
ITU-T	X.1500	Cybersecurity information exchange techniques	Abr-11	https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1500-201104-I!!PDF-E&type=items
ITU-T	X.1520	Common vulnerabilities and exposures	Abr-11	https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1520-201104-S!!PDF-E&type=items
ITU-T	X.1521	Common Vulnerability Scoring System	Abr-11	https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1521-201104-I!!PDF-E&type=items
ITU-T	X.1600	Security framework for cloud computing	Fev-14	www.itu.int/en/ITU-T/studygroups/2013-2016/13
ITU-T	X.idmcc	Requirements of IdM in cloud computing	Fev-14	http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=9413
ITU-T	Y.3501	Cloud Comp Framework & High-level Requirements	Mai-13	https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.3501-201305-I!!PDF-E&type=items
ITU-T	Y.3510	Cloud Computing Infrastructure requirements	Mai-13	https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.3510-201305-I!!PDF-E&type=items
ITU-T	Y.3520	resource management framework for e2e cloud	Jun-13	www.itu.int/en/ITU-T/studygroups/2013-2016/13

ITU-T	Y.3520	Cloud computing framework for end to end resource management.	Jun-13	https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.3520-201306-I!!PDF-E&type=items
ITU-T	Y.ccdef	Cloud Computing overview and vocabulary	Abr-14	
ITU-T	Y.ccic	Framework of Inter-cloud	Fev-14	www.itu.int/en/ITU-T/studygroups/2013-2016/13
ITU-T	Y.ccra	Cloud Computing Reference Architecture	Jun-14	www.itu.int/en/ITU-T/studygroups/2013-2016/13
ITU-T	Y.daas	Requirements Reference Architecture of DaaS	Fev-14	www.itu.int/en/ITU-T/studygroups/2013-2016/13
NIST	FIPS 140-2	Security Requirements for Cryptographic Modules	Nov-01	http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
NIST	FIPS 180-4	Secure Hash Standard (SHS)	Mar-12	http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf
NIST	FIPS 186-4	Digital Signature Standard (DSS)	Jul-13	http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf
NIST	FIPS 197	Advanced Encryption Standard (AES)	Nov-01	http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
NIST	FIPS 198-1	The Keyed-Hash Message Authentication Code (HMAC)	Jun-08	http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf
NIST	FIPS 199	Standards for Security Categorization of Federal Information and Information Systems	Fev-04	http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
NIST	FIPS 200	Minimum Security Requirements for Federal Information and Information Systems	Mar-06	http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf
NIST	FIPS 201-1	Personal Identity Verification (PIV) of Federal Employees and Contractors	Mar-06	http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf
OASIS	KMP	Key Management Interoperability Protocol (KMIP)	Out-10	http://docs.oasis-open.org/kmip/spec/v1.0/os/kmip-spec-1.0-os.pdf
OASIS	SPML	Service Provisioning Markup Language (SPML)	Abr-06	http://www.oasis-open.org/committees/download.php/17708/pstc-spml-2.0-os.zip
OASIS	WS-Federation	Web Services Federation Language (WS-Federation) Version 1.2	Mai-09	http://docs.oasis-open.org/wsfed/federation/v1.2/os/ws-federation-1.2-spec-os.pdf
OASIS	WS-Trust 1.4	WS-Trust 1.4	Abr-12	http://docs.oasis-open.org/ws-sx/ws-trust/v1.4/errata01/os/ws-trust-1.4-errata01-os-complete.pdf
OASIS	OData	Open Data Protocol		https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=odata
OASIS	TOSCA	Topology and Orchestration Specification for Cloud Applications (TOSCA)	Mai-13	http://docs.oasis-open.org/tosca/TOSCA/v1.0/cs01/TOSCA-v1.0-cs01.html
OASIS	SAML	Security Assertion Markup Language (SAML)	Mar-05	http://docs.oasis-open.org/security/saml/v2.0/saml-2.0-os.zip
OASIS	XACML	eXtensible Access Control Markup Language (XACML)	Jan-13	http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.pdf
OASIS	CAMP	Cloud Application Management Platform (CAMP)	Ago-12	https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=camp
OASIS	TOSCA	Topology and Orchestration Specification for Cloud Applications (TOSCA),Version 1.0	Nov-13	http://docs.oasis-open.org/tosca/TOSCA/v1.0/os/TOSCA-v1.0-os.pdf
ODCA	n/a	Master Usage Model: Compute Infrastructure as a Service	Nov-12	http://www.opendatacenteralliance.org/docs/ODCA_Compute_IaaS_MasterUM_v1.0_Nov2012.pdf
ODCA	n/a	Master Usage Model: Service Orchestration	Nov-12	http://www.opendatacenteralliance.org/docs/ODCA_Service_Orch_MasterUM_v1.0_Nov2012.pdf

ODCA	n/a	Master Usage Model: Commercial Framework	Mar-13	http://www.opendatacenteralliance.org/docs/ODCA_Commercial_Framework_MasterUM_v1.0_Mar2013.pdf
ODCA	n/a	Usage: Data Security Framework	Mar-13	http://www.opendatacenteralliance.org/docs/Data_Security_Framework_Rev1.0.pdf
ODCA	n/a	Virtual Machine (VM) Interoperability in a Hybrid Cloud Environment	Abr-13	http://www.opendatacenteralliance.org/docs/Virtual_Machine_%28VM%29_Interoperability_in_a_Hybrid_Cloud_Environment_Rev1.2.pdf
ODCA	n/a	Master Usage Model: Software-Defined Networking	Jun-13	http://www.opendatacenteralliance.org/docs/Software_Defined_Networking_Master_Usage_Model_Rev1.0.pdf
ODCA	n/a	Master Usage Model: Scale out Storage	Jun-13	http://www.opendatacenteralliance.org/docs/Scale_Out_Storage_Master_Usage_Model_Rev1.0.pdf
ODCA	n/a	Master Usage Model: Information as a Service	Jun-13	http://www.opendatacenteralliance.org/docs/Information_as_a_Service_Master_Usage_Model_Rev1.0.pdf
ODCA	n/a	Usage: Standard Units of Measure for IaaS	Mar-13	http://www.opendatacenteralliance.org/docs/Standard_Units_of_Measure_For_IaaS_Rev1.1.pdf
OGF	GFD.192	Web Services Agreement (WS-Agreement)	Out-11	http://ogf.org/documents/GFD.192.pdf
OGF	GFD.183	Open Cloud Computing Interface - Core	Jun-11	http://ogf.org/documents/GFD.183.pdf
OGF	GFD.184	Open Cloud Computing Interface - Infrastructure	Jun-11	http://ogf.org/documents/GFD.184.pdf
OGF	GFD.185	Open Cloud Computing Interface - RESTful HTTP Rendering	Jun-11	http://ogf.org/documents/GFD.185.pdf
OGF	GFD.193	WS-Agreement Negotiation	Out-11	http://ogf.org/documents/GFD.193.pdf
OGF	GFD.183	Open Cloud Computing Interface (OCCI) Core	Jun-11	http://www.ogf.org/documents/GFD.183.pdf
OGF	DFDL	Data Format Description Language (DFDL)	Jun-11	http://www.ogf.org/documents/GFD.174.pdf
OGF	GFD.184	Open Cloud Computing Interface - Infrastructure	Jun-11	https://www.ogf.org/documents/GFD.184.pdf
OGF	n/a	Open Cloud Computing Interface - Platform	Jul-13	http://www-inf.it-sudparis.eu/SIMBAD/tools/OCCI/docs/platform.pdf
OpenID Foundation	n/a	OpenID Authentication 1.1	Mai-06	https://openid.net/specs/openid-authentication-1_1.html
PCI	n/a	Payment Card Industry (PCI) Data Security Standard	Out-10	https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf
QuEST Forum	TL9000	TL 9000 Measurements Handbook	Jul-12	http://www.tl9000.org/handbooks/measurements_handbook.html
QuEST Forum	TL9000	TL 9000 Requirements Handbook	Nov-09	http://www.tl9000.org/handbooks/requirements_handbook.html
SLA@SOI	D.A5a	SLA: An abstract syntax for Service Level Agreements	Out-10	http://sla-at-soi.eu/results/models/
SNIA	CDMI	Cloud Data Management Interface - ISO 17826:2012	Jun-12	http://www.snia.org/cdmi
TIA	ANSI/TIA-942-A	Telecommunications Infrastructure Standards for Data Centers	Mar-13	http://global.ihs.com/search_res.cfm?RID=TIA&INPUT_DOC_NUMBER=ANSI/TIA-942
W3C		XML Encryption Syntax and Processing	Abr-13	http://www.w3.org/TR/xmlenc-core1/