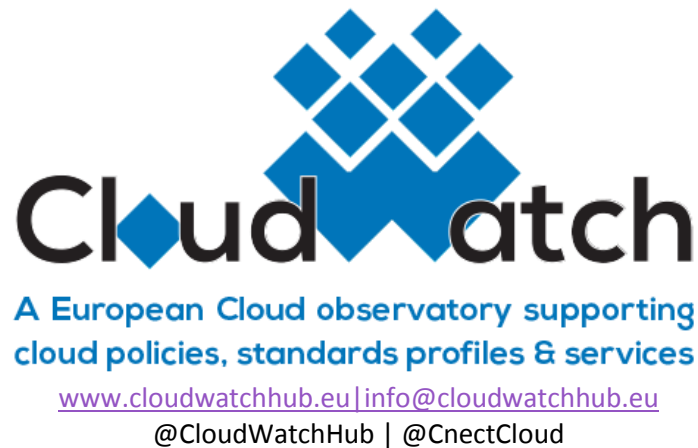


## D2.1 Reference Model Framework Report

---



This report provides a framework for the presentation of use cases for the purpose of the derivation of standardization requirements and the development of standard profiles for various areas from the cloud computing domain. It is intended to be of value for researchers and standardization experts that employ a use case driven approach.

## CloudWATCH Mission

The CloudWATCH mission is to accelerate the adoption of cloud computing across European private and public organisations. CloudWATCH offers independent, practical tips on why, when and how to move to the cloud, showcasing success stories that demonstrate real world benefits of cloud computing. CloudWATCH fosters interoperable services and solutions to broaden choice for consumers. CloudWATCH provides tips on legal and contractual issues. CloudWATCH offers insights on real issues like security, trust and data protection. CloudWATCH is driving focused work on common standards profiles with practical guidance on relevant standards and certification Schemes for trusted cloud services across the European Union.

The CloudWATCH partnership brings together experts on cloud computing; certification schemes; security; interoperability; standards implementation and roadmapping as well as legal professionals. The partners have a collective network spanning 24 European member states and 4 associate countries. This network includes: 80 corporate members representing 10,000 companies that employ 2 million citizens and generate 1 trillion in revenue; 100s of partnerships with SMEs and 60 global chapters pushing for standardisation, and a scientific user base of over 22,000.

## Disclaimer

CloudWATCH (A European Cloud Observatory supporting cloud policies, standard profiles and services) is funded by the European Commission's Unit on Software and Services, Cloud Computing within DG Connect under the 7<sup>th</sup> Framework Programme.

The information, views and tips set out in this publication are those of the CloudWATCH Consortium and its pool of international experts and cannot be considered to reflect the views of the European Commission.

## Executive Summary

A major objective of the CloudWatch project is to develop a common standards profile for technical interoperability of cloud services, building on existing cloud federation and integration efforts in Europe and elsewhere, and leading to publication by a recognised standards groups operating in this area. A federated cloud profile can be applied across research, government and business communities enabling the sharing of resources for maximum benefit.

Hence, one of the main goals of the CloudWatch project is to identify standards profiles in the area of cloud computing (in particular in the area of “infrastructure as a service”) and to support their development in cooperation with relevant Standardization Bodies. For this purpose, a use case driven approach is employed. This report provides a framework for the presentation of use cases as a first processing step towards this goal. It utilizes a cloud computing reference architecture that has been developed within the CloudWatch project (based on previous work in ISO/IEC and ETSI) to identify and classify elements that comprise a use case. From this reference architecture, templates for the formalized description of use cases have been defined. Moreover, selection criteria have been defined that will be used to identify use cases for further processing, i.e., the derivation of standardization requirements and finally standard profiles.

The work presented in this deliverable will be used as input for the CloudWatch Deliverable D2.2 (Use Case Report) that will comprise an actual list of use cases expressed by the approach described in this report.

The approach described in this report is based on previous work in the context of standardization in ISO/IEC, ITU-T and ETSI by Fraunhofer and CSA, and further refined and adapted for the use in the CloudWatch project by a collaborative effort of Fraunhofer and the University of Oxford.

## Table of Contents

<b>CloudWATCH Mission</b>	2
<b>Disclaimer</b>	2
<b>Document Information Summary</b>	Errore. Il segnalibro non è definito.
<b>Executive Summary</b>	3
<b>Table of Contents</b>	4
<b>Figures</b>	5
<b>1 Introduction</b>	6
<b>2 Cloud Use Case Reference Model</b>	8
2.1 Cloud Computing Reference Model	8
2.1.1 Methodology	9
2.1.2 Roles and Activities	10
2.1.3 Functional Layers and Components	12
2.1.4 Cross-cutting Aspects	13
2.1.5 Usage Scenarios and Use Cases	14
<b>3 Selection Criteria</b>	16
<b>4 Templates</b>	17
4.1 Usage Scenario Template	18
4.2 Legal Use Case Template	18
4.3 Organizational Use Case	19
4.4 Technical Use Case Template	20
<b>5 Conclusion and Next Steps</b>	21
<b>References</b>	23
<b>Annex 1 – Use Case Workshop Invitation (Excerpt)</b>	24
<b>Annex 2 – Simplified Use Case Template</b>	27
<b>Annex 3 – Document Log</b>	Errore. Il segnalibro non è definito.

## Figures

Figure 1. Standard profile development approach .....	6
Figure 2. Relationship between actors, roles, activities, layers, and components/functions .....	10
Figure 3. Roles and sub-roles .....	11
Figure 4. Layers and multi-layer functions .....	13
Figure 5. Usage scenarios and use cases.....	15

## 1 Introduction

A major objective of the CloudWatch project is to develop a common standards profile for technical interoperability of cloud services, building on existing cloud federation and integration efforts in Europe and elsewhere, and leading to publication by a recognised standards groups operating in this area. A federated cloud profile can be applied across research, government and business communities enabling the sharing of resources for maximum benefit.

This report defines a **cloud use case reference model framework**: The purpose of this framework is to provide a classification of use cases according to their

- ◆ Application domain: **academic, industrial, public sector**
- ◆ Category: **legal, organisational, technical**
- ◆ Stakeholders involved: the main **actors** that constitute the use case and their responsibilities
- ◆ **Functions/components**: The technical items within a cloud infrastructure or related to a cloud service that are exercised in the use case.

The usage of the framework within the CloudWatch project is motivated as follows: For the development of cloud standard profiles the project employs a use case driven approach comprising five steps (compare Figure 1)

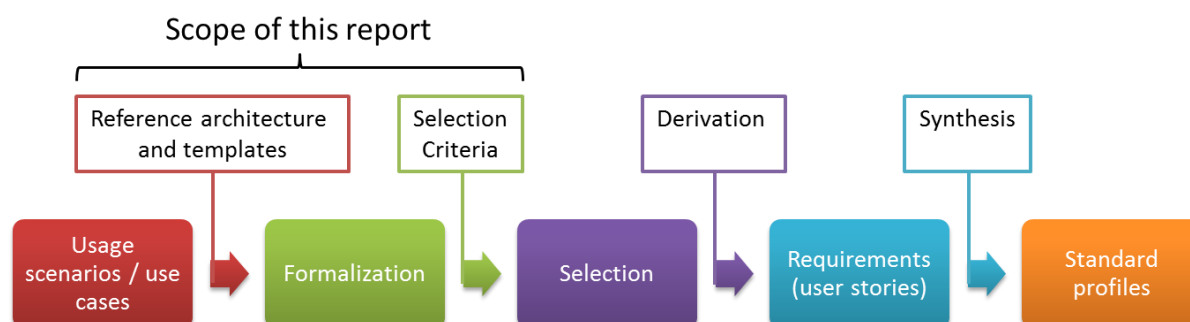


Figure 1. Standard profile development approach

- ◆ The development process starts with an initial input of use cases and usage scenarios for cloud computing originating from various sources. Due to the fact that a large number of organisations and activities have used a similar approach, there is no shortage on use cases (for instance,

ISO/IEC JTC1 SC38 WG3 collected more than 40 use cases [ISO/IEC13b] ETSI Cloud Standards Coordination Task Group 2 came up with more than 100 use cases [CSC13]). These use cases vary in their level of abstraction, scope, and purpose.

- ◆ Therefore, to make the initial set of use cases useable for the CloudWatch project, a certain degree of formalization is required. We use an approach similar to the methodology developed in ISO/IEC JTC1 SC38 [ISO/IEC13a,b]: In order to classify the technical, organisational and legal elements that are mentioned in those use cases, a cloud computing reference architecture is defined that describes the term “cloud computing”. Moreover, templates are provided to express those use cases in a uniform way.
- ◆ The next step comprises the selection of an appropriate set of use cases for the original set for further processing (CloudWatch Deliverable D2.2). For this purpose, selection criteria have to be defined and applied.
- ◆ From the set of use cases selection in the previous steps, standardization requirements are derived (those requirements are sometimes analysed by means of so-called user stories<sup>1</sup> (CloudWatch Deliverable D2.3).
- ◆ Finally, standards profiles are synthesized; their implementation is performed in collaboration with relevant Standardization Bodies (CloudWatch Work Package 4).

(An additional CloudWatch Deliverable D2.4 addresses policy and compliance requirements identified in the use cases and that cannot currently be included in the profile due to the need for additional legislation or policy development.)

This report aims on preparing the first two transitions in the use case processing chain outlined above. It provided a use case reference model (Section 2) that comprises two main parts: Section 2.1 describes a cloud computing reference architecture that allows a classification of elements used in use case descriptions. The cloud computing reference architecture has been developed on the basis of several sources:

- ◆ The upcoming ISO/IEC standard “Information Technology — Cloud Computing — Reference Architecture” that is under development by a collaborative team comprising experts from

---

<sup>1</sup> The term user stories is borrowed from the area of agile software development, see <http://www.agilemodeling.com/artifacts/userStory.htm> for an example.

ISO/IEC JTC 1/SC 38 WG3 and ITU-T SG 13 [Hib13, PSB13]<sup>2</sup>. Fraunhofer is an active contributor to this work; CSA maintains a liaison to SC 38.

- ◆ The final report of the ETSI Cloud Standards Coordination Group [CSC13].

The second part of the use case reference model aims on providing a unified representation of use cases. In general, we distinguish between legal, organizational, and technical aspect. Various use cases can be grouped into so-called usage scenarios: Scenarios describe common elements of various use cases and thus provide a general usage context. Hence, scenarios can be used to relate a set of use cases to a certain application context, and thus are a first step for the identification of relevant standards profiles and related Standardization Bodies. A detail description of these terms is provided by Section 2.1.5 (actual templates are given in Section 4).

To move from the “Formalization” to the “Selection” step in the use case processing chain, selection criteria are described in Section 3).

As mentioned above, Section 4 provides templates for use case formalization following the approach given in Section 2.1.5.

The final Section 5 comprises conclusions and a brief outlook on next steps.

## 2 Cloud Use Case Reference Model

The cloud use case reference model used in the CloudWatch project is based on

- (a) a cloud reference architecture that provides us with a terminological framework to describe use cases and to compare them, and
- (b) a structured representation format for use cases comprising a number of templates.

Its purpose is to provide a unified presentation of use cases that is mapped against the cloud computing reference architecture. Thus, it allows for comparing and grouping use cases and to prepare the derivation of requirements for standards profiles.

### 2.1 Cloud Computing Reference Model

Cloud computing systems are described using an architectural approach comprising four views:<sup>3</sup>

---

<sup>2</sup> Since the standard is not published yet, we have to refer to secondary material.



View	Description	In Scope
User view	Describes the system context; the actors, the roles, the sub-roles and the cloud computing activities	Yes
Functional View	Describes the functions necessary for the support of cloud computing activities an implementation neutral way	Yes
Implementation View	Implementation specific consideration of a cloud service within service parts and/or infrastructure parts: Specific technologies, supplementary services and platforms, are considered here.	No
Deployment View	how the functions of a cloud service are technically operated within already existing infrastructure elements or within new elements to be introduced in this infrastructure	No

While the user view and the functional view are important elements of use case descriptions related to standardization activities, the implementation and deployment view are related to the actual development of technical cloud systems and components and thus not in the scope of this report.

### 2.1.1 Methodology

These architectural views are utilized to build-up a terminology framework for the description of use cases and usage scenarios (see Section 2.1.4).

The **user view** is based on an actor model comprising the following elements:

- ◆ An **actor** is a person or organisation (or an automated system acting on behalf of a person or organisation) who uses a cloud system or components of a cloud system.
- ◆ Actors assume **roles**. Roles (and **sub-roles**) are defined by a set of activities that an actor assuming a certain role is supposed to perform. Another interpretation of a role is that of an organisational element.
- ◆ An **activity** described the usage of a number of cloud components with the purpose to achieve a certain goal or outcome. Using the organisational interpretation of roles, activities imply certain responsibilities of the organisational entities described by a role.

Use cases usually describe – on a given level of abstraction – an activity of a number of activities.

The **functional view** comprises of technical **components** that are supposed to provide certain functions. These components are structured into **layers**. Certain functions address more than one

<sup>3</sup> This approach is compatible with the international standard ISO/IEC 10746-1 (Open Distributed Processing)

layer, and components providing those functions are therefore referred to as **multi-layer components**.

Finally, certain aspects cannot be associated with the user or functional view but address both organisational and functional issues. We refer to those aspects to as **cross-cutting aspects**.

Figure 2 summarizes the model structure of the cloud computing reference model.

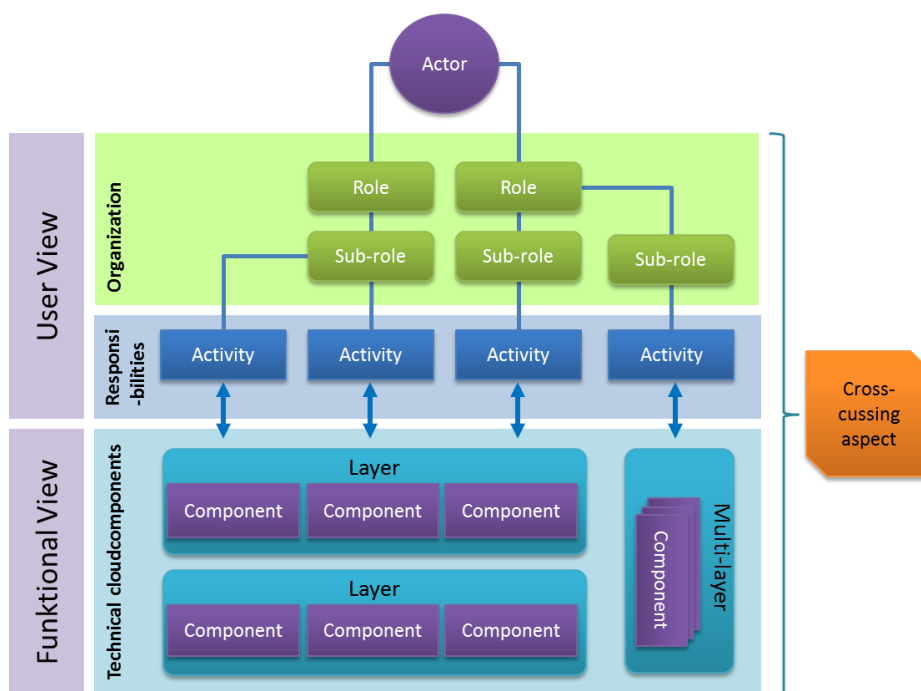
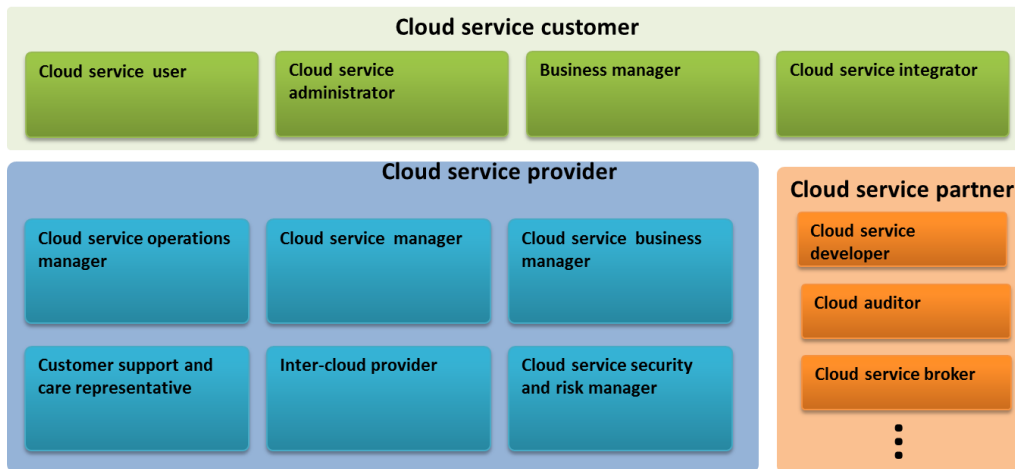


Figure 2. Relationship between actors, roles, activities, layers, and components/functions

### 2.1.2 Roles and Activities

Following [CSC13], we use three top-level roles, namely the cloud service customer, the cloud service provider, and the cloud service partner. Each of these roles has several sub-roles (cf. Figure 3).



*Figure 3. Roles and sub-roles*

The **cloud service customer** comprises the following sub-roles:

- ◆ Cloud service user – The actual user of a cloud service.
- ◆ Cloud service administrator – Actor who administers cloud services on the customer side: Adds and removes users, manages access rights, performs service configuration, etc.
- ◆ Cloud service business manager – Actor who manages business aspects on the customer side, responsible for determining business incentives of employing a particular cloud service, contracting an appropriate provider, etc.
- ◆ Cloud service integrator – Actor who integrates a particular cloud services into the in-house IT of the customer, and with other cloud services.

The sub-roles of the **cloud service provider** are

- ◆ Cloud service operations manager – Actor who performs operational management activities (e.g., inventory management, capacity planning, problem management).
- ◆ Cloud service manager – Actor who performs service specific management activities (e.g., service level management, service deployment).
- ◆ Cloud service business manager – Actor responsible for financial and business aspects of a cloud service (e.g., management of business plans, customer relationship, supplier management)
- ◆ Customer support and care representative – Actor responsible for reacting to customer issues and queries (i.e., incident management).

- ◆ Inter-cloud provider – Actor responsible for technical aspects regarding federated or multiple cloud architectures (cloud burst scenarios and invocation of 3<sup>rd</sup> services).
- ◆ Cloud service security and risk manager – Actor responsible for the planning and implementation of security controls. This includes risk analysis.

As opposed to the previous roles, the **cloud service partner** role is open. The following list of sub-roles is meant to provide examples rather than a complete description.

- ◆ Cloud service developer – Developer of new cloud services. An actor assuming this role might be part of the provider's organisation or part of an external organisation. The developer makes use of development functions (see below).
- ◆ Cloud auditor – Actor performing conformance audits with regard to legal regulations, financial requirements, or quality/process standards (ISO/IEC 27000, ISO 9000, etc.).
- ◆ Cloud service broker – Actor responsible for negotiating relationships between customers and providers. Cloud service brokers do not necessarily offer inter-cloud capabilities, but if so, the broker assumes simultaneously the cloud service provider sub-role of an inter-cloud provider.

### 2.1.3 Functional Layers and Components

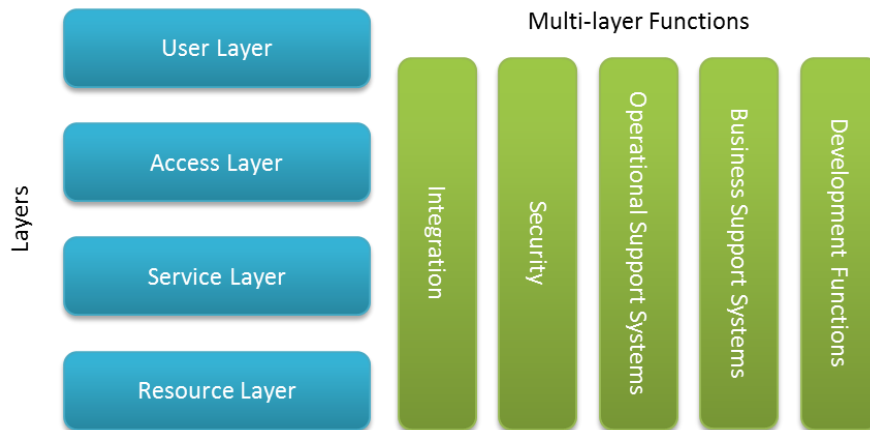
The cloud computing reference model comprises four layers (cf. Figure 4):

- ◆ User layer: User functions, administrator functions, and business functions that are available by the cloud service customer.
- ◆ Access layer: Access control functions and connection management.
- ◆ Service layer: Capabilities provided as services to the cloud service customer.
- ◆ Resource layer: Physical resources and resource abstraction mechanisms.

Additionally, a number of multi-layer functions are defined:

- ◆ Integration functions: Security, monitoring, service, and peer service integration functions
- ◆ Security: Authentication and identity management, authorization and service policy management, cryptographic functions and encryption management.
- ◆ Operational support systems: Service catalogue, service provisioning functions, monitoring and reporting, service policy management, service automation, service level management, incident and problem management, platform and virtualization management, peer service management.

- ◆ Business support systems: Produce catalogue, account management, subscription management, and billing.
- ◆ Development functions: Developer environments, build and test management, deployment management.



*Figure 4. Layers and multi-layer functions*

#### 2.1.4 Cross-cutting Aspects

Cross cutting aspects include both architectural and operational considerations, which may apply to multiple elements of a Cloud. Such cross-cutting aspects may impact multiple roles, activities, and components, and may not be clearly assigned to individual roles or components.

Cross-cutting aspects are:

- ◆ **Interoperability:** Ability of a cloud service customer to interact with a cloud service and exchange information according to a prescribed method and obtain predictable results. The term also includes the ability for one cloud service to work with other cloud services
- ◆ **Portability:** Ability to move cloud service customer data or their applications between multiple cloud service providers at low cost and with minimal disruption.
- ◆ **Reversibility:** Ability of the cloud service customers to retrieve their cloud service customer data and application artefacts and for the cloud service provider to delete all cloud service customer data as well as contractually specified cloud service derived data after an agreed or regulatory defined period.
- ◆ **Security:** Security capabilities for cloud services include: access control, confidentiality, integrity and availability.

- ◆ **Privacy:** Protection of the assured, proper, and consistent collection, processing, communication, use and disposition of personally identifiable information in the relation to cloud services.
- ◆ **Resiliency:** Ability of a system to provide and maintain an acceptable level of service in the face of faults (unintentional, intentional, or naturally caused) affecting normal operation.
- ◆ **Performance:** A set of non-functional facets relating to the operation of a cloud service such as availability of the service; response time to complete service requests, transaction rate at which service requests are executed, etc.
- ◆ **Auditability:** Availability of means to ensure that services are provided and used consistent with the associated service agreements between the cloud service customers, cloud service providers and cloud service partners.
- ◆ **Maintenance and versioning:** Preservation and improvement of the function of services and underlying resources. Versioning ensures changes become traceable and roll-backs can be performed.
- ◆ **Service levels and service level agreement:** A cloud computing service level agreement (SLA) is a service level agreement between a cloud service provider and a cloud service customer based on a taxonomy of cloud computing specific terms to set the quality of the cloud services delivered.

### 2.1.5 Usage Scenarios and Use Cases

The cloud computing reference architecture outlined in the previous section provides us with the terminology and background to describe the use cases for the CloudWatch project.

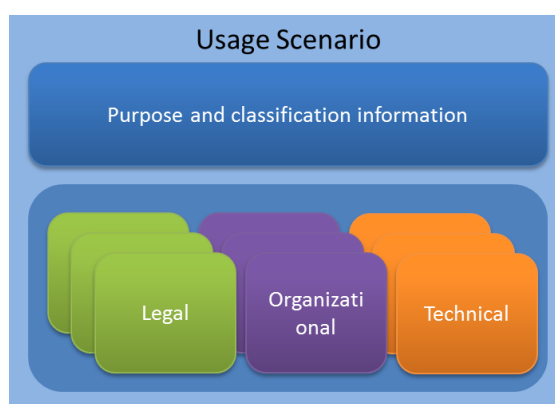
Use cases are usually employed as tool for software or system engineering. This document proposes the employment of usage scenarios and use cases as an analysis tool to identify specific characteristics and requirements of cloud computing service various purposes, such as:

- ◆ Interoperability requirements to analyse standardization requirements (gaps, overlaps)
- ◆ Analysis of compliance with regard to European regulations
- ◆ Software and system definition in the sense of a preliminary identification of system components

By a **usage scenario** we mean a concrete (real life, or fictitious but realistic) usage context of a cloud based system or service: a business case or the usage of a set of cloud services for a particular

purpose. In the context of the CloudWatch project, scenarios will be utilized to group a set of use cases with regard to a specific application area or technological context that implies a set of interrelated standards (i.e., a standards profile).

A **use case** describes the activities of a number of the actors while using such a system or service in a particular way. A usage scenario usually comprises of a number of use cases. A usage scenario therefore serves as a concrete “cover story” with the purpose to demonstrate a certain concept or idea.



*Figure 5. Usage scenarios and use cases*

We moreover distinguish between three categories of use cases:

- ◆ **Legal use cases** describe certain activities in the context of a law or regulation to understand whether this activity is compliant to a given regulatory framework. For instance, data security mechanisms of a certain cloud system can be analysed with regard to data protection regulations within the European Union.
- ◆ **Organisational use cases** aim on the analysis of organisational structures and processes. For instance, change management is one of the major driving management processes of IT service provisioning. Since cloud computing automates various aspects of IT service management, organisational use cases can illustrate how classical service management disciplines are performed within a cloud-based data centre.
- ◆ **Technical use cases** describe technical aspects of cloud systems and components. Examples are usage of protocols and interfaces, document and data exchange mechanism, or security and privacy mechanisms.

It is not imply that each use case can be uniquely identified with one of these categories. If a use case is related to more than one category, two separate descriptions will be used that reference each other (the usage scenario description templates introduced in Section 4.1 contain a specific field labelled “Related use cases” for this purpose).

### 3 Selection Criteria

The CloudWATCH project performs two distinct tasks in reference to use cases:<sup>4</sup>

- ◆ Identify international use cases and open collaborative models
- ◆ Collate use case requirements, providing input criteria for interoperability profile

In particular, an activity is “*to develop a framework for use case selection to identify and collect a portfolio of international cloud use cases*” as an outcome of the first task and pre-requisite of the second one (refer also to diagram shown in Figure 1).

The selection criteria for use cases are guided by the requirements of the analysis of use cases; we will dissect each of the use cases in turn for their requirements around interoperability. Final output from these tasks will be a single report giving the user stories, and their derived technical interoperability requirements.

Therefore, candidate use cases and scenarios will be assessed against the depth and completeness of information given on each of the following:

- ◆ The use cases focus on (legal, organisational, or technical) requirements around interoperability.
- ◆ The scenario describes a set of co-ordinating services that in turn imply requirements regarding a set of standards.
- ◆ Is there any provider or community that offer or use the described set of services? If so, does the CloudWatch project maintain a direct personal contact?
- ◆ Cataloguing of necessary or provided external interfaces.
- ◆ Overall functional requirements are explained sufficiently clear to derive standardization requirements.

---

<sup>4</sup> These tasks are described in the CloudWatch Description of Work (DOW) as Task 2.1 and Task 2.2, respectively.



- ◆ User stories are available.
- ◆ The 'who', 'what' and 'why' of the requirement.

Each use case will have a 'champion' who completes the template document and each champion will have the opportunity for self-evaluation of the use case against the above criteria. These templates and evaluations will be live, public and iterative, and will form the basis of the derivation of standards profiles.

## 4 Templates

In the following sections, we introduce templates for usage scenarios and use cases. Fields are either mandatory or optional; in addition, we allow the definition of additional fields if this is appropriate for a particular purpose. As indicated above, we summarize a number of use cases under the umbrella of a common usage scenario.

Both scenario and use case template contain entries defining the user view and the functional view as described in Section Cloud Computing Reference Model2.1. The field describing the user view, **"Actors, roles, and activities"**, is further divided into several sub-entries:

- ◆ The name of an actor that assumes one or several roles
- ◆ The roles the actor assumes, and
- ◆ For each role a description of the activities in question.

The functional view is described by the field **"Components"**. This field is also sub-divided in a list of layers or multi-layer function groups, and a description of the components of these layers/multi-layers that play a role in the use case or scenario.

Finally, the field **"Cross-cutting aspects"** comprises a list of cross-cutting aspects addressed in the scenario or use case.

The usage scenario should take into account the main architectural components (i.e., actors, roles/sub-roles, activities, layers/multi-layers, components, cross-cutting aspects) addressed in the associated set of use cases.

## 4.1 Usage Scenario Template

Usage scenario		
<b>ID</b> (mandatory)	<b>Title</b> (mandatory)	
<b>Description</b> (mandatory)	Main “storyline” for the use cases	
<b>Categories</b> (mandatory)	Technical, organizational, legal, ...	
<b>Domain</b> (optional)	E.g., public sector services	
<b>Goals and purpose</b> (mandatory)	What is demonstrated by the scenario?	
<b>Actors, roles, and activities</b> (optional, use case descriptions should address)	Actor name	
	Role name	Description of activity 1
		Description of activity 2
	<i>(Add rows as appropriate to describe other actors and roles)</i>	
<b>Service layers</b> (optional)	IaaS/VM layer, PaaS layer, etc.	
<b>Deployment model</b> (optional)	Private, public, community, hybrid, ...	
<b>Components</b> (optional, use case descriptions should address)	Layer / multi-layer name	Description of component/function 1
		Description of component/function 2
	<i>(Add rows as appropriate to describe other components)</i>	
<b>Cross-cutting aspects</b> (optional, mandatory in the use case descriptions)	List cross-cutting aspects addressed in the usage scenario	
<b>Related use cases</b> (mandatory)	List of use cases related to this scenario (use identifiers as given in the use case templates)	
<b>Additional field</b> (optional)	Add fields as appropriate	

## 4.2 Legal Use Case Template

Legal use case		
<b>ID</b> (mandatory)	<b>Title</b> (mandatory)	
<b>Description</b> (mandatory)	Short summary of the use case	
<b>Actors, roles, and activities</b> (mandatory)	Actor name	
	Role name	Description of activity 1
		Description of activity 2
	<i>(Add rows as appropriate to describe other actors and roles)</i>	
<b>Goals and aspirations for</b>	Background and main message of the use case	

<b>the use case</b> (mandatory)		
<b>Legal domain</b> (mandatory)	Data privacy regulations, licensing, contracting, etc.	
<b>Area</b> (mandatory)	E.g., Europa, US, . . .	
<b>Components</b> (optional)	Layer / multi-layer name	Description of component/function 1
		Description of component/function 2
	<i>(Add rows as appropriate to describe other components)</i>	
<b>Cross-cutting aspects</b> (mandatory)	List cross-cutting concerns aspects in the use case	
<b>Legal frameworks, laws, etc., to be taken into account</b> (mandatory)	Laws, policies, etc. which are of relevance	
<b>Required preconditions</b> (optional)	Any preconditions necessary to understand the use case	
<b>Compliance criteria</b> (mandatory)	Explanation why the use case is an illustration on how legal requirement can be implemented	
<b>Description of procedures to ensure legal compliance</b> (optional)	Explanation how the use case shows the implementation of legal requirements	
<b>Existing specifications to rely on</b> (optional)	Specifications and standards already dealing with aspects related to the use case	
<b>Additional field</b> (optional)	Add fields as appropriate	

### 4.3 Organizational Use Case

Organizational use case		
<b>ID</b> (mandatory)	<b>Title</b> (mandatory)	
<b>Description</b> (mandatory)	Short summary of the use case	
<b>Actors, roles, and activities</b> (mandatory)	Actor name	
	Role name	Description of activity 1
		Description of activity 2
	<i>(Add rows as appropriate to describe other actors and roles)</i>	
<b>Goals and aspirations for the UC</b> (optional)	Background and main message of the use case	
<b>Organization domain</b> (mandatory)	E.g., security procedures, data privacy procedures, etc.	
<b>Regulations and policies</b>	Policies, standards, best practices to be taken into account	

<b>to be taken into account</b> (optional)		
<b>Description of organization procedures</b> (mandatory)	The “workflow” (or procedures) on organizational level used to achieve the goal of the use case	
<b>Components</b> (optional)	Layer / multi-layer name	Description of component/function 1
		Description of component/function 2
	<i>(Add rows as appropriate to describe other components)</i>	
<b>Cross-cutting aspects</b> (mandatory)	List cross-cutting aspects addressed in the use case	
<b>Required preconditions</b> (optional)	Any preconditions necessary to understand/implement the use case	
<b>Criteria for success</b> (optional)	The expected output and the side effects	
<b>Failure conditions</b> (optional)	What can go wrong	
<b>Failure handling</b> (optional)	what to do about it	
<b>Related UCs and those that are pre-requisite</b> (optional)	May refer to technical UC describing the technical means to implement this UC.	
<b>Existing specifications to rely on</b> (optional)	Specifications and standards already dealing with aspects related to the use case	
<b>Additional field</b> (optional)	Add fields as appropriate	

#### 4.4 Technical Use Case Template

Technical use case		
<b>ID</b> (mandatory)	<b>Title</b> (mandatory)	
<b>Description</b> (mandatory)	Short summary of the use case	
<b>Actors, roles, and activities</b> (mandatory)	Actor name	
	Role name	Description of activity 1
		Description of activity 2
	<i>(Add rows as appropriate to describe other actors and roles)</i>	
<b>Primary Actor</b> (optional)	The actor who initiates the technical use case	
<b>Goals and aspirations for the UC</b> (optional)	Background and main message of the use case	
<b>Components</b> (mandatory)	Layer / multi-layer name	Description of component/function 1
		Description of component/function 2
	<i>(Add rows as appropriate to describe other components)</i>	

<b>Cross-cutting aspects</b> (mandatory)	Lists cross-cutting aspects addressed in the use case
<b>Preconditions</b> (optional)	Assumptions made prior to the execution of the use case
<b>Input parameters needed for initialization</b> (optional)	Initial input values for the execution of the use case
<b>Criteria for success</b> (optional)	Expected process, outcome, side effects. Described by sequence charts, etc.
<b>Failure conditions</b> (optional)	what can go wrong
<b>Failure handling</b> (optional)	what to do about it
<b>Related use cases and those that are pre-requisite</b> (optional)	Relevant use cases for the associated usage scenario.
<b>Existing specifications to rely on</b> (optional)	Specifications and standards already dealing with aspects related to the use case
<b>Additional field</b> (optional)	Add fields as appropriate

## 5 Conclusion and Next Steps

In this report, we have provided an approach for the formalization of use cases and usage scenarios basing on the employment of a cloud computing reference architecture as a means of classification of the various elements that comprises a use case. Moreover, templates have been provided to express use cases in a uniform and comparable way, addressing legal, organisational, and technical aspects. Use cases are furthermore grouped into usage scenarios that describe an application area or technological context of these use cases and therefore help to identify an associated standards profile.

The purpose of this work is to provide formalized methodology for the presentation and processing of use cases towards the definition of standards profiles and the supporting their development.

An obvious open issue is how to implement the derivation of standardization requirements from a use case selection. To resolve this issue, a work shop will be organized during the CloudWatch Concertation Meeting (12-13 March 2014, Brussels, Belgium). During this workshop, this issue will be addressed from various perspectives (academic, industrial, and public sector). In addition, the audience (representatives from various projects funded by the European Commission and related

initiatives) will be asked to provide an answer to this question from their own perspectives using an online survey.

An excerpt of the invitation of the work shop (stripped by organisational details) has been added as Annex 1. Annex 2 consist a simplified version of the templates given in Section 4 of this report that will be used to approach an external audience.

## References

- [ISO/IEC13a] ISO/IEC JTC 1/SC 38/WG 3 Standing Document 1, Methodology and Guidelines for Cloud Computing Usage Scenario and Use Case Analysis, 9 April 2013, avail. at  
<http://isotc.iso.org/livelink/livelink?func=ll&objId=8919753&objAction=browse&viewType=1>
- [ISO/IEC13b] ISO/IEC JTC 1/SC 38/WG 3 Standing Document 2, Compendium of Cloud Computing Usage Scenarios and Use Cases, 7 March 2013, avail. at  
<http://isotc.iso.org/livelink/livelink?func=ll&objId=8919753&objAction=browse&viewType=1>
- [CSC13] ETSI Cloud Standards Coordination, Final Report, November 2013, avail. at  
<http://csc.etsi.org/Application/documentApp/documentinfo/?documentId=204&fromList=Y>
- [Hib13] E. A. Hibbard, Latest in Cloud Computing Standards, CSA Congress 2013, Orlando, FL, December 4, 2013, avail. at <https://community.hds.com/docs/DOC-1001302>.
- [PSB13] B. Piprani, D. Sheppard, and A. Barbir, Comparative Analysis of SOA and Cloud Computing Architectures using Fact Based Modeling, OTM Workshops 2013: 524 - 533, avail.  
<http://www.slideshare.net/abarbir/presentation1-v5-20130911>

## Annex 1 – Use Case Workshop Invitation (Excerpt)

### Background & Purpose

CloudWATCH has produced a *Reference Model Framework Report (D2.1)* to guide the selection, capture and analysis of Use Cases from three different classes of user community: Enterprise, Government and Academic. The purpose of the workshop is to bring together representatives from those user communities to utilise the framework in the capture of use cases pivotal in the future development of those communities. Interoperability is a key feature in many of the RTD projects, so it represents an effective time and cost saving to engage with these at the Concertation Meeting.



## Value Proposition (standards profiles)

Although it takes time, effort and commitment, the capture and documentation of use cases is relatively easy and straightforward: this is just one of the aims of the workshop. We provide templates derived from the *Reference Model Framework Report* and invite participants to fill in the forms (preferably in advance of the workshop). We then capture and collate the information in preparation for analysis.

However, the true value lies in being able to extract from the captured collection of use cases relevant and meaningful standards profiles for each of the participating user communities: this process is hard. The primary goal of the workshop is to engage with community representatives in the formulation of just such an extraction process that will result in standards profiles that are widely accepted, and widely regarded as representative and meaningful.

## Use Case Selection Criteria

The *Reference Model Framework Report* sets out criteria for the selection of use cases for further analysis. Candidate use cases are to be assessed against the depth and completeness of information given on each of the following:

- ◆ Technical requirements around interoperability.
- ◆ Set of co-ordinating services.
- ◆ Meta-services and their access.
- ◆ Any current community utilized solutions.
- ◆ Cataloguing of necessary external interfaces.
- ◆ Overall functional requirements.
- ◆ User stories.
- ◆ The 'who', 'what' and 'why' of the requirement.

Each use case will have a 'champion' who completes the template document and each champion will have the opportunity for self-evaluation of the use case against the above criteria.

## Use Case Capture

The *Reference Model Framework Report* presents four templates for the capture of use cases and usage scenarios: we are in the process of turning these into an online capture survey for use prior to, during, and after the workshop, in an iterative process of information capture and refinement.

The final survey will be live, public and persistent, encouraging complete, detailed and in-depth submissions with opportunities for capturing commentary from the community and iterative revision by the author.

## Self-Evaluation of Use Cases

Included in the use case capture survey will be a series of questions designed for self-evaluation against the depth and completeness of the information provided as related to the selection criteria. Responses will be in the form of a rating [1-5], giving an estimate of how successfully the use case might contribute to the overall extraction of standards profiles. These ratings will be gathered and collated on a live updating summary page, possibly for display on a public screen at the workshop.

## Structure of the Workshop

The workshop will encourage active participation in the use case capture process, and in the formulation of a process for building standards profiles. Presentations by representatives of each of the community sectors will analyse the capture process and give a critique of the profiling process as participants continue with the iterative revision and self-evaluation of their submissions.

## Follow-up

The analysis of submitted use cases and the extraction and compilation of standards profiles for the three community sectors will continue for some months after the workshop. CloudWATCH will engage with its network of SDO contacts from among the BIGI representatives, including members from OASIS, OGF, SNIA, IEEE and DMTF, for eventual convergence and consensus of the standards profiles. All workshop participants will be invited to continue to contribute in an iterative process of evaluation until the final output document is produced, which will serve as content for the final user stories for a deliverable in month 18 of CloudWATCH. All participants and affiliations will be acknowledged.

## Annex 2 – Simplified Use Case Template

Use Case		
Title		
Description		Short summary of the use case
Goals and aspirations for the use case		Background and main message of the use case; context of the use case
Legal aspects	Legal domain	Data privacy regulations, licensing, contracting, etc.
	Legal frameworks, laws, etc., to be taken into account	Laws, policies, etc. which are of relevance
	Compliance criteria	Explanation why the use case is an illustration on how legal requirement can be implemented
Organizational aspects	Organization domain	E.g., security procedures, data privacy procedures, etc.
	Regulations and policies to be taken into account	Policies, standards, best practices to be taken into account
	Description of organization procedures	The “workflow” (or procedures) on organizational level used to achieve the goal of the use case
	Compliance criteria	Explanation why the use case is an illustration on how organisational requirement can be implemented
Technical aspects	Preconditions	Assumptions made prior to the execution of the use case
	Criteria for success	Expected process, outcome, side effects. Described by sequence charts, etc.
	Failure conditions and responses	Description of what can go wrong, and what to do about it.
Existing specifications to rely on		Specifications and standards already dealing with aspects related to the use case
New specifications required		Specifications and standards needed to establish the goals of the use case
Additional comments		Add comments, remarks, suggestions, as you see fit