ETSI TR 103 126 V1.1.1 (2012-11)

CLOUD;
Cloud private-sector user recommendations

Reference
DTR/CLOUD-0011-UserRec

Keywords
CLOUD, Requirements, USER

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://ipr.etsi.org).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee CLOUD (CLOUD).

1 Scope

The present document provides an overview of private sector user recommendations for Cloud services especially from the viewpoint of large enterprises in the European context.

The present document defines the objectives to be met by future standardisation requirements for the provision of cloud services.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

Not applicable.

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] "Cloud Computing Use Cases White Paper Version 4.0".

NOTE: Available at: http://cloudusecases.org

[i.2] USERS Recommendations from the European CIO Association for the success of the CLOUD computing in Europe, 30 January 2012.

NOTE: Available at http://ec.europa.eu/information_society/activities/cloudcomputing/docs/consolidated_list_of_recommendations_users_%20perspective.pdf%5b1%5d.pdf

[i.3] "The NIST Definition of Cloud Computing", Special Publication 800-145, September 2011.

NOTE: Available at: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[i.4] ETSI TR 102 997 (V1.1.1): "CLOUD; Initial analysis of standardization requirements for Cloud services".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions given in the NIST Definition of Cloud Computing [i.3] apply:

"Service Models:

Software as a Service (SaaS): *The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.*

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. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.*

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. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).*

Deployment Models:

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.*

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.*

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.*

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)."*

The following terms and definitions also apply:

customer: entity which purchases services offered by another entity

end user: person or organization using a cloud service

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

CRM	Customer Relationship Management
DMTF	Distributed Management Task Force
EC	European Commission
EU	European Union
IaaS	Infrastructure as a Service

ID	Identity
IT	Information Technology
NAC	Network Access Control
PaaS	Platform as a Service
PII	Personally Identifying Information
QoS	Quality of Service
SaaS	Software as a Service
SLA	Software Level Agreement
VM	Virtual Machine

4 Use cases of cloud services

The following clause presents three high level use cases based on use case scenarios of the "Cloud Computing Use Cases White Paper Version 4.0" [i.1] and the EuroCIO Requirements [i.2]. These use cases are the basis for the present document's abstraction of today's large Enterprise needs. The recommendations presented below are derived from an overall assessment of these three scenarios and will be mapped later on to these scenarios.

4.1 Enterprise to Cloud to Enterprise

This use case involves an enterprise using cloud services to support its internal processes. In this scenario, the enterprise uses cloud services to augment its resources, for example:

- Using cloud storage to extend storage for large data volumes, for archival of seldom-used data, to provide resilience and to support data sharing across the enterprise and with partners.
- Using virtual machines (VMs) in the cloud to bring additional processor capacity online to handle peak loads of services and applications (and, of course, shutting down those VMs when they are not needed anymore).
- Using applications in the cloud (Software as a Service (SaaS)) for certain enterprise functions (email, calendaring, Customer Relationship Management CRM, etc.).
- Using cloud databases as part of an application's processing. This could be extremely useful for sharing that database with partners, government agencies, etc.

4.2 Enterprise to Cloud to End User

In this scenario, an enterprise is using the cloud to deliver data and services to the end user. When the end user interacts with the enterprise, the enterprise accesses the cloud to retrieve data and / or manipulate it, sending the results to the end user. The end user can be someone within the enterprise, a customer, or a member of the public.

4.3 Enterprise Community Cloud

This use case potentially includes both public and private clouds where the infrastructure is shared among enterprises with a common purpose (e.g. an integrated supply chain). A Community cloud can be operated by one of the organisations in the community or by a 3rd party cloud provider.

A 3rd party broker can also deliver a Community cloud; the difference is that a broker does not have any cloud resources of its own. Resources in this case may come from the community members or external (e.g. public) cloud providers. In any variant of the Community Cloud use case, it is assumed that management of the cloud resources is carried out on behalf of the customers and based on their terms.

EXAMPLE: A community cloud has an infrastructure shared among enterprises with a common purpose.

5 Functional recommendations to Cloud Scenarios

This clause provides a non-exhaustive list of functional recommendations based on general conclusions from considering the high level use cases described above. These identify priority issues to which Cloud providers, enterprises and end users should find solutions to reduce barriers to adoption of Cloud services.

These functional recommendations will be mapped later on to the previously defined three high level use case scenarios of cloud services.

5.1 Identity and authentication

An end user accessing a cloud service may need to be identified and authenticated.

Enterprises typically have their own policies for managing identity and access control. Cloud services will need to coexist with these in each of the usage scenarios considered. A cloud provider should specify how identity and authentication are managed and ideally offer some flexibility to improve consistency with enterprise systems. Specific considerations include: the way that passwords are managed (encryption, key management), constraints on password format (minimum length, permitted mix of characters), evaluation of password strength when typing, expiry dates for passwords (enforcing change), setting of initial passwords and requirements for change.

Federated identity: In addition to the basic identity needed by an end user, an enterprise user is likely to have an identity with the enterprise. The ideal is that the enterprise manages a single ID, with an infrastructure federating other identities that might be required by cloud services.

It is therefore desirable for a cloud service provider to offer delegation of authentication to the internal access control systems of the enterprise, and to validate "client certificates" for data authentication.

Identity and identity verification may be carried out by the enterprise acting as an identity provider in a federated identity scenario or by an independent 3rd party and result in the allocation of a pseudonym to the user in order to mask the true identity of the user from a cloud service provider.

Secure eAuthentication methods for internet transactions are essential. Common standards that permit safe but seamless use of services would be a major boon to cloud adoption.

5.2 Access control

Access to data and services hosted by a cloud provider from an enterprise user should inherit the data access control of the enterprise. In particular cloud services should not allow escalation of privileges over those afforded to the user when directly connected to services in the enterprise.

Secure client access: In addition to the basic access by an end user, there might be compliance and security reasons for checking the security status of the client (by network access control NAC) for access from outside an enterprise's security perimeter.

5.3 Data Management and Regulatory Compliance

Enterprise cloud service users expect cloud service providers to indicate with which national and international policies and regulations they comply.

The cloud provider should ensure that the provided service complies with data protection and data privacy regulation. In particular where data is transferred across international borders, especially in the case of non-anonymised personal data (Personally Identifying Information (PII)), the national, regional and international regulation for data protection and privacy should be respected.

Regulatory environments are not consistent between different countries and regions. Even within the European Union (EU) there are differences in the national implementations of EU directives. Enterprise customers are looking for clarity on security, privacy and applicable jurisdiction. It is recommended that cloud providers provide straightforward information on how and where data is handled so that potential customers can make informed decisions.

In addition the cloud user and cloud service provider should ensure compliance with national, regional and international requirements for access to information by law enforcement agencies in support of national, regional and international legal processes.

Depending on the kind of data the enterprise is managing on the end user's behalf, there might be legal or other restrictions on the location of the physical server where the data is stored. In particular, much current legislation focuses on PII. Enterprises would like similar protections extended to the privacy and security of company data and the recommendation is that cloud providers offer to handle this data sensitively and with clear statements of policy. This includes any use of subcontractors. When subscribing to a cloud service, the customer should be able to choose the country(ies) where the provider is authorized to locate, circulate and/or administer the cloud service user's data.

There should be no movement of data to or through another region or country without the cloud service user's prior consent.

Cloud service providers are expected to provide the list of countries where their data centres are located and a map of the data flow across countries including countries from where data may be accessed by the provider (or by any government and in which case).

Providers should follow the local (e.g. financial) on-going regulations by adapting their cloud SaaS accordingly.

5.4 Metering and monitoring

All cloud services need to be metered and monitored. This includes cloud infrastructure and network access but also deployed services and applications. This is for instance required for supervising the agreed level of service quality (QoS) as defined in SLA's and to trigger corrective actions if required, but also for cost control, chargebacks and provisioning.

5.5 Network access

"The anticipated convergence of computing, storage and networking into a single integrated infrastructure is becoming a reality. The distinction between network services and the applications they support is disappearing. From the user's point of view, the application experience is what matters and this depends on all the supporting systems performing effectively. This closer integration of IT and network resources is of special interest for real-time and interactive applications (e.g. from the telecommunications area) with particular requirements on network performance. Deploying these applications in the cloud will become feasible when IT and network resources are integrated as a unified infrastructure" [i.4].

Furthermore if some data or service is in the Cloud, accessing it requires ubiquitous and anytime access over high speed networks matching the cloud application needs. Therefore network providers and the corresponding regulation needs adaptation not to hinder the development of cloud dependant markets.

To exclude any public internet latency, it may be that metrics such as availability and performance (e.g. response time) are measured at the cloud service provider's entry point. In general, SLAs are expected to specify an explicit measurement methodology for each metric (quantified in terms). This will clarify the limits of the expectation the customer has of the service. In case the variability of public internet access is not acceptable to an enterprise, it is recommended that there is an option to use private circuits or managed VPNs between customer and cloud service provider.

For media intensive and real time services on the cloud the network is playing a key role.

"Such applications involve several cloud resources in their end-to-end operation, with implications for computing, storage and network performance. Consumers of networked media are geographically distributed and require encoding and delivery that is appropriate to their terminal equipment. Transcoding from an original base format to meet the needs of diverse users is computationally intensive. So too is dynamic rendering of shared virtual environments. Caching techniques or logistical networking may allow the results to be reused by many consumers, at the cost of additional storage. Optimised media creation, adaptation, archiving, distribution and delivery based on the use of cloud infrastructure could be an attractive Platform-as-a-Service (PaaS) offering with scope for standardising interfaces to common features" [i.4].

5.6 Management and Governance

Today cloud providers make it very easy to open an account and begin using cloud services; that ease of use creates the risk that individuals in an enterprise might use cloud services with their enterprise credentials on their own initiative. Enterprises want to be able to enforce their own governance policies and look to cloud service providers to provide information on the end user usage attributed to the enterprise account.

The activation or change of a service instance may involve the enterprise to validate or not the required service. This is related to the identity management issues identified above. The enterprise should also be able to set quotas and be warned in case the services are used above agreed limits.

5.7 Security

Use cases of enterprise cloud service customer require more stringent security requirements than an ordinary end user expected.

Enterprise cloud service customers expect cloud service providers to offer, for each of their service, different levels of security from which they can choose.

The cloud service provider should describe the levels of data security, confidentiality, integrity, availability, including data backup, and the means the cloud service provider employs to deliver these levels of data security (e.g. through certifications to be listed). Relevant operational details are of interest, including any antivirus and antimalware protection as well as network intrusion detection and prevention.

A cloud service provider is expected to promptly notify an enterprise user of any data breach (e.g. to enable compliance to any local data breach notification duties). Terms of service should also specify responsibility for breach notification. Enterprises may want the ability to prevent the cloud service provider from making public statements related to the content of any breach. Cloud providers should also proactively forward data of any activity relating to (possible) attempts to break into the data and other suspicious activity that may have a relevance to the security of the data.

Enterprise cloud service customers need a security certification guaranteeing minimum operating standards irrespective of location. Independent certification and audit organizations could base their work on such standard. Cloud providers are expected to offer the means for a certified and trustworthy third party audit organization to carry out audits of its cloud services, periodically or at the request of customers. Procedures for audit are expected to be defined as part of the terms of service.

Ownership of the data remains in all cases with the cloud service user. The cloud service provider should be precluded from accessing the data for any purpose other than that explicitly permitted by the user organization.

Users' traceability logs (tracking who did what when, including physical access i.e. administrators) are user's data to be accessible at any time to the customer administrator.

Data including communications should be encrypted by the provider, in particular when going through the internet. The contract should specify the agreed encryption algorithm and key length for data in-flight and data at rest.

Additionally, a higher/stronger EU wide strength of data encryption would increase enterprise confidence in cloud services. A particular issue is that some countries specify maximum key lengths for encryption, with different limits in each country. This forces providers to apply the lowest strength to be allowed to circulate the data across borders, weakening security. It is therefore desirable that EU Member States modify their regulations regarding maximum encryption strengths, possibly replacing them with other obligations on organizations to provide access to law enforcement agencies.

5.8 Interoperability

"Interoperability is closely related to portability. Here we interpret interoperability as the ability to federate multiple clouds to support a single application. In other words, interoperability involves software and data simultaneously active in more than one cloud infrastructure, interacting to serve a common purpose.

Considering cloud interoperability in general, the term "Intercloud", is starting to gain some acceptance. It is analogous to the Internet and based on a similar vision - connecting individual, essentially uncoordinated cloud infrastructures and giving control to the users. One of the lessons of the Internet is that the use of common protocols (or interfaces) readily accessible to developers has great benefits in stimulating innovation (...)

a cloud service provider or an enterprise cloud service customer may take on this coordination role, using services from a number of third party providers to meet the overall performance guarantee to the end user. One example could be a compute cloud provider using a network provider for delivery. This scenario requires standards for the sharing of management information such as SLA goals between service providers without exposing too much confidential detail of how the goals are met.

Even these allow us to suggest a number of dimensions for the discussion of Cloud interoperability:

- ***Application/Service:*** *Interoperability standards should support distributed applications with predictable behaviour and performance. Components of a single application could be deployed across multiple cloud infrastructure providers and possibly reconfigured while running, or with limited interruption, to respond to changes in usage patterns or resource availability, for example. Application configuration should be resilient to changes in the configuration within each cloud - for example scaling or migration of computational resources.*

- ***Management:*** *Standardised interfaces should be provided by cloud service providers so that a single application can be managed in a consistent way, end-to-end - substantially independent of the details of its deployment across multiple cloud infrastructures. It will be possible for a management application to control and coordinate components in multiple clouds Standardised management functionality for deployment and migration of virtual machine images between different cloud infrastructures is required. Management interoperability requires interactions between multiple independent actors responsible for application management and infrastructure management.*

- ***Data:*** *Standards are required to support the deployment of equivalent virtual machine images and application data to different cloud infrastructures. A basic requirement for cloud interoperability is network connectivity between cloud environments, appropriate to carry application traffic. In particular, security and other cross-domain data management issues need to be handled in standard ways.*

- ***Network aspects:*** *Network access to computational resources is fundamental to cloud services. Standards are required to support both uniform access to individual cloud computing resources and concatenation or federation of clouds in different locations. Interconnection between clouds should support the quality requirements of applications. Network connectivity will in general be based on the use of shared physical resources in a similar way to computing and storage. Standards for allocation and admission control will be needed" [i.4].*

5.9 Portability & Deployment

Cloud computing with the strong industrial drivers and the initial uptake already in place has a strong tendency to impel de-facto standards (vendor lock in).

The aspect "Not to be Locked In" drives the need of portability standards to ensure that enterprise customers are able to access an open market of cloud services and can change and interconnect providers with suitable effort. The scope of open standards should cover data formats, access protocols and programming interfaces.

"Portability in general refers to the ability to migrate applications between different clouds. This is required to allow customers of cloud services to avoid the situation of being locked into a specific cloud infrastructure provider, having made the decision to run an application in the cloud. This adds to the perceived risks associated with moving to cloud computing. A potential customer needs a high level of trust in the technical and commercial ability of a chosen provider to support critical business applications in the long term.

Current cloud infrastructure providers offer their own proprietary interfaces to application developers. Standardised interfaces to manage cloud infrastructures and the different types of resource they provide are required. Reducing the mismatch between different cloud infrastructure systems would not only enable a competitive market but also enable new business models where different cloud infrastructures can be traded according to price and demand.

At one extreme, the ability to automatically migrate a complete running application (including any necessary monitoring and management features) from one cloud infrastructure to another would clearly be attractive to customers (but much less so to cloud infrastructure providers, particularly in the current market).

Portability of a virtual machine images is being addressed by the DMTF Open Virtualisation Format (OVF). This should provide a good basis for limited portability but its support for complex configuration and interactions with any supporting systems is currently limited. These issues are naturally within the scope of a service provider.

Portability of data is essential for a typical business application. The ability for a customer to retrieve application data from one cloud infrastructure provider and import this into an equivalent application hosted by an alternative provider reduces the risk of long-term dependency. This would probably involve a not insignificant amount of effort from the customer (or an application service provider - the details will be largely application specific and not the responsibility of a cloud infrastructure provider). Achieving data portability depends on effective standardisation of data import and export functionality between cloud infrastructure providers" [i.4].

Software licensing has always been complex. The cloud makes it more so. It is recommended to review the basis of licensing proposed in a cloud environment. Aspects of portability and reuse of existing licenses at deployment phase and portability aspects have to be defined carefully to ensure life costs benefits. Specific issues are: credit for existing licenses and perpetual license usage.

5.10 Reversibility

Large enterprises are already using cloud solutions to support their data and information systems. The real issue is that once you have your cloud solution provider, it is extremely difficult to change provider. Each cloud solution provider uses a proprietary set of interfaces and data formats. Opening up this market requires standardisation, at the level of architecture, building blocks and system level. Therefore there is a need for standardisation.

Enterprise cloud service users should be able to retrieve all or part of their data on demand and autonomously (i.e. without special action on the part of the cloud service provider). They should be able to select data and filter specific items of interest.

If the user can not autonomously retrieve data, as a minimum the provider should be contractually bound to give the data back in a defined time period through the internet or on physical storage, with significant penalties (specified in the SLA).

The scope of reversibility extends to beyond simple stored files and database records to complex data such as business process logic encoded in an application, raw transactional, master data, aggregated data, blobs, logs, report definitions, parameterization & configuration tables, and so forth.

By default, the format in which data is returned should be in the same format in which it was provided. If data was created in the cloud, the format should be standard and reusable, not losing information.

Enterprise cloud service users expect the retrieval duration to be limited.

The cloud service user expects a guaranteed minimum period of time (i.e. X months, specified in the SLA) for data retention and accessibility after the end of service by the cloud service provider before all information will be permanently deleted in the systems of the cloud provider.

An agreed upon data destruction policy is needed (e.g. to delete data on all physical devices, including backup tapes and any other multiple off-line duplication for remote copying).

Once the contract between the user and its provider has terminated and once all user's data are fully retrieved then the provider will confirm and assure that all data have been erased from its systems.

Enterprises have concerns about measures associated with bankruptcy or other significant changes to the business of the cloud service provider. In particular, it is recommended that a cloud service user is assured of the timely return of its data. It should be clear that the data remains the property of the customer. Mechanisms and procedures for retrieval of data should be put in place and described in the contractual terms associated with the service. Regulatory and/or industry solutions to issues such as this would be welcome.

5.11 SLAs and Benchmarks

"Service Level Agreements (SLAs) in this context are understood to be unambiguous statements of the expectations and responsibilities of both users and providers of cloud services.

An SLA is a contract between the provider and the customer of a service specifying the function performed by the service, the agreed bounds of performance, the obligations on both parties to the contract and how any deviations are to be handled. An SLA is made in a business context and therefore will include all aspects of the interaction between the provider and customer relevant to the service" [i.4].

Enterprises who sign contracts based on SLAs will need a standard way of benchmarking performance.

Enterprise cloud service users expect unambiguous cloud service provider offers/SLAs. Offers from different cloud service providers should use the same terminology so that offers can be compared. The service level should be guaranteed by cloud service providers, and measurable by cloud service users.

Cloud service providers' offers/SLAs should address at least the following items:

- Information on end user service availability, including guaranteed availability, activation time, and any interruption of service due to service maintenance.
- Information on performance including guaranteed response time.
- Information on the availability of analytics assessing the quality of the delivered service to Cloud Service User and audit bodies. Enterprise Cloud Service Users expect those analytics to always be accessible for them and audit bodies.
- Procedure in case of incident activation time, including any interruption of service due to service maintenance.

Contractual clauses, to be signed by the cloud provider, is today a good starting point for every data importer in a non-EU country. Subcontractors should be bound as well.

Contractual clauses should include the applicable jurisdiction.

SLA should specify what happens in the event of breach.

End users can be disturbed by regularly changing cloud services, so an option for a static service is welcome (presumably cheaper), or at least to have the choice of the moment when the upgrade/evolution occurs.

A user entering a cloud service expects this service to be accessible for a minimum duration.

Any service termination should be communicated at least X months in advance.

The SLA should specify the pricing model. An example of pricing model is usage based.

Any subcontractor should be identified.

5.12 Lifecycle Management

Enterprises need be able to manage the lifecycle of applications and documents. This need includes versioning of applications and the retention and destruction of data. Discovery (i.e. in a legal sense, where there is a requirement to make available material which may reasonably lead to admissible evidence in litigation) is a major issue for many organizations. There are substantial legal liabilities if certain data is no longer available. Some of this material may be stored in cloud services and so there is a need for clear specification of how the lifecycle of information is managed. This covers data retention, including resilience and availability. In addition, in some cases an enterprise will want to make sure data is destroyed at some point, consistent with applicable regulation and corporate policy.

6 Mapping of functional recommendations to Cloud Scenarios

The list of functional recommendations is mapped to the previous defined three high level use case scenarios of cloud services. Table 1 shows the relevance of the requirements to the scenarios.

Table 1: mapping of functional recommendations to scenarios

	Enterprise to Cloud to Enterprise	Enterprise to Cloud to End User	Enterprise Community Cloud
1. Identity and authentication		✓	✓
2. Access Control		✓	✓
3. Regulatory compliance	✓	✓	✓
4. Metering and monitoring		✓	✓
5. Network access			
6. Management and Governance		✓	✓
7. Security	✓	✓	✓
8. Interoperability		✓	✓
9. Deployment & Portability	✓	✓	✓
10. Reversibility		✓	✓
11. SLAs and Benchmarks		✓	✓
12. Lifecycle Management	✓		✓

History

Document history		
V1.1.1	November 2012	Publication