International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

FG Cloud TR

Version 1.0
(02/2012)

Focus Group on Cloud Computing
Technical Report

Part 5: Cloud security

FOREWORD

The procedures for establishment of focus groups are defined in Recommendation ITU-T A.7. The ITU-T Focus Group on Cloud Computing (FG Cloud) was established further to ITU-T TSAG agreement at its meeting in Geneva, 8-11 February 2010, followed by ITU-T study group and membership consultation.

Even though focus groups have a parent organization, they are organized independently from the usual operating procedures of the ITU, and are financially independent. Texts approved by focus groups (including Technical Reports) do not have the same status as ITU-T Recommendations.

INTELLECTUAL PROPERTY RIGHTS

The ITU draws attention to the possibility that the practice or implementation of this Technical Report may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU-T Focus Group participants or others outside of the Technical Report development process.

Table of Contents

1. Scope

The scope of this Technical Report is to identify study subjects on cloud security that need to be worked on and studied in ITU-T, in collaboration with related SDOs. The method of identification is to initially review the ongoing activities on cloud security in related SDOs, and to identify several security threats and security requirements for cloud service users and service providers based on these reviews. Finally, a list of subjects on cloud security for study by ITU-T is provided as a Technical Report for TSAG.

2. Definitions

2.1 Terms defined elsewhere

2.1.1 cybersecurity [b-ITU-T X.1205]: The collection of tools, policies, security concepts, security safeguards, guidelines, risk-management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise availability, integrity (which may include authentication and non-repudiation, and confidentiality).

NOTE – Some specific national regulation and legislation may require implementation of mechanisms to protect personally identifiable information.

2.1.2 security incident [b-ITU-T E.409]: Any adverse event whereby some aspect of security could be threatened.

2.1.3 on-demand self-service [b-FG Technical Report (ecosystem)]: A user can unilaterally provision computing capabilities, such as server time, network storage and communication and collaboration services, as needed automatically, without requiring human interaction with each service's provider.

2.1.4 broad network access [b-FG Technical Report (ecosystem)]: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).

2.1.5 appliance [b-CSA Glossary]: A self-contained IT system that can be plugged into an existing IT infrastructure to carry out a single purpose.

2.1.6 application virtualization [b-CSA Glossary]: A virtual implementation of the application programming interface (API) that a running application expects to use.

2.1.7 authentication [NIST-SP800-53]: Verification of the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

2.1.8 certificate [b-Virginia Tech]: A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its Subscriber, (3) contains the Subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it.

2.1.9 client [b-NIST 800-146]: A machine or software application that accesses a cloud over a network connection, perhaps on behalf of a subscriber.

2.1.10 cloud computing [b-FG Technical Report (ecosystem)]: Cloud computing is a model for enabling service user's 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. Cloud computing enables cloud services.

2.1.11 cloud infrastructure as a service (IaaS) [b-FG Technical Report (ecosystem)]: A category of cloud services where the capability provided by the cloud service provider to the cloud service user is to provision processing, storage, intra-cloud network connectivity services (e.g. VLAN, firewall, load balancer, and application acceleration), and other fundamental computing resources of the cloud infrastructure where the cloud service user is able to deploy and run arbitrary application.

NOTE: The cloud service user does not manage or control the resources of the underlying cloud infrastructure but has control over operating systems, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

2.1.12 cloud platform as a service (PaaS) [b-FG Technical Report (ecosystem)]: A category of cloud services where the capability provided to the cloud service user is to deploy onto the cloud infrastructure user-created or acquired applications developed using platform tools supported by the cloud service provider. NOTE: platform tools may include programming languages and tools for application development, interface development, database development, storage and testing. The cloud service user does not manage or control the underlying cloud infrastructure, but has control over the deployed applications and possibly application hosting environment configurations.

2.1.13 cloud service provider (CSP) [b-FG Technical Report (ecosystem)]: An organization that provides and maintains delivered cloud services.

2.1.14 cloud service partner (CSN) [b-FG Technical Report (ecosystem)]: A person or organization who provides support to cloud service provider's service offer building (e.g. service integration)

2.1.15 cloud service [b-FG Technical Report (ecosystem)]: A service that is delivered and consumed on demand at any time, through any access network and using any connected devices using cloud computing technologies.A service that has the essential characteristics of cloud computing.

2.1.16 cloud software as a service (SaaS) [b-FG Technical Report (ecosystem)]: A category of cloud services where the capability provided to the cloud service user is to use the cloud service provider's applications running on a cloud infrastructure.

NOTE: All applications have the common characteristic to be non real time and may be of different kinds, including IT and business applications, and may be accessible from different user devices. The cloud service user does not manage or control the underlying cloud infrastructure with the possible exception of limited user-specific application configuration settings.

2.1.17 cloud service user (CSU) [b-FG Technical Report (ecosystem)]: A person or organization that consumes delivered cloud services.

2.1.18 compliance [b-CSA Glossary]: The act of adhering to, and demonstrating adherence to, a standard or regulation.

2.1.19 control [b-NIST 800-146]: The ability to decide, with high confidence, who and what is allowed to access subscriber data and programs, and the ability to perform actions.

2.1.20 disk image [b-NIST 800-125]: A virtual representation of a real-disk drive.

2.1.21 hypervisor [b-NIST 800-125]: The virtualization component that manages the guest OSs on a host and controls the flow of instructions between the guest OSs and the physical hardware.

2.1.22 hybrid cloud [b-NIST DFN]: The cloud infrastructure is a composition of two or more clouds (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).

2.1.23 image [b-NIST 800-125]: A file or directory that contains, at a minimum, the encapsulated components of a guest OS. Logical partitioning: The hypervisor allowing multiple guest OSs to share the same physical resources.

2.1.24 measured service [b-FG Technical Report (ecosystem)]: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and user of the utilized service.

2.1.25 multi-tenancy [b-FG Technical Report (ecosystem)]**:** A characteristic of cloud in which resources are shared amongst multiple-cloud tenants. There is an expectation on the part of the cloud tenant that its use of the cloud is isolated from other tenants' use of any shared resources; that tenants in the cloud are restricted from accessing or affecting another tenant's assets; that the cloud tenant has the perception of exclusive use of, and access to, any provisioned resource. The means by which such isolation is achieved vary in accordance with the nature of the shared resource, and can affect security, privacy and performance.

2.1.26 partitioning [b-NIST 800-125]: Managing guest operating system access to hardware so that each guest OS can access its own resources but cannot encroach on the other guest OSs' resources or any resources not allocated for virtualization use.

2.1.27 private cloud [b-NIST DFN]: The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.

2.1.28 public cloud [b-NIST DFN]: The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

2.1.29 rapid elasticity [b-FG Technical Report (ecosystem)]: Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out, and rapidly released to quickly scale in. To the user, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

2.1.30 resource pooling [b-FG Technical Report (ecosystem)]: The provider's computing resources are pooled to serve multiple users using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to user demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data centre). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

2.1.31 Sec-aaS [b-CSA GuideV3]: see the Technical Report (Introduction to the cloud ecosystem: Definitions, taxonomies, use cases, high-level requirements and capabilities)

2.1.32 service agreement [b-NIST 800-146]: A legal document specifying the rules of the legal contract between a subscriber and provider.

2.1.33 service level agreement (SLA) [b-CSA Glossary]: An abbreviated service agreement stating the technical performance promises made by a provider, including remedies for performance failures. An SLA is composed of three parts: (1) a collection of promises made to subscribers, (2) a collection of promises explicitly not made to subscribers, i.e., limitations, and (3) a set of obligations that subscribers must accept.

2.1.34 snapshot [b-NIST 800-125]: A record of the state of a running image, generally captured as the differences between an image and the current state.

2.1.35 tagging or colouring [b-CSA Glossary]: The assignment of additional descriptor attributes to hardware, virtual machines, guest-operating systems, data elements and network traffic which facilitate policy constraints, privilege and obligations.

2.1.36 virtual machine (VM) [b-CSA Glossary]: An efficient, isolated, logical duplicate of a real machine.

2.1.37 virtualization [b-NIST 800-146]: The simulation of the software and/or hardware upon which other software runs.

2.2 Terms defined in this document

2.2.1 assurance: The degree of confidence that the process or Technical Report meets defined characteristics or objectives.

2.2.2 information exchange policy: The terms and conditions associated with the use and sharing of cybersecurity information.

2.2.3 VPN: Private communication network that is based on the public network (uses information security and channelling protocol in order to maintain security of information transferred over the general network).

2.2.4 IPsec VPN: IPSec works on the network layer of the OSI model- securing all data that travels between the two endpoints without an association to any specific application. The majority of IPSec VPN solutions require third-party hardware and software. In order to access an IPSec VPN, the workstation or device must have an IPSec client software application installed. It provides the network edge to the client's security; and only encrypts the channel from the client to the VPN gateway.

2.2.5 SSL VPN: SSL VPNs are an alternative to IPsec that rely on a web browser, instead of custom VPN clients, to log on to the private network. SSL is running on the application layer, independent of the underlying protocol. It provides application security services rather than network security services. It guarantees the safety of end-to-end and entire process encryption from client to server.

3. Abbreviations and acronyms

This Technical Report uses the following abbreviations and acronyms

A&A	Assessment and Authorization
AAA	Authentication, Authorization, and Audit
BCP	Business Continuity Plan
CAIQ	Consensus Assessment Initiative Questionnaire
CCSK	Certificate of Cloud Security Knowledge
CIM	Common Information Model
CSA	Cloud Security Alliance
ECE	Event Condition Expectation

GRC	Governance, Risk Management and Compliance
IdM	Identity Management
LOA	Level of Assurance
NAS	Network-Attached Storage
PII	Personally Identifiable Information
SAN	Storage Area Network
SAS	Statements on Auditing Standards

4. Overview of SDO activities on cloud security

4.1 ENISA

One of the most widely-read reference documents on cloud security, *Cloud computing: benefits, risks and recommendations for information technology,* by ENISA, uses a risk-assessment approach to analyse the security issues raised by cloud services.

Starting by an evaluation of the assets of a cloud infrastructure, this Technical Report identifies 23 of the main assets of IT systems that should be taken into account for the asset evaluation. A list is given of 53 different vulnerabilities corresponding to all of the assets. The most important results of this report are:

1. A prioritised list of organizational, technical, and legal risks, for clients of cloud providers.
2. An assurance framework allowing cloud customers to compare different providers according to their security practices. The assurance framework focuses on controls which address the specific risks that have been identified and are adapted to cloud scenarios.
3. A comprehensive analysis of legal issues raised by cloud computing, and advice for contractual negotiations or selection of providers on the basis of their contractual conditions and proposed SLAs.

The assurance framework has also been published separately, and has been used by several government organizations to support the selection of cloud contracts. As a follow-up to this report, ENISA has also participated in the Common Assurance project (http://common-assurance.com/) and, in 2011, is surveying procurement practices in relation to cloud computing. In 2011, a best practice guide for setting and evaluating conditions for cloud contracts and SLAs will be published.

As a second follow-up, ENISA has also produced the report: *Security and Resilience in Governmental Clouds*, which provides a decision-making model that can be used by governments considering using cloud computing to determine which architectural solution would best suit their security requirements.

The main objectives of the report are:

- to highlight the pros and cons of community, private and public clouds models with regard to information security and resilience,
- to guide public bodies in the definition of their information security and resilience requirements when evaluating cloud options
- to support EU MSs in the definition of their national cloud strategy with regard to security and resilience.

4.2 CSA

The Cloud Security Alliance (CSA) is a non-profit organization formed to promote the use of best practices for providing security assurance within cloud computing, and provide education on the uses of cloud computing to help secure all other forms of computing.

CSA's objectives are:

- to promote a common level of understanding between the consumer and the provider of cloud computing with regard to security requirements and attestation of assurance
- to promote independent research into best practices for cloud computing security
- to launch awareness campaigns and educational programmes on the appropriate uses of cloud computing, and cloud security solutions
- to create consensus lists of issues and guidance for cloud security assurance

CSA first published the security guidance for critical areas of focus in cloud computing. This document introduces 13 areas, which are supported by an ad-hoc working group structure. Rather than correlating the domains to the work groups, the work groups are formed to support and supplement the requirements defined in the CSA guidance and break the guidance into functional tasks

4.2.1 Governance, risk management and compliance (GRC) stack

This stream is responsible for coordinating four other streams:

1. cloud control matrix
2. consensus assessment initiative
3. cloud trust protocol
4. cloud audit.

Its goal is to provide a comprehensive framework to cloud providers, allowing them to answer in a standard way to the most usual tenant issues concerning cloud computing.

4.2.2 Security guidance for critical areas of focus in cloud computing

Security guidance has now reached its third revision and each domain's core research is being released as its own white paper (https://cloudsecurityalliance.org/research/security-guidance/).

The third version is a collection of documents, with the following thirteen domains:

Domain 1:	Cloud computing architectural framework
Domain 2:	Governance, risk and compliance
Domain 3:	Legal and electronic discovery
Domain 4:	Audit and assurance
Domain 5:	Information lifecycle management
Domain 6:	Portability and interoperability
Domain 7:	Traditional security, business continuity and disaster recovery
Domain 8:	Data operations
Domain 9:	Incident response, notification, and remediation
Domain 10:	Application security
Domain 11:	Encryption and key management
Domain 12:	Identity and access management
Domain 13:	Security as a service

4.2.3 Cloud control matrix (CCM)

The cloud control matrix provides a mapping between tenant security issues (defined in CAI), standards, and control topics recorded during a cloud audit. This document is annually enhanced and forms the basis for the ISO/IEC JTC1/SC27 ISMS control standard

4.2.4 Consensus assessment initiative questionnaire (CAIQ)

The consensus assessment initiative questionnaire (CAIQ) is composed of 148 yes/no questions. These questions enable providers to offer details on how they meet the CSA CMM control objectives. The questions also form the basis for establishing service level objectives that may be written into business-to business-agreements and measured using the Cloud Audit and Cloud Trust Protocol.

4.2.5 Cloud metrics

Cloud metrics is a companion project of CCM and cloud audit defining objective criteria related to security control items. Cloud metrics encompasses xDas, CEE and Syslog-ng and collaborates with the DMTF Cloud Audit Data Federation Work Group.

4.2.6 Cloud data governance

Cloud computing stakeholders need to be aware of the best practices for governing and operating data and information in the cloud. This effort encompasses the labelling and “colouring” of virtual assets for forensic analysis and legislative action. Issues addressed in this group include the use of obligatory predicates, labels subject denoting legal hold, line of business specific meta tagging, and the application of semantic technologies such as RuleML, CEP, LegalRuleML, Legislative XML, OWL, RDF, SBVR, SWRL, RIF-OWL, LKIF, SWRL and ECE (Event Condition Expectation) This is in line with the concerns highlighted by section II (Domain 5: Information Lifecycle Management) in the CSA Guidance v3.0.

4.2.7 Trusted cloud initiative (TCI)

The trusted cloud initiative (TCI) presents a multi-tier architecture integration TOGAF (The Open Group) ITIL, and SABSA (Zachman security model), with individual security elements mapped to CMM controls

4.2.8 Top threats to cloud computing

The top threats document gives a snapshot of the seven main cloud security issues as seen by tenants.

4.2.9 Cloud Audit (formerly A6)

The goal of Cloud Audit is to provide a common interface and namespace that allows cloud computing providers to automate the audit, assertion, assessment, and assurance (A6) of their cloud computing environments and allow authorized consumers of their services to do likewise via an open, extensible and secure interface and methodology. The second goal is to provide a comparison basis between providers.

4.2.10 Cloud Trust Protocol (CTP)

The Cloud Trust Protocol details a mechanism to communicate enhanced SCAP – CYBEX/RID/ CEE exchanges and offers a *representational state transfer* (REST – http://en.wikipedia.org/wiki/Representational_State_Transfer) mechanism with *hypermedia as the engine of application state* (HATEOAS – http://en.wikipedia.org/wiki/HATEOAS). The Cloud Trust Protocol stores supporting documentation and result sets using an updated Cloud Audit URI approach (https://tools.ietf.org/html/draft-hoff-cloudaudit-00) .

4.2.11 Common assurance maturity model (partner project with ENISA)

This stream provides an objective framework for transparently benchmarking capabilities to deliver information assurance maturity of selected solutions across ones supply chain

4.2.12 CloudSIRT

CSA launched this initiative to enhance the capability of the cloud community to prepare for and respond to vulnerabilities, threats, and incidents in order to preserve trust in cloud computing.

4.2.13 Security as a service

CSA is embarking on this new research project to provide research for gaining greater understanding on how to deliver security solutions via cloud models.

Like these 11 working groups, each guidance domain is functionally supported by one or more working groups. A telecommunication working group is in development, and will cover topics such as implementation and interoperability, communication with other telecommunication bodies, and a security certification scheme.

Lastly, the CSA has published a certificate of cloud security knowledge (CCSK) based on the security guidance document.

4.3 DMTF

DMTF does not have a specific working group dealing with security. There is some work done in different working groups, but currently the only document which can be identified as being published is a white paper dealing with CIM User and Security Model Version 2.7 (DSP 0139), and dates back to June 2003. Below is the abstract of this white paper.

- Abstract DSP 0139: The DMTF Common Information Model (CIM) is a conceptual information model for describing computing and business entities in enterprise and Internet environments. It provides a consistent definition and structure of data, using object-oriented techniques. The CIM Schema establishes a common conceptual framework that describes the managed environment. The User and Security Model provides classes to manage and retrieve organizational data and information about "users" of services and their credentials. As part of this work, systems' accounts for users, and the key services involved in managing authentication and authorization are modeled. This white paper contains a short description of the CIM User and Security Model and an example instantiation of the model, complete with MOF files.

In addition, there are inputs from the Academic Alliance Partner Research program that DMTF is running. There are four contributions with regard to security, namely:

- Distributed network security: IP-based networks form the base of today's communication infrastructure. The interconnection of formerly isolated networks brings up severe security issues. The standard approach to protect the user's own network from abuse is the usage of filter mechanisms at the border of the foreign network. The rising complexity of protocols and the use of encryption techniques render most of these border-oriented systems useless, as they are not able to track or analyze the transferred data. The approach discussed in this article is split into three parts:

  first, we invent distributed sensors which enlarge the amount of data available for analysis by accessing information directly at its source;

  second, to integrate these into the classic border-oriented system we create an abstract interface and management system, based on the common information model (CIM).

finally, we divide the management system itself into independent components, distribute them over the network, and gain a significant increase in performance.

- Toolkit for Policy Based Security Management, by Andreas Pilz, Technische Universität München.
- Architecture for Managing Clouds White Paper (DSP-IS0102): This white paper is one of two Phase 2 deliverables from the DMTF cloud incubator and describes the reference architecture as it relates to the interfaces between a cloud service provider and a cloud service consumer, including security architecture. The goal of the incubator is to define a set of architectural semantics that unify the interoperable management of enterprise and cloud computing.
- Cloud Auditing Data Federation is an activity in collaboration with the Cloud Security Alliance Metrics and Controls developing a metric and measure ontology that may be expressed through the cloud-audit protocol and used to satisfy service level obligations

4.2 NIST

The role of the National Institute of Standards and Technology (NIST) in cloud computing is to promote the effective and secure use of the technology within government and industry by providing technical guidance and promoting standards. NIST provides NIST's definition of cloud computing as well as related guidance. This definition will serve as a foundation for NIST's upcoming publication on cloud models, architectures, and deployment strategies.

NIST is responsible for accelerating the U.S. Federal Government's secure adoption of cloud computing. In order to execute this responsibility, NIST is leading a number of efforts to develop cloud standards and guidelines, in close consultation and collaboration with standards bodies, the private sector, and other stakeholders. The NIST work involves two complementary efforts. One effort is tactical in nature, and is entitled Standards Acceleration to Jumpstart the Adoption of Cloud Computing (SAJACC). The other effort is strategic, and is called a Strategy to Build a U.S. Government (USG) Cloud Computing Technology Roadmap.

- NIST recently published the following two Cloud Computing Special Publications: A NIST Definition of Cloud Computing, SP800-145.pdf, September 2011
- DRAFT Cloud Computing Synopsis and Recommendations Draft-NIST-SP800-146.pdf, May 2011

NIST also released for comment the following two Cloud Computing Special Publications:

- NIST Special Publication 500-293, U.S. Government Cloud Computing Technology Roadmap, Release 1.0 (Draft), Volume I High-Priority Requirements to Further USG Agency Cloud Computing Adoption
- NIST Special Publication 500-293, U.S. Government Cloud Computing Technology Roadmap, Release 1.0 (Draft), Volume II Useful Information for Cloud Adopters

Through its efforts in developing these documents, NIST is helping to translate U.S. Federal Government operational requirements into cloud-related data portability, interoperability and security technical requirements. Included in these documents is the output from several public working groups, chaired by NIST. These working groups are a key component of the NIST cloud outreach program and are designed to integrate the NIST internal cloud computing efforts with a broader dialogue with academia, SDOs, industry and government stakeholders. The NIST-chaired cloud public working groups include the following: USG Business Use Cases, Reference Architecture and Taxonomy, Standards Roadmap, Standards Acceleration to Jumpstart the adoption of Cloud Computing (SAJACC), and Cloud Security. Working in parallel, these working groups are developing material that will be integrated into the IR. The intent is to use the documents to prioritize cloud initiatives which support U.S. government agencies. The expectation is that the set of priorities, or the Roadmap, will also be used broadly by industry, Standards Development Organizations (SDOs), cloud adopters, and policy makers. The long term goal of NIST is to provide leadership and guidance around the cloud computing paradigm and to encourage its use within industry and the federal government.

The NIST definition of cloud computing (SP 800-145, September 2011) includes five essential characteristics, three service models (IaaS/PaaS/SaaS), and four deployment models (public cloud/private cloud/community cloud/hybrid cloud). These definitions have already been widely adopted by many organizations, including ISO/IEC JTC 1/SC38. Equally important, NIST has produced a number of cloud related Special Publications, some of which are in the final stages of publication. For example, prior to the NIST's work on the Cloud Computing Technology Roadmap, NIST and others in the U.S. Federal Government published a Federal Chief Information Officer document, entitled *Proposed Security Assessment & Authorization for U.S. Government Cloud Computing*. This document was based on NIST Special Publications (800-37R1, and 800-53) and is organized into three parts. One part presents a list of baseline security controls for low and moderate impact cloud systems. NIST Special Publication 800-53R3 provided the foundation for the development of these security controls. The second part of this document describes the process under which authorized cloud computing systems will be monitored. This section defines continuous monitoring deliverables, reporting frequency, and responsibility for cloud service provider compliance with FISMA. The third part of the document describes various aspects of an authorization (including sponsorship, leveraging, maintenance, and continuous monitoring), a joint authorization process, and roles and responsibilities for federal agencies and cloud service providers in accordance with the risk management framework detailed in NIST Special Publication 800-37R1.

In connection with cloud security, the publication *Proposed Security Assessment & Authorization for U.S. Government Cloud Computing* was produced by the U.S. Government (FedRamp) based on NIST Special Publications (800-37R1, 800-53). The document on cloud computing describes the U.S. Government's proposed *Assessment and Authorization (A&A) for U.S. Government Cloud Computing*. The document is organized into three Chapters as follows:

Chapter 1: Cloud computing security requirement baseline

This chapter presents a list of baseline security controls for low and moderate impact cloud systems. NIST Special Publication 800-53R3 provided the foundation for the development of these security controls.

Chapter 2: Continuous monitoring

This chapter describes the process under which authorized cloud computing systems will be monitored. This section defines continuous monitoring deliverables, reporting frequency, and responsibility for cloud service provider compliance with FISMA.

Chapter 3: Potential assessment and authorization approach

This chapter describes the proposed operational approach for A&As of cloud computing systems. This reflects upon all aspects of an authorization (including sponsorship, leveraging, maintenance and continuous monitoring), a joint authorization process, and roles and responsibilities for federal agencies and cloud service providers in accordance with the risk management framework detailed in NIST Special Publication 800-37R1.

NIST is in the process of finalizing the publication *Cloud Computing Challenging Security Requirements for USG Adoption of Cloud Computing* which can be downloaded from:

(http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/CloudSecurity/NIST_Security_Requirements_for_US_Government_Cloud.pdf). The target date for completion of this document is March 2012.

4.3 ISO/IEC JTC1/SC27

Based on the recommendations contained in the Report (SC 27 N10220) of the joint ISO/IEC JTC 1/SC 27 WG 1/WG 4/WG 5 *Study Period on Cloud computing security and privacy* (April 2011 to August 2011), ISO/IEC JTC 1/SC 27 agreed to develop cloud computing security and privacy projects in the following two areas:

- security controls to be developed by ISO/IEC JTC 1/SC 27/WG 1 (ISO/IEC 27017);
- data protection to be developed by ISO/IEC JTC 1/SC 27/WG 5 (ISO/IEC 27018); as a new work item, pending its National Bodies' approval.

In addition, it was agreed that further consideration of the recommendations, contained in the report SC 27 N10220 and the meeting report SC 27 N10614, and the need to investigate additional new projects will be the subject of discussion in an extended six-month Study Period (October 2011 to March 2012).

4.4 ISO/IEC JTC1/SC38

ISO/IEC JTC 1/SC38 (*DAPS; Distributed Application Platforms and Services*) has established a SC38/WG3 in order to provide candidates of standardization issues on cloud computing to JTC 1 and to develop NPs (New Work Item Proposals) on cloud computing, to be studied in JTC 1.

Currently, the security issues in JTC1 SC38/SGCC are under consideration.

4.5 Global Inter-Cloud Technology Forum (GICTF)

The Global Inter-Cloud Technology Forum (GICTF) does not have any specific working groups dealing with security. However, issues related to disaster recovery and business continuity are worked out in depth as important use cases for inter-cloud computing. Furthermore, SLA metrics, including security attributes for the inter-cloud environment, have also been investigated in a white paper entitled *Use Cases and Functional Requirements for Inter-Cloud Computing*.

4.6 ITU-T SG17

ITU-T SG17 has been designated the lead Study Group for Telecommunication Security, whose tasks include the developing and maintaining of security outreach material; the coordination of security-related work; the identification of needs, and the assignment and prioritization of work, to encourage timely development of telecommunication security Recommendations.

SG17 has been working on cloud computing security since April 2010, and the following four work items were recognized and are currently in progress.

- Security guideline for cloud computing in the telecommunication area (X.ccsec)
- Security requirements and framework of the cloud-based telecommunication service environment (X.srfcts)
- Security functional requirements for the software as a service (SaaS) application environment (X.sfcse)
- Requirement of IdM in cloud computing (X.idmcc)

Summaries of the above draft Recommendations are in Annex III.

In addition to the above work items, the following work items have been discussed collaboratively with ISO/IEC JTC1/SC27 and CSA:

- In the arena of the Cybersecurity Information Exchange (CYBEX), three Recommendations: ITU-T X.1500 (Overview), ITU-T X.1520 (CVE) and ITU-T X.1521 (CVSS), were approved in April 2011. In addition, SG17 has embarked on work toward *Continuous security monitoring using CYBEX techniques*. As part of these activities, members of Cloud Computing Focus Group also applying this work to virtualization/cloud computing environments, jointly with CSA.
- A set of guidelines on information security management for telecommunications has also been studied in ITU-T X.1051, ITU-T X.1055 and ITU-T X.1056. Security controls to be applied for cloud computing, based on ISO/IEC 27002 (and/or ITU-T X.1051), are also a topic of joint discussion by ISO/IEC JTC1/SC27 and CSA.

4.9 OASIS (Identity in the Cloud Technical Committee)

The OASIS IDCloud (Identity in the Cloud) Technical Committee (TC) works to address the serious security challenges posed by identity management in cloud computing. The IDCloud TC identifies gaps in existing identity management standards and investigates the need for profiles to achieve interoperability within current standards. It performs risk and threat analyses on collected use cases and produces guidelines for mitigating vulnerabilities.

The purpose of the TC is to harmonize definitions/terminologies/vocabulary concerning identity in the context of cloud computing; to identify and define use cases and profiles; and to identify gaps in existing identity management standards as they apply in the cloud.

[Within Scope]

1. The TC will identify and may collect and publish new and/or existing definitions, terminologies and vocabulary concerning identity for cloud computing, as determined.
2. The TC will define use cases for identity deployment, provisioning and management in a cloud computing context. These may be existing use or new use cases, as the TC determines.
3. The TC will define the interoperability profile(s) of existing protocols and formats for usage of Identity in the Cloud, based on the identified use cases. Profiles are subsets of specifications and combinations of such subsets.
4. The TC will identify gaps in existing identity management interoperability protocols and format standards at OASIS and other standards bodies, and utilize the OASIS liaison process for communicating the gaps.
5. In all of its work, the TC should, to the extent feasible, prefer widely implementable, interoperable and modular standards, extensions, profiles and methods that permit use by a variety of participants.
6. The TC will build on and use existing standards and specifications when possible. When there is a need to extend existing OASIS standards, the TC will not undertake that exercise but will work with the Technical Committee representing the standard to provide the extension as part of that Technical Committee. As an example, if the TC requires extensions in standards such as SAML or WS-Trust, then this TC will identify the remaining work to be undertaken by the TCs responsible for those standards, or their successors.
7. The TC will build profiles for Identity in Cloud computing.

[Out of Scope]

1. Access control methods, levels of assurance (LOA) for security, and definitions and structures for expressing personally identifiable information (PII). The TC may reference or

suggest re-use or extension of such methods in the context of cloud computing, but will not develop them.

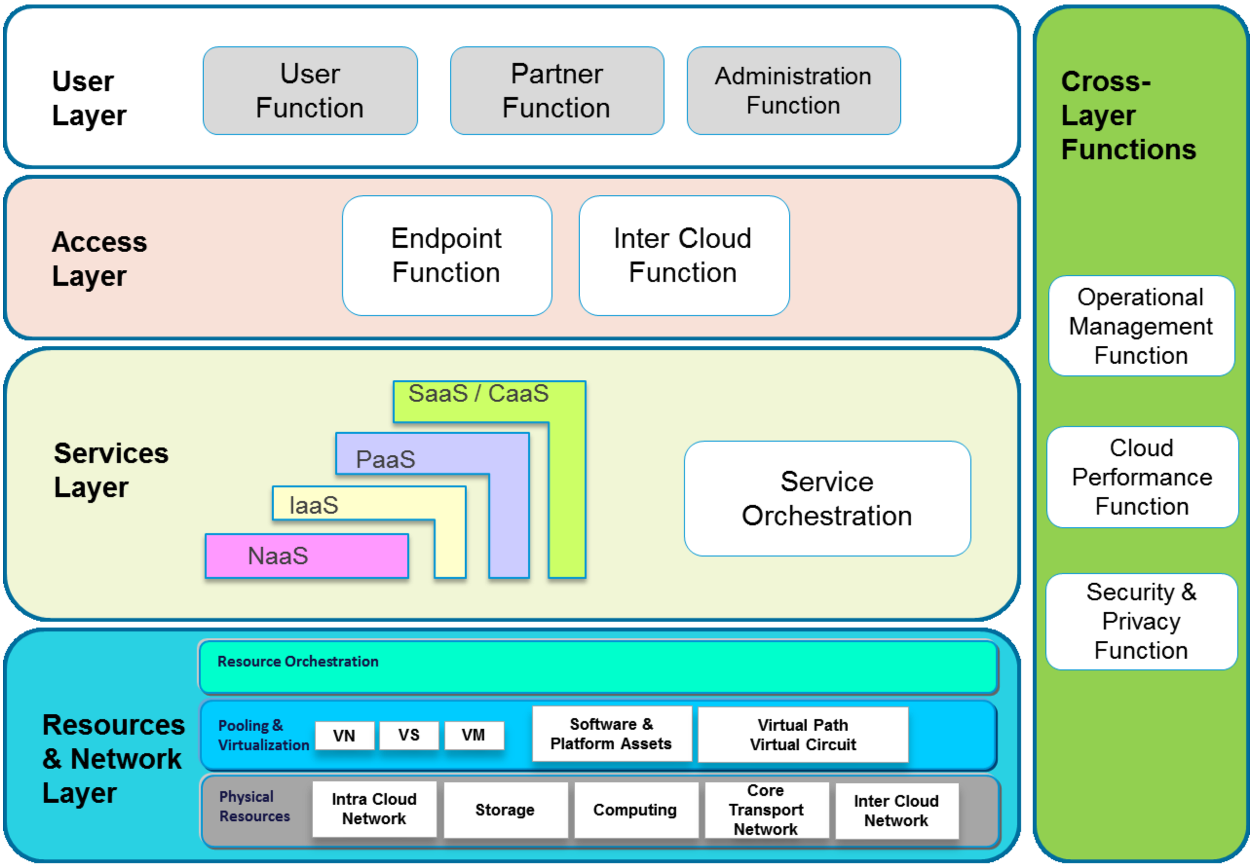
2. APIs or implementations
3. Creation of new protocols or formats

[List of Technical Reports]

1. A document describing in detail the specific use cases of identity deployment, and provisioning and management in a cloud computing context that the TC plans to address in their work product. This document will be completed and approved by the TC by July 2010.
2. A set of profiles and gaps, as described in paragraphs #3 and #4 under scope, to be approved as a Committee Specification by December 2010, and the remainder, if any, to be approved as Committee Specifications by June 2011. The TC may elect to create one or more of such Technical Reports in whatever combination it deems appropriate.
3. Optionally, such other Technical Reports within the scope listed in paragraphs 1-6 (including collections of definitions, terminology and vocabularies, and risk/threat assessments), as the TC may elect, until the later of June 2011 or such later date as the TC may elect to conclude.

5. Main technical components (background)

The security architecture and functions are highly dependent on the reference architecture. This section briefly describes the reference architecture and shows the main security issues concerning this architecture.



As shown in the figures, key functions of a cloud management system are divided into four layers, respectively:

- Resources and network layer
- Services layer
- Access layer
- User layer

Each layer includes a set of functions:

- The resources and network layer manages the physical and virtual resources.
- The services layer includes the main categories of cloud services, namely, NaaS, IaaS, PaaS, SaaS/CaaS, the service orchestration function and the cloud operational function.
- The access layer includes API termination function, and Inter-Cloud peering and federation function.
- The user layer includes end-user function, partner function and administration function.

Other functions, like management, security and privacy, etc., are considered as cross-layer functions that cover all the layers.

The main principle of this architecture is that all these layers are supposed to be optional. This means that a cloud provider who wants to use the reference architecture may select and implement only a subset of these layers.

However, from the security perspective, the principal of separation requires each layer to take charge of certain responsibilities. In the event that the security controls of one layer are bypassed (e.g. access layer), other security functions could compensate and thus should be implemented either in other layers or as cross-layer functions.

6. Threats for cloud security

6.1 Threats for cloud service users

6.1.1 Responsibility ambiguity

Cloud service users consume delivered resources through service models. The customer-built IT system thus relies on the services. The lack of a clear definition of responsibility among cloud service users and providers may evoke conceptual conflicts. Moreover, any contractual inconsistency of provided services could induce an anomaly or incidents. However, the problem of which entity is the data controller and which one is the data processor, stays open at an international scale (even if the international aspect is reduced to a minimal third party outside of a specific region such as the EU).

6.1.2 Loss of governance

The decision by an enterprise to migrate a part of its own IT system to a cloud infrastructure implies giving partial control to the cloud service providers. This loss of governance depends on the cloud service models. For instance, IaaS delegates only hardware and network management to the provider, while SaaS also delegates OS, application, and service integration, in order to provide a turnkey service to the cloud service user.

6.1.3 Loss of trust

It is sometime difficult for a cloud service user to recognize his provider's trust level due to the black-box feature of the cloud service. There is no measure to obtain and share the provider's security level in a formalized manner. Furthermore, the cloud service users have no abilities to evaluate the security implementation level achieved by the provider. Such a lack of sharing at the security level with regard to the cloud service provider will become a serious security threat for cloud service users in their use of cloud services.

6.1.4 Service provider lock-in

A consequence of the loss of governance could be a lack of freedom as to how to replace a cloud provider by another. This could be the case if a cloud provider relies on non-standard hypervisors or virtual machine image format, and does not provide tools to convert virtual machines to a standardized format.

6.1.5 Non-secure cloud service user access

As most of the resource deliveries are through remote connection, non-protected APIs, (mostly management APIs and PaaS services) are among the easiest attack vectors. Attack methods such as phishing, fraud, and exploitation of software vulnerabilities, still achieve results. Credentials and passwords are often reused, which amplifies the impact of such attacks. Cloud solutions add a new threat to the landscape. If an attacker gains access to your credentials, he can eavesdrop on your activities and transactions, manipulate data, return falsified information, and redirect your clients to illegitimate sites. Your account or service instances may become a new base for the attacker. From here, he may leverage the power of your reputation to launch subsequent attacks.

6.1.6 Lack of information/asset management

When applying to use cloud computing services, the cloud service user will have serious concerns about lack of information/asset management from cloud service providers, such as location of sensitive asset/information, lack of physical control for data storage, reliability of data backup (data retention issues), countermeasures for BCP and disaster recovery and so on. Furthermore, the cloud service users also have important concerns on exposure of data to foreign governments and on compliance with privacy laws, such as the EU data protection directive.

6.1.7 Data loss and leakage

This threat may be strongly related to the above clause. However, loss of an encryption key or a privileged access code will bring serious problems to the cloud service users. Accordingly, lack of cryptographic management information, such as encryption keys, authentication codes and access privilege, will lead to sensitive damages, such as data loss and unexpected leakage to the outside. For example, insufficient authentication, authorization, and audit (AAA) controls; inconsistent use of encryption and/or authentication keys; operational failures; disposal problems; jurisdiction and political issues; data centre reliability; and disaster recovery, can be recognized as major behaviours in this threat category and may partially connect with the above clause.

6.2 Threats for cloud service providers

6.2.1 Ambiguity in responsibility

Different user roles, such as cloud service provider, cloud service user, client IT administrator, data owner, may be defined and used in a cloud system. Ambiguity in such user roles and in the definition of responsibilities related to data ownership, access control, infrastructure maintenance, etc., may induce business or legal dissention (especially when dealing with third parties, when the cloud service provider is somehow a cloud service user).

6.2.2 Protection inconsistency

Due to the decentralized architecture of a cloud infrastructure, its protection mechanisms are likely to be inconsistent among distributed security modules. For example, an access denied by one IAM module may be granted by another. This threat may be put to profit by a potential attacker, thereby compromising both the confidentiality and integrity.

6.2.3 Evolutional risks

One conceptual improvement of cloud computing is to postpone some choices from the design phase to the execution phase. This means that some dependent software components of a system may be selected and implemented when the system executes. However, conventional risk assessment methodology can no longer match such an evolution. A system which is assessed as secure during the design phase may exploit vulnerabilities during its execution due to the newly implemented software components.

6.2.4 Business discontinuity

The "as a service" feature of cloud computing allocates resources and delivers them as a service. The whole cloud infrastructure, together with its business workflows, thus relies on a large set of services, ranging from hardware to application. However, the discontinuity of service delivery, such as a black-out or delay, may have a severe impact on the availability.

6.2.5 Supplier lock-in

The platform of a service provider is built by some software and hardware components by suppliers. Some supplier-dependent modules or workflows are implemented for integration or functionality extension. However, due to the lack of standard APIs, the portability to migrate to another supplier is not obvious. The consequence of provider lock-in could be a lack of freedom as to how to replace a supplier.

6.2.6 License risks

Software licenses are usually based on the number of installations, or the numbers of users. Since created virtual machines will be used only a few times, the provider may have to acquire far more licenses than are really needed at a given time. The lack of a "clouded" license management scheme that allows payment only for used licenses, may cause software use conflicts.

6.2.7 Bylaw conflict

Depending on the bylaws of the hosting country, data may be protected by different applicable jurisdictions. For instance, the USA Patriot Act may authorize such seizures. The EU protects cloud service user's private data, which should not be processed in countries that do not provide a sufficient level of guaranteed protection. An international cloud service provider may conflict with the bylaws of its local data centres, which is a legal threat to be taken into account.

6.2.8 Bad integration

Migrating to the cloud implies moving large amounts of data and major configuration changes (e.g., network addressing). Migration of a part of an IT infrastructure to an external cloud service provider requires profound changes in the infrastructure design (e.g. network and security policies). A bad integration caused by incompatible interfaces or inconsistent policy enforcement may evoke both functional and non-functional impacts.

6.2.9 Non-secure administration API

The administration middleware standing between the cloud infrastructure and the cloud service user may be not secure if insufficient attention is devoted to sanitation of cloud service user inputs and authentication. Non-protected APIs, mostly administration APIs, become a target of choice for attackers. This is not specific to the cloud environment. However, the service-oriented approach makes APIs a basic building block for a cloud infrastructure. Their protection becomes a major concern of the cloud security.

6.2.10 Shared environment

As cloud resources are virtualized, different cloud service users (possibly competitors) share the same infrastructure. One key concern is related to architecture compartmentalization, resource isolation, and data segregation. Any unauthorized and violent access to cloud service user's sensitive data may compromise both the integrity and confidentiality.

6.2.11 Hypervisor isolation failure

The hypervisor technology is considered as the basis of cloud infrastructure. Multiple virtual machines co-hosted on one physical server share both CPU and memory resources which are virtualized by the hypervisor. This threat covers the failure of mechanisms to isolate attacks that could be launched on a hypervisor to gain illegal access to the memory of other virtual machines.

6.2.12 Service unavailability

Availability is not specific to the cloud environment. However, because of the service-oriented design principle, service delivery may be impacted while the cloud infrastructure in not available. Moreover, the dynamic dependency of cloud computing offers many more possibilities to an attacker. A typical denial of service attack on one service may clog the whole cloud system.

6.2.13 Data unreliability

Data protection includes access to data for confidentiality as well as integrity. Cloud service users have concerns about how providers handle their data, and whether their data is disclosed or illegally altered. Even if cloud service user trust is not at the core of cloud security, it is a major marketing differentiator for a cloud service provider to advance the migration of an IT system to the cloud environment.

6.2.14 Abuse by cloud service provider

The decision by a cloud service user to migrate a part of its own IT to a cloud infrastructure, implies giving partial control to the provider. This becomes a serious threat to a cloud service user's data, notably regarding role and privileges assignment to providers. Coupled with lack of transparency regarding cloud provider practices, this may lead to misconfiguration or malicious insider attack. Such security breaches will damage the provider’s reputation and result in lower cloud service user confidence.

7. Security requirements for cloud security

7.1 Requirements for cloud service users

(Requirement-U1) Method to trust the security level of a cloud provider

Description:

A security assessment, security audit, or security certification/accreditation scheme, shall be established in order for a cloud service user to select an appropriate cloud service provider based on his security requirements. A cloud service user shall be able to easily evaluate or ask a trusted third-party to audit an existing cloud infrastructure. Furthermore, security criteria for the selection shall be implemented so as to provide mutual understanding of the security level between the cloud service user and the service provider. The cloud service user shall also implement his own security policy by integrating the cloud service provider security policy and negotiating SLAs, and shall propose several different commercial solutions.

When using cloud services from a cloud service provider, the cloud service user is required to establish trust relationships with the CSP using standardized techniques. These standard mechanisms include the exchange of certificates, cryptographic materials (e.g., the keys), identity management, as well as a security policy that can be used to establish subsequent trust relationships and policies.

Related threats:

Responsibility ambiguity (6.1.1)

Loss of governance (6.1.2)

Loss of trust (6.1.3)

Lack of information/asset management (6.1.6)

(Requirement-U2) Information/asset management

Description:

Location of sensitive asset/information of a cloud service user, physical control for data storage, reliability of data backup, and countermeasures for BCP and disaster recovery shall be appropriately implemented as a requirement in the cloud service user perspective. On the one side, the cloud infrastructure pre-defines its security policy. On the other side, a cloud service user requires agility to treat the protection of this infrastructure, and he shall decide and implement his own security policies.

Related threats:

Responsibility ambiguity (6.1.1)

Loss of trust (6.1.3)

Service provider lock-in (6.1.4)

Lack of information/asset management (6.1.6)

(Requirement-U3) Confidentiality/integrity of data

Description:

Cryptographic management information such as encryption keys, authentication codes, and access privileges, shall be securely managed and controlled as a requirement from the perspective of the cloud service user. This is required to protect against loss or leakage of data as a result of insufficient authentication, authorization, and audit (AAA) controls; inconsistent use of encryption and/or authentication keys; operational failures; disposal problems, and so on.

Related threats:

Loss of trust (6.1.3)

Non-secure cloud service user access (6.1.5)

Data loss and leakage (6.1.7)

(Requirement-U4) Proper account/identity management

Description:

IDs to be used for account/service management between cloud service user and cloud service providers shall be appropriately implemented as a requirement from the cloud service user perspective. This is required not only for protecting against phishing, fraud, and exploitation of software vulnerabilities, but also for ensuring the use of the account/service in the inter-cloud environment.

Related threats:

Loss of trust (6.1.3)

Non-secure cloud service user access (6.1.5)

Data loss and leakage (6.1.7)

(Requirement-U5) Service interoperability, portability and reversibility

Description:

For many technical or commercial reasons, such as an unacceptable increase in cost at time of contract renewal or an unacceptable decrease in service quality, a cloud service user may want to change its cloud service provider. In these cases, service portability, interoperability and reversibility shall be considered to minimize the damage to the user's business. The cloud service user shall be able to migrate all or part of its system to another service provider, to use and integrate services from different providers, or completely leave the cloud infrastructure.

Related threats:

Loss of governance (6.1.2)

Service provider lock-in (6.1.4)

(Requirement-U6) Interoperable service interface and virtualization mechanisms

Description:

Virtual machines, API's and service interfaces shall, whenever possible, be implemented in accordance with industry standards and designed with the intent to be interoperable with other members of the vendor community. No feature shall be implemented that prohibits migration or transplantation of a virtual machine by its authors, in accordance with the policies defined at the time of creation of the virtual machines.

Related threats:

Service provider lock-in (6.1.4)

Data loss and leakage (6.1.7)

(Requirement-U7) Secure virtual machine

Description:

Virtual machines shall be permitted intrinsic security capabilities and policy awareness. Virtual machines that are designed to enforce policy and restrict transport and instantiation due to policy constraints, shall not be prohibited from enforcing the author's policy on itself, or be deceived by the hypervisor or hardware into performing an action contrary to policy constraints.

Related threats:

Loss of trust (6.1.3)

Data loss and leakage (6.1.7)

7.2 Requirements for cloud service providers

(Requirement-S0) Proper security management

Description:

Security self-assessment, and security audit/security certification by a third party, shall be established in order for a cloud service provider to provide appropriate cloud services based on the user's security requirements. Furthermore, appropriate security criteria shall be implemented so as to provide mutual understanding of the security level between the cloud service user and the service provider. The cloud provider shall also implement his own security policy by integrating the cloud service user security policy, negotiating SLAs, and proposing several different commercial solutions.

Related Threats:

Responsibility ambiguity (6.2.1)

Protection inconsistency (6.2.2)

Evolutional risks (6.2.3)

Business discontinuity (6.2.4)

Supplier lock-in (6.2.5)

Bylaw conflict (6.2.7)

Bad integration (6.2.8)

Non-secure administration API (6.2.9)

Service unavailability (6.2.12)

Abuse right of cloud service provider (6.2.14)

(Requirement-S1) Hypervisor protection

Description:

Computing virtualization is the basis of cloud computing and virtual machines shall be well-isolated to share memory, CPU, and storage capacities. The hypervisor is proposed to host multiple virtual machines on one physical server. However, the strict isolation between VMs may fail if the hypervisor is compromised. A new variety of attacks, such as installation of rootkits inside the hypervisor (hyperjacking) or use of covert channels, calls for higher degrees of assurance. For a cloud service provider, the hypervisor used shall offer criteria to ensure protection for itself and for hosted VMs, e.g. by moving antivirus and anti-spam processing from VM to hypervisors.

Related threats:

Non-secure administration API (6.2.9)

Hypervisor isolation failure (6.2.11)

Service unavailability (6.2.12)

(Requirement-S2) Storage isolation

Description:

A cloud service provider provides flexible storage capacities which enforce extensibility. A VM may be dynamically affected with new storage according to its execution requirement. Different kinds of storage solutions, such as a storage area network (SAN) or network-attached storage (NAS), may be deployed in one data centre. The interoperability and protection of various storage technologies becomes an open issue. A cloud service provider shall ensure the isolation of its storage systems without any constraint on the selected adopted solution.

Related threats:

Business discontinuity (6.2.4)

Shared environment (6.2.10)

Service unavailability (6.2.12)

(Requirement-S3) Network isolation

Description:

Virtual network technologies, like VLAN for level 1 and VPN for level 2 or level 3, are used in cloud infrastructures. Compared to traditional networks, a virtualized network of cloud computing appears more vulnerable since the network isolation is no longer physical but logical. Network zones, where traffic could be segregated physically, are replaced with logical security domains, where traffic between VMs is filtered by “virtual” firewalls. Network perimeter controls shall also be securely implemented to prevent the unexpected behaviour of a service from affecting other coexisting services and lead to security problems. As a result, isolation is less precise, and the security guarantees are weaker.

Related threats:

Shared environment (6.2.10)

Service unavailability (6.2.12)

(Requirement-S4) Protection for network elasticity

Description:

The flexible allocation and rapid provisioning of secure network resources respond to dynamic evolutions of the cloud execution environment. Protection mechanisms shall adapt to this elasticity. Some existing solutions are inspired by flexible and dynamic management VPNs, with the notion of virtual private clouds. In order to enable multiple tenants to dynamically share the same network infrastructure, the protection of network elasticity shall be treated by cloud service providers, since they establish the elastic network connection, guarantee both performance and QoS, and will be the only people who can control it. A flexible yet strong network protection is one of the key issues for an end-to-end cloud service.

Related threats:

Service unavailability (6.2.12)

(Requirement-S5) Interoperability

Description:

A data centre is usually constructed by a set of heterogeneous hardware and software, ranging from servers, disk arrays, switches, hypervisors and middleware, to software. The interoperability of such solutions remains a main concern. As cloud service provider, he shall analyze the safety of co-existence and cooperation of these heterogeneous solutions. Furthermore, the coordination and consolidation of diverse security policies and mechanisms is an important issue. The cloud service provider shall guarantee the coherence of various security policies and their implementations.

Related threats:

Protection inconsistency (6.2.2)

Supplier lock-in (6.2.5)

Non-secure administration API (6.2.9)

(Requirement-S6) Identity management

Description:

The number and diversity of principles using cloud services internally and externally, and the volume of resources accessed, call for end-to-end solutions for managing identities, not only for their protection, but also for the management of multiple administrators, users and resources. Improper administration of identity may induce new vulnerabilities in such a dynamic and open cloud infrastructure. Identity shall be appropriately managed.

Related threats:

Non-secure administration API (6.2.9)

Hypervisor isolation failure (6.2.11)

Data unreliability (6.2.13)

Abuse right of cloud service provider (6.2.14)

(Requirement-S7) Disaster recovery

Description:

Availability is one of the three main security objectives of IT systems (in addition to confidentiality and integrity). A cloud system shall remain available at any moment. Disaster recovery represents the capability to respond to catastrophic disasters and to recover to a safe state. This mechanism may guarantee the continuity of a provided service. As with cloud computing, all the resources are delivered by the “as a service” mode, and availability is more important in the cloud context, rather that in a traditional one.

Related threats:

Business discontinuity (6.2.4)

Service unavailability (6.2.12)

(Requirement-S8) Data traceability

Description:

Major concerns in a shared and virtualized infrastructure include not only loss of control by users over their data, but also locating data and controlling its whole lifecycle. At any given time, a cloud service provider should know exactly where both user data and VMs data are stored, processed, or accessed from. Without special care, data cloud can move around freely among organizations, or even over international borders. Both during and after usage it should not be possible for third parties (including hosting providers) to access that data. This raises legal and political issues, since several jurisdictions specifically require that the provider have such knowledge and control mechanisms. Data hosted abroad might also be exposed to foreign governments. Furthermore, data traceability is needed to prove to users that data comes from a trusted source.

Related threats:

Evolutional risks (6.2.3)

Business discontinuity (6.2.4)

Data unreliability (6.2.13)

(Requirement-S9) Secure VM migration

Description:

Secure VM migration shall ensure that a VM being migrated between hosts within a cloud and between clouds can be secured both at rest and in motion. The usages anticipate ways, either by a console manager or programmatically, to maintain a log file and reporting capability in order to determine:

- where the VM is being hosted
- whether it is at rest or in motion
- which users have permission to the VM
- what controls protect it from unauthorised access and modification.

The VM migration also asks for security policy negotiation and the moved VM should adapt its security policy to its new host.

Related threats:

Non-secure administration API (6.2.9)

Shared environment (6.2.10)

Hypervisor isolation failure (6.2.11)

(Requirement-S10) Trusted compute pools

Description:

Live migration in the cloud allows for flexibility in the placement of VMs in a data centre or between clouds. On the other hand, this flexibility breaks down the security models built around known “out-of-band” attested platforms. It will create pools of machines that support capabilities and methods that allow for each of the machines to be validated/attested by external entities, based on known and expected signatures. Virtualization managers responsible for live migration, or other VM movement operations, can now attest the target to be trustworthy before performing a VM instantiation or movement to the platform.

Related threats:

Shared environment (6.2.10)

Hypervisor isolation failure (6.2.11)

(Requirement-S11) Security models federation

Description:

An organization may want to use multiple cloud service providers that have different security models. Some use certificates, others use REST web services interfaces via API keys, some simply use basic http authentication. In order to use multiple services, cloud service providers shall broker the different security connections in a manner which will enable an organization to use various cloud services together.

Related threats:

Responsibility ambiguity (6.2.1)

Protection inconsistency (6.2.2)

Evolutional risks (6.2.3)

Supplier lock-in (6.2.5)

Bad integration (6.2.8)

Non-secure administration API (6.2.9)

Service unavailability (6.2.12)

(Requirement-S12) Multi-tenancy isolation

Description:

Cloud computing provides potential cost saving through massive resource sharing that occurs on a very large scale. This situation exposes many potentially vulnerable interfaces. For example, different tenants use services on the same cloud simultaneously. As a result, a tenant may have access to other tenants' virtual machines, network traffic, actual/residual data, etc. Also, a tenant may impact the normal operation of other tenants, by stealing their data or identities. The cloud service provider shall:

- encrypt data in transit and at rest
- harden the virtual machine (VM) so that exposure to attacks on the virtualization layer is minimized
- provision special virtual environments with a physical separation for cloud service users with special security requirements

Related threats:

Business discontinuity (6.2.4)

Non-secure administration API (6.2.9)

Shared environment (6.2.10)

Hypervisor isolation failure (6.2.11)

(Requirement-S13) IP and license management and jurisdictional compliance

Description:

License and intellectual property will be managed by the provider in accordance with the laws governing the jurisdiction of instantiation. The evidence of compliance with regional laws and regulations shall be made available and any modification or renewal event shall be transmitted. The provision of the license shall be managed according to mutually agreed-upon service license agreements.

Related threats:

Evolutional risks (6.2.3)

Supplier lock-in (6.2.5)

License risks (6.2.6)

Bylaw conflict (6.2.7)

(Requirement-S14) Segregation of role, resource and responsibility

Description:

Methods and procedures shall be established as an internal check on activities through separation of asset custody, authorization of transactions from custody of associated assets and operational responsibilities from record-keeping responsibilities. No single individual or organization should have control over two or more phases of a transaction or operation without operational oversight by a third party. Cloud tenants should assign responsibilities to ensure a crosscheck of duties.

Related threats:

Responsibility ambiguity (6.2.1)

Protection inconsistency (6.2.2)

Evolutional risks (6.2.3)

Non-secure administration API (6.2.9)

Shared environment (6.2.10)

Abuse right of cloud service provider (6.2.14)

(Requirement-S15) Information and data quality assurance

Description:

Methods and procedures shall be established to ensure the logical correctness and reliability of the hypervisor, virtual machine, software executing operations and operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Protection mechanisms shall be put in place to protect against unauthorized modification or destruction of information.

Related threats:

Evolutional risks (6.2.3)

Data unreliability (6.2.13)

Abuse right of cloud service provider (6.2.14)

8. Study subjects on cloud security

The following study subjects can be provided based on considerations of security threats and requirements in clauses 6 and 7. The mapping among security threats, requirements and study subjects is in clause 9.

8.1 Security architecture/model and framework

In order to provide appropriate security controls for cloud computing environments, security architecture/model and framework should firstly be captured in an integrated manner in connection with the following study subjects.

This study subject should include providing a consistent lexicon, security architecture requirements, and a security reference model.

Related requirements:

(Requirement-U1)	Method to trust cloud providers' security level
(Requirement-U2)	Information/asset management
(Requirement-S10)	Trusted compute pools
(Requirement-S11)	Security models federation
(Requirement-S12)	Multi-tenancy isolation
(Requirement-S14)	Segregation of role, resource and responsibility

8.2 Security management and audit technology

In order for cloud service users to consistently assess trust/security level of cloud service providers, the following study sub-subjects should be accomplished:

a) **Guidelines for identifying security requirements for cloud service user** should be studied. In the course of this identification of security requirements, a business process analysis, an information asset classification, and a review of own security policy, should be carried out in order for cloud service users to identify which parts of their business and information/assets will be outsourced to certain cloud service provider(s). After identifying which business parts and information/assets are to be designated to cloud services, the security requirements of the cloud service user should be clarified and specified for the next step (selection of cloud service providers).

b) **Security guidelines or security criteria for assessing and auditing cloud service providers** should be studied. The work will be accomplished to provide measures to assess/audit cloud service providers from the cloud service user's perspective, based on a unified ISO ISMS/ SSAE16 SOC2 / ISAE3402 control structure. For security auditing, a cloud auditor can make an assessment of the security controls in the system. The assessment includes whether the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the cloud system. This recommendation will be applied to cloud service users for selecting an appropriate cloud service provider based on an assertion of trust/security level from the cloud service providers. The work will also include providing guidelines for a periodical review of the selected cloud service provider(s). Security guidelines or security criteria for assessing and auditing cloud service providers should be studied. The work will be accomplished to provide measures to assess/audit cloud service providers from the cloud service user's perspective, based on the unified ISO ISMS/ SSAE16 SOC2 / ISAE3402 control structure. This recommendation will be applied to cloud service users for selecting an appropriate cloud service provider, based on an assertion of trust/security level from the cloud service providers. The work will also include providing guidelines for a periodical review of the selected cloud service provider(s).

c) **Standardized SLA (Service Level Agreement) template** should be studied for the part concerning cloud security. This work for the provision of an SLA template should be jointly studied with other experts, especially for network and system.

d) **Risk management and mitigation** should be studied as an extension of IT operational risk. Risk should be expressed quantitatively in terms of areas, causes and types of loss incurred. Operational risk in a cloud environment should be treated as a function of the business impact and the likelihood of the incident scenario that can be translated to the tenant institution's total value at risk (VaR). A risk ontology should be chosen on the basis of the cloud service user's business needs, and should be aimed at simplifying financial calculations associated with cloud migration. Special attention shall be afforded to the definition of operational risk by the Basel Committee on Banking Supervision (BCBS)

e) **Security monitoring** should be studied to allow the cloud service user to ascertain security levels at any given point-in-time, and to ensure its compliance reporting meets all geographical and industry-based regulations. The security monitoring requests that the cloud provider permits the organization (cloud service user) subscribing to the cloud services to query the actual security status of specific elements of its services. In an infrastructure as a service (IaaS) offering, these may include security status of the physical and virtual machine, the network and storage. In a platform as a service (PaaS) or software as a service (SaaS), the patch status of a piece of software may be important. In both of these cases (PaaS and SaaS), applications are provided through the cloud and their update status would need to be monitored. Access to this information should be secured to each cloud service user to prevent the data from being used by unauthorized parties to exploit the cloud environment. The issue how to protect the data should be the subject of data and privacy protection.

Related requirements:

(Requirement-U1) Method to trust cloud providers' security level

(Requirement-U2) Information/asset management

(Requirement-S0) Proper security management

(Requirement-S11) Security models federation

(Requirement-S13) IP and license management and jurisdictional compliance

(Requirement-S14) Segregation of role, resource and responsibility

(Requirement-S15) Information and data quality assurance

8.3 Business continuity planning (BCP) and disaster recovery

The rapid pace of change and lack of transparency within cloud computing requires that traditional security, business continuity planning (BCP), and disaster recovery (DR) professionals be continuously engaged in vetting and monitoring the chosen cloud providers.

The challenge is to collaborate on risk identification, recognize interdependencies, integrate, and leverage resources in a dynamic and forceful way. Cloud computing and its accompanying infrastructure assist in diminishing certain security issues, but may increase others and can never eliminate the need for security. While major shifts in business and technology continue, traditional security principles remain.

Related requirements:

(Requirement-U3) Confidentiality/integrity of data

(Requirement-S0) Proper security management

(Requirement-S2) Storage isolation

(Requirement-S7) Disaster recovery

8.4 Storage security

Information/asset of the cloud service user should be securely and reliably stored and managed by cloud service providers. The study subject on storage security is heavily related to the solutions to the cloud service users' threats and concerns. Under this subject, the following study sub-subjects should be accomplished:

1. Storage management (including self-encryption)
2. Backup system security (including storage replication)
3. Storage network gateways
4. Long-term storage (on-line and off-line)

Related requirements:

(Requirement-U3)	Confidentiality/integrity of data
(Requirement-S2)	Storage isolation
(Requirement-S8)	Data traceability
(Requirement-S11)	Security models federation
(Requirement-S15)	Information and data quality assurance

8.5 Data and privacy protection

Countermeasures against data loss and leakage should be studied, focusing on security (confidentiality and integrity) and data privacy in the use of cloud services. The main objective of this study is to produce a set of technical specifications based on cryptography and privacy technologies. The following study sub-subjects should be accomplished to produce a set of guidelines for technical specifications:

1. Technical specification for encryption and integrity protection of data in transit
2. Technical specification for implementation methods of key management process
3. Technical specification for implementation of strong access control.
4. Method to analyse data protection to discover, monitor and protect data wherever it is used or stored

Related requirements:

(Requirement-U3)	Confidentiality/integrity of data
(Requirement-S8)	Data traceability
(Requirement-S11)	Security models federation
(Requirement-S15)	Information and data quality assurance

8.6 Account/identity management

Countermeasures against account/service hijacking in cloud services should be studied. The main objective of this study is to produce a set of technical specifications based on IdM (Identity management) technologies. The following study sub-subjects should be accomplished to produce a set of guidelines for technical specifications:

1. Development of strong cloud-based authentication and authorization architecture and mechanisms (including strong two-factor authentication techniques)
2. Detection method to proactively monitor unauthorized activities
3. Study on strong network authentication
4. Guideline on how to guarantee secure use of account credentials between users and providers

An approach is described in Annex II which can be considered as a potential solution for the account/identity management in cloud.

Related requirements:

(Requirement-U4)	Proper account/identity management
(Requirement-S6)	Identity management
(Requirement-S11)	Security models federation
(Requirement-S14)	Segregation of role, resource and responsibility
(Requirement-S15)	Information and data quality assurance

8.7 Network monitoring and incident response

To ensure the security and information quality within the cloud service chain, an organized approach to addressing and managing the aftermath of a security breach or attack (also known as an incident) should be studied. The goal of this effort should be the management of the situation in a way that limits damage and reduces recovery time and costs. An incident response plan should include a policy that defines, in specific terms, what constitutes an incident and should provide a step-by-step process to be followed when an incident occurs. When an attack is detected, the response may include simply filing a report, or sending a notification to the source of the attack, a request for mitigation, or the request to locate the source.

One of the more difficult cases is that in which the source of an attack is unknown, requiring the ability to trace the attack traffic iteratively upstream through the network for the possibility of any further actions to take place. In cases when accurate records of an active session between the victim system and the attacker or source system are available, the source is easy to identify. The problem of tracing incidents becomes more difficult when the source is obscured or spoofed, logs are deleted, and the number of sources is overwhelming. If the source of an attack is known or identified, it may be desirable to request that actions be taken to stop or mitigate the effects of the attack.

A proactive inter-network communication method to facilitate network monitoring, the sharing of incident-handling data while integrating existing detection, tracing, source identification, and mitigation mechanisms, for a complete incident-handling solution should be considered. Incident handling involves the detection, reporting, identification, and mitigation of an attack, whether it be a system compromise, socially-engineered phishing attack, or a denial-of-service (DoS) attack. This effort should coordinate with CERT activities among cloud service providers in order to protect against malicious activities inside/outside of the cloud environment. The exchange of Cyber security information is essential for this purpose; use of Recommendation ITU-T X.1500 (CYBEX), in conjunction with cloud security controls covering incident response under ISO/IEC SC27, is recommended.

Related requirements:

(Requirement-S0)	Proper security management
(Requirement-S3)	Network isolation
(Requirement-S4)	Protection for network elasticity
(Requirement-S11)	Security models federation

8.8 Network security management

To ensure the protection of networks used in cloud services and the protection of the supporting infrastructure, the secure management of networks requires careful consideration to dataflow, legal implications, monitoring, and protection. Networks should be adequately managed and controlled, in order to be protected from threats, and to maintain security for the cloud systems and applications using the network, including information in transit.

Cloud network security can be divided into three study subjects:

- intra-data centre network organization and isolation
- cloud service delivery
- use of the virtualization layer to deliver network services.

The first study subject represents networking virtualization to support enterprise collaboration in a virtualized environment. The security of such a kind of networking includes, in principle, the network isolation and the firewall organization. Based on the requirement-S3, since the network isolation is no longer physical but logical in cloud environments, a virtualized network of cloud computing shall be adequately managed and controlled. Based on the requirement-S4, since flexible allocation and rapid provisioning of secure network resources respond to dynamic evolutions of the cloud execution environment, protection mechanisms should be provided to assure network elasticity.

The second study subject is the delivery of a cloud service. This supports the cloud service user access to the virtualized resources. A cloud service provider shall provide its cloud service users with a secure end-to-end access to the virtualized resources. Conventional VPN (MPLS, IPsec or SSL VPN) is a potential and promising solution whereby cloud service users can use secure tunnels of VPN to access the virtual data centre. A potential solution, which provides a separation of user security domain, is elaborated in Annex I.

The third study subject is the use of the virtualization layer to provide network services on a virtual platform. In this model, a carrier-class router would no longer be an operating system running on a dedicated physical hardware, but would rather be the same operating system running on a slice of physical resources. In this study area, the need to assure logical network isolation in conjunction with logical isolation between VMs brings up severe security issues.

In the case of virtualized networking, the level of security depends on logical isolation between infrastructure and hardware resources (CPU, memory, storage, link bandwidth, routers, and switches). This approach exposes cloud networks to a new set of attacks, intrusions or virus targeting the virtualization interface. This architecture needs to address new security attack vectors focused on the hypervisor during the bootstrapping procedure, to interrupt another virtual machine's I/O or memory accesses over the virtualization layer.

Related requirements:

(Requirement-U3)	Confidentiality/integrity of data
(Requirement-S1)	Hypervisor protection
(Requirement-S3)	Network isolation
(Requirement-S4)	Protection for network elasticity
(Requirement-S8)	Data traceability

8.9 Interoperability and portability security

The security of co-existence and cooperation of a set of heterogeneous hardware and software, ranging from servers, disk arrays, switches, hypervisors, middleware, to software should be ensured. Portability and interoperability must be considered because cloud service users shall have the capability to change their cloud service provider. Consequently, the methods and standards about portability and interoperability should be researched. Under this subject, the following study sub-subjects should be accomplished:

1. Methods to preserve or enhance the security functionality provided by the legacy application and achieve a successful data migration in SaaS migration.
2. Methods to minimize the amount of application rewriting and preserve or enhance security controls in PaaS migration.
3. Methods to assure both the application and data are able to migrate to and run at a new cloud provider in IaaS migration.
4. Standards about interoperability and portability between cloud service providers.

Related requirements:

(Requirement-U5)	Service interoperability, portability and reversibility
(Requirement-U6)	Interoperable service interface and virtualization mechanisms
(Requirement-S4)	Protection for network elasticity
(Requirement-S5)	Interoperability
(Requirement-S12)	Multi-tenancy isolation

8.10 Virtualization security

Providing multi-tenant cloud services at the infrastructure, platform, or software is often basically supported by some form of virtualization technologies. However, use of these technologies brings additional security concerns and this study subject focuses on these security issues when using virtual machine (VM) technology in the infrastructure of the cloud services.

In particular, the hypervisor is applied to host multiple virtual machines on one physical server. Based on the requirement-S1, considering new variety of attacks, such as installing rootkits inside the hypervisor (hyperjacking) or using covert channels, hypervisors used in a cloud service provider should be analyzed in terms of vulnerability and securely managed.

Related requirements:

(Requirement-U6)	Interoperable service interface and virtualization mechanisms
(Requirement-U7)	Secure virtual machine
(Requirement-S0)	Proper security management
(Requirement-S1)	Hypervisor protection
(Requirement-S9)	Secure VM migration
(Requirement-S10)	Trusted compute pools
(Requirement-S12)	Multi-tenancy isolation

8.11 Obligatory predicates

Based on the Theory of Constraints (E.M. Goldratt), no supply chain is stronger than the chain's weakest link. Therefore, it is fundamental to cloud operations – an acknowledged instance of an information technology supply chain – that the system's constraints must be defined for integrity of the supply chain to be preserved. To this end, the contractual and regulatory business-defined requirements should be abstracted into logical predicates that may be added transitively as constraints based on conditional factors. While it is acknowledged that actual interpretation of legislation and regulation is normally considered out-of-scope for the ITU-T, the abstraction of operational constraints which may include contractual agreements, service level obligations, legislation, regulation, standards, case law, treaty, and legal opinion, into a set of first order operational predicates with normative effects, clearly falls within the field of information theory as embodied by the field of legal informatics and jurimetrics (Hans Wolfgang Baade, 1963). By abstracting business constraints into obligatory predicates which can be parsed as standard algebraic postulates subject to equality, inequality, and transitive verb relations, complex jurisdictional issues such as "Lawful Interception" may be resolved through logical operations that are mathematically consistent with legal norms, provided that the normative constraints are adequately mapped. This approach acknowledges the role that legislation, regulation, and standards play in influencing the definition and source management of cloud services. Since it is acknowledged that the cloud supply chain might cross jurisdictional boundaries, the services and management operations are governed by legal obligations at multiple local, federal, international and industry levels. To help organizations meet these obligations, a framework for the legal compliance and governance steps from both a geographical and industry perspective is needed. This approach should assist in identification of legal obligations, as well as potential barriers to adoption (such as sovereign risk, industry regulator compliance, government regulatory compliance, data ownership and confidentiality, etc.) and help manage the process for source management, cloud service engagement, and ongoing risk management of legal compliance needs. It is suggested, that technologies such as Rule, LegalRuleML, Legislative XML, OWL, RDF, SBVR, SWRL, RIF, and LKIF be investigated as methods to express obligatory predicates within the cloud supply chain to reconcile the constraints of multiparty operations.

Related requirements:

(Requirement-U1)	Method to trust cloud providers' security level
(Requirement-U2)	Information/asset management
(Requirement-U5)	Service interoperability, portability and reversibility
(Requirement-S0)	Proper security management
(Requirement-S13)	IP and license management and jurisdictional compliance
(Requirement-S14)	Segregation of role, resource and responsibility

9. Conclusion

This Technical Report provides a valuable list of study topics on cloud security for ITU-T standardization activities. It observes the current state of cloud security standardization in several SDOs and fora, such as ENISA, CSA and NIST, as discussed in clause 4. Based on the review of cloud security activities in these SDOs and fora, this Technical Report identifies cloud security threats and requirements in clause 6 and clause 7 respectively. Finally, the cloud security study topics are prioritized based on the cloud security threats and requirements highlighted in clause 8, as follows:

- Security architecture/model and framework (high priority)
- Security management and audit technology (high priority)
- Business continuity planning (BCP) and disaster recovery (low priority)
- Storage security (medium priority)
- Data and privacy protection (high priority)
- Account/identity management (high priority)
- Network monitoring and incident response (high priority)
- Network security management (high priority)
- Interoperability and portability security (medium priority)
- Virtualization security (high priority)
- Obligatory predicates (high priority)

From the technical perspective, a priority (high, medium or low) is assigned to each study topic. This priority has been estimated principally through discussion in FG Cloud in view of the related risk levels, the impact to the cloud market, and so on.

The relationship among security threats (clause 6), requirements (clause 7) and study subjects (clause 8) is provided by means of Tables in Appendix A.

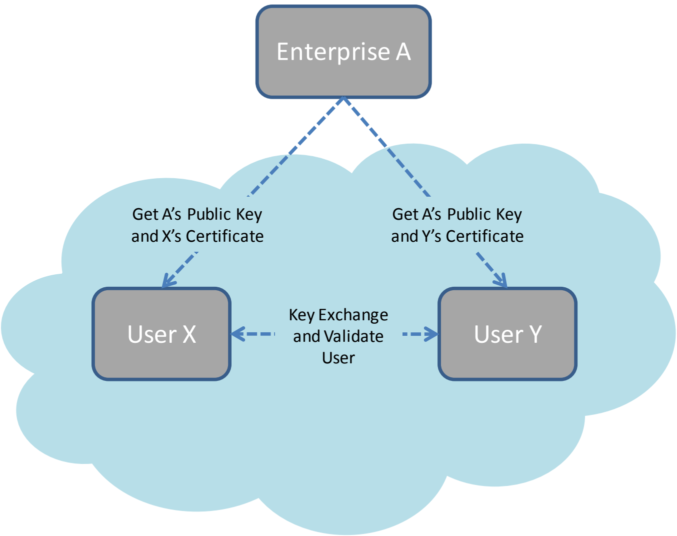
The prioritization should be used as referenced criteria for ITU-T members. The above list may not be exhaustive for ITU-T cloud security study topics; however, ITU-T members may benefit from this document to use as a starting point for work in cloud security.

Annex I
Practical Scenarios on PKI mechanisms for cloud

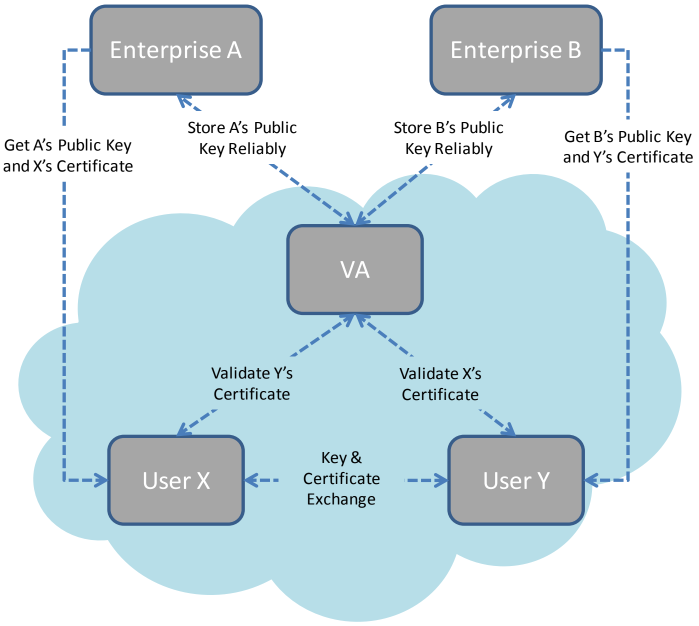
On**e** key scenario to be kept in mind is that **today** most individual users do not have a commercial certificate. Certificates for users have to be enterprise-specific, which puts the burden on enterprises to acquire these certificates. To avoid this complexity, it is proposed that the cloud providers and enterprises themselves can act as **c**ertificate and **v**alidation **a**uthorities for users.

Consider the following scenarios:

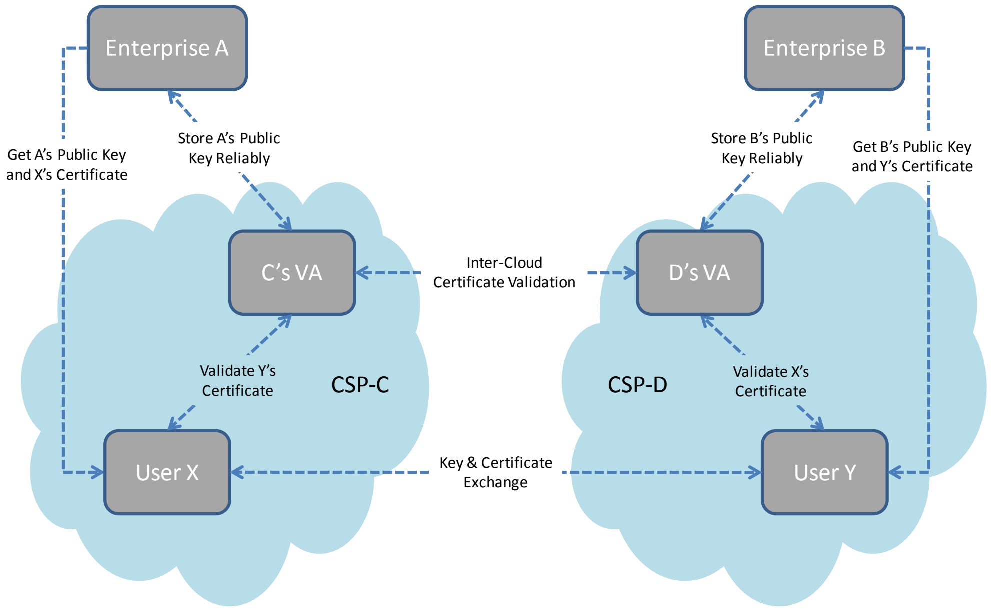
- Scenario 1 – user X and Y belong to enterprise A. X and Y also have a presence on the cloud, where they need to communicate securely. For X and Y to validate to each other, they can use an **e**nterprise**-**provided public key. The enterprise may itself have its private key, which can be used to sign X’s and Y’s public keys. X and Y would be able to validate each other’s public key by decoding the certificate signed by A, if they have A’s public key. In this scenario, E that signs X’s and Y’s public keys, also acts as a Certificate Authority.


Enterprise A
Get A's Public Key and X's Certificate
Get A's Public Key and Y's Certificate
User X
Key Exchange and Validate User
User Y

- Scenario 2 – user X and Y belong to enterprises A and B, respectively. However, X may not have B’s public key, or even if it has it, may not trust it. The certificate given by Y (which has been signed by B) cannot therefore be trusted by X. In this case, there is need for a third party to validate certificates that have been signed by A and B for users across these enterprises. This can be achieved by installing a validation authority (VA) inside the cloud. The VA simply needs to reliably store the public keys for A and B. These keys may be stored when an enterprise signs up with a cloud provider, makes a legal agreement, and presents its credentials. User X can then send Y’s certificate to the cloud VA, which will validate the certificate because it already has B’s public key stored in a reliable fashion.


Enterprise A
Enterprise B
Get A's Public Key and X's Certificate
Store A's Public Key Reliably
Store B's Public Key Reliably
Get B's Public Key and Y's Certificate
VA
Validate Y's Certificate
Validate X's Certificate
User X
Key & Certificate Exchange
User Y

- Scenario 3 – Cloud service users X and Y belong to enterprises A and B, and they are hosted across two cloud service providers C and D. cloud service provider C holds A's public key reliably, while cloud service provider D holds B's public key reliably. If Y sends its public key certificate to Y, then Y will send it for authentication to the VA in provider D. Since provider D's VA cannot authenticate C's public key, it will send it to provider C's VA for authentication. Provider C's VA stores the public key for enterprise B and will validate it for provider D's cloud service user X. This inter-VA interaction requires inter-cloud agreements between C and D.


Enterprise A
Enterprise B
Get A's Public Key and X's Certificate
Store A's Public Key Reliably
Store B's Public Key Reliably
Get B's Public Key and Y's Certificate
C's VA
Inter-Cloud Certificate Validation
D's VA
Validate Y's Certificate
CSP-C
CSP-D
Validate X's Certificate
User X
Key & Certificate Exchange
User Y

Annex II
Secure access to cloud

II.1 Definition:

Cloud published service endpoints (CPSE): the points where the user's cloud APIs and VPN sessions are terminated and authenticated.

Cloud **s**ervices **g**ateway (CSG)**:** network entity that monitors user traffic for SLAs, QoS and other access**-**related functions. The CSG also acts to separate different cloud service user traffics from one another.

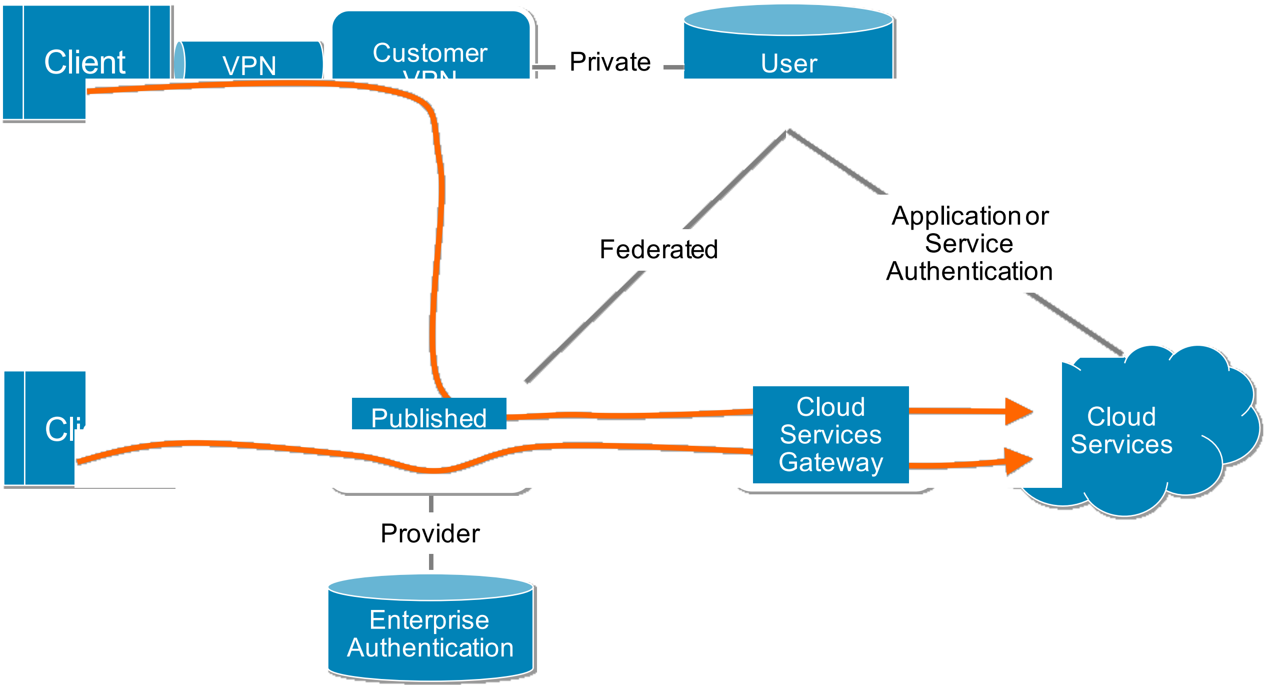
Identity Tunnel (IT)**:** a**n** IP tunnel in the cloud network that carries authenticated traffic for a given class of cloud service users. **For example,** the IP tunnel may carry traffic for all Gold cloud service users of a service. Tunnels help to simplify the application of QoS and SLAs in the cloud network.

II.2 Secure access methods

In any cloud service (infrastructure, software or platform) the end-service provider or enterprise will control the access to the services. If these services are being hosted on the cloud, then the cloud provider (which may be different from the service provider or enterprise) also needs to protect their network from unauthorized accesses.

However, since the cloud provider and the service provider or enterprise are legally different entities, each one may in certain cases need to isolate its respective user information.

II.2.1 Kinds of secure access scenarios



In this regard, the following three broad scenarios are envisioned:

a. **Private authentication**: The cloud service users always access cloud services via the enterprise VPN. The enterprise and the cloud provider in turn share a secure pre-configured authenticated and secure tunnel. All access control to the cloud network is controlled by the enterprise via its VPN authentication. This scenario will work well for hybrid clouds.

b. **Provider authentication**: The cloud service users access cloud services via the provider's CPSEs. An enterprise-wide authentication user or an individual identity per enterprise user might be provisioned in the provider's authentication database. The provider can use this database to identify the enterprise and network to which the user is authorized. The enterprise and cloud provider can maintain separate user databases although either a unique enterprise-wide identity or a per-user/group identity will need to be provisioned in the provider's authentication database. Such methods may be useful in public clouds where the users do not have a separate enterprise VPN and authentication mechanism. If the user accesses the same cloud services through enterprise and provider VPNs, then two distinct VPN login methods will be needed, one for enterprise another for provider access.

c. **Federated authentication**: The enterprise agrees to federate its identity systems with the cloud providers. In this case, the user uses the enterprise VPN authentication procedures even when accessing the provider's VPN. When a new user access arrives on the CPSE, it delegates its authentication to the enterprise system. The enterprise authentication database in the provider network may be used to determine which enterprise database to delegate the request to. Federated identity systems may also be used in case of inter-cloud scenarios.

II.2.2 Application authentication is separate from VPN authentication

In all the above scenarios, the user may have to further authenticate itself with the enterprise user authentication mechanisms using SSH, HTTP or other procedures. This is consistent with the two layer authentication widely used in all enterprises.

In case of private or federated methods of authentication, parts of the user database in the enterprise network may be used for both VPN authentication and the service authentication. In the public authentication method, the provider's authentication may differ from the service specific authentication configured by the cloud service users.

II.2.3 Propagating identity information in orchestration network

For several cloud services, it is important to know the user's identity and enterprise affiliation in the cloud network. For instance, to satisfy QoS requirements (bandwidth, delay) of a specific enterprise cloud service user, the cloud network needs to associate the user's IP address with their enterprise identity. Since the user has already been authenticated at the enterprise or provider edge, this identity needs to be propagated to cloud network entities that will enable this service.

A simple scheme for achieving this is cloud service user specific tunnels between CPSEs and CSGs. When a user is authenticated at the provider or enterprise edge (and traffic received via a pre-authenticated enterprise specific VPN tunnel), the CPSE will know the user's enterprise affiliation and possibly their identity as well. The CPSE can then direct the user traffic over a cloud service user-specific identity tunnel through the CSG towards the cloud services. These identity tunnels must be manually or automatically pre-set up between the CPSEs and CSGs.

While the CSG is unaware of the user's identity it can apply policies and SLAs to the tunnel. This mechanism helps to propagate needed identity information through the cloud network without having each cloud entity access the user databases (which could be thereby compromised).

Annex III
Summaries of draft ITU-T Recommendations on cloud computing security in SG17

X.ccsec, *Security guideline for cloud computing in telecommunication area*

Recommendation **X.ccsec** analyzes security challenges for cloud computing in the telecommunication area, and describes some security considerations for cloud computing service providers and consumers as a guidance to help them deploy cloud computing services as well as choose cloud computing services.

X.srfcts: *Security requirements and framework of the cloud-based telecommunication service environment*

Recommendation **X.srfcts** describes both general and specific security requirements of cloud-based telecommunication services that include: service creation, service integration, service delivery, data storage, and key management, etc. This Recommendation also aims to describe the security framework with integration of various security functions that can provide differentiated security levels for various cloud-based services.

X.sfcse: *Security functional requirements for the Software as a Service (SaaS) application environment*

Recommendation **X.sfcse** provides a generic functional description for a secure service-oriented Software as a Service (SaaS) application environment that is independent of network types, operating system, middleware, vendor specific products or solutions. In addition, this Recommendation is independent of any service or scenarios specific model (e.g., web services, Parlay X or REST), assumptions or solutions. This Recommendation aims to describe a structured approach for defining, designing, and implementing secure and manageable service-oriented SaaS application environment capabilities in the telecommunication cloud computing environment.

X.idmcc: *Requirements of IdM in cloud computing*

Recommendation **X.idmcc** focuses on the harmonization of telecommunication services in the cloud-computing environment. This Recommendation would launch from the use-case and requirements analysis in consideration of existing industry efforts, and it would concentrate on how to harmonize the telecommunication services and the Internet services based on a common identity management infrastructure in the cloud computing environment.

Appendix A
Mapping among threats, requirements and study subjects
(Informative)

The security threats described in clause 6, security requirements described in clause 7, and study subjects identified in clause 8, are shown from the perspective of the cloud service user and the service provider in the following tables.

Each table consists of security threats and security requirements, and the number indicated in the text of the tables corresponds to that of study subject in clause 8.

Notation:

Vertical axis: Security threats in clause 6

Horizontal axis: Security requirements in clause 7

Number in the table: number of study subject in Clause 8 as follows.

1	Security Architecture/Model and Framework (8.1)
2	Security Management and Audit Technology (8.2)
3	BCP/Disaster Recovery (8.3)
4	Storage Security (8.4)
5	Data and Privacy Protection (8.5)
6	Account/Identity Management (8.6)
7	Network Monitoring and Incident Response (8.7)
8	Network Security Management (8.8)
9	Interoperability and Portability Security (8.9)
10	Virtualization Security (8.10)
11	Obligatory Predicates (8.11)

RU: Requirement for cloud service user
RS: Requirement for cloud service provider

A.1 Mapping for the cloud service users' perspective

	RU1: Method to trust cloud providers' security level	RU2: Information/ asset management	RU3: Confidentiality/ integrity of data	RU4: Proper account/ identity management	RU5: Service interoperability, portability and reversibility	RU6: Interoperable service interface and virtualization mechanisms	RU7: Secure virtual machine.
6.1.1 Responsibility ambiguity	1, 2	1, 2					
6.1.2 Loss of governance	2, 11				9, 11		
6.1.3 Loss of trust	2	2	3	6			10
6.1.4 Service provider lock-in		2			9	9	
6.1.5 Cloud service user			5, 8	6			

remote access							
6.1.6 Lack of information/asset management	2, 11	2, 11			11		
6.1.7 Data loss and leakage			4, 5, 8	6		10	10

A.2 Mapping for cloud service provider perspective (RS0-RS8)

	RS0 Proper security management	RS1: Hypervisor protection	RS2: Storage isolation	RS3: network isolation	RS4: Protection for network elasticity	RS5: Inter-operability	RS6: Identity manage ment	RS7: Disaster recovery	RS8: Data traceability
6.2.1 Responsibility ambiguity	2, 11								
6.2.2 Protection inconsistency	2					9			
6.2.3 Evolutional risks	2								5
6.2.4 Business discontinuity	2, 3		3					3	5
6.2.5 Supplier lock-in	2					9			
6.2.6 License risks									
6.2.7 Bylaw conflict	2, 11								
6.2.8 Bad integration	2								
6.2.9 Non-secure administration API	2, 10	10				9	6		
6.2.10 Shared environment			4	8					
6.2.11 Hypervisor isolation failure		10					6		
6.2.12 Service unavailability	2, 7	8, 10	3, 4	7, 8	7, 8, 9			3	
6.2.13 Data unreliability							6		4, 5, 8
6.2.14 Abuse right of cloud service provider	2, 7, 11						6		

A.3 Mapping for cloud service provider perspective (RS9-RS15)

	RS9: Secure VM migration	RS10: Trusted compute pools	RS11: Security models federation	RS12: Multi-tenancy	RS13: IP & license management & jurisdictional compliance	RS14: Segregation of role, resource and responsibility	RS15: Information & data quality assurance
6.2.1 Responsibility ambiguity			1			1, 2, 11	
6.2.2 Protection inconsistency			5, 6			6	
6.2.3 Evolutional risks			2		2	2	2
6.2.4 Business discontinuity				9			
6.2.5 Supplier lock-in			2		2		
6.2.6 License risks					11		
6.2.7 Bylaw conflict					2, 11		
6.2.8 Bad integration			5				
6.2.9 Non-secure administration API	10		2	10		2	
6.2.10 Shared environment	10	1, 10		1, 9, 10		1, 2	
6.2.11 Hypervisor isolation failure	10	1, 10		1, 10			
6.2.12 Service unavailability			2, 4, 7				
6.2.13 Data unreliability							4, 5, 6
6.2.14 Abuse right of cloud service provider						2	2

Bibliography

[b-ITU-T X.1205]	Recommendation ITU-T X.1500 Overview of cybersecurity.
[b-ITU-T E.409]	Recommendation ITU-T E.409 Incident organization and security incident handling: Guidelines for telecommunication organizations.
[b-FG Technical Report (ecosystem)]	FG Technical Report Introduction to the cloud ecosystem: definitions, taxonomies, use cases, high level requirements and capabilities.
[b-GICTF FED]	Introduction to Global Inter-Cloud Technology Forum (GICTF) and its Roadmaps (Cloud-i-0026).
[b-OASIS IDCloud]	OASIS Identity in the Cloud Technical Committee, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=id-cloud
[b-DMTF WhitePaper]	Architecture for Managing Clouds White Paper (DSP-IS0102), http://www.dmtf.org/sites/default/files/standards/documents/DSP-IS0102_1.0.0.pdf
[b-NIST-SP800-53]	Recommended Security Controls for Federal Information Systems, December 2006, Special Publication 800-53.
[b-NIST 800-125]	Guide to Security for Full Virtualization Technologies, Special Publication 800-125.
[b-NIST 800-144]	Guidelines on Security and Privacy in Public Cloud Computing, Draft Special Publication 800-144, http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800-144_cloud-computing.pdf
[b-NIST DFN]	Definition of Cloud Computing, January 2011, Draft Special Publication 800-145, http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf
[b-NIST 800-146]	Cloud Computing Synopsis and Recommendation, January 2011, Draft Special Publication 800-146, http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf
[b- FedRAMP]	Proposed Security Assessment & Authorization for U.S. Government Cloud Computing, http://www.cio.gov/pages.cfm/page/Federal-Risk-and-Authorization-Management-Program-FedRAMP
[b-CSA Glossary]	Appendix: Cloud Security Alliance Glossary. https://cloudsecurityalliance.org/research/security-guidance/
[b-CSA GuideV2]	Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, December 2009, https://cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf
[b-CSA GuideV3]	Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, November 2011, https://cloudsecurityalliance.org/research/security-guidance/
[b-CSA Top Threats]	Top Threats to Cloud Computing V1.0, https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf
[b-csoonline]	SaaS, PaaS, and IaaS: a Security Checklist for Cloud Models – http://www.csoonline.com/article/print/660065
[b- owasp]	Cloud – 10 Risks with Cloud IT Foundation Tier, https://www.owasp.org/index.php/Cloud-10_Risks_with_Cloud_IT_Foundation_Tier
[b- TCG]	Cloud Computing and Security – A Natural Match, http://www.trustedcomputinggroup.org/files/resource_files/1F4DEE3D-1A4B-B294-D0AD0742BA449E07/Cloud%20Computing%20and%20Security%20Whitepaper_July29.2010.pdf

[b- Karger]	Paul A. Karger, Multi-Level Security Requirements for Hypervisors, ISBN: 0-7695-2461-3
[b- RSA]	A Proposed Security Architecture for Next-Generation Data Centre, RSA Office of the CTO
[b- ETRI]	Sangjin Jeong(ETRI), Myung-Ki Shin (ETRI) Takashi Egawa (NEC), Hideki Otsuki (NICT), Network Virtualization Problem Statement.
[b- Ormandy]	Tavis Ormandy, An Empirical Study into the Security Exposure to Hosts of Hostile Virtualized Environments.
[b- Garfinkel]	Tal Garfinkel , Mendel Rosenblum, A Virtual Machine Introspection Based Architecture for Intrusion Detection.
[b- Xu-1]	Dahai Xu, Ying Li,, Mung Chiang, and A. Robert Calderbank, Elastic Service Availability: Utility Framework and Optimal Provisioning.
[b- Gerstel-1]	Ori Gerstel and Galen Sasaki, Quality of Protection (QoP): A Quantitative Unifying Paradigm to Protection Service Grades.
[b- Gerstel-2]	Ori Gerstel, and G. Sasaki, A General Framework for Service Availability for Bandwidth-Efficient Connection-Oriented Networks.
[b- Li]	Wenjuan Li and Lingdi Ping, Trust Model to Enhance Security and Interoperability of Cloud Environment.
[b- Xu-2]	Dahai Xu, Ying Li,, Mung Chiang, and A. Robert Calderbank, Elastic Service Availability: Utility Framework and Optimal Provisioning.
[b-Virginia Tech]	Glossary, Virginia Tech.

Printed in Switzerland
Geneva, 2012