International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1601

(01/2014)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Cloud computing security – Overview of cloud computing security

Security framework for cloud computing

Recommendation ITU-T X.1601

International Telecommunication Union

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	**X.1600–X.1601**
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1601

Security framework for cloud computing

Summary

Recommendation ITU-T X.1601 describes the security framework for cloud computing. The Recommendation analyses security threats and challenges in the cloud computing environment, and describes security capabilities that could mitigate these threats and address security challenges. A framework methodology is provided for determining which of these security capabilities will require specification for mitigating security threats and addressing security challenges for cloud computing. Appendix I provides a mapping table on how a particular security threat or challenge is addressed by one or more corresponding security capabilities.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1601	2014-01-24	17	11.1002/1000/12036-en

Keywords

Cloud computing, privacy protection, security capabilities, security challenges, security framework, security threats.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation 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 members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T X.1601

Security framework for cloud computing

1 Scope

This Recommendation analyses security threats and challenges in the cloud computing environment, and describes security capabilities that could mitigate these threats and address security challenges. A framework methodology is provided for determining which of these security capabilities will require specification for mitigating security threats and addressing security challenges for cloud computing.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 authentication [b-NIST-SP-800-53]: Verification of the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

3.1.2 capability [b-ISO/IEC 19440]: Quality of being able to perform a given activity.

3.1.3 data controller [b-key definition**]:** A person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

3.1.4 data processor [b-key definition]: In relation to personal data, this means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

3.1.5 hypervisor [b-NIST-SP-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.

3.1.6 personally identifiable information [b-ISO/IEC 29100]: Any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal.

3.1.7 security domain [b-ITU-T X.810]: A set of elements, a security policy, a security authority and a set of security-relevant activities in which the set of elements are subject to the security policy for the specified activities, and the security policy is administered by the security authority for the security domain.

3.1.8 security incident [b-ITU-T E.409]: A security incident is any adverse event whereby some aspect of security could be threatened.

3.1.9 service level agreement (SLA) [b-ISO/IEC 20000-1]: A documented agreement between the service provider and customer that identifies services and service targets.

NOTE 1 – A service level agreement can also be established between the service provider and a supplier, an internal group or a customer acting as a supplier.

NOTE 2 – A service level agreement can be included in a contract or another type of documented agreement.

3.1.10 threat [b-ISO/IEC 27000]: A potential cause of an unwanted incident, which may result in harm to a system or organization.

3.1.11 virtual machine (VM) [b-NIST-SP-800-145]: An efficient, isolated, logical duplicate of a real machine.

3.1.12 vulnerability [b-NIST-SP-800-30]: A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 cloud computing: A paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with on-demand self-service provisioning and administration.

3.2.2 cloud service: One or more capabilities offered via cloud computing (clause 3.2.1) invoked using a declared interface.

3.2.3 cloud service customer: A party (clause 3.2.12) which is in a business relationship for the purpose of using cloud services (clause 3.2.2).

3.2.4 cloud service partner: A partner engaged in support of, or auxiliary to, activities of either a cloud service provider (clause 3.2.5) or a cloud service customer (clause 3.2.3).

3.2.5 cloud service provider: A party (3.2.12) which makes cloud services (clause 3.2.2) available.

3.2.6 cloud service user: A person associated with a cloud service customer (clause 3.2.3) that uses cloud services (clause 3.2.2).

3.2.7 communications as a service (CaaS): A cloud service category in which the capability provided to the cloud service customer (clause 3.2.3) is real-time communication and collaboration.

NOTE – CaaS can provide both platform capabilities type and application capabilities type.

3.2.8 community cloud: A cloud deployment model that exclusively supports and is shared by a specific collection of cloud service customers (clause 3.2.3); resources are controlled by at least one member of this collection.

NOTE – Shared requirements include, but are not limited to, mission, information security requirements, policy, and compliance considerations.

3.2.9 infrastructure as a service (IaaS): A cloud service category in which the cloud capabilities type provided to the cloud service customer (clause 3.2.3) is an infrastructure capabilities type.

NOTE – The cloud service customer (clause 3.2.3) does not manage or control the underlying physical and virtual resources but does have control over operating systems, storage, and deployed applications that use the physical and virtual resources. The cloud service customer (clause 3.2.3) may also have limited ability to control certain networking components (e.g., host firewalls).

3.2.10 multi-tenancy: Allocation of physical and virtual resources whereby multiple tenants (clause 3.2.18) and their computations and data are isolated from and are inaccessible to one another.

3.2.11 network as a service (NaaS): A cloud service category in which the capability provided to the cloud service customer (clause 3.2.3) is transport connectivity and its related network capabilities.

NOTE – NaaS can provide any of the three cloud capabilities types.

3.2.12 party: A natural person or organization.

3.2.13 platform as a service (PaaS): A cloud service category in which the cloud capabilities type provided to the service customer (clause 3.2.3) is a platform capabilities type.

3.2.14 private cloud: A cloud deployment model that is shared exclusively by a single cloud service customer (clause 3.2.3) and resources are controlled by the cloud service customer (clause 3.2.3).

3.2.15 public cloud: A cloud deployment model that is potentially available to any cloud service customer (clause 3.2.3) and resources are controlled by the cloud service provider (clause 3.2.5).

3.2.16 security challenge: A security "difficulty" other than a direct security threat arising from the nature and operating environment of cloud services, including "indirect" threats. See clauses 7 and 8.

3.2.17 software as a service (SaaS): A cloud service category in which the cloud capabilities type provided to the cloud service customer (clause 3.2.3) is an application capabilities type.

3.2.18 tenant: Group of cloud service users (clause 3.2.6) sharing access to a set of physical and virtual resources.

NOTE – Typically, and within the context of multi-tenancy (clause 3.2.10), the group of cloud service users (clause 3.2.6) that form a tenant will all belong to the same cloud service customer (clause 3.2.3) organization. There might be cases where the group of cloud service users (clause 3.2.6) involves users from multiple different consumers, particularly in the case of community cloud (clause 3.2.8) deployments, but these are specialized exceptions. However, a given cloud service customer (clause 3.2.3) organization might have many different tenancies with a single cloud service provider (clause 3.2.5), perhaps representing different business groups within the organization (e.g., sales versus accounting), since there may be good reason to keep the data and activities belonging to those different groups well separated for business and commercial reasons.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API Application Programming Interface

BCP Business Continuity Plan

CaaS Communications as a Service

CPU Central Processing Unit

CSC Cloud Service Customer

CSN Cloud Service Partner

CSP Cloud Service Provider

CSU Cloud Service User

DNS Domain Name System

IaaS Infrastructure as a Service

IAM Identity and Access Management

ICT Information and Communication Technology

IP Internet Protocol

IT Information Technology

NaaS Network as a Service

OS Operating System

PaaS Platform as a Service

PII Personally Identifiable Information

PKI Public Key Infrastructure

SaaS Software as a Service

SIM Subscriber Identity Module

SLA Service Level Agreement

VM Virtual Machine

5 Conventions

None.

6 Overview

Cloud computing is a paradigm for enabling convenient, on-demand network access to a shared pool of configurable 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 customers can use these resources to develop, host and run services and applications on-demand in a flexible manner in any device, anytime and anywhere in the cloud computing environment. Cloud computing services are usually delivered in certain service categories, e.g., infrastructure as a service (IaaS), platform as a service (PaaS), software as a service (SaaS), network as a service (NaaS), etc. These service categories enable cloud computing customers to launch or change their business quickly and easily without establishing new information and communication technology (ICT) infrastructure and systems and provide opportunities to provision resources elastically, as needed. For example, some cloud service providers (CSPs) might provide abstracted hardware and software resources which may be offered as a service (e.g., IaaS or NaaS). Other cloud service providers may provide cloud specific platforms (PaaS) or applications (SaaS) to enable customers and partners to rapidly develop and deploy new applications which can be configured and used remotely.

There are security threats and challenges in adopting cloud computing, and security requirements vary to a great extent for different cloud computing service deployment models and service categories. The distributed and multi-tenant nature of cloud computing, the prevalence of remote access to cloud computing services and the number of entities involved in each process make cloud computing inherently more vulnerable to both internal and external security threats than other paradigms. Many of the security threats can be mitigated with the application of traditional security processes and mechanisms. Security touches upon and impacts many parts of a cloud computing service. Therefore, the security management of the cloud computing services, as well as the associated resources, is a critical aspect of cloud computing.

Before the migration of the ICT system to cloud computing, a potential cloud service customer (CSC) should identify their security threats (see clause 7 below) and security challenges (see clause 8).

Based on these threats and challenges, a set of high-level security capabilities (see clause 9) are identified. Specific requirements for these capabilities are out of the scope of this Recommendation, but they will need to be identified for specific implementations of cloud computing services, based on risk assessment against the identified threats and challenges.

Based on the risk assessment, a CSC can determine whether to adopt cloud computing, and can make informed decisions over service providers and architecture. The above risk assessment should be performed by using an information security risk management framework (e.g., the risk management framework defined in [b-ISO/IEC 27005]). See also clause 10 below for a suggested framework methodology.

This Recommendation distinguishes between security threats and security challenges. Security threats are those associated with attacks (both active and passive), and also environmental failures or disasters. Security challenges comprise difficulties arising from the nature and operating environment of cloud services. When not properly addressed, security challenges may leave doors open for threats.

Based on these identified security threats and challenges, the security capabilities are described to mitigate security threats and address security challenges for cloud computing.

7 Security threats for cloud computing

Threats have the potential to harm assets such as information, processes and systems and therefore organizations. Threats may be of a natural or human origin, and could be accidental or deliberate. A threat may arise from within or from outside the organization. Threats can be classified as accidental or intentional and may be active or passive.

The specific threats encountered are highly dependent on the chosen specific cloud service. For example, for a public cloud, threats can arise from the split responsibilities between the CSC and CSP: complexities of specifying jurisdiction over data and processes, consistency and adequacy of data protection, and maintenance of privacy, etc. However, for a private cloud, the threats are simpler to address because the CSC controls all the tenants hosted by the CSP. Even though some of the threats identified in this Recommendation are also covered by existing industry documents (e.g., Recommendation ITU-T X.800), all the threats are relevant to cloud computing. The applicability of individual threats will depend on the specific cloud service.

This clause describes the various security threats that can arise in a cloud computing environment.

7.1 Security threats for cloud service customers (CSCs)

The following threats are those that directly affect CSCs. They may affect the CSCs' personal or business interests, privacy, lawfulness or safety. Not all CSCs will be at risk by all threats. The risk will be unequal depending on the nature of the CSC and of the cloud computing service being used. For example, a cloud service specific to the transcoding of commercial video files has no requirements to protect personally identifiable information (PII), but will have strong requirements around the protection of digital assets.

7.1.1 Data loss and leakage

As the cloud service environment is typically a multi-tenant one, loss or leakage of data is a serious threat to the CSC. A lack of appropriate management of cryptographic information, such as encryption keys, authentication codes and access privilege, could lead to significant damages, such as data loss and unexpected leakage to the outside. For example, insufficient authentication, authorization, and audit 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 sources of this threat and may be associated with the challenges described in clauses 8.1.2 "Loss of trust", clause 8.1.3 "Loss of governance" and clause 8.1.4 "Loss of privacy".

7.1.2 Insecure service access

Identity credentials, including those of CSC administrators, are especially vulnerable to unauthorized users in the highly distributed environment of cloud computing, since unlike traditional telecommunications it is often difficult to rely on location (e.g., landline) or the presence of a specific hardware element(e.g., a mobile subscriber identity module (SIM)) to reinforce authentication of identity. As most of the service offerings are remote, unprotected connections expose potential vulnerability. Even when the connections are protected or local, other attack methods (such as phishing, fraud, social engineering and exploitation of software vulnerabilities)

may also succeed. If an attacker gains access to users' or administrators' credentials, they can eavesdrop on activities and transactions, manipulate data, return falsified information, and redirect a CSC's clients to illegitimate sites. Passwords are often reused across multiple websites and services, which amplify the impact of such attacks since a single break can expose multiple services. Cloud computing solutions also add a new threat to the landscape. The CSC's account or service instances may become a new base for an attacker. From this point onwards, the attacker may leverage the power of the CSC's reputation and resources to launch subsequent attacks.

7.1.3 Insider threats

Where human beings are involved, there is always a risk of individuals acting in a manner that is not consistent with the security of the service. CSC employees sharing "administrator" passwords, or otherwise leaving credentials unsecure (e.g., written on notes stuck to a screen), careless or inadequately trained users (or family members in a consumer setting), or malicious actions by disgruntled employees will always pose a significant threat.

7.2 Security threats for cloud service providers (CSPs)

This clause identifies threats that directly affect CSPs. Such threats might affect the ability of a CSP to offer services, to do business, to retain customers, and to avoid legal or regulatory difficulties. Threats to a given CSP will also depend on their specific service offerings and environments.

7.2.1 Unauthorized administration access

The cloud computing service will include interfaces and software components that allow the CSC's own staff to administer those aspects of the cloud computing service that are under the CSC's control, such as the addition or removal of CSC employee accounts, connections to the CSC's own servers, changes to service capacity, updating the domain name system (DNS) entries and websites, etc. Such administrative interfaces can become a target of choice for attackers who impersonate the CSC's administrators to attack a CSP. Because such cloud computing services have to be accessible to the CSC's own staff, the protection of these services becomes a major concern for cloud computing security.

7.2.2 Insider threats

Where humans are involved, there is always a risk of individuals acting in a malicious or careless manner that puts the security of the service at risk.

CSP employees sharing "administrator" passwords, or otherwise leaving credentials unsecure (e.g., written on notes stuck to a screen), careless or inadequately trained users, or malicious actions by disgruntled employees will always pose a significant threat to any business.

CSPs in particular need to seriously consider the trustworthiness of their own employees. Even with good screening of employees, there is always the risk of a skilled intruder successfully obtaining a position on the CSP's data centre staff. Such an intruder might be seeking to undermine the CSP itself, or may be intending to penetrate specific CSC systems that are being supported, especially if the CSC is a high-profile corporation or government agency.

8 Security challenges for cloud computing

Security challenges comprise difficulties other than security threats arising from the nature and operating environment of cloud services, including "indirect" threats. An indirect threat is where a threat to one participant of a cloud service may have adverse consequences for others.

The challenges identified in this Recommendation are the ones that when not properly addressed, may leave the door open to threats. These challenges need to be considered when considering cloud computing services.

8.1 Security challenges for cloud service customers (CSCs)

This clause describes security challenges associated with environmental difficulties or indirect threats that may give rise to more direct threats to the interests of the CSC.

8.1.1 Ambiguity in responsibility

CSCs consume delivered resources through different service categories and deployment models. The customer-built ICT system thus relies on these services. Any lack of a clear definition of responsibility among CSCs and CSPs may introduce conceptual and operational conflicts. Any contractual inconsistency of provided services could induce an anomaly or incidents. For example, the problem of which entity is the data controller and which one is the data processor may be unclear at an international scale, even if the international aspect is reduced to a minimal third party outside of a specific region such as the European Union.

Due to legal and regulatory requirements, any related doubt (e.g., whether a given CSC or CSP is a "data controller" or "data processor") may lead to ambiguity as to which set of regulations they are required to adhere to. If this interpretation varies in different jurisdictions, a given CSC or CSP could find themselves subject to conflicting regulations on the same service or portion of data.

8.1.2 Loss of trust

Sometimes, it is difficult for a CSC to recognize their CSP's trust level due to the black-box feature of the cloud computing service. If there are no means of obtaining and sharing the provider's security level in a formalized manner, CSCs have no means to evaluate the security implementation level achieved by the provider. Such a lack of sharing at the security level with regard to CSP could become a serious security threat for some CSCs in their use of cloud computing services.

8.1.3 Loss of governance

The decision by CSCs to migrate a part of their own ICT system to a cloud computing infrastructure implies giving partial control to a CSP. This could be a serious threat to a CSC's data, notably regarding the role and privilege assignment to the provider. Coupled with a lack of transparency regarding cloud computing provider practices, this may lead to misconfiguration, or even enable a malicious insider attack.

When adopting cloud computing services, some CSCs may have concerns over a lack of control over their information and assets hosted in CSPs, over data storage, reliability of data backup (data retention issues), countermeasures for business continuity plans (BCPs) and disaster recovery, etc.

For example:

- A CSC wishes to delete a file for legal reasons, but the CSP retains a copy that the CSC does not know about.
- A CSP gives the CSC's administrator privileges that go beyond the CSC's policy.
- Some CSCs may have concerns regarding the exposure of data by a CSP to foreign governments which could impact the CSC's compliance with privacy laws, such as the European Union data protection directives.

8.1.4 Loss of privacy

When a CSP processes private information, there is a possibility of there being a violation of privacy which does not comply with privacy regulations or laws. This includes the leakage of private information, or the processing of private information for a purpose that is not authorized by the CSC and/or the data subject.

8.1.5 Service unavailability

Availability is not specific to the cloud computing environment. However, because of the service-oriented design principle, service delivery may be impacted when upstream cloud computing

services are not completely available. Moreover, the dynamic dependency of cloud computing offers more possibilities to an attacker. For example, a denial-of-service attack on one upstream service may affect multiple downstream services in the same cloud computing system.

8.1.6 Cloud service provider lock-in

High dependency on a single CSP could make it more difficult to replace a CSP by another. This could be the case where a CSP relies on non-standard functions or formats and does not provide interoperability. This could become a security threat if the lock-in CSP fails to address the security vulnerabilities, thus leaving the CSC vulnerable but unable to migrate to another CSP.

8.1.7 Misappropriation of intellectual property

When the CSC's code is run or other assets are stored by the CSP, the challenge exists that this material could be leaked to third parties or misappropriated for unauthorized use. This could include a violation of copyright or exposure of trade secrets.

8.1.8 Loss of software integrity

Once the CSC's code is running in the CSP, there is the possibility of the code being modified or infected while it is out of the direct control of the CSC, thus causing their software to misbehave in some way. Although this possibility exists outside the CSC's control, it could seriously affect their reputation and thus their business.

8.2 Security challenges for cloud service providers (CSPs)

This clause describes security challenges associated with environmental difficulties or indirect threats that may give rise to more direct threats to the interests of the CSP.

8.2.1 Ambiguity in responsibility

Different roles (CSP, CSC, and cloud service partner (CSN)) may be defined in a cloud computing system. Ambiguity of the definition of responsibilities related to issues such as data ownership, access control or infrastructure maintenance may impact business or legal disputes (especially when dealing with third parties, or when CSP is also a CSC or a CSN). This ambiguity risk increases when the CSP is operating and/or offering services across multiple jurisdictions where contracts and agreements may exist in different languages or legal frameworks. See also clause 8.2.4, "Jurisdictional conflict" below.

8.2.2 Shared environment

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 CSCs consume services from the same cloud simultaneously. As a result, the CSC could potentially have unauthorized access to other tenants' virtual machines, network traffic, actual/residual data, etc. Any such unauthorized or malicious access to another CSC's assets might compromise integrity, availability and confidentiality.

For example, multiple virtual machines co-hosted on one physical server share both the central processing unit (CPU) and memory resources which are virtualized by the hypervisor. This example of challenges covers the failure of hypervisor isolation mechanisms, thus allowing unauthorized access to the memory or storage of other virtual machines.

8.2.3 Inconsistency and conflict of protection mechanisms

Due to the decentralized architecture of a cloud computing infrastructure, its protection mechanisms might be inconsistent among distributed security modules. For example, an access denied by one security module may be granted by another. This inconsistency might cause problems for an

authorized user, and might be exploited by an attacker, thereby compromising confidentiality, integrity and availability.

8.2.4 Jurisdictional conflict

Data in the cloud can be moved around between data centres, or even across international borders. Depending on the host country, data will be governed by different applicable jurisdictions. For example, some jurisdictions, such as the European Union, require extensive protection of personally identifiable information, which cannot usually be processed in places that do not provide a sufficient level of guaranteed protection. As a second example, some jurisdictions may treat communications as a service (CaaS) as unregulated information service while others treat it as a regulated telephony service. This jurisdictional conflict can lead to legal complications.

8.2.5 Evolutionary risks

One advantage of cloud computing is to postpone some choices from the system design phase to the execution phase. This means that some dependent software components of a system may be selected and implemented only when the function requiring them has been executed. However, conventional risk assessment methodology can no longer match such a dynamically evolving system. A system which has passed a security assessment during the design phase might have new vulnerabilities introduced during its lifetime due to changes in software components.

8.2.6 Bad migration and integration

Migrating to the cloud often implies moving large amounts of data and major configuration changes (e.g., network addressing). Migration of a part of an ICT system to an external CSP might require substantial changes in the system design (e.g., network and security policies). A bad integration caused by incompatible interfaces or inconsistent policy enforcement might result in both functional and non-functional impacts. For example, virtual machines that run behind a firewall in a private data centre are accidently exposed to the open Internet in the CSP's cloud.

8.2.7 Business discontinuity

Cloud computing allocates resources and delivers them as a service. The whole cloud computing ecosystem is composed of many interdependent parts. The discontinuity of any part (such as a blackout, denial-of-service or delay) might affect cloud computing service availability connected with clause 8.1.5 "Service unavailability", and then cause business discontinuity.

8.2.8 Cloud service partner lock-in

The platform of the CSP is built using software and hardware components from various suppliers. Some components may include proprietary features or extensions that are useful to the CSP. However, relying on these proprietary features limits the CSP's ability to migrate to another component supplier.

While lock-in is a business issue, it is not in itself a security threat. However, it can sometimes give rise to security concerns. For example, if the CSN who supplies a key component goes out of business, it may be that no further security patches are available. Where vulnerability in the component emerges, it may be very difficult or expensive to mitigate the risk.

8.2.9 Supply chain vulnerability

A CSP is at risk if hardware or software delivered to the platform through their supply chain undermines CSC or CSP security, for example, the accidental or deliberate introduction of malware or exploitable vulnerabilities.

A case in point would be a bad code from the CSN. This security challenge exists for a CSN code running in the CSP, such as customer facing, a virtual machine (VM) guest operating system (OS),

applications, platform components, or audit/monitoring software (e.g., for a partner providing a service audit).

Another example is when a CSP is running a code provided by a partner; the CSP is at risk if the partner fails to provide the necessary security updates in a timely manner.

8.2.10 Software dependencies

When vulnerability is detected, it may not be possible to apply updates immediately because doing so would break other software components (though those components may not otherwise require updating). This is particularly true if the dependency exists between components provided by one or more CSNs, rather than the CSPs themselves.

8.3 Security challenges for cloud service partners (CSNs)

This clause considers challenges that directly affect CSNs. Such challenges might affect the ability of a CSN to do business, to get paid, to protect their intellectual property, and to avoid legal or regulatory difficulties. Security challenges to a given CSN will depend on their specific business and environments, such as development, integration, audit, or otherwise.

8.3.1 Ambiguity in responsibility

Where there is a mix of CSP and CSN code running in the service, it may not be apparent to the CSC where the responsibility for mitigation and handling of security incidents resides. It may be quite difficult to determine the responsible entity by technical analysis. This could result in mutual finger-pointing between the CSP and CSN(s) as to who is at fault, which could result in further breaches if the root cause is not found.

8.3.2 Misappropriation of intellectual property

When partners submit codes or other assets to the CSP for execution, the security challenge exists that this material could be leaked to third parties or misappropriated for unauthorized use. This could include a violation of copyright or the exposure of trade secrets.

8.3.3 Loss of software integrity

Once the partner's code is running in the CSP, there is a possibility of the code being modified or infected while it is out of the direct control of the CSN, thus causing their software to misbehave in some way. Although this possibility exists outside the CSN's control, it could seriously affect their reputation and thus their business.

9 Cloud computing security capabilities

This Recommendation identifies the following security capabilities against identified cloud computing security threats and challenges. Parameters related with these security capabilities may be stipulated in the security service level agreement (SLA), for example, an incident response time.

9.1 Trust model

A common trust model is necessary for any system where multiple providers cooperate to provide a trustworthy service.

Because of the highly distributed and multi-stakeholder nature of cloud computing, the cloud computing environment will need to incorporate an overall trust model. This trust model will enable the creation of islands and/or federations of trusted entities, such that disparate elements of the system will be able to authenticate the identity and authorized rights of other entities and components. Each island or federation of trust will be based on one or more trusted authorities (e.g., a public key infrastructure (PKI) certificate authority).

Multiple trust models exist today for both cloud and non-cloud purposes. The specific trust model to be adopted is out of the scope of this Recommendation.

9.2 Identity and access management (IAM), authentication, authorization and transaction audit

Multiple administrators and users are involved in cloud computing services, and these cloud computing services are accessed and used internally (CSPs) and externally (CSCs). Identity management is needed, not only to protect identities, but also to facilitate the access management, authentication, authorization and transaction audit processes in such a dynamic and open cloud computing infrastructure.

One or more common trust models (clause 9.1) are needed by IAM for the authentication of identities, and by developers, hypervisors and other system components for the authentication of system components such as downloaded software modules, applications or datasets.

IAM contributes to the confidentiality, integrity and availability of services and resources, and thus becomes essential in cloud computing.

Furthermore, IAM may enable the implementation of single sign-on and identity federation for clouds using different authentication mechanisms or distributed in different security domains.

Transaction audit protects against repudiation, enables forensic analysis after a security incident, and acts as a deterrent to attacks (both intrusion and insider). Transaction audit implies more than simple logging, but also includes active monitoring to flag up suspicious activities.

9.3 Physical security

Physical security needs to be achieved. Access to premises containing CSP equipment is restricted to authorized persons and only to those areas directly necessary for their job functions; this is part of the IAM process. However, the extent of physical security will depend on the value of the data and the extent to which multiple customers are permitted access.

9.4 Interface security

This capability secures interfaces open to CSCs and/or other contracted CSPs through which various kinds of cloud computing services are delivered, and secures communications based on these interfaces. Mechanisms available to ensure interface security include but are not limited to: unilateral/mutual authentication, integrity checksum, end-to-end encryption, digital signature, etc.

9.5 Computing virtualization security

Computing virtualization security refers to the security of the whole computing virtualization environment. It protects the hypervisor from attacks, protects the host platform from threats originating in the computing virtualization environment, and keeps VMs secure throughout the life-cycle. Specifically, this capability enables VM isolation, and protects the VM images and suspended VM instances in storage and during migration.

For CSP, the hypervisor often provides protection for hosted VMs, for example, by providing anti-virus and anti-spam processing inside hypervisors, so that VMs do not need to implement these functions separately. The hypervisor will normally be configured with the minimum set of services. Unnecessary interfaces and application programing interfaces (APIs) will normally be closed, and irrelevant service components will normally be disabled.

VMs covered by this capability include those created by CSC in IaaS, as well as any VMs created by SaaS and PaaS. Virtual machines will usually be well isolated when sharing memory, a central processing unit (CPU) and storage capacities. Virtual machines will usually have intrinsic security capabilities and policy awareness (e.g., in the guest operating system).

9.6 Network security

In a cloud computing environment, network security enables both physical and virtual network isolation, and secures communications among all participants. It enables network security domain partition, network border access controls (e.g., firewall), intrusion detection and prevention, network traffic segregation based on security policies, and it protects the network from attacks in both the physical and virtual network environments.

9.7 Data isolation, protection and privacy protection

This capability addresses general data protection issues which often have legal implications.

- Data isolation

In a cloud computing context, a tenant is prevented from accessing data belonging to another tenant, even when the data is encrypted, except when explicitly authorized. Data isolation may be realized logically or physically, depending on the required isolation granularity and the specific deployment of cloud computing software and hardware.

NOTE 1 – In cloud computing, isolation occurs at the tenant level. A given CSC may have multiple tenants in the cloud, for example, to separate different subsidiaries, divisions or business units.

- Data protection

Data protection ensures that CSC data and derived data held in a cloud computing environment is appropriately protected so that it can only be accessed or changed as authorized by the CSC (or according to applicable law). This protection may include some combination of access control lists, integrity verification, error correction/data recovery, encryption and other appropriate mechanisms.

When a CSP provides storage encryption for CSCs, this function can be client-side encryption (e.g., within a CSP application) or server-side encryption.

- Privacy protection

Private information can include PII and confidential corporate data. The collection, use, transfer, handling, storage and destruction of private information can be subject to privacy regulations or laws. This restriction applies to both CSPs and their CSCs, e.g., a CSC must be able to permanently delete a data table containing private information, even though the CSP is not aware of the table contents. CSPs may also need to support the handling, e.g., searching of a CSCs' data in their transformed or encrypted form.

Privacy protection extends to private information that may be observed or derived from CSC activities, such as business trends, relationships or communications with other parties, activity levels and patterns, etc.

Privacy protection is also responsible for ensuring that all private information (including observed or derived data) is used only for those purposes which have been agreed between a CSC and CSP.

A risk assessment of private information (noted as "privacy risk assessment") can assist a CSP in identifying the specific risks of privacy breaches involved in an envisaged operation. The CSP should identify and implement capabilities to address the privacy risks identified by the risk assessment and treatment of private information.

NOTE 2 – In some jurisdictions, individual natural persons (i.e., human users) are treated separately from their employers for privacy purposes. In such circumstances, privacy of the cloud service user (CSU) will be appropriately protected in addition to that of the cloud service customer (CSC) or cloud service tenant.

9.8 Security coordination

Since different cloud computing services imply different implementations of security controls, this security capability coordinates heterogeneous security mechanisms to avoid protection conflicts.

Parties playing different roles in the cloud computing ecosystem, e.g., CSP, CSC, CSN, have different degrees of control over the physical or virtual resources and services, including the control of security.

For each party, there will be various security mechanisms including hypervisor isolation, IAM, network protection, etc.

One of the purposes of cloud computing is to enable a combination of these different parties to collaboratively design, build, deploy and operate various physical and virtualized resources together. Therefore, a CSP needs to be able to coordinate different security mechanisms across the different parties. Security coordination depends on the interoperability and harmonization of diverse security mechanisms.

9.9 Operational security

This capability provides security protection for the daily operation and maintenance of cloud computing services and infrastructure.

This operational security capability includes:

- defining sets of security policies and security activities such as configuration management, patch upgrade, security assessment, incident response (see also clause 9.10 "Incident management"), and ensuring these security measures are correctly enforced to fulfil the requirements of applicable laws and contracts including any security SLA;
- monitoring the CSP's security measures and their effectiveness, and giving appropriate reports to affected CSCs and applicable third-party auditors (acting as a CSN), which can enable the CSC to measure whether a CSP is delivering on SLA security commitments.

In the event that the CSP's security measures or their effectiveness changes, all downstream CSPs and CSCs will be alerted to such changes.

These reports and alerts enable authorized CSCs to see appropriate incidents, audit information, and configuration data relating to their cloud computing services.

9.10 Incident management

Incident management provides incident monitoring, prediction, alerting and response. In order to know whether the cloud computing service is operating as expected through the whole infrastructure, continuous monitoring is necessary (e.g., monitoring the real-time performance of virtualized platform and virtualized machine). This enables systems to capture the service security status, identify abnormal conditions, and provide early warning of security system overloads, breaches, service discontinuity, etc. After the occurrence of security incidents, the problem is identified and the incident is quickly responded to, either automatically or with the intervention of a human administrator. Closed incidents are logged and analysed for possible underlying patterns which can then be proactively addressed.

9.11 Disaster recovery

Disaster recovery represents the capability to respond to catastrophic disasters, to recover to a safe state and to resume normal operations as quickly as possible. This capability provides continuity of provided service with minimum interruption.

9.12 Service security assessment and audit

This capability enables the security evaluation of cloud computing services. It enables an authorized party to verify that a cloud service complies with the applicable security requirements. Security assessment or security audit could be performed by the CSC, CSP or a third party (CSN), and security certification could be performed by an authorized third party (CSN).

Appropriate security criteria are implemented so as to provide a mutual understanding of the security level between the CSC and CSP.

Each CSP and each of their services may have the security level regarding the CSP's security controls and their effectiveness. Advertised security levels of the CSPs and their services will help facilitate the comparison and selection of appropriate CSPs and cloud computing services. Independent trusted third parties may be used to provide reliable, independent and neutral security level assessments.

To avoid a CSP conducting individual security audits for each CSC, common service audit results will be appropriately reused. For a CSP covering a wide range of cloud computing services, security audits may be conducted on each cloud computing service. The CSP may provide the appropriate audit results of all or part of the cloud computing services to an authorized CSC (e.g., potential customer), and to certain other CSPs and CSNs (e.g., third-party auditor).

For a cloud computing service chain, the security audit results of a downstream service provider will integrate the relevant security audit results of upstream service providers.

9.13 Interoperability, portability and reversibility

This capability enables the coexistence and cooperation of heterogeneous components (interoperability), it enables CSCs to replace one CSP with another where appropriate (portability), and enables CSCs to transfer their ICT system from a cloud computing environment back to a non-cloud computing ICT infrastructure (reversibility). This reversibility will also enable the "right to be forgotten" if this is required by local laws or regulations.

NOTE 1 – This capability is only responsible for the interoperability and portability of cloud computing security functions, not of the actual data, metadata or message formats, which are the responsibility of other cloud computing platform functions. For example, this capability might provide transitional encryption, key management and identity information so that data and other content can be moved between two different encryption systems without exposing either the system(s) or the data in transit.

NOTE 2 – The "right to be forgotten" is not yet clearly defined and may in some cases be constrained by regulatory requirements to retain certain data for a minimum period, such as call records or connection information. It may therefore also be necessary to retain the relevant keys or other security information for the same period.

9.14 Supply chain security

A CSP uses a number of suppliers to build their services. Some of these will be cloud industry participants, e.g., a CSN, while others will be traditional information technology (IT) equipment or service suppliers, e.g., hardware manufacturers with no direct relationship with cloud computing. This capability enables the establishment of a trust relationship between the CSP and all participants in the supply chain by security activities. These supply chain security activities involve identifying and gathering information about the CSP's acquired components and services that are used to provide cloud computing services, and enforcing supply chain security policies.

For example, typical supply chain security activities in a CSP may include:

- confirmation of background information about the participants in the supply chain;
- validation of hardware, software and services employed by the CSP;
- inspection of the hardware and software purchased by the CSP so as to ensure that it was not tampered with while in-transit;
- providing mechanisms to verify the provenance of cloud service software, for example, code provided by a CSN. Where applicable, CSNs and their host CSPs provide a process to verify the integrity of the CSN's software component to ensure that it is exactly as delivered and has not been modified or compromised. Some CSNs may demand the means to verify this directly by themselves.

This capability is continuous to cover ongoing system evolution and updates.

10 Framework methodology

To develop a security framework for cloud computing means understanding what threats and challenges exist, as was discussed in clauses 7 and 8, for the chosen specific cloud service along with the business, technology and regulatory requirements which are to be taken together to identify security controls, policies and procedures that will be needed for a given cloud service. The capabilities described in clause 9 to address and mitigate these threats and challenges are then used to develop the security controls, policies and procedures for the chosen specific cloud computing service. This Recommendation focuses on what the needs are for security in a cloud computing environment, the threats and challenges of a traditional computing environment exist within the cloud environment and as such following the standards and best practices defined by the industry should be followed in addition to this Recommendation.

The methodology described here should be followed to create the framework that will identify what security controls, policies and procedures will be needed for a specific given cloud computing service. It is not possible to provide a single normative framework for all cloud computing services, since they vary greatly in business model, services offered and implementation choices:

- Step 1: Use clauses 7 and 8 to identify security threats and security implications of the challenges in the cloud computing service under study.
- Step 2: Use clause 9 to identify the needed high-level security capabilities based on identified threats and challenges which could mitigate security threats and address security challenges.
- Step 3: Derive security controls, policies and procedures which could provide the security abilities that are needed based on identified security capabilities.

NOTE – A set of appropriate requirements with respect to the security capabilities will need to be determined by the CSC and CSP using appropriate standards. This determination will be based on the risk assessment.

To identify which security threats and challenges are relevant for the cloud service under study, each threat or challenge should be reviewed. One approach could be as simple as a table showing a 'Y' next to the threat or challenge.

For an example using this approach, when the CSP provides file storage as a service to individual users, the CSP would like to understand what security threats and challenges users are mainly concerned about, and to analyse what security threats and challenges that CSP mainly needs to address. Table 1 demonstrates this approach.

Table 1 – Example of security framework analysis step 1 for file storage as a service

Area of analysis	Specific threat or challenge	Is this applicable to this service?
Clause 7.1 Security threats for cloud service customers (CSC)	Clause 7.1.1 Data loss and leakage	Y
	Clause 7.1.2 Insecure service access	Y
	Clause 7.1.3 Insider threats	
Clause 7.2 Security threats for cloud service providers (CSPs)	Clause 7.2.1 Unauthorized administration access	Y
	Clause 7.2.2 Insider threats	Y

Table 1 – Example of security framework analysis step 1 for file storage as a service

Area of analysis	Specific threat or challenge	Is this applicable to this service?
Clause 8.1 Security challenges for cloud service customers (CSCs)	Clause 8.1.1 Ambiguity in responsibility	Y
	Clause 8.1.2 Loss of trust	Y
	Clause 8.1.3 Loss of governance	Y
	Clause 8.1.4 Loss of privacy	Y
	Clause 8.1.5 Service unavailability	Y
	Clause 8.1.6 Cloud service provider lock-in	Y
	Clause 8.1.7 Misappropriation of intellectual property	
	Clause 8.1.8 Loss of software integrity	
Clause 8.2 Security challenges for cloud service providers (CSPs)	Clause 8.2.1 Ambiguity in responsibility	Y
	Clause 8.2.2 Shared environment	Y
	Clause 8.2.3 Inconsistency and conflict of protection mechanisms	Y
	Clause 8.2.4 Jurisdictional conflict	Y
	Clause 8.2.5 Evolutionary risks	
	Clause 8.2.6 Bad migration and integration	Y
	Clause 8.2.7 Business discontinuity	Y
	Clause 8.2.8 Cloud service partner lock-in	
	Clause 8.2.9 Supply chain vulnerability	Y
	Clause 8.2.10 Software dependencies	
Clause 8.3 Security challenges for cloud service partners (CSNs)	Clause 8.3.1 Ambiguity in responsibility	
	Clause 8.3.2 Misappropriation of intellectual property	
	Clause 8.3.3 Loss of software integrity	

Once the security threats and challenges have been identified, the security capabilities that could mitigate these threats and address these challenges can be identified. In Table I.1 there is an example of a mapping of cloud computing security threats and challenges to security capabilities. The letter 'Y' in a cell formed by the intersection of the table's columns and rows designate that a particular security threat and challenge is addressed by a corresponding security capability. This table shows all the threats and challenges and the corresponding security capability.

Once the capabilities required have been identified, the security controls, policies and procedures can be determined as to what is needed. Examples of controls that could be used are "Operations security" (clause 12 in [b-ISO/IEC 27002]) and "Information security incident management" (clause 16 in [b-ISO/IEC 27002]) which can be derived from the identified capabilities in clauses 9.9 and 9.10, respectively.

A cloud service may have a supply chain comprised of multiple CSPs. The companies participating in such a supply chain can refer to ITU and Industry standards on the topic of supply chain security (e.g., [b-ISO/IEC 28000]). Each CSP will need to clearly delineate their responsibility in the cloud computing service chain, and develop their security controls, policies and procedures based on the derived security capabilities by this three-step approach. To provide consistent security to CSCs, the upstream CSP may need to negotiate with their downstream CSPs on these security capabilities based on their security responsibilities. When needed, CSCs should follow this three-step procedure as well.

In addition, the above three-step procedure should be carried out periodically or when needed (e.g., when a serious security breach occurs, or when a CSP changes its upstream CSP).

Appendix I

Mapping of cloud computing security threats and challenges to security capabilities

(This appendix does not form an integral part of this Recommendation.)

Table I.1 shows a mapping of cloud computing security threats and challenges to some of the possible security capabilities.

The letter 'Y' in a cell formed by the intersection of the table's columns and rows designate that a particular security threat and challenge is addressed by a corresponding security capability.

Table I.1 – Mapping of cloud computing security threats and challenges to security capabilities

			Clause 9 Cloud computing security capabilities													
			Clause9.1 Trust model	**Clause 9.2 Identity and access management (IAM), authentication, authorization and transaction audit**	**Clause 9.3 Physical security**	**Clause 9.4 Interface security**	**Clause 9.5 Computing virtualization security**	**Clause 9.6 Network security**	**Clause 9.7 Data isolation, protection and privacy protection**	**Clause 9.8 Security coordination**	**Clause 9.9 Operational security**	**Clause 9.10 Incident management**	**Clause 9.11 Disaster recovery**	**Clause 9.12 Service security assessment and audit**	**Clause 9.13 Interoperability, portability and reversibility**	**Clause 9.14 Supply chain security**
Clause 7 Security threats for cloud compu-ting	Clause 7.1 Security threats for cloud service customers (CSCs)	Clause 7.1.1 Data loss and leakage	Y	Y	Y				Y				Y			
		Clause 7.1.2 Insecure service access	Y	Y		Y	Y	Y								
		Clause 7.1.3 Insider threats		Y	Y									Y		
	Clause 7.2 Security threats for cloud service providers (CSPs)	Clause 7.2.1 Unautho-rized administra-tion access	Y	Y	Y	Y										
		Clause 7.2.2 Insider threats		Y	Y									Y		

Table I.1 – Mapping of cloud computing security threats and challenges to security capabilities

			Clause 9 Cloud computing security capabilities													
			Clause9.1 Trust model	**Clause 9.2 Identity and access management (IAM), authentication, authorization and transaction audit**	**Clause 9.3 Physical security**	**Clause 9.4 Interface security**	**Clause 9.5 Computing virtualization security**	**Clause 9.6 Network security**	**Clause 9.7 Data isolation, protection and privacy protection**	**Clause 9.8 Security coordination**	**Clause 9.9 Operational security**	**Clause 9.10 Incident management**	**Clause 9.11 Disaster recovery**	**Clause 9.12 Service security assessment and audit**	**Clause 9.13 Interoperability, portability and reversibility**	**Clause 9.14 Supply chain security**
Clause 8 Security challenges for cloud compu-ting	Clause 8.1 Security challenges for cloud service customers (CSCs)	Clause 8.1.1 Ambiguity in responsi-bility		Y							Y					
		Clause 8.1.2 Loss of trust	Y											Y		
		Clause 8.1.3 Loss of governance		Y	Y				Y		Y	Y	Y	Y		
		Clause 8.1.4 Loss of privacy		Y					Y					Y		
		Clause 8.1.5 Service unavailab-ility								Y	Y	Y	Y			Y
		Clause 8.1.6 Cloud service provider lock-in													Y	
		Clause 8.1.7 Misappropri ation of intellectual property		Y	Y				Y		Y					
		Clause 8.1.8 Loss of software integrity		Y			Y		Y							

Table I.1 – Mapping of cloud computing security threats and challenges to security capabilities

			Clause 9 Cloud computing security capabilities													
			Clause9.1 Trust model	**Clause 9.2 Identity and access management (IAM), authentication, authorization and transaction audit**	**Clause 9.3 Physical security**	**Clause 9.4 Interface security**	**Clause 9.5 Computing virtualization security**	**Clause 9.6 Network security**	**Clause 9.7 Data isolation, protection and privacy protection**	**Clause 9.8 Security coordination**	**Clause 9.9 Operational security**	**Clause 9.10 Incident management**	**Clause 9.11 Disaster recovery**	**Clause 9.12 Service security assessment and audit**	**Clause 9.13 Interoperability, portability and reversibility**	**Clause 9.14 Supply chain security**
Clause 8 Security challenges for cloud compu-ting	Clause 8.2 Security challenges for cloud service providers (CSPs)	Clause 8.2.1 Ambiguity in responsi-bility		Y							Y					
		Clause 8.2.2 Shared environment					Y	Y	Y							
		Clause 8.2.3 Inconsis-tency and conflict of protection mechanisms								Y					Y	
		Clause 8.2.4 Jurisdic-tional conflict							Y		Y					
		Clause 8.2.5 Evolution-ary risks									Y				Y	Y
		Clause 8.2.6 Bad migration and integration				Y	Y	Y	Y	Y	Y					
		Clause 8.2.7 Business discon-tinuity										Y	Y			
		Clause 8.2.8 Cloud service partner lock-in														Y

Table I.1 – Mapping of cloud computing security threats and challenges to security capabilities

			Clause 9 Cloud computing security capabilities													
			Clause9.1 Trust model	**Clause 9.2 Identity and access management (IAM), authentication, authorization and transaction audit**	**Clause 9.3 Physical security**	**Clause 9.4 Interface security**	**Clause 9.5 Computing virtualization security**	**Clause 9.6 Network security**	**Clause 9.7 Data isolation, protection and privacy protection**	**Clause 9.8 Security coordination**	**Clause 9.9 Operational security**	**Clause 9.10 Incident management**	**Clause 9.11 Disaster recovery**	**Clause 9.12 Service security assessment and audit**	**Clause 9.13 Interoperability, portability and reversibility**	**Clause 9.14 Supply chain security**
Clause 8 Security challenges for cloud compu-ting	Clause 8.2 Security challenges for cloud service providers (CSPs)	Clause 8.2.9 Supply chain vulnera-bility														Y
		Clause 8.2.10 Software depen-dencies														Y
	Clause 8.3 Security challenges for cloud service partners (CSNs)	Clause 8.3.1 Ambiguity in responsi-bility		Y							Y					
		Clause 8.3.2 Misappro-priation of intellectual property		Y	Y				Y		Y					
		Clause 8.3.3 Loss of software integrity		Y			Y		Y							

Bibliography

[b-ITU-T E.409] Recommendation ITU-T E.409 (2004), *Incident organization and security incident handling: Guidelines for telecommunication organizations*.

[b-ITU-T X.810] Recommendation ITU-T X.810 (1995) | ISO/IEC 10181-1:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview*.

[b-ISO/IEC 19440] ISO/IEC 19440:2007, *Enterprise integration – Constructs for enterprise modelling*.

[b-ISO/IEC 20000-1] ISO/IEC 20000-1:2011, *Information technology – Service management – Part 1: Service management system requirements*.

[b-ISO/IEC 27000] ISO/IEC 27000:2012, *Information technology –Security techniques – Information security management systems – Overview and vocabulary*.

[b-ISO/IEC 27002] ISO/IEC 27002:2005, *Information technology – Security techniques – Code of practice for information security management*.

[b-ISO/IEC 27005] ISO/IEC 27005:2011, *Information technology – Security techniques – Information security risk management*.

[b-ISO/IEC 28000] ISO/IEC 28000:2007, *Specification for security management systems for the supply chain*.

[b-ISO/IEC 29100] ISO/IEC 29100:2011, *Information technology – Security techniques – Privacy framework.*

[b-NIST-SP-800-30] NIST Special Publication 800-30 (2012), *Guide for Conducting Risk Assessments*.

[b-NIST-SP-800-53] NIST Special Publication 800-53 Rev.3 (2009), *Recommended Security Controls for Federal Information Systems and Organizations*.

[b-NIST-SP-800-125] NIST Special Publication 800-125 (2011), *Guide to Security for Full Virtualization Technologies*.

[b-NIST-SP-800-145] NIST Special Publication 800-145 (2011), *The NIST Definition of Cloud Computing*.

[b-CSA Matrix] CSA (2013), *Cloud Controls Matrix,* Cloud Security Alliance.

[b-key definition] Key definitions of the Data Protection Act, Information Commissioners Office <http://www.ico.gov.uk/for_organisations/data_protection/the_guide/key_definitions.aspx>

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2014