|  |  |
| --- | --- |
| **Telecommunication Standardization Bureau** |  |
|  |  |

Geneva, 6 March 2012

|  |  |
| --- | --- |
| Ref: | **TSB Circular 266** COM 17/MEU |
|  |  |
| Tel: | +41 22 730 5866 |
| Fax: | +41 22 730 5853 |
| E-mail: | [tsbsg17@itu.int](mailto:tsbsg17@itu.int) |
|  |  |

|  |
| --- |
| - To Administrations of Member States  of the Union  **Copy:**  - To ITU-T Sector Members;  - To ITU-T Associates;  - To ITU-T Academia;  To the Chairman and Vice-Chairmen  of Study Group 17;  - To the Director of the Telecommunication Development Bureau;  - To the Director of the Radiocommunication Bureau |

|  |  |
| --- | --- |
| Subject: | **Approval of revised Question 8/17** |

Dear Sir/Madam,

1 At the request of the Chairman of Study Group 17, *Security*, I have the honour to inform you that, in accordance with the procedure described in Resolution 1, Section 7, § 7.2.2, of WTSA (Johannesburg, 2008), Member States and Sector Members present at the last meeting of this Study Group which was held in Geneva from 20 February to 2 March 2012, agreed by reaching consensus to approve the following revised Question:

*Question 8/17* *Cloud computing security* (see Annex 1)

2 **Question 8/17 is therefore approved.**

3 The resulting Recommendations are assumed to fall under the traditional approval process (TAP).

Yours faithfully,

Malcolm Johnson  
Director of the Telecommunication  
Standardization Bureau

**Annex: 1**

## ANNEX 1 (to TSB Circular 266)

## Question 8/17 – Cloud computing security

(Revised Question)

### Motivation

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. The cloud computing model is defined by five essential characteristics (on-demand, delivery over a broad network access, resource pooling, rapid elasticity, self and measured services), five cloud computing service categories, i.e., Software as a Service (SaaS), Communication as a Service (CaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Network as a Service (NaaS), and different deployment models (public, private, hybrid…). The advent of the cloud computing approach as the preferred vehicle for discovering, externalizing, composing, service re-use within workflows, applications, communication enabled applications places new emphasis on the need for security.

Forecasted benefits of cloud computing include flexible and dynamic resource provisioning, and simpler and automated administration of IT infrastructure. Virtualization makes possible to share of nearly unlimited resources, with scalability improvements and massive cost reductions for infrastructure management. However, open systems and shared resources of cloud computing raise many concerns about security, which is perhaps the most important barrier to the adoption of cloud computing. Moving to the cloud implies to shifting from safe, traditional, in-house IT systems to unsafe, “cloudified”, open infrastructures. It thus requires in-depth rethinking of security.

Cloud computing was considered for several years as service-centric IT and controlled by Internet players. However, telecommunication players have an important role to play in the emerging cloud computing market and ecosystem. As cloud services are delivered through telecommunication networks, telecommunication players should guarantee a high assurance level. Strong but flexible security protection will be a key enabler for the whole cloud market and eco-system.

In addition, the flexible use of rich resources in cloud computing environments will enable new security services that the current premise defences cannot provide (e.g. anti-malware services as a cloud service). Thus, there is need to examine what kind of security measures cloud computing can offer in the near future.

Draft Recommendations ITU-T X.ccsec, X.srfcts and X.sfcse provide a set of Recommendations on security service for cloud security overview, architecture and framework, cross-layers cloud security and specific security of network services. Currently there is a strong need for securing cloud computing enabled critical voice, multi-media, identity based services, information assurance services, identity and data services, and emergency based services. This Question is intended to develop new Recommendations based on the Focus Group Cloud Technical Report Part 5 for:

1. best practices and guidelines development to guide on how to provide security in a cloud computing based environment;
2. responsibility clarification, and security requirements and threats definition for the main actors and related roles in the cloud computing ecosystem;
3. security architecture based on the reference architecture provided by Q.27/13;
4. security management and audit technologies for the trust management.

Q8/17 will collaborate with related Questions such as Q2/17, Q3/17, Q4/17, Q7/17, Q10/17 and Q11/17 to develop Recommendations on cloud computing security.

Recommendations and Supplements under responsibility of this Question as of 2 March 2012: ITU-T X.ccsec, X.sfcse, X.fssvpn.

### Question

Study items to be considered include, but are not limited to:

1. What new Recommendations or other type of documents should be developed for main actors like service providers, service users and services partners, and other key industry stakeholders to advance cloud computing security?
2. What new Recommendations should be developed for security architecture and security functionalities organization in line with the reference architecture?
3. What new Recommendations should be developed for security management, assurance mechanisms, audit technologies, and associated risks assessment to establish trust among different actors?
4. Under the auspices of the Joint Coordination Activity on cloud computing (JCA-cloud), what collaboration is necessary to minimize duplication of efforts with other Questions, study groups, and SDOs?
5. How security as a service should be developed to protect ICT systems?

### Tasks

Tasks include, but are not limited to:

1. Developing Recommendations or other type of documents to advance cloud computing security.
2. Developing Recommendations to identify security requirements and threats to secure cloud computing services based on the general requirements of cloud computing specified by ITU-T Study Group 13.
3. Developing Recommendations to define security architecture and to organize security functions based on the reference architecture specified by ITU-T Study Group 13.
4. Developing Recommendations to define a strong, flexible and elastic security management architecture and implementation for cloud computing systems.
5. Developing Recommendations to identify assurance mechanisms, audit technologies, risk assessment with the objective of achieving trustworthy relationships within the cloud computing ecosystem.
6. Taking charge of all the activities on cloud computing security in Study Group 17.
7. Representing the work of Study Group 17 related to cloud computing security in the Joint Coordination Activity on cloud computing (JCA-Cloud).

### Relationships

Recommendations:

• Y-series Recommendations on cloud computing

Questions:

• ITU-T Qs 1/17, 2/17, 3/17, 4/17, 7/17, 10/17 and 11/17

Study Groups:

• ITU-T SGs 2, 13, 16.

Standardization bodies:

• ISO/IEC JTC 1/SCs 27 and SC 38; OASIS; IETF and other relevant bodies as identified

Other bodies:

• DMTF; CSA (Cloud Security Alliance).

**\_\_\_\_\_\_\_\_\_\_**