12th of June, 2015

International Standardization for Cloud Security Control, ISO/IEC27017

Code of practice for information security controls based on ISO/IEC 27002 for cloud services

Chair of ISO/IEC JTC1/SC27/WG1 Japan

Project editor of ISO/IEC 27017

Chair of Cloud Security Control Committee

Satoru Yamasaki

Table of contents

Cloud Security Control Standard

Title

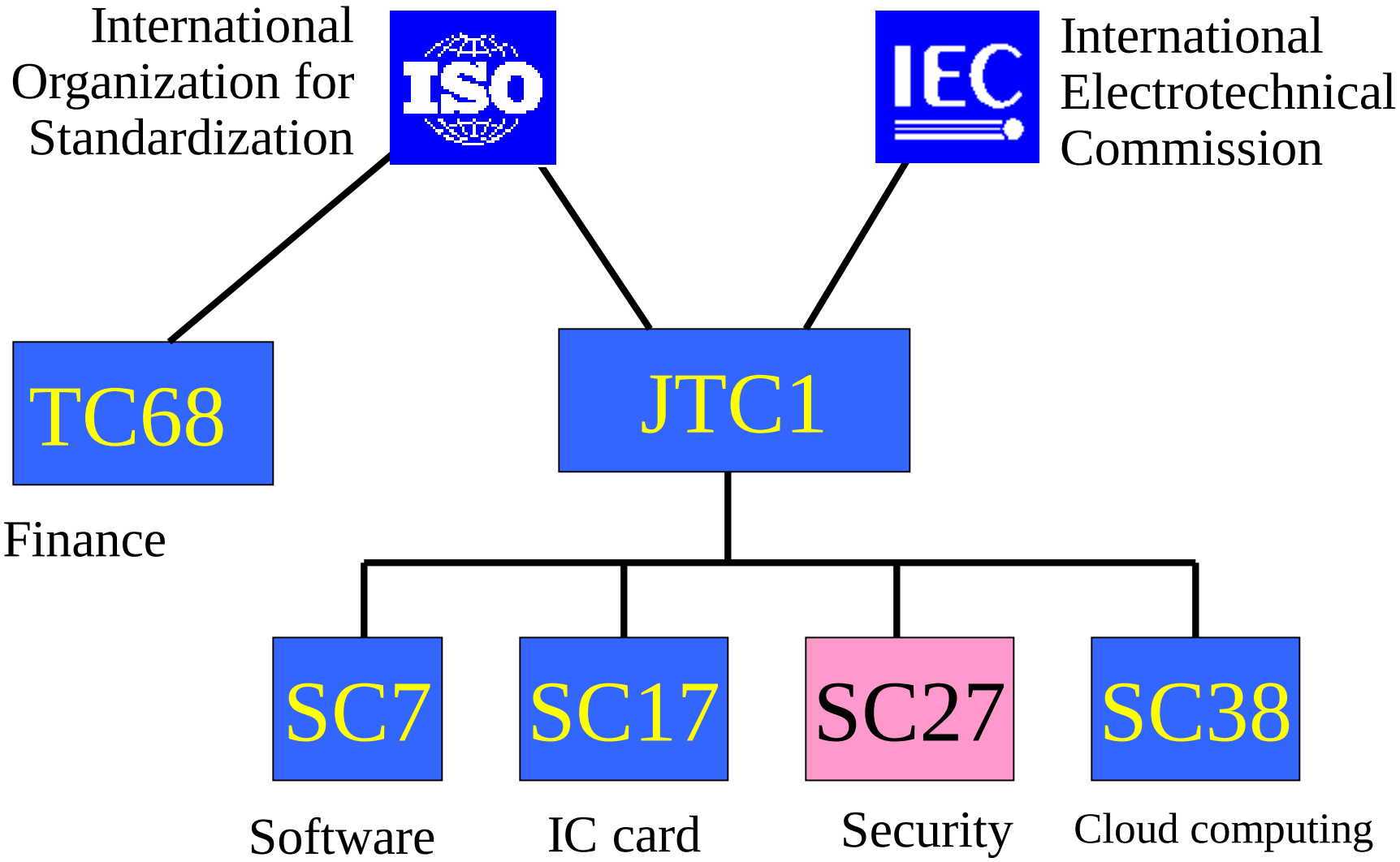
ISO/IEC 27002 === General security controls

Code of practice for information security controls

ISO/IEC 27017 === Cloud security controls

Code of practice for information security controls
based on ISO/IEC 27002 for cloud services

International Organization for Standardization



WG formation in SC27

WG1:ISO/IEC 27000 ISMS family of standards

WG2: Security technology, mechanism

WG3: Security evaluation criteria

WG4:

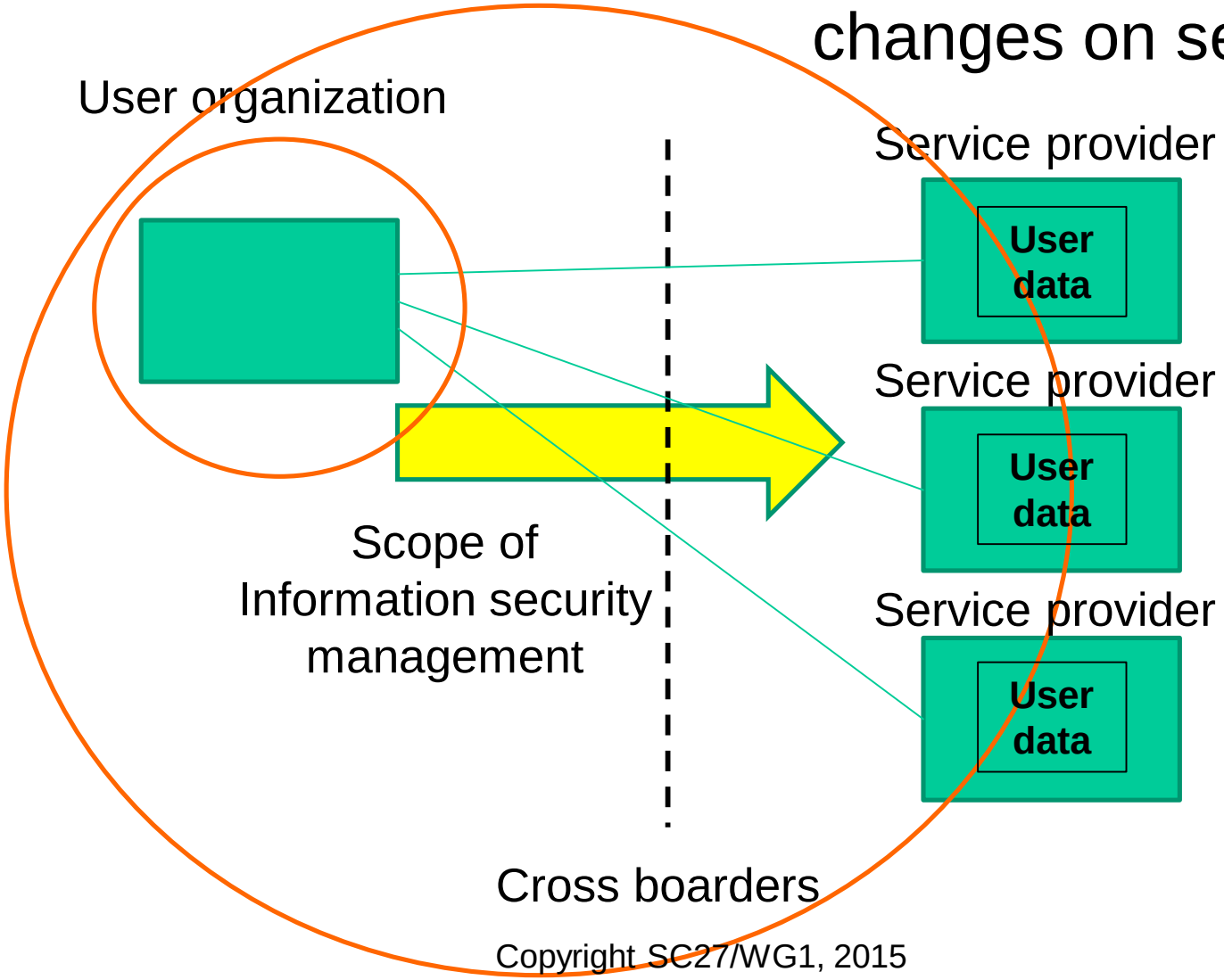
- Network security
- Application security
- BCP services, others

WG5:

- Privacy
- Identity management
- Biometrics

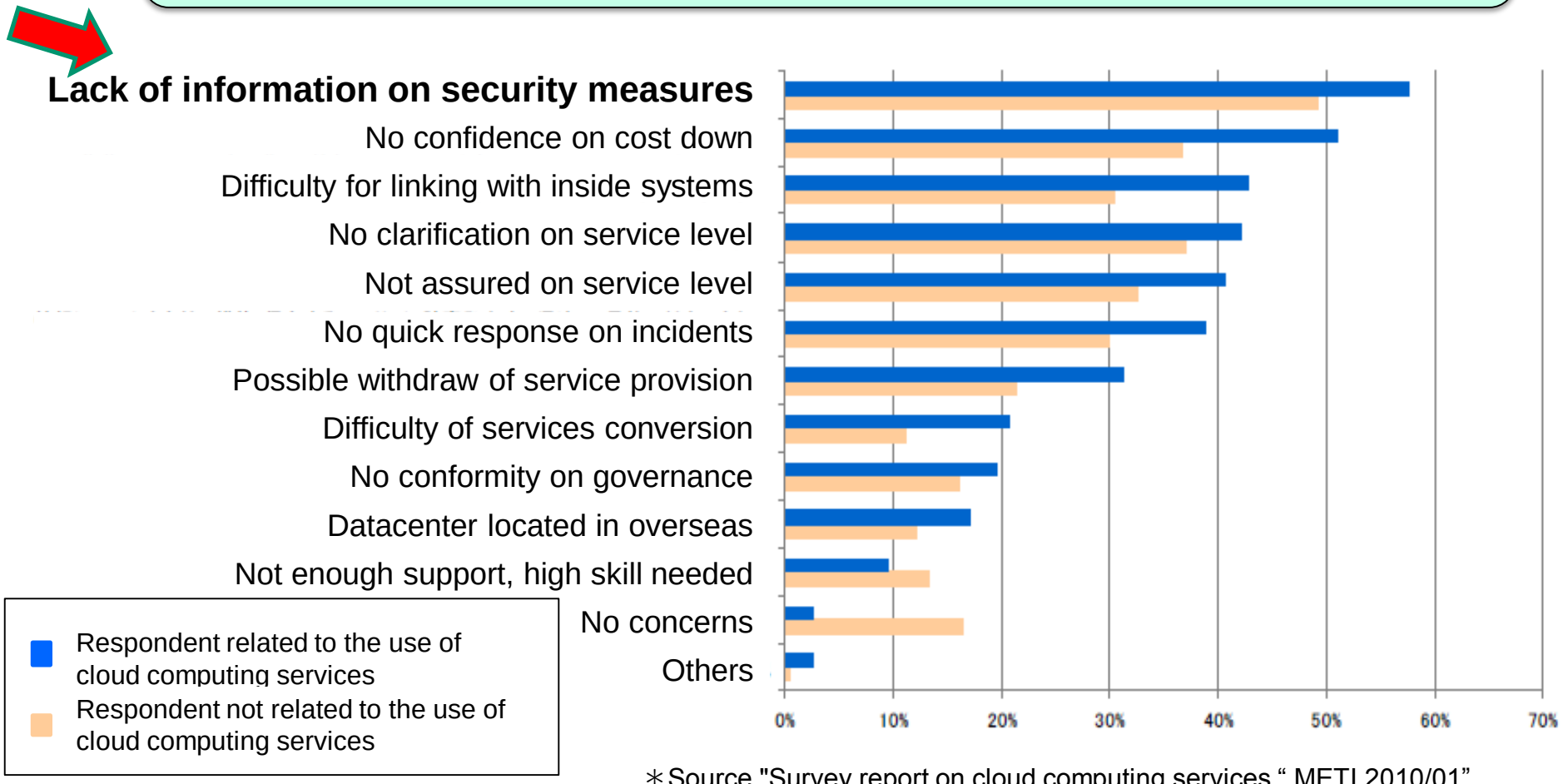
1. Background

Cloud computing services affect environmental changes on security



(1)lack of information on security

■The biggest concern on cloud services is “lack of information on security measures of service providers”.

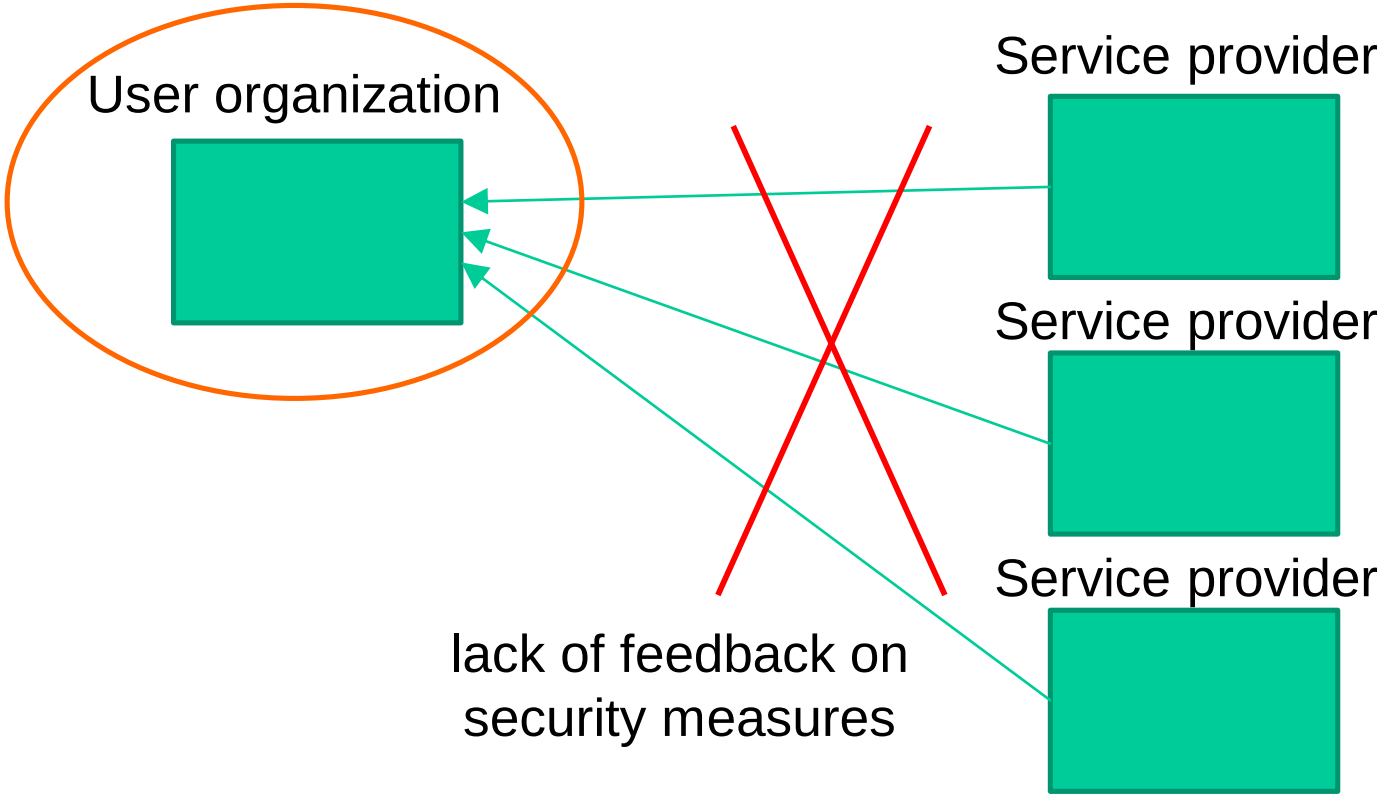


＊Source "Survey report on cloud computing services “ METI 2010/01”

Respondent number=500

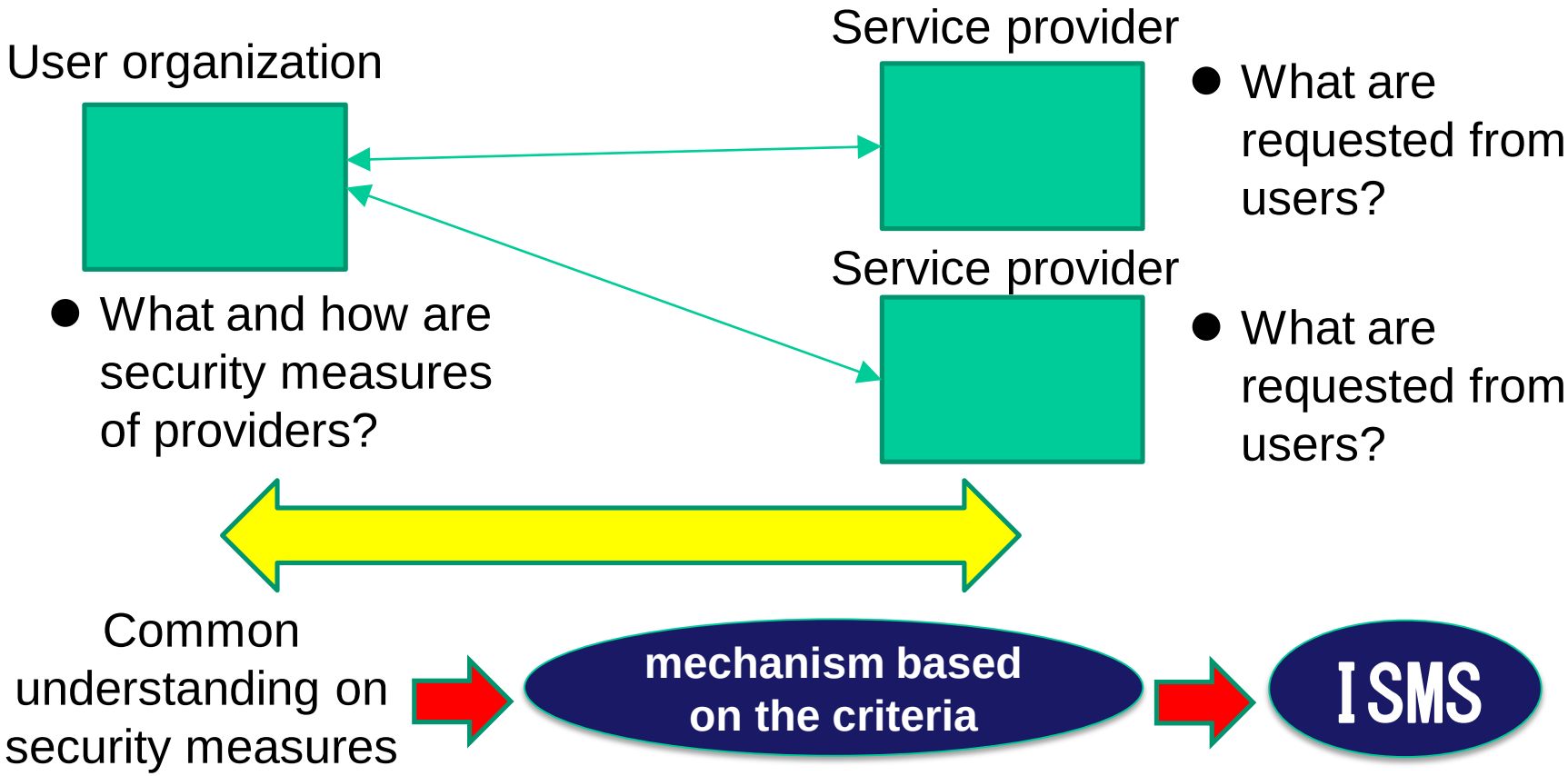
(2)lack of feedback to users

- Especially, there is a lack of feedback to user organization on security measures from service providers.



2. Approach - ISMS certification -

To establish a mechanism for common understanding between user and service providers based on the criteria



2. Approach - ISMS certification -

ISMS Certification

ISO/IEC 27001

- Requirements (Main Body)
- Annex A (based on 27002)

Sector specific controls

27017 Cloud Security Controls

Other sector specific controls (27011 etc.)

- ***27017 Cloud Security Control set is referred with 27001 Annex A to determine the required security controls for ISMS risk assessment and ISMS audit.***
- ***27017 can be applied combining the other sector specific security controls such as 27011 (telecommunication controls).***

2. Approach - ISMS certification -
- ISO/IEC27001とISO/IEC27009, 27006の関係 -

ISMS Requirements

ISO/IEC 27001 (extended by 27009)
- Determine required controls
- Compare with 27001 Annex A and (***sector-specific control sets***)
- Produce SoA

Requirements to CB

ISO/IEC 27006
- Certification documents (+SoA Version, ***Sector-specific control ID***)

Sector specific control set

27017 Cloud Security Controls

Sector specific control set

27011 Telecom Org. Controls

27002 Information security Controls

Requirements to Sector specific standards

ISO/IEC 27009
- Rule for ***Sector-specific standards***
  - Requirements
  - Control sets

3. Organizations and their roles

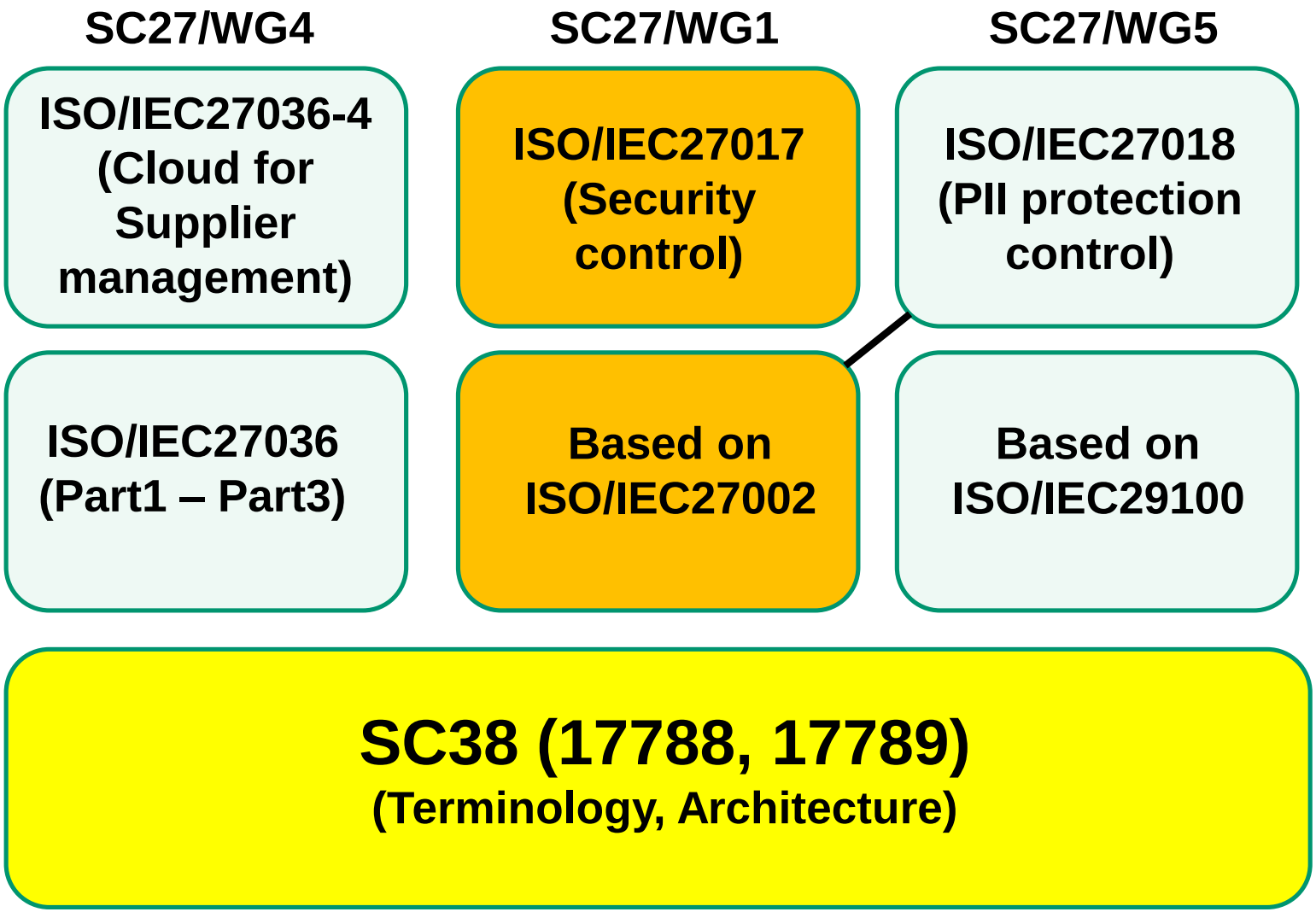
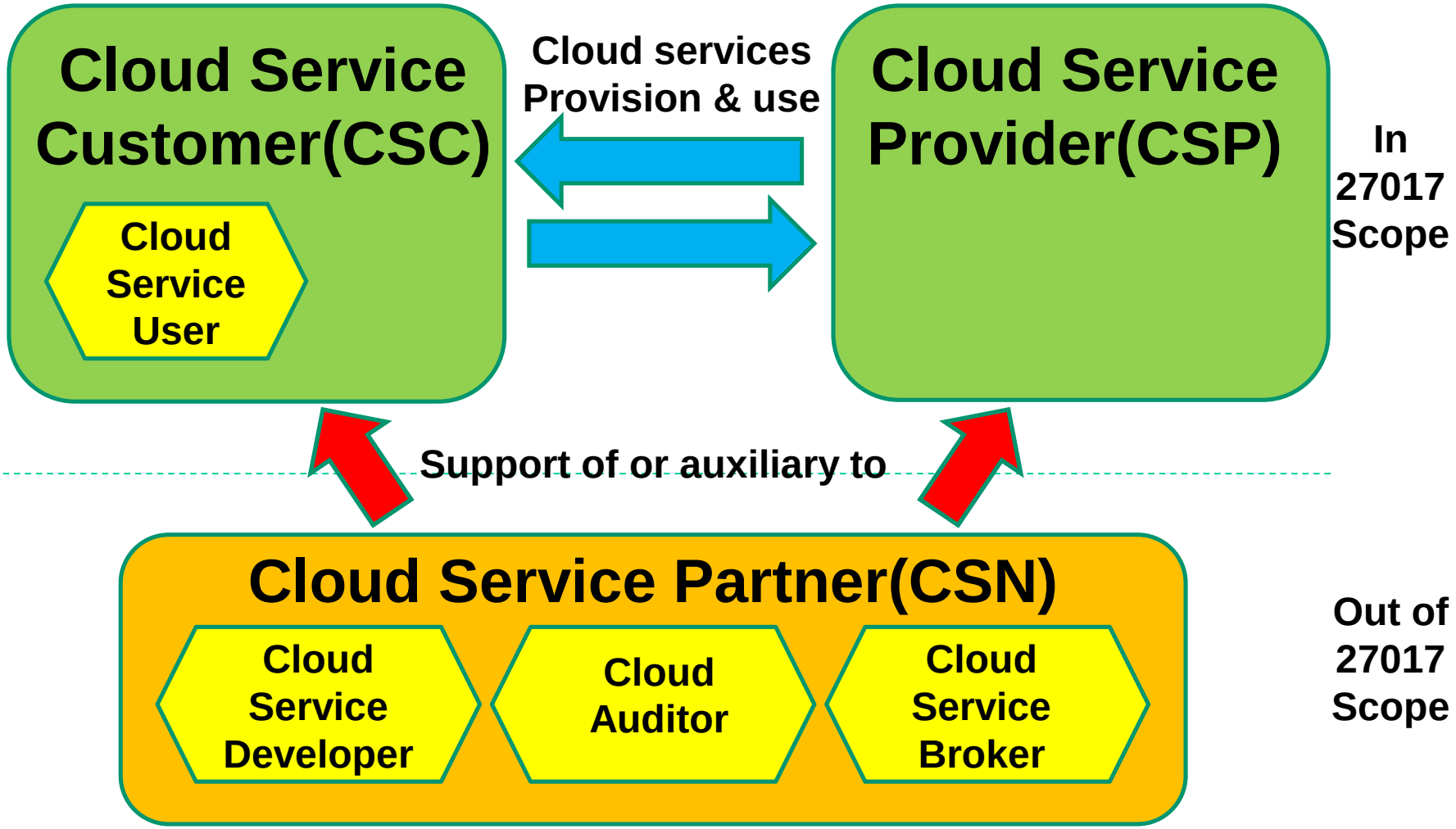


Table of contents

1. Scope of ISO/IEC27017

- ISO/IEC17789:Reference architecture -



2. Structure - Clauses (27002/27017) -

Clauses of 27002 and 27017 are the same.
5 Information security polices
6 Organization of information security
7 Human resource security
8 Asset management
9 Access control
10 Cryptography
11 Physical and environmental security
12 Operations security (Example 12.3.1)
13 Communications security
14 System acquisition, development and maintenance
15 Supplier relationships
16 Information security incident management
17 Information security aspects of business continuity management
18 Compliance
Annex A (27017) Cloud Service Extended Control Set

2. Structure - 27017 specific to cloud services -

ISO/IEC27017

Code of practice for information security controls
based on ISO/IEC 27002 for cloud services

ISO/IEC27002 （Main body）

- Objective
- Control
- Implementation guidance
- Other information

ISO/IEC27017 （Main body）

- Objective
- Control
- + specific Imple-mentation guidance
- + Other information

Under per Control
（**Implementation guidance and other information**）

ISO/IEC27017 （Annex A）

- New Objective
- New Control
- + specific Imple-mentation guidance
- + Other information

Under
（**Objectives、Controls, imple.guida, other**）

2. Structure - 27017 Format -

ISO/IEC 27017 describes Control, Implementation guidance and Other information.

a. Control format

- Each subclause

  Control X.X.X and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific implementation guidance also applies.

- Subclause header

  Implementation guidance for cloud services

  Other information for cloud services.

b. Implementation guidance format (Table format)

- **Type1**

Cloud service customer	Cloud service provider
Implementation guidance	Implementation guidance

- **Type2**

Cloud service customer	Cloud service provider
Implementation guidance	

c. Annex A uses the unique ID as the controlnumber

- 27009 defines as rules, ‘A unique identifies shall be used, and 27011 as example’.
- 27011 uses ‘TEL.’, and therefore ‘CLD. X.X.X’ is used

3. Terms and definitions

- Normative references -

- **2. Normative References**

  The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.。

  - ***ISO/IEC 27000***, Information technology - Security techniques - Information security management systems - Overview and vocabulary
  - ***Y.3500* | *ISO/IEC 17788***, Information technology - Cloud computing - Overview and vocabulary
  - ***Y.3502* | *ISO/IEC 17789,*** Information technology - Cloud computing - Reference architecture
  - ***ISO/IEC 27002:2013***, Information technology - Security techniques - Code of practice for information security controls

3. Terms and definitions

- ISO/IEC 17788 specific to cloud computing -

- Terms and definitions specific to cloud computing (ISO/IEC17788)

  - **Cloud Computing**

    3.2.5 cloud computing:

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

    NOTE – Examples of resources include servers, operating systems, networks, software, applications, and storage equipment

    .

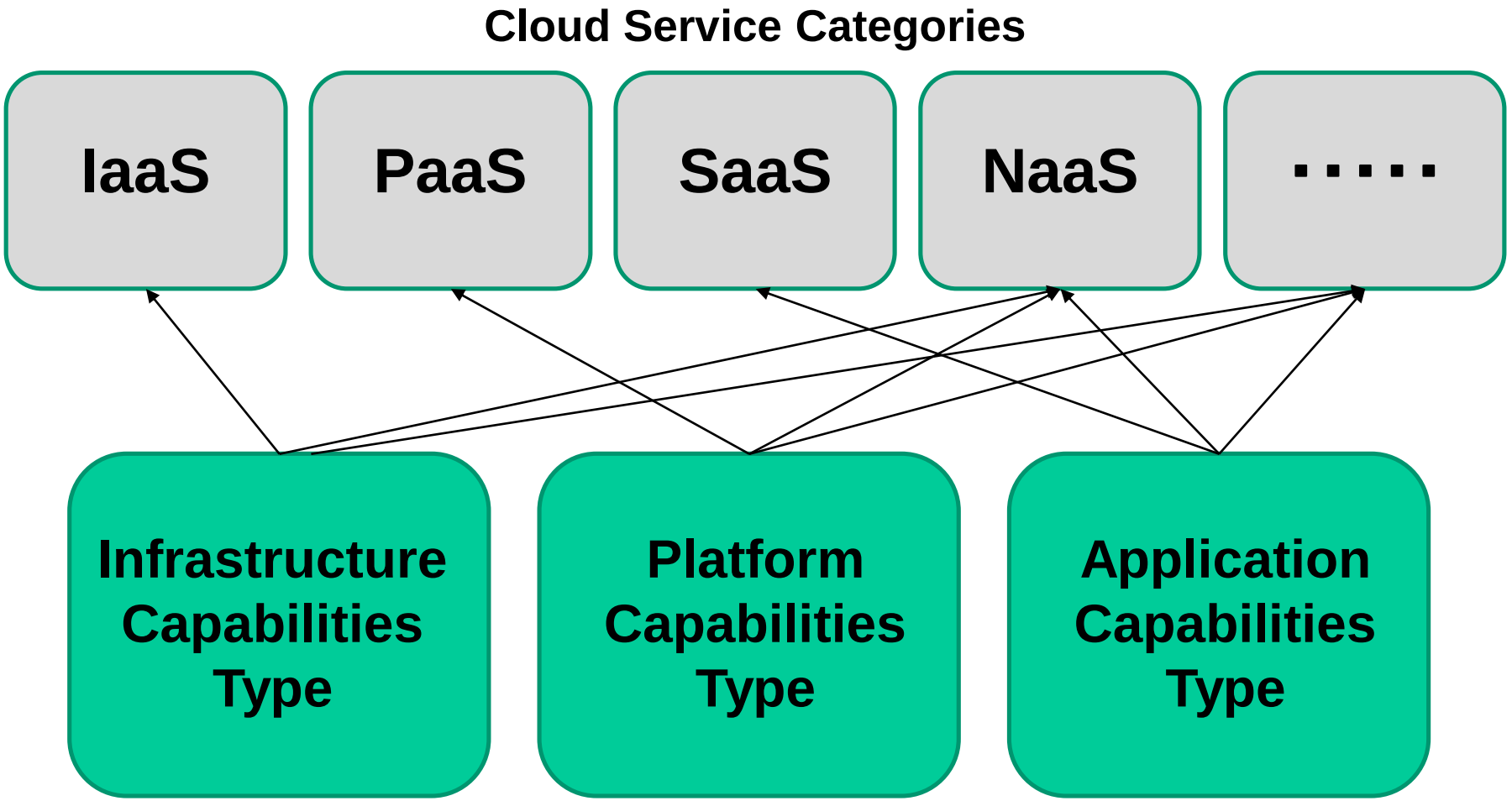
  - **Cloud Service**

    3.2.8 cloud service:

    one or more capabilities offered via cloud computing (3.2.5) invoked using a defined interface

3. Terms and definitions

- ISO/IEC 17788 specific to cloud computing -



3. Terms and definitions

- ISO/IEC 17788 specific to cloud computing -

- Terms and definitions specific to cloud computing (ISO/IEC17788)
  - **Cloud Capabilities Type**

    3.2.4 cloud capabilities type:

    classification of the functionality provided by a cloud service (3.2.8) to the cloud service customer (3.2.11), based on resources used

    NOTE – The cloud capabilities types are application capabilities type (3.2.1), infrastructure capabilities type (3.2.25) and platform capabilities type (3.2.31).

  - **Cloud Service Category**

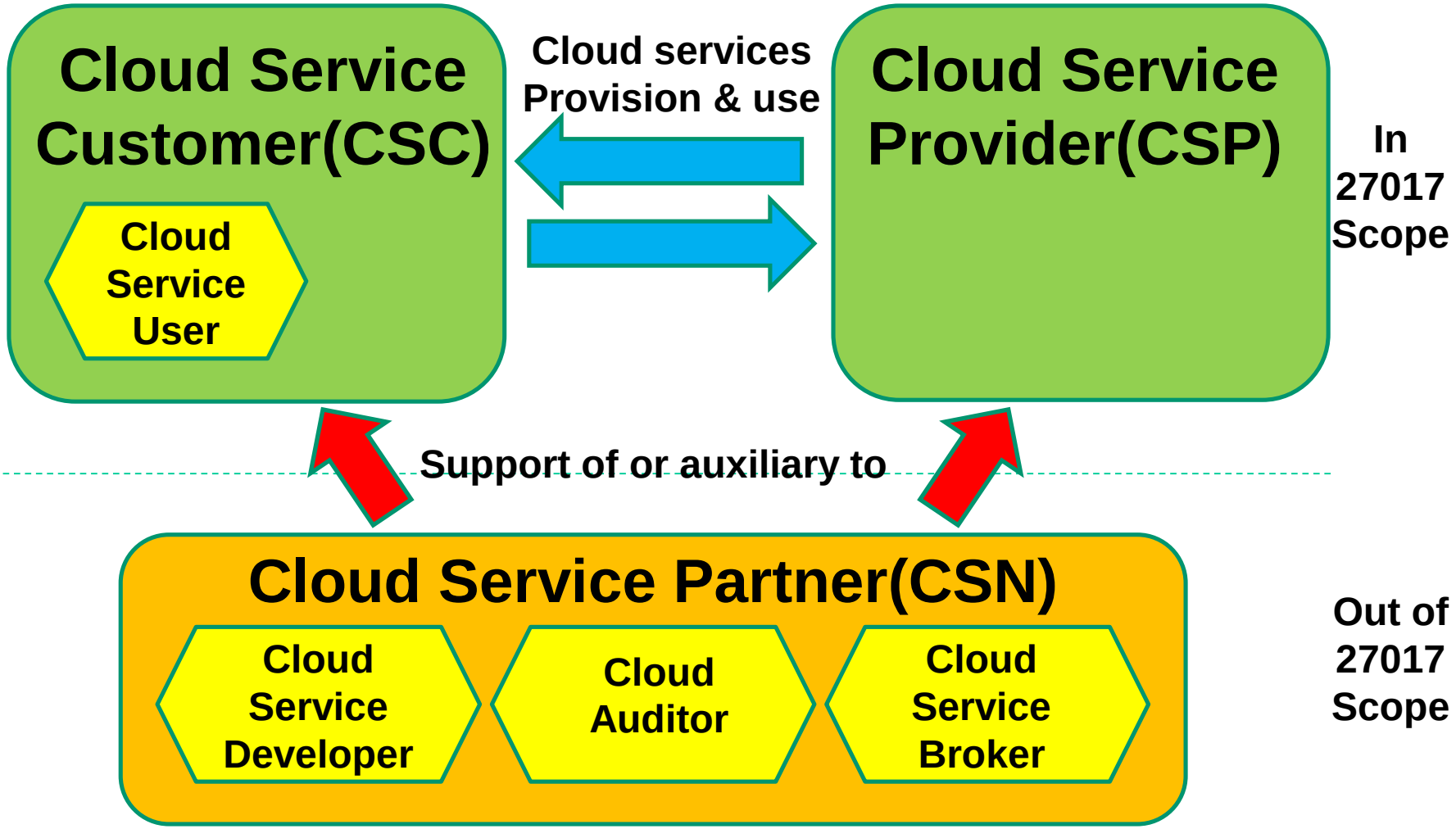
    3.2.10 cloud service category:

    group of cloud services (3.2.8) that possess some common set of qualities

    NOTE – A cloud service category can include capabilities from one or more cloud capabilities types (3.2.4).

3. Terms and definitions

- ISO/IEC 17788 specific to cloud computing -



3. Terms and definitions

- ISO/IEC 17788 specific to cloud computing -

- Terms and definitions specific to cloud computing (ISO/IEC17788)
  - **Cloud Service Customer**

    3.2.11 cloud service customer:

    party (3.1.6) which is in a business relationship for the purpose of using cloud services (3.2.8)
  - **Cloud Service Provider**

    3.2.15 cloud service provider:

    party (3.1.6) which makes cloud services (3.2.8) available
  - **Cloud Service Partner**

    3.2.14 cloud service partner:

    party (3.1.6) which is engaged in support of, or auxiliary to, activities of either the cloud service provider (3.2.15) or the cloud service customer (3.2.11)

    Note. ISO/IEC 27017 does not apply this term.
  - **Cloud Service User**

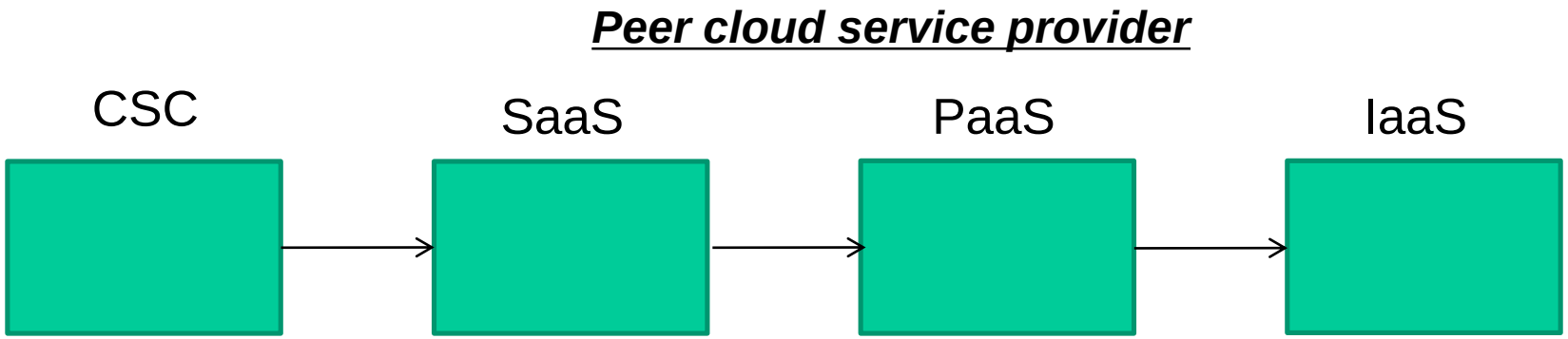
    3.2.17 cloud service user:

    natural person, or entity acting on their behalf, associated with a cloud service customer (3.2.11) that uses cloud services (3.2.8)

3. Terms and definitions

- ISO/IEC 17789 Reference Architecture -

- Terms and definitions specific to cloud computing (ISO/IEC17789)
  - **peer cloud service provider**
    - cloud service provider who provides one or more cloud services for use by one or more other cloud service providers as part of their cloud services



4. Example - ISO/IEC27002（12.3.1）-

- **Example of Implementation guidance for CSC and CSP**
  - **27002: 12.3.1 Information backup**
    - **Control**

      Backup copies of information, software and system images should be taken and tested regularly in accordance with an agreed backup policy.

      ➔ This is not described in 27017, however this is applied as Control.

    - **Implementation guidance**

      A backup policy should be established to define the organization's requirements for backup of information, software and systems.

      The backup policy should define the retention and protection requirements.

      Adequate backup facilities should be provided to ensure that all essential information and software can be recovered following a disaster or media failure.

      When ***designing a backup plan***, the following items should be taken into consideration:

      a) accurate and complete records of the backup copies and documented restoration procedures should be produced; …….

      ➔ This is not described in 27017, however this is applied as implementation guidance.

4. Example - ISO/IEC27017（12.3.1 CSC）-

- **Example of Implementation guidance for CSC**
  - **27017: 12.3.1 Information backup**

Control 12.3.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

cloud service customer
Where the cloud service provider provides backup capability as part of the cloud service, the cloud service customer should request the specifications of the backup capability from the cloud service provider. The cloud service should also verify that they meet their backup requirements. The cloud service customer is responsible for implementing backup capabilities when the cloud service provider provides none.

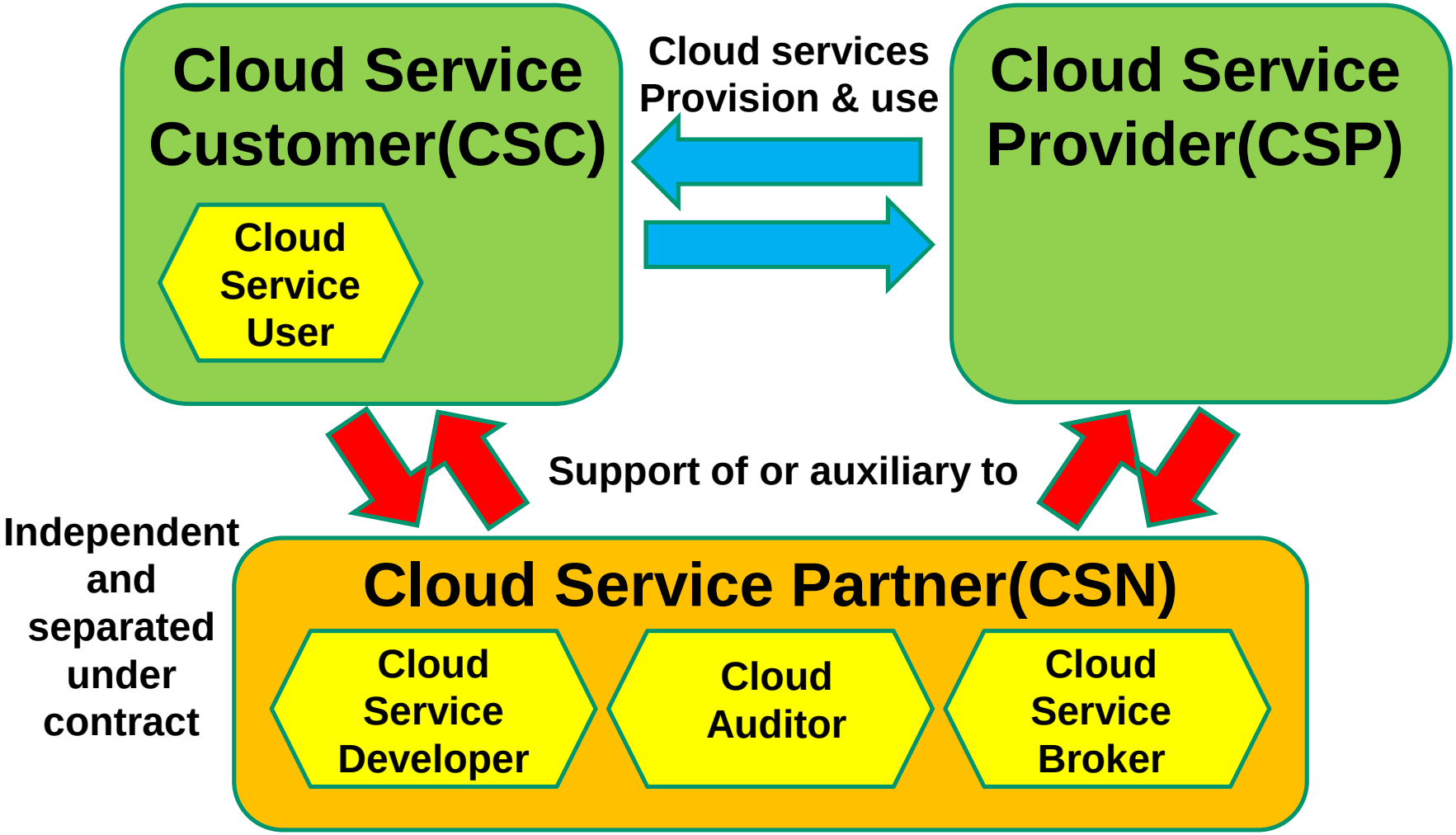
4. Example - ISO/IEC27017（12.3.1 CSP）-

- **Example of Implementation guidance for CSP**
  - **27017: 12.3.1 Information backup**

cloud service provider
The cloud service provider should provide the specifications of its backup capabilities to the cloud service customer. The specifications should include the following information, as appropriate: - scope and schedule of backups; - backup methods and data formats, including encryption, if relevant; - retention periods for backup data; - procedures for verifying integrity of backup data; - procedures and timescales involved in restoring data from backup; - procedures to test the backup capabilities; - storage location of backups. The cloud service provider should provide secure and segregated access to backups, such as virtual snapshots, if such service is offered to cloud service customers.

Table of contents

Background for New Study for Future Projects CSN roles and sub-roles independent and separated from CSC or CSP organization.



1. New Study for Future Projects
(1) Title

A new Study for Future Projects was proposed with the following title

- 12-month JTC 1/SC 27/WG 1Study Period
- Objectives
  1. To analyse and create Use Cases on information security for cloud services
  2. To analyse and identify potential gaps between Use Cases and relevant International Standards to Cloud Security (e.g. ISO/IEC 27017, ISO/IEC 27036, ISO/IEC 17788, ISO/IEC 17789)
  3. To propose standards to achieve potential gaps identified by the above study

Thanks for your listening

Chair of ISO/IEC JTC1/SC27/WG1 Japan
Project editor of ISO/IEC 27017
Chair of Cloud Security Control Committee

Satoru Yamasaki