

December 2, 2011

Dr. Robert Bohn

National Institute of Standards and Technology,

Department of Commerce

100 Bureau Dr., Stop 2000, Gaithersburg, MD 20899-2000

(Via e-mail: [ccroadmap.comments@nist.gov](mailto:ccroadmap.comments@nist.gov).)

Re: JEITA's comments on NIST Special Publication 500-293, US Government Cloud Computing  
Technology Roadmaps Volume I/II Release 1.0 (Draft)

Dear Dr. Bohn,

The Japan Electronics and Information Technology Industries Association (JEITA) is an industrial organization established with the aim of making a contribution to the development of electronic information and technology industries and of economy and the prosperity of culture. The Solution Services Committee of JEITA's Information Technology and Industrial Systems Board is committed to surveys to ascertain the scale of Japan's software and service market and an image of what the information system procurement system ought to be in the Japanese government, to clarify the definition of a cloud business model, and to review what must be kept in mind in entering into a cloud service agreement. The Committee also has an SLA/SLM Working Group, which was organized to disseminate service level agreements (SLAs) and service level management (SLM) through, for example, the publication of the "SLA Guidelines for Private Sector IT Systems" that describes how to use SLAs as visualization tools. The Committee studied the Cloud Computing Technology Roadmaps mentioned in the title and recently published by NIST.

We think aspects of risk management should be included in "2.3 Requirement 3: Technical Specifications for High-Quality Service-Level Agreements" of "Volume I" and "6.2 Service-Level Agreement Taxonomy" of "Volume II," both of which touch on SLAs.

In addition, Requirement 3 of 2.3 in Volume I defines "SLAs as measurable." However, considering the uniqueness of clouds, SLAs will become clearer if items to be defined in agreements or understandings are added as factors defining service levels besides measurable items.

Attached hereto is a summary of corresponding contents of the “Report on the Application of SLAs as Means to Control Risks Associated with Cloud Services (published in March 2011)” compiled by the Committee for reference.

Hidehiko Suzuki  
Chairperson, Solution Services Committee  
Japan Electronics and Information Technology Industries Association

Tomoaki Dogen  
Chief, SLA/SLM Working Group  
Solution Services Committee  
Japan Electronics and Information Technology Industries Association

The Solution Services Committee is conducting surveys and research focusing on SLAs and SLM for the purpose of studying, creating, and proposing a business environment in the field of solution services with awareness that the importance of the balance among quality, costs, and risks will rise while IT service users and providers share common understanding. Considering SLAs to be tools to “visualize” the function, scope, quality, and performance of IT services and to maintain a proper balance among costs, risks, and service quality, the Committee has been committed to the dissemination of SLAs and SLM through the publication of the “SLA Guidelines for Private Sector IT Systems” (hereinafter referred to as the “SLA Guidelines”) from Nikkei Business Publications, Inc.

## 1. Controlling Risks When Using Cloud Services

### 1.1 Background

The “Report by the Study Group on Cloud Computing and Japan’s Competitiveness” issued by the Ministry of Economy, Trade and Industry (on August 16, 2010) said that “cloud computing means an information processing scheme (architecture) designed to ‘provide/use information processing services as necessary through a network’.”

As the definition of “cloud services,” the one established by the National Institute of Standards and Technology (NIST) is widely cited. NIST defines the “three services models” as 1) Software as a Service (SaaS), 2) Platform as a Service (PaaS), and 3) Infrastructure as a Service (IaaS), and they are classified according to what is to be provided. The “four deployment models” mean 1) private cloud, 2) community cloud, 3) public cloud, and 4) hybrid cloud, which are grouped based on the difference of cloud users.

As a fifth model, a virtual private cloud, which combines the benefits of private and public clouds, is drawing attention. In a virtual private cloud, resources used by users belonging to different organizations or public users and resources physically or logically separated are made use of.

### 1.2 What is a cloud service?

#### (1) Definition of cloud services

The Solution Services Committee defined services from various aspects, thinking that the viewpoints of both service providers and service users are important for services. The Committee has set a definition of cloud services as follows with the viewpoints of service providers and service users taken into

account:

IT services provided for service users by service providers by means of cloud computing.

(2) Benefits of cloud services

The benefits of cloud services are defined from the viewpoints of service users (see Table 1).

Table 1: Benefits of cloud services (from viewpoints of service users)

	Category	Description
1	Benefit of reduced introduction period	1) Cloud services are available immediately whenever they are required. 2) Cloud services are available as long as service users require.
2	Benefit of reduced costs	1) Investment costs can be reduced because software and hardware are shared. 2) Service users pay the rates charged only for the services they used.
3	Benefit of resources	1) Service users can use the latest environment because service providers upgrade systems and versions. 2) Service providers provide security management.
4	Benefit of system extensibility	Cloud services are virtualized in general and can flexibly deal with the expansion of the frequency and scope of service use by service users.

(3) Scope of cloud services considered

The Committee defined the scope of cloud services to be considered to study the application of SLAs to cloud services.

There are five deployment models of cloud computing – “private,” “community,” “public,” “hybrid,” and “virtual private.” The Committee decided to consider models of high independence in which service providers and service users are just like independent companies.

In consequence, “public” and “virtual private” models were selected as the scope of cloud services to be considered in 2010.

1.3 Risks associated with the use of cloud services

When considering the application of SLAs to cloud services, the Committee first defined risks associated with the use of cloud services, including service-specific risks.

(1) Cloud service-specific risks and identification

Given the architecture of cloud services, cloud service-specific risks exist, which are different from risks relating to conventional IT services.

The Committee identified cloud service risks according to the procedure described below.

<Step 1> Issues confronting cloud services were derived from reference reports (see Fig. 1).

<Step 2> The Committee uniquely defined risks corresponding to the issues.

<Step 3> The Committee added undefined risks upon its discretion.

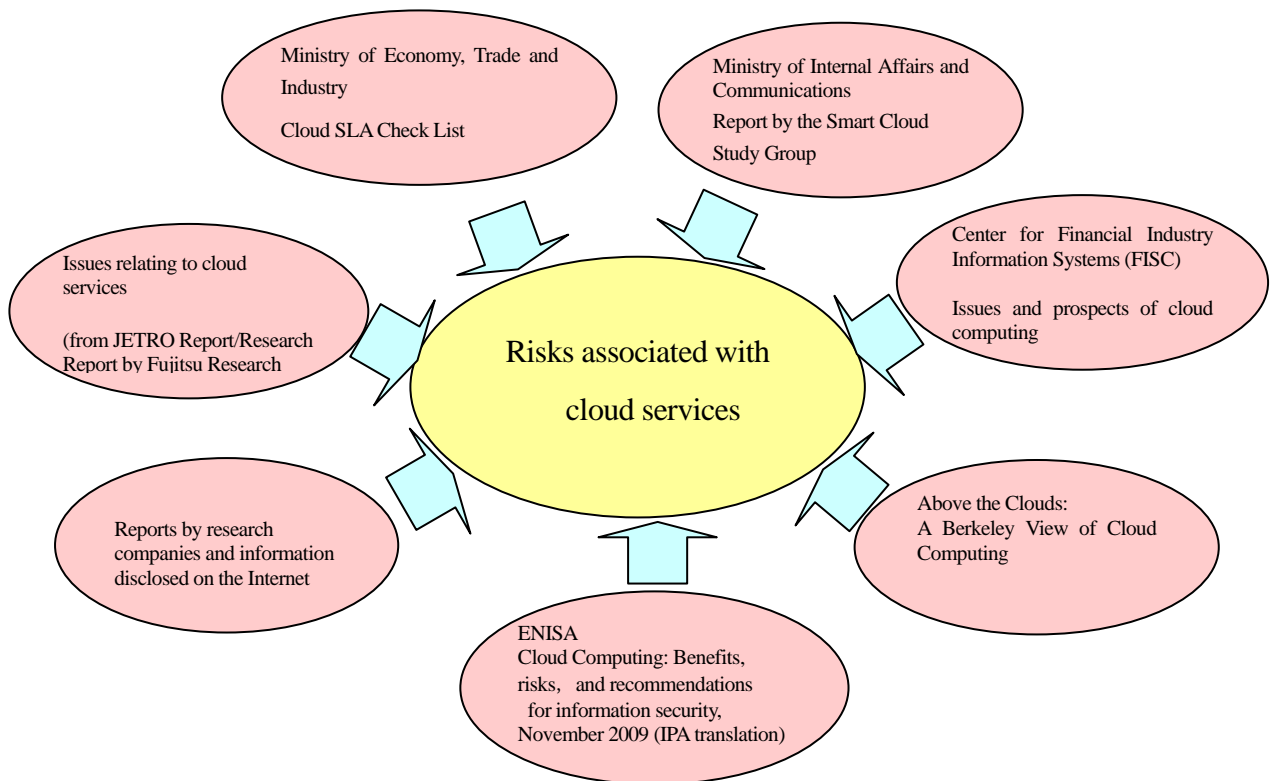


Fig. 1: Deriving risks associated with cloud services from reference reports

#### 1.4 Application of SLAs to cloud services

Regarding issues concerning cloud services as risks when a company's personnel in charge of IT apply cloud services to the information system of the company, the Committee defined SLAs as means to control risks and studied them for the purpose of visualizing cloud services and risks by agreement between service providers and service users.

##### (1) Concept behind the application of SLAs to cloud services

The use of cloud services brings about a service provider-service user relationship as is the case with ordinary outsourcing.

Although provided cloud services are visible because of their characteristics, provided service environments are less visible to service users and tend to become less involved in cloud services.

In such cases, SLAs are effective tools in visualizing services between service users and service providers.

SLAs the Committee studied are broad-sense SLAs that include not only service level items but also definitions in service specifications or arrangements in agreements.

In the study, the Committee identified risks expected to occur when cloud services are applied, and positioned broad-sense SLAs as means to control the risks.

Shown below are how to control cloud services by means of SLAs (see Table 2).

Table 2: How to control cloud services by means of SLAs

Control by means of SLA		Virtual private cloud		Public cloud
		Physical separation	Logical separation	
Narrow-sense SLA	Standard service level items	○	○	◎
	Addition to standard service level items	◎	○	△
Broad-sense SLA	Check items	○	○	◎
	Specifications/RFI	◎	○	△

## 1.5 Concept behind service level items and methods for applying them

### (1) Concept behind service level items

We studied service level items suitable as approaches to controlling risks with a view of visualizing cloud service risk control and thereby realizing the avoidance, reduction, and transfer of risks through the application of SLAs to cloud service risks. However, we found out the problems listed below.

- Service level items that can be specified in SLAs alone cannot deal with the entire risk control relating to cloud services.
- There are risks that cannot be controlled without using qualitative service level items (that cannot be quantitatively expressed).
- Some approaches to realizing risk control are not proper for service level items that should be specified in SLAs.

The Committee consequently decided to grasp service level items as means to control cloud service risks in a broad sense. Service level items as approaches to risk control can be classified into the following three categories based on their characteristics:

- Automatic: Item that can be quantitatively expressed and is automatically measurable with a tool.
- Manual: Item that is not quantitatively expressed but is checked by a person (achieved/not achieved, present/absent, etc.).
- Specification: Item that is not specified in an SLA but is specified as a service requirement, agreement condition, or service specification.

(2) Methods for applying service level items

Different methods for applying service level items are used at the respective stages of the life cycle of the use of cloud services. Methods for applying them are shown below (see Table 3).

Table 3: Methods for applying service level items

Life cycle	Implementation category of controlling method		
	Automatic	Manual	Specification
Preliminary study	Check list	Check list	Check list
Presentation of service requirements	RFI/RFP	RFI/RFP	RFI/RFP
Conclusion of agreement	SLA	SLA/Service agreement	Service agreement
Use	SLA	SLA/Confirmation of contents of agreement	Confirmation of contents of agreement
End	—	Confirmation of contents of agreement	Confirmation of contents of agreement

1.6 Risk control by service level items

The Committee compiled a “Cloud Service Risk Control Sheet” defining risk control methods using service level items.

(1) Purpose

The purpose of the “Cloud Service Risk Control Sheet” is to serve as guidelines for cloud service users to use optimum cloud services for business requirements.

(2) Organization

The organization of the “Cloud Service Risk Control Sheet” is as shown below (see Fig. 2).

1) Classification

The risks that will occur during the use of cloud services are classified into the following nine categories according to their properties:

- Availability, reliability, security, performance, data management, transfer, area of responsibility, laws and regulations, extensibility

2) Risk when using cloud services

The risks that will occur when using cloud services are stated.

3) Risk assessment

The degree of the effect and possibility of each risk are assessed as “High,” “Medium,” and “Low.”

4) Control method

The measures cloud service users should take to control (avoid/reduce/transfer) risks are stated.

5) Implementation category

The service level items for implementing risk control methods are classified into three categories – “automatic,” “manual,” and “specification” – according to their characteristics.

6) Example of service level item

Examples of specific service level items are stated.

7) Remarks

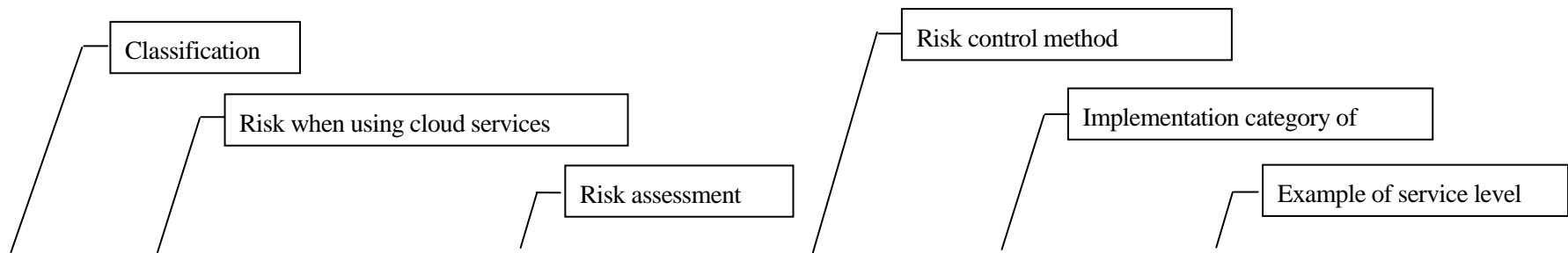
A supplementary description of each of the abovementioned items or another important information is stated.

(3) Expected effects

The Committee expects various effects from the “Cloud Service Risk Control Sheet” by using it as described below.

- 1) The Cloud Service Risk Control Sheet can be used as a preliminary check list when considering the use of cloud services.
- 2) When selecting a cloud service or cloud service provider, the user can present service requirements that can fulfill his/her company’s business requirements by assessing risks.
- 3) The user can identify what should be agreed upon in an SLA and what should be agreed upon as a service agreement or service specification when entering into a service agreement with a cloud service provider.





No.	Classification	Risk when using cloud services	Risk assessment		Control method	Implementation category			Example of service level item	Remarks
			Degree of effect	Possibility		Automatic	Manual	Specification		
1	Availability	The sudden discontinuation of services by the service provider hinders the user's operations.	High	Low	Entrust programs and data to a third party in advance so that the services can be continued even if the service provider suddenly discontinues the provision of services.			○	Arrangements against the sudden discontinuation of services Entrustment of programs and data to a third party	
2	Availability	Sudden changes to the contents of services or the sudden discontinuation of services by the service provider hinders the user's operations.	High	Low	Include in the agreement the provision that the service provider shall inform the user of any changes to the contents of services, sudden discontinuation, etc. in advance.			○	Arrangements against sudden changes to the contents of services or the discontinuation of services Service time Notification of plan discontinuation schedule	
3	Availability	The unstable provision of services hinders the user's operations.	High	Medium	Determine service levels, and regularly monitor and assessing them.	○			Operation rate Mean time to repair (MTTR) Recovery time objective (RTO) Number of failures Service provision time zone (to deal with failures) Service provision time zone (to respond to general inquiries)	
4	Availability	A serious failure with provided services hinders the user's operations.	High	Low	The service provider and the service user determine in advance alternative action to take if early recovery is impossible.			○	Alternative action against serious failures	

5	Availability	The provision of services will be interrupted if the resource is not properly separated among users.	High	Low	When entering into an agreement, check how to manage the database among multiple tenants, the management of the database encryption key (whether the key is common to all tenants or is exclusive to each tenant), etc. If necessary, specify the division of the database and the individual management of the encryption key in the agreement.			○	Key management requirements in the case of storage by multiple tenants	
6	Availability	In case of a disaster, operations cannot be continued if disaster restoration training is not properly provided.	High	Medium	At the time of the conclusion of the agreement, check and determine details and frequency of disaster restoration training, including the system restoration/support system in case of a disaster.			○	BCP Contingency plan	

Remarks

Fig. 2: Organization of “Cloud Service Risk Control Sheet”

## 1.7 How to use the “Cloud Service Risk Control Sheet”

This section describes how to use the “Cloud Service Risk Control Sheet” when considering risk control in using cloud services.

Assuming a life cycle (“Preliminary study,” “Presentation of service requirements,” “Agreement,” “Use,” and “End”) in the use of cloud services as situations in which they are used, important matters that should be considered from the standpoint of risk management at each stage and examples of how to use the “Cloud Service Risk Control Sheet” when considering themes matters are shown below (see Fig. 3).

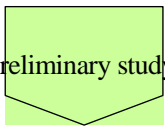
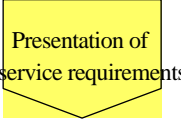
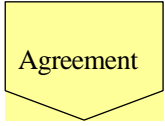
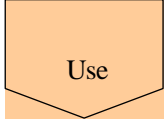
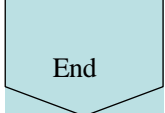
Life cycle	Important matter to consider (from the standpoint of risk management)	Example of how to use the “Cloud Service Risk Control Sheet”
 Preliminary study	Screening out and assessing risks associated with the use of cloud services	<ul style="list-style-type: none"> <li>✓ Take a bird’s eye view of risks associated with the use of cloud services.</li> <li>✓ Identifying important risks based on the degree of effect and possibility of individual risks.</li> <li>✓ Use the results of the abovementioned study as reference for planning toward the use of cloud services.</li> </ul>
 Presentation of service requirements	Checking the cloud service provider’s action and policy against risks	<ul style="list-style-type: none"> <li>✓ Check the cloud service provider’s action and policy against important risks.</li> </ul>
 Agreement	Considering required specifications Entering into an SLA	<ul style="list-style-type: none"> <li>✓ Consider the specifications that should be contained in the agreement.</li> <li>✓ Consider the items that should be continuously managed and contained in the SLA.</li> </ul>
 Use	Checking the status of management according to the action and policy against risks	<ul style="list-style-type: none"> <li>✓ Use the status of management as reference when reviewing the agreement (adding or deleting service level items) according to the use of cloud services.</li> </ul>
 End	Assessing risks and taking action against them at the end of the provision of cloud services.	<ul style="list-style-type: none"> <li>✓ Recheck the contents of the agreement to see if proper action is taken at the end of the provision of cloud services.</li> </ul>

Fig. 3: How to use the “Cloud Service Risk Control Sheet”

## 2. Report on U.S. Survey Regarding Cloud Services

To finalize service level items toward the use of cloud services, the Committee conducted a hearing survey on U.S. cloud service users and service providers from the following three aspects:

- (1) Obtain RFI/RFP requirements concerning the use of cloud services in key systems, which are difficult to obtain in Japan. In particular, conduct a hearing survey on the City Office of Los Angeles as a case of designating and using strict security requirements to Google Apps, which is a public cloud.
- (2) Investigate the issues that have actually come to the surface in connection with cloud services that are

popular ahead of Japan, and collect information about them. Identify the service levels that should be determined between the service user and the service provider as solutions to these issues.

- (3) Conduct a survey on what action cloud service users engaged in actual operations take to retain and protect data and comply laws and regulations, with emphasis placed on actual compliance with the U.S.A. Patriot Act, to formulate a concept of SLAs with regard to the retention and protection of data in Japan.