Guide to Protecting Cloud Service Users and Ensuring Compliance

For Appropriate Risk Management by Top Management

Version 1.0

June 2011

ASP-SaaS-Cloud Consortium

Table of Contents

This guide is published by ASP-SaaS-Cloud Consortium through the process of public comment requests. This guide is described based on the discussion in FY 2010 of Cloud User's Rights Protection Review Committee of ASP-SaaS-Cloud Promotion Conference that is co-founded by Japan's Ministry of Internal Affairs and Communications and ASPIC.

Chapter 1 Purpose and outline of this guide

1. How to read this guide

(1) Purpose of this guide

Cloud services are currently expanding all over the world. There are many cloud service providers that offer borderless global services. As cloud service providers and services become increasingly diverse, so there are an increasing number of both excellent providers and services that can bring clear profits to users and risky providers and services that do not satisfy users' security policies. Therefore it becomes important for users to be able to cleverly choose reliable cloud providers and services.

This guide provides enterprises that intend to use public cloud services (see Reference 1) with comprehensive information on risk management processes and points requiring confirmation. The aim is to help them choose cloud service providers and services that match their risk management policies, implement adequate risk management systems and use services safely. We chose public cloud services because this service model typically brings particular merits and characteristics of cloud services. However, this guide also provides enterprises that plan to use private cloud services (see Reference 1) with useful information on risk management processes.

(2) Who should read this guide?

This guide describes issues that corporate managers who plan to use or already use public cloud services are recommended to read.

1. Corporate managers of large corporations with a board of directors and listed corporations:
   The guide helps corporate managers to fulfill their duty of diligence and establish adequate risk management systems and processes that enable corporations to safely use cloud services.
2. Corporate managers of small and medium-sized corporations:
   The guide helps corporate managers to dispel illusions that all cloud services are risky, remove the need for in-house IT specialists, and enable cloud services to be used safely and cost-effectively.
3. Corporate managers of a global enterprise:
   The guide illustrates the checkpoints for protecting users' rights and ensuring users' compliance when global enterprises use borderless global cloud services.

(3) How to read this guide

This guide consists of three chapters and three references.

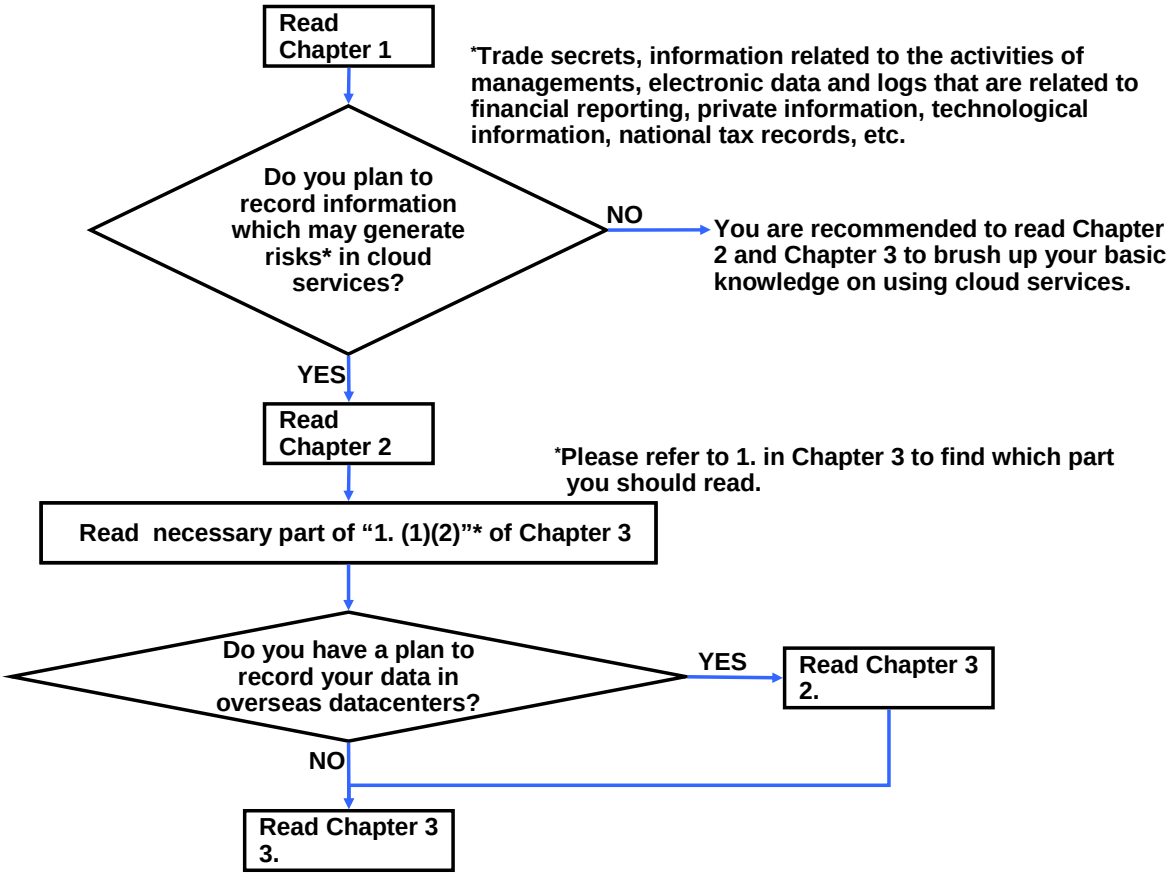
Chapter 1 describes the following:

- How to read this guide
- Merit of cloud services and need to implement risk management systems

- Legal structures related to user's rights and ensuring compliance that are covered in version 1 and will be covered in the following versions.

Chapter 2 describes recommended risk management processes that should be executed at each stage of the cloud service utilization cycle. In this chapter, both recommended directions to persons in charge by corporate managers and issues that should be judged and determined by corporate managers are covered.
Chapter 3 describes points requiring confirmation from three viewpoints. Guidelines and rules for the enforcement of laws that are necessary to confirm protection of users' rights and ensure their compliance are listed in Reference 3.

All corporate managers are recommended to read Chapter 1.
Corporate managers who are going to implement risk management systems for cloud services should read Chapter 2 and Chapter 3.
Corporate managers who have already implemented risk management systems for cloud services can use this guide to strengthen their system with pinpoint countermeasures by reading the necessary part of Chapter 3.
The parts of this guide that each user should read differ according to the type of user information to be recorded in cloud services and location of the datacenter. Please refer to the figure on the next page.



(4) Main focus of this guide and related guidelines (see reference 2)

This guide provides corporate managers with comprehensive information on risk management processes and points requiring confirmation at each stage of the cloud service utilization cycle. This guide is unique because it stresses the protection of users' rights and ensuring their compliance.

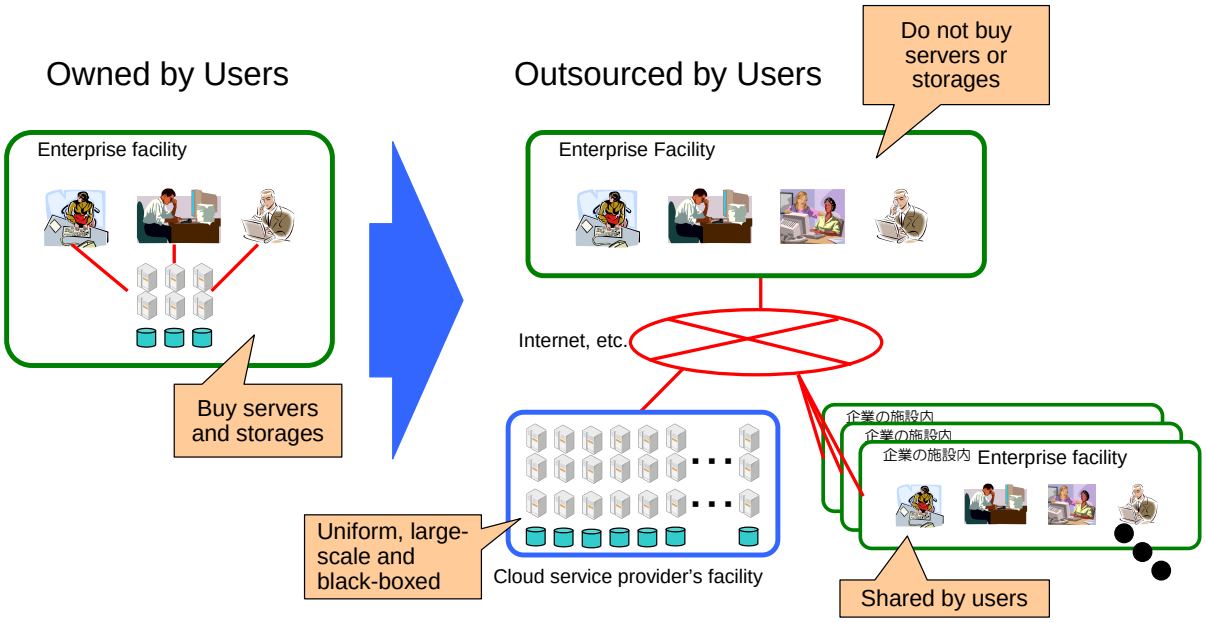
There is another guideline and another guidance that are written for cloud service users:

- Guideline for Information Security Management when using cloud Services (METI, Apr. 2011)
- Guidance for Safe Use of Cloud Services by Small and Medium-Sized Enterprises (IPA, Apr. 2011)

2. Many advantages of cloud services

(1) Paradigm shift from “owning computing resources” to “outsourcing computing resources”

Helped by the rapid popularization of broadband networks in Japan, enterprises are steadily entering an era in which they outsource IT systems instead of developing them by themselves. Recently many cloud service providers have come to equip datacenters with a large amount of black-boxed computing resources. As a result, users are now able to select and start using services and computing resources promptly after they select them from catalogs.



(2) Clear advantages of public cloud

Cloud services offer many advantages. Some of them as follows:

* These advantages are not limited to public clouds, but they are obvious in the case of public clouds.

Powerful tools for speedy corporate management

In general, it is necessary to invest in ICT systems and networks when enterprises launch new business or entrepreneurial ventures are set up. Cloud services enable enterprises to outsource the necessary ICT resources in a short time and in an inexpensive way. Thus, it becomes easier for enterprises to realize speedy management by actively testing out new businesses.

Tools for focused investment in competitiveness and differentiation of enterprises

The competitiveness of enterprises is improved if they can differentiate themselves

from other enterprises. By applying cloud services to administrative and accounting work that do not relate to strategic differentiation, enterprises can turn ICT cost and manpower into strategic differentiation in their business fields.
Also, enterprises do not need to incur costs for upgrading their systems.
Furthermore, small and medium-sized enterprises can improve the quality of their administrative and accounting work by using the same functions as large enterprises that are provided by cloud services.

Tool for green activities by enterprises

Enterprises can effectively decrease their CO_2 emissions by using cloud services that are operated in datacenters with high energy efficiency.

Tools to improve abilities to respond to natural disasters

Widespread natural disasters may occur at any time. Cloud services are a useful tool for enterprises to ensure a business continuity plan in the event of a large natural disaster.

Release or relief from burden of tasks related to ICT procurement

Small and medium-sized enterprises can start using ICT more easily because the ICT procurement process becomes much easier by using cloud services.

Release or relief from burden of ICT operation and maintenance tasks

Releasing or relieving enterprises of the burden of ICT operation and maintenance tasks is a very attractive advantage of cloud services for small and medium-sized enterprises that lack ICT specialists.

Release or relief from burden of information security tasks

Small and medium-sized enterprises often have some problems in information security in their ICT systems because they may have an insufficient number of employees who specialize in information security.
By using cloud services that are operated at datacenters with a high level of information security and sufficient number of information security specialists, small and medium-sized enterprises can expect to see improvements in the level of their information security management.

3. Why risk management is necessary when using cloud services

Although public cloud services have many advantages, risk control over cloud service providers may become limited because physical ICT resources are black-boxed and their operation and maintenance are outsourced. This limited governance may potentially generate various kinds of secondary risks (see Reference 1). For instance, the following accidents may occur:

1. A claim over ownership of trade secrets is not approved because an enterprise does not sufficiently manage its secrets.
2. Society could lose its trust in an enterprise if such enterprise divulges a large amount of private information.
3. Technical information that is restricted in terms of sending it to foreign countries could possibly be leaked by cloud service providers whose datacenters are located overseas.
4. Secret information could be divulged if cloud service providers do not delete users' data completely.

It should be a duty of corporate managers in large enterprises with a board of directors and in listed enterprises to establish risk management systems.

By thinking of the issues described above, corporate managers are recommended to take the initiative in developing systems that apply risk management processes to each stage of the cloud service utilization cycle.

4. Coverage of this guide in terms of users' rights and ensuring their compliance

This guide stresses the protection of users' rights and ensuring their compliance. The kind of legal structures that Version 1 of this guide covers is shown in the following text box. In the following version, we intend to extend the coverage of legal structures that should be focused on.

Legal structures covered by Version 1 of this guide

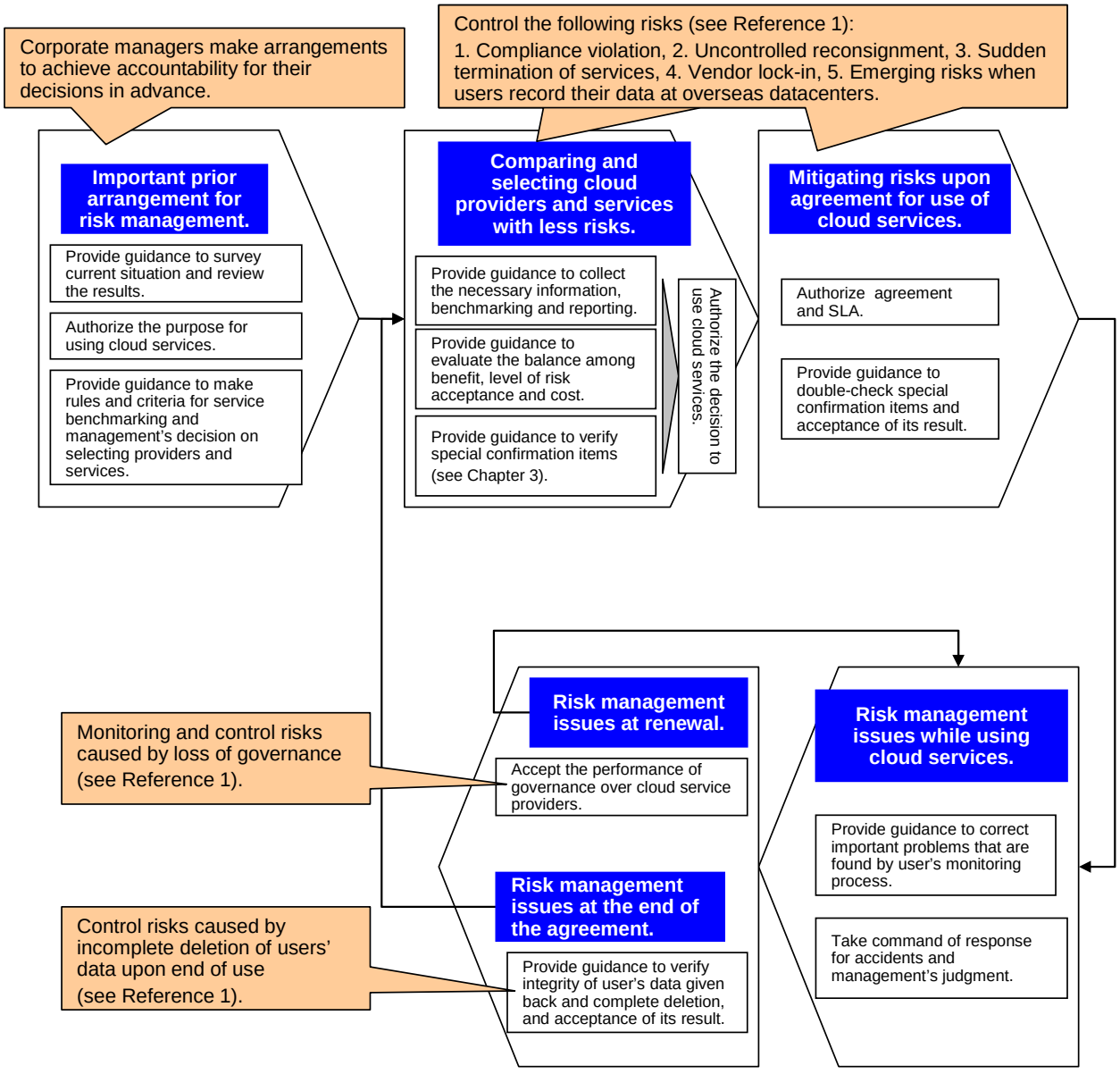
1. Protecting users' rights
   - Protection of Trade Secrets by Unfair Competition Prevention Act (management of trade secrets)
2. Ensuring users' compliance
   - The Companies Act and so-called J-SOX Act
   - The Personal Information Protection Law
     Health insurance and welfare; broadcasting and postal area; economy and industry; employment management; legal issues; corporate pensions; foreign affairs; financial matters; agriculture; forestry and fisheries area; land and transport; and the environment.
   - The Foreign Exchange and Foreign Trade Control Law (prevention of outflow of technological information)
   - The Law Concerning Preservation of National Tax Records in Electronic Form, the Corporation Tax Act, and so on (preserving books in electronic form)

Legal structures that will be covered in later versions of this guide

1. Protecting users' rights
   - Legal structures related to intellectual property right (industrial property right, copyright and so on)
2. Ensuring users' compliance
   - The Personal Information Protection Law
     Healthcare and nursing, monetary and credit matters, business area using study results in medical and genetics fields and the related information, labor-related issues, education, and police and defense
   - Legal structures that allows preservation of books, ledgers, drawings and so on based on the Electronic Documents Act
   - Industry acts such as the Construction Industry Act

Chapter 2 Effective risk management system for cloud service users

The risk management cycle of cloud services consist of important prior arrangement for risk management, comparing and selecting cloud providers and services with less risks, mitigating risks upon agreeing to use cloud services, coping with risk management issues while using cloud services, coping with risk management issues at renewal and coping with risk management issues at the end of the agreement.
The following figure shows the necessary guidance, acceptance and authorization for corporate managers to execute at each stage of the risk management cycle of cloud services.



1. Important prior arrangement for risk management

The purpose of prior arrangement for risk management is to survey the current situation, prepare corporate managers for using cloud services, and determine which providers to choose and which services to choose.
The survey on the current situation aims to ensure that:

(1) Corporate managers take the initiative in understanding the value and risk acceptance level of information that is to be recorded in cloud services.
(2) Corporate managers, based on this knowledge, try to figure out what level of service and information security is realized and the cost required to keep this level. These items are basic knowledge for enterprises to choose the level of requirements to be imposed on cloud service providers.

Corporate managers provide personnel in charge of information systems with guidance to survey the current situation and review the results.
Corporate managers provide user divisions of cloud services with guidance to clarify the concrete benefit from using cloud services and accept the results. When choosing services, the most important criterion is benefit. Therefore, benchmarking other criteria should be processed on the premise that a certain amount of benefit is obtained.
Corporate managers provide personnel in charge of information systems with guidance to create (1) a checklist of criteria for selecting cloud service providers and services and (2) a checklist of special points to confirm that are described in Chapter 3, and authorize these checklists. By using these checklists, it becomes possible to select cloud service providers and services in a highly transparent way.

1. Provide guidance to survey current situation and review the result.

Review current policies of your enterprise which relate to information that are to be recorded in cloud services.

1. Review current policies of your enterprise (information security policy, privacy protection policy, trade secret management policy, IT general control policy and so on) which relate to information that is to be recorded in cloud services.
2. Prior to recording this information in cloud services, corporate managers provide personnel in charge of information systems with guidance to improve in-house policies and authorize the improvement if necessary.

Survey value and risk acceptance level of information that is to be recorded in cloud services.

1. Corporate managers provide personnel in charge of information systems with guidance to survey value and risk acceptance level of information that is to be recorded in cloud services.
2. Corporate managers provide guidance to classify the information written above so that it becomes clear that the information relates to the enterprise's rights, compliance and so on.
3. Use the result for decision making on whether the information is allowed to be recorded in cloud services.

Survey current level of information security management and services used in-house.

1. Corporate managers provide personnel in charge of information systems with guidance to survey the current information security management, service level and necessary cost that are applied to the information to be recorded in cloud services.
2. Utilize the result as a reference to consider what level of service and information security cloud service providers should offer.

2. Authorize the purpose for using cloud services.

Clarify benefit of using cloud services.

1. Corporate managers provide the user division of cloud services with guidance to clarify concrete benefits (i.e., purposes) obtained from using cloud services and accept the result.
2. Corporate managers should decide whether to use cloud services so that actual benefit is the criterion of the first order.
3. Define quantitative benefit as a key performance Indicator (KPI).

3. Provide guidance to make rules and criteria for service benchmarking and management's decision on selecting providers and services.

Provide guidance to create policies, criteria and manuals and authorize them.

Corporate managers provide personnel in charge of information systems with guidance to create the following rules, criteria and checklists and authorize them.

1) Criteria to choose providers and services
   - Criteria to evaluate sound management of providers
   - Criteria to verify service level requirements
   - Criteria to verify information security requirements
   - Checklist to check agreement statement and so on
2) Checklists for special points to confirm described in Chapter 3

2. Comparing and selecting cloud providers and services with less risks

At this stage, personnel in charge of practical tasks collect information from cloud service providers and compile benchmarking results at first. Then, based on this report, corporate managers make a decision on whether to use cloud services. They consider whether they will certainly obtain benefits and the ideal balance between risk acceptance level and cost. After this decision, corporate managers provide guidance to help personnel choose cloud service providers and services in accordance with predefined criteria for selecting service providers and authorize the results.

However, upon selecting cloud service providers and services, it is necessary to confirm that providers and services satisfy the following conditions:

(1) Providers can offer services and service levels that satisfy the special points to confirm described in Chapter 3.

(2) Providers can offer an agreement of use that satisfies the user’s policies and needs.

1. Provide guidance to collect necessary information, benchmarking and reporting.

Corporate managers provide personnel in charge of information systems with guidance to collect information from cloud service providers, compile benchmarking results and report the results. This in accordance with the criteria of selecting providers prepared at the prior arrangement stage and the checklists for special confirmations described in Chapter 3.

2. Provide guidance to evaluate the balance among benefit, level of risk acceptance and cost.

Evaluate the balance among benefit, level of risk acceptance and cost.

1. With top priority, it is necessary to get benefits certainly and achieve the appropriate purpose of using cloud services. For example, in the case of small and medium-sized enterprises, the purpose may be to improve information security management systems. In this case, it is fairly easy to select cloud services that satisfy the purpose of use.
2. On the premise of getting benefits and satisfying user's in-house policies, compare and evaluate the balance of costs that is necessary to realize adequate information security management and service levels and risk acceptance level of the information that is to be recorded in cloud services. Moreover, compare and evaluate the risk level between situations where the information is kept recorded in-house and situations where the information is recorded in cloud services.
3. Corporate managers provide personnel in charge of information systems with guidance to create evaluation reports and review the results.

3. Provide guidance to verify special confirmation items.

Provide guidance to verify special confirmation items

1. Corporate managers provide personnel in charge of information systems with guidance to verify special points to confirm described in Chapter 3.
2. If the information recorded in cloud services relates to the enterprise's rights, compliance and so on, corporate managers provide personnel in charge of information systems with guidance to collect information required to check confirmation items described in 1. of Chapter 3 from cloud providers.
3. If users have a plan to record their data at overseas datacenters, corporate managers provide personnel in charge of information systems with guidance to collect information required to check confirmation items described in 2. of Chapter 3 from cloud providers.
4. Corporate managers provide personnel in charge of information systems with guidance to collect information required to checkpoints requiring attention due to a potential awareness gap between users and cloud service providers described in 3. of Chapter 3 from cloud providers.

4. Authorize the decision to use cloud services.

1. Based on the evaluation results of the balance among benefit, level of risk acceptance and cost, corporate managers decide whether or not to use cloud services.
2. Based on the evaluation results, personnel in charge of information systems select cloud service providers and services in accordance with the criteria of selecting cloud services that is authorized at the prior arrangement stage. Corporate managers authorize the selection of cloud service provider and services.
3. Upon authorization of the selection of cloud service provider and services, it is necessary to confirm that the selected provider should be able to offer services that satisfy special confirmation items described in Chapter 3. Corporate managers accept the confirmation results.
4. If user's security policy requires, corporate managers provide personnel in charge of information systems with guidance to verify whether or not selected cloud service provider can cooperate with user's internal audit and accept the confirmation results.

3. Mitigating risks upon agreeing to use cloud services

Upon agreeing to use cloud services, it is best to confirm the content of agreements carefully and in detail by using checklists that are prepared in advance and corporate managers must accept the result. Personnel in charge of information systems should double-check the content of service level agreements (SLA) and establish an agreement with the authorization of corporate managers based on the results of selecting providers and services executed in the previous stage (i.e., comparing and selecting cloud providers and services with less risks).
Upon executing an SLA, please refer to “3. Preventing an awareness gap between users and cloud services providers” in Chapter 3. Corporate managers should provide personnel in charge of information systems with guidance to execute final confirmation according to the points requiring attention. This is because there may be an awareness gap between users and cloud service operators, as described in 3. of Chapter 3.

1. Authorize agreement and SLA

Authorize agreement and SLA.

1. Corporate managers provide personnel in charge of information systems with guidance to confirm the content of agreements carefully and in detail by using the checklists that are prepared in advance. If there are no problems, corporate managers authorize the result.
2. Regarding SLA, corporate managers have already authorized the decision on choosing cloud service providers and services that can realize the required service level at an acceptable cost based on the criteria for selecting providers and services. This was done at the stage of benchmarking of cloud service providers and services. Therefore at this stage, personnel in charge compare the proposed SLA by the provider with in-house policy and confirm if it is acceptable in detail.
3. After this confirmation process, corporate managers authorize the result and conclude a SLA.

2. Provide guidance to double-check special confirmation items and acceptance of its result.

Provide guidance to double-check special confirmation items and acceptance of its result.

1. The points requiring attention due to potential awareness gap between users and cloud service providers are described in 3. of Chapter 3.
2. Corporate managers provide personnel in charge of information systems with guidance to execute final confirmation according to the points requiring attention due to a potential awareness gap between users and cloud service providers and accept the result.
3. In reality, because careful survey has already been done at the stage of benchmarking of cloud service providers and services, this task is not a negotiation but is likely to be a double-checking of items.

4. Risk management issues while using cloud services

The main role of corporate managers at this stage is to cope with unexpected problems and accidents.

(1) Provide guidance to correct important problems that are found during user's monitoring process

Important problems such as a serious loss of governance over cloud service providers or important violation of service level agreements may be found during user's everyday monitoring process. In this case, corporate managers should provide personnel in charge of information systems with guidance to investigate the cause and create a countermeasure plan, review the plan and accept it.

(2) Take command of response for unexpected accidents and management's judgment

Unexpected serious events include widespread natural disasters and large-scale divulgation of private information. If these should occur, corporate managers must take command in responding to these events and make managerial decisions.

5. Risk management issues at renewal or end of agreement

At this stage, enterprises decide whether they will continue using the same cloud services next year.
If the enterprise decides to continue using the services, corporate managers should receive an annual report that describes the actual performance of governance over cloud service providers last year from personnel in charge of information systems and review the report. Enterprises may ask the cloud service provider to submit third-party assurance in order to prove that the enterprise adequately governed the cloud service provider.
If the enterprise decides to change the cloud service provider and services, it must confirm that user's data are appropriately given back and completely deleted after that. If the enterprise use public cloud services, this task must be ensured and confirmed. Corporate managers should provide personnel in charge of information systems with guidance to verify the result very carefully and accept the work completion report.

1. Risk management issues at renewal

Accept the performance of governance over cloud service Providers.

1. Many laws require adequate governance over outsourcing providers of IT systems.
2. Corporate managers provide personnel in charge of information systems with guidance to report actual performance of governance over cloud service providers last year and accept the report.
3. Corporate managers can choose to have the enterprise ask the cloud service provider to submit the third-party assurance in order to prove that the enterprise governed cloud service provider adequately.
4. In this case, ask cloud service providers to submit a verification report that is described based on the "Information Security Verification Service" defined by the research report No. 39 (May, 2010) of IT Committee, Japanese Institute of Certified Public Accountants,

* From the perspective of ensuring internal control over financial reporting, it is important that cloud service providers have obtained SAS70 as it falls into the proof of governance control over outsourcing providers. If it is not limited to financial reporting, SAS70 cannot be deemed to be a "third-party certificate." But in reality, it is widely referred to as showing the management style of the cloud service provider.

2. Risk management issues at the end of the agreement

Provide guidance to verify integrity of user's data given back and complete deletion, and acceptance of its result.

1. It is very important for users of cloud services to receive their data with the format that is possible to process by users themselves. Corporate managers guide personnel in charge of information systems with guidance to decide rules related to user's data given back (necessary period, method, data format, etc.) in advance, and receive data surely by following the rules. Corporate managers review and accept the results.
2. If users use public cloud services, it is necessary to confirm that users' data is completely deleted by receiving data deletion certificate document, or if it is difficult, an alternative method with high reliability. Corporate managers provide personnel in charge of information systems with guidance to confirm complete deletion of user's data and accept the completion report. If an alternative method other than receiving data deletion certificate document is applied, corporate managers require personnel in charge of information systems to carefully verify the adequateness of the method.

Chapter 3 Points to confirm

In this chapter, we will describe the points to confirm from three viewpoints so as to ensure the protection of cloud service users and ensure compliance of cloud users.

1. Points to confirm to protect cloud users' rights and ensure their compliance

This section describes our approaches to verify that (1) users' rights are protected based on domestic laws and regulations and (2) users' compliance is ensured based on domestic laws and regulations with regard to the use of cloud services. Please select and read the related descriptions according to the type of information that you plan to record in cloud services.

Type of information to be recorded in cloud services:		Related descriptions
Protecting users' rights	Trade secrets	(1)
Ensuring users' compliance	Information related to the activities of management, electronic data and logs that are related to financial reporting	(2) A
	Private information	(2) B
	Technological information	(2) C
	National tax records	(2) D

(1) Protecting users' rights

The typical rights of cloud service users protected by domestic laws and regulations in both civil and criminal terms include trade secrets of the users and intellectual property rights of the users.

With regard to trade secrets, it is essential to ensure three requirements to be eligible for legal protection: a) the concerned information shall be managed as a secret, b) it shall be useful information, c) it shall not be publicly known. Corporate managers need to pay special attention to the fact that using cloud services may risk one of the aforementioned requirements, which is *a) managed status of secrets*. Enterprises must verify that there is no discrepancy with internal management policies and operation rules for trade secrets when using cloud services and/or that such discrepancy should not risk *a) managed status of secrets*. This is based on the "Trade Secrets Management Guidelines" (see Reference 3) formulated by METI.

Important points to confirm in checking based on Trade Secrets Management Guidelines

1. Contract details related to method of managing secrets
   - Identification and limitation of access and its administrator, protection from external intrusion, and data deletion and disposal
   - Management related to ensuring legal competency etc.
2. Contract details related to organizational management to ensure appropriate functioning of management of secrets etc.
   - Cooperation with internal audits

In conducting the verification, personnel in charge shall investigate the details and corporate managers shall review the investigation details. Based on this review result, corporate managers shall make judgments, such as trade secrets are recorded in cloud services, the information to be recorded in cloud services is not managed as trade secrets, or trade secrets are not recorded in cloud services.

* Other than those cited here, some other elements such as intellectual property rights (industrial property rights, copyrights etc.) may be included. We plan to expand descriptions on the protection of rights when we revise this guide in future.

(2) Ensuring users' compliance

The following laws and regulations relate to ensuring users' compliance:

Laws and regulations related to ensuring users' compliance

A. Corporate Law, Financial Instruments and Exchange Act (so-called J-SOX Act): Internal governance of listed enterprises and large corporations
B. Privacy Protection Law
C. Foreign Exchange and Foreign Trade Act (Foreign Exchange Act): Preventing technological information from flowing overseas
D. Law Concerning Preservation of National Tax Records in Electronic Form (Law for Preserving Electronic Documents), Corporate Tax Law etc.: Preservation of electronic data such as books etc.
E. Industry laws that users comply with on routine basis: Regulations set by competent authorities etc.

Depending on the laws and regulations, different approaches are applied when checking whether users' compliance is ensured in using cloud services. The following section describes this confirmation method based on each law and regulation other than industry laws. In conducting the confirmation, personnel in charge shall investigate the details and corporate managers shall review the investigation details. Corporate managers shall decide whether to introduce cloud services based on this review result.

* We plan to expand descriptions on ensuring compliance when we revise this guide in future with regard to industry laws and such like set by the competent authorities that users comply with on a daily basis.

A. Confirmation related to internal governance

For large corporations with a board of directors, enterprises must verify that the use of cloud services does not disturb the establishment of a system to ensure appropriate business operations, as requested by Article 100, Paragraph 1 of the Rules for the Enforcement of Corporate Law. For instance, developing a risk management policy and establishing a risk management and monitoring system are required. It is essential to develop a system that can verify that these policies and systems work appropriately and practically later on.
Similarly, in the case of listed enterprises, it is important to ensure a verification system based on the J-SOX Act in using cloud services. Verification shall for example demonstrate that risk management policies and systems work appropriately and practically.
These elements are not described in detail in this guide. Please refer to the description on COSO frameworks.

B. Confirmation related to protecting private information
Guidelines for protecting private information established by each government agency (see Reference 3) determine the guidelines for supervising private data consignees. The confirmation to ensure compliance in using cloud services shall be carried out also based on these guidelines.
The contents of the guidelines differ significantly depending on the government agencies that established each guideline. Therefore, confirmation shall be carried out by choosing appropriate guidelines for the industry area of your company (see Reference 3).

Considerations in referring to guidelines related to protecting private information (differences among various guidelines)

1. Does the guideline request establishment of a standard in selecting data consignees?
2. Requirement items to be included in the consignment contract (level of specificity, handling of repeated consignment, handling of contract termination etc.)
3. Does the guideline request scheduled and/or unscheduled audits of the consignees?
4. Does the guideline request obligation of reporting to consigners in the event of an accident such as leakage of personal data? Further, does the guideline request clarification of consignees' liability in the event of an accident?
5. Does the guideline request a periodical review of the contract details?
6. Does the guideline refer to the anonymization of personal data at consignment?

* This guide covers various areas including health insurance and welfare; broadcasting and postal area; economy and industry; employment management; legal issues; corporate pensions; foreign affairs; financial matters; agriculture; forestry and fisheries area; land and transport; and the environment. Besides, guidelines for protecting private information have been established in some areas including healthcare and nursing, monetary and credit, business areas using study results in medical and genetics fields and the related information, labor-related matters, education, and police and defense. We plan to expand descriptions on ensuring compliance when we revise this guide in future.

C. Confirmation to prevent technological information from flowing overseas
When using cloud services at an overseas datacenter, it is essential to give consideration to the risks concerning the flow of technological information

overseas, as cited in the separate list of the Export Trade Control Ordinance. The Guidelines on Preventing Technology Outflow established by METI (see Reference 3) state as follows: “Consideration should be given to avoid careless exposure of important know-how in documents. If any know-how is included in a drawing or document, the information shall be managed in a stringent manner as a trade secret or such like.” Therefore, by deciding whether or not it is possible to store the trade secret in overseas datacenters, corporate managers can make their decision on whether or not it is possible to record the technological information in cloud services using overseas datacenters.

D. Confirmation related to preserving national tax records in electronic form
Rules for the Enforcement of Law for Preserving Electronic Documents set the following requirements concerning the preservation of national tax records in electronic form[1] (see Reference 3).

Requirements concerning the preservation of electronic documents in Rules for the Enforcement of Law for Preserving Electronic Documents
1. Ensuring authenticity (ensuring history for data correction and deletion)
2. Ensuring mutual correlation (possibility to verify correlation between recorded items and items recorded in ledgers)
3. Establishing related documents (documents to identify procedural steps related to establishment and preservation of electromagnetic records)
4. Ensuring legibility (possibility to display and print out the information in a reader-friendly format)
5. Ensuring searchability (search function based on transaction date, accounting item, transaction amount etc.)
6. Providing electronic signatures and time stamps

Corporate managers shall decide whether it is possible to use cloud services after examining any possible problem from various aspects. Such aspects include ensuring authenticity and the related legal competence, method to ensure legibility, continuation of services to ensure long-term preservation based on legal requirements, operation-related issues for electronic signatures and time stamps.

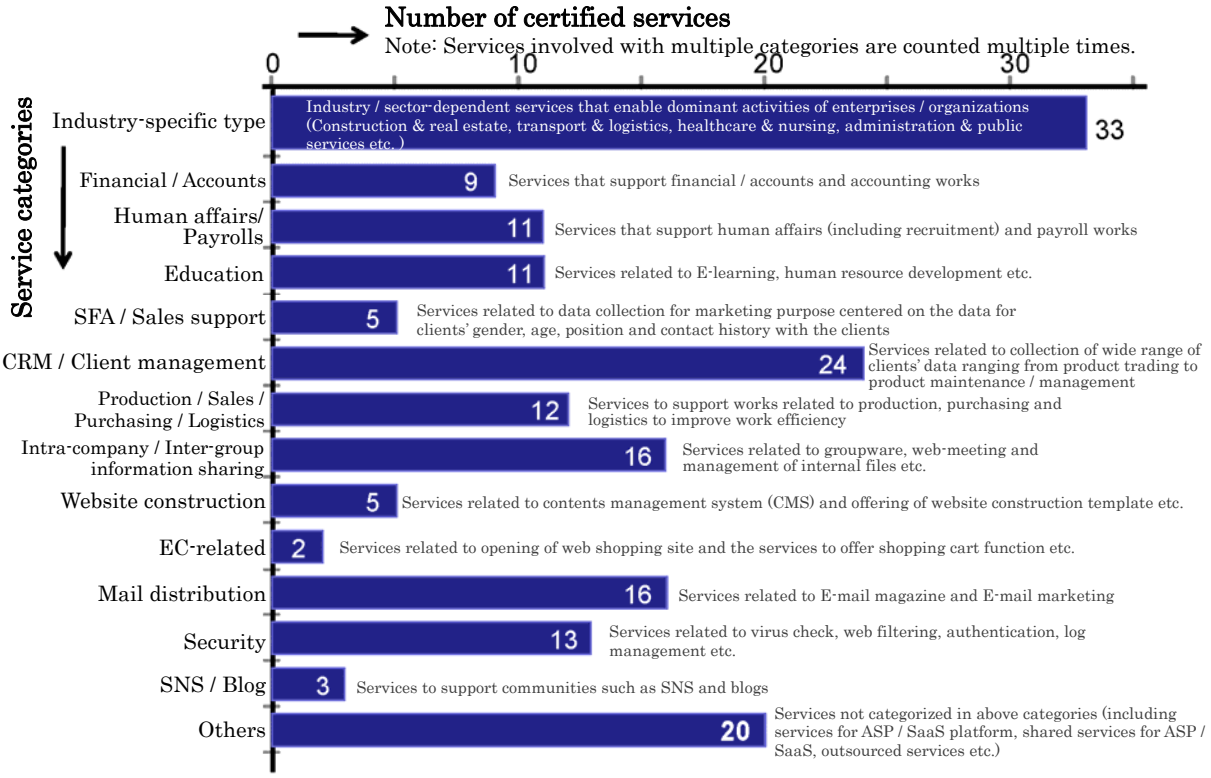
* With regard to preserving electronic documents based on the Law for Preserving Electronic Documents, we plan to expand descriptions on ensuring compliance when we revise this guide in future. This is because other government agencies approve electronic preservation of documents such as books, ledgers and drawings.

(3) Active use of ASP-SaaS Information Disclosure Certification System for Safety and Reliability
The status of information disclosure and the commitment of cloud service providers are important in collecting information to be used for making

[2] This refers to cases where a computing process is consigned to an external organization and a processing program not internally developed is used. These conditions often arise when using cloud services in general.

management decisions. In selecting an appropriate provider, it is recommendable, at least for the time being, to give priority to the qualified cloud service providers who are certified with ASP-SaaS Information Disclosure Certification for Safety and Reliability[2]. This is a system operated by the Foundation for MultiMedia Communications. The cloud services providers qualified for this certification show thorough commitment to information disclosure related to safety and reliability of the services they provide to their customers.

Currently, examinations on the Guidelines for Disclosure of Information Related to Safety and Reliability of cloud Services and certification system for this purpose are going on. We expect in future that the new guidelines and certification system will play an important role in this area.



Number of certified services for each service category in "ASP-SaaS Information Disclosure Certification System for Safety and Reliability"

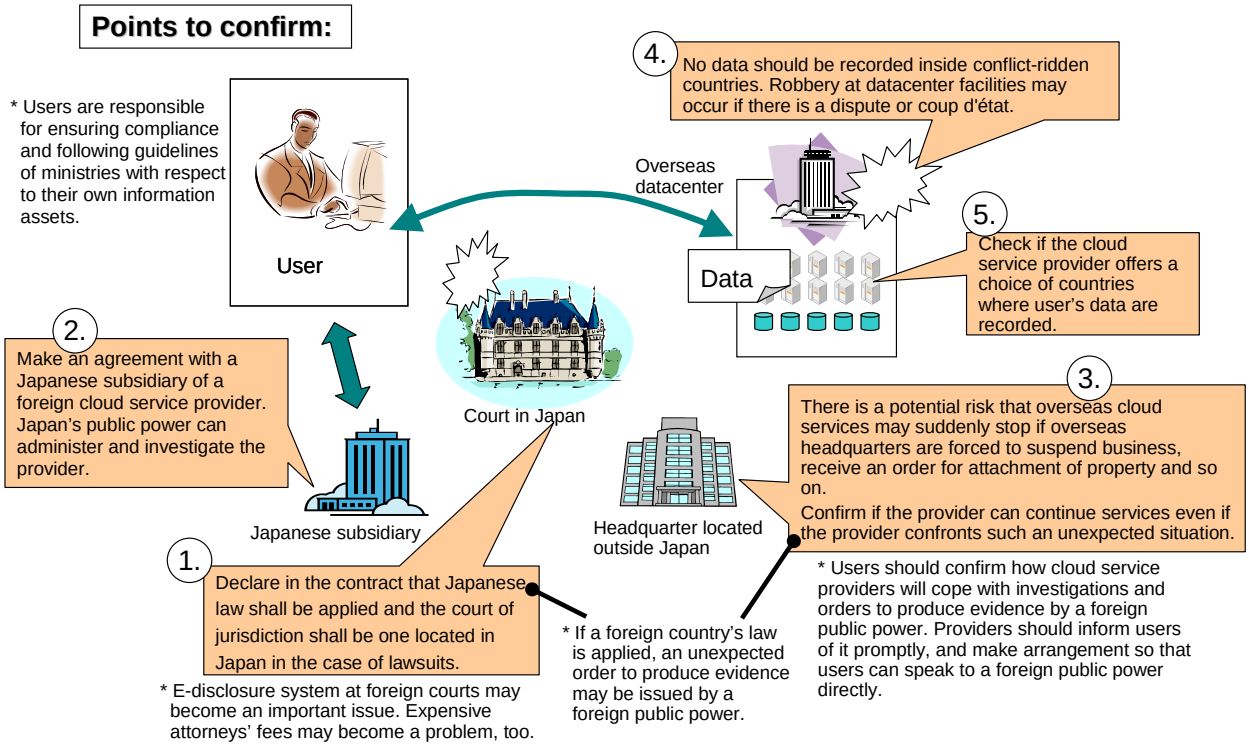
* This graph was created based on the information cited in the website for ASP and SaaS Information Disclosure Certification System for Safety and Reliability (http://www.fmmc.or.jp/asp-nintei/)

[2] http://www.fmmc.or.jp/asp-nintei/

2. Special points to confirm when users' data are recorded at overseas datacenters

It is essential to confirm which countries' laws including Japanese laws can possibly be applied to potential conflicts if cloud service users record their data in overseas datacenters or choose services of foreign providers whose headquarters are located outside of Japan.
Users are recommended to pay attention to the following points:

1. Users should include descriptions in their contracts that state Japanese law shall be applied and the court of jurisdiction shall be one located in Japan in the case of any lawsuits.
2. Users should make an agreement with a Japanese subsidiary of a foreign cloud service provider.
3. Users should confirm the way of giving notices and the ability to continue business that the foreign cloud service provider has in case there is any unexpected and unavoidable investigation by a foreign public power.
4. Users are strongly recommended not to record data inside conflict-ridden countries.



* Suppose users select a country where their data are recorded. It does not guarantee that the laws of the selected country are applied in the case of lawsuits. Users should ensure not only item 5, but also item 1.

3. Preventing an awareness gap between users and cloud services providers

There are some points requiring attention because there may be an awareness gap between users and cloud service providers when closing a contract for cloud services. As these points constitute items for special confirmation in selecting services, corporate managers shall instruct their personnel in charge of information systems to pay adequate attention to them.

(1) Split of responsibilities between users and providers in cloud services

We often observe an awareness gap between users and cloud service providers concerning split responsibilities. Corporate managers shall instruct their personnel in charge of information systems to establish a policy to prevent a gap of awareness regarding split responsibilities in terms of the following issues, particularly:

1. Operation management of networks among users, cloud service providers and communication providers
2. Management operation of OSes and computing resources
3. Operation management at application level
4. Operation management of machines and equipment installed by cloud service providers in the company's facility

(2) Points requiring attention due to a potential awareness gap between users and cloud service providers

When using a cloud service, a potential awareness gap about responsibility is often observed at a basic policy level between users and cloud service providers with regard to compliance breach risk, governance loss risk, the risk of abrupt service termination, and the risk of imperfect data deletion at service termination. The aforementioned gap may be a main factor giving rise to these risks in a conspicuous manner. As a specific countermeasure, you need to carefully listen to the position statement of cloud service providers to eliminate any awareness gap. Then, a provider and services that satisfy your policy and needs should be selected by comparing providers. There are eight essential check points as below:

1. Is there any difference in awareness for compliance obligation?
   Explanation: There may be a discrepancy at a management policy level in the attitude to security of compliance in terms of privacy information protection, non-disclosure of trade secrets and establishment and operation of internal governance between users and cloud service providers. In this case, conformance with compliance obligations requested by users in using cloud services may be compromised. It is necessary to confirm in detail the cloud service providers' attitude towards ensuring compliance with regard to the aspects considered important by your company.

2. Is there any difference in awareness concerning how to fulfill accountability in the event of a “major incident” such as leakage of private information and trade secrets?
   Explanation: Even if a major incident should occur on the cloud service provider side, user companies are often requested to play a main role in fulfilling accountability. For instance, an outflow of private information from the cloud service providers is one of these cases, when the user company received the information from its clients. In such a case, it is necessary to coordinate awareness for responsibilities between users and cloud service providers so that the user company can fulfill its accountability appropriately and make concerted efforts with the cloud service providers. Before entering into a contract, you should confirm specific actions such as contents of information and the way they are to be offered.

3. Compensation for damages and breach of operation assurance
   Explanation: There may be an awareness gap about the range of compensation for damages when a user suffers a loss attributable to the cloud service provider. For instance, the amount of compensation is usually determined as a reduction of service charge. It is essential to notice that no compensation for damages by loss of business opportunity and loss of data are assured by cloud service providers.

4. Procedure to change service contents based on a request from the cloud service provider
   Explanation: With regard to application services, the renewal of service functions are left to the discretion of cloud service providers and the users do not have to pay for the modification costs. On the other hand, a type of modification not desired by users may be conducted. Therefore, it is essential to confirm the specific procedure to be taken by cloud service providers in the renewal of service functions.

5. Procedures in the case of service termination based on a reason cited by cloud service provider
   Explanation: An abrupt termination of cloud services may have a serious impact on their users. It is necessary to choose a financially stable service provider and confirm the advance notice period before closing a contract.

6. Confirmation of the handling of users’ data and its ownership
   Explanation: A discrepancy may be observed sometimes between users and the cloud service providers with regard to awareness about ownership of the data preserved and stored within the framework of cloud service offering. Such a potential awareness gap between the parties tends to become obvious as a difference of policy for secondary use of users’ data. It is necessary to confirm the policy of cloud service providers with regard to the range of ownership of user’s data and choose the provider that can offer the policy which agrees well with user’s policy.
   * Ownership right: rights to create, modify and delete data

7. Complete deletion of users’ data
   Explanation: An awareness gap may occur between users and cloud service providers with regard to “complete deletion of users’ data.” Particularly, it is necessary to carry out thorough investigation so that there is no awareness gap about how to delete the data, and confirm whether or not the cloud service provider can offer a data deletion method acceptable to the users.

Reference 1 Glossary

In this reference, we will explain the technical terms used in this guide.

Service models

1. Infrastructure as a Service (IaaS):
   The capability provided to the user is to provide processing, storage, networks, and other fundamental computing resources where the user is able to deploy and run arbitrary software, which can include operating systems and applications.
2. Platform as a Service (PaaS):
   The capability provided to the user is to deploy onto the cloud infrastructure user-created or acquired applications created using programming languages and tools supported by the provider.
3. Application Services* (the term ASP-SaaS is used often):
   The capability provided to the user is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser.

Service deployment models

1. Private cloud:
   Cloud infrastructure is operated solely for an organization.
2. Public cloud:
   Cloud infrastructure made available to the general public or a large industry group and owned by an organization selling cloud services.
3. Hybrid cloud:
   Cloud infrastructure is a composition of a private cloud and public cloud that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability.

Other terms

1. Service Level Agreement (SLA):
   A document that describes agreements on operations management established between the user and the cloud service provider. The agreements are established for reliability and performance of services, quality of safety management, quality of customer services and so on. It is preferable to describe necessary and sufficient agreements on SLA documents so as to keep charges affordable.

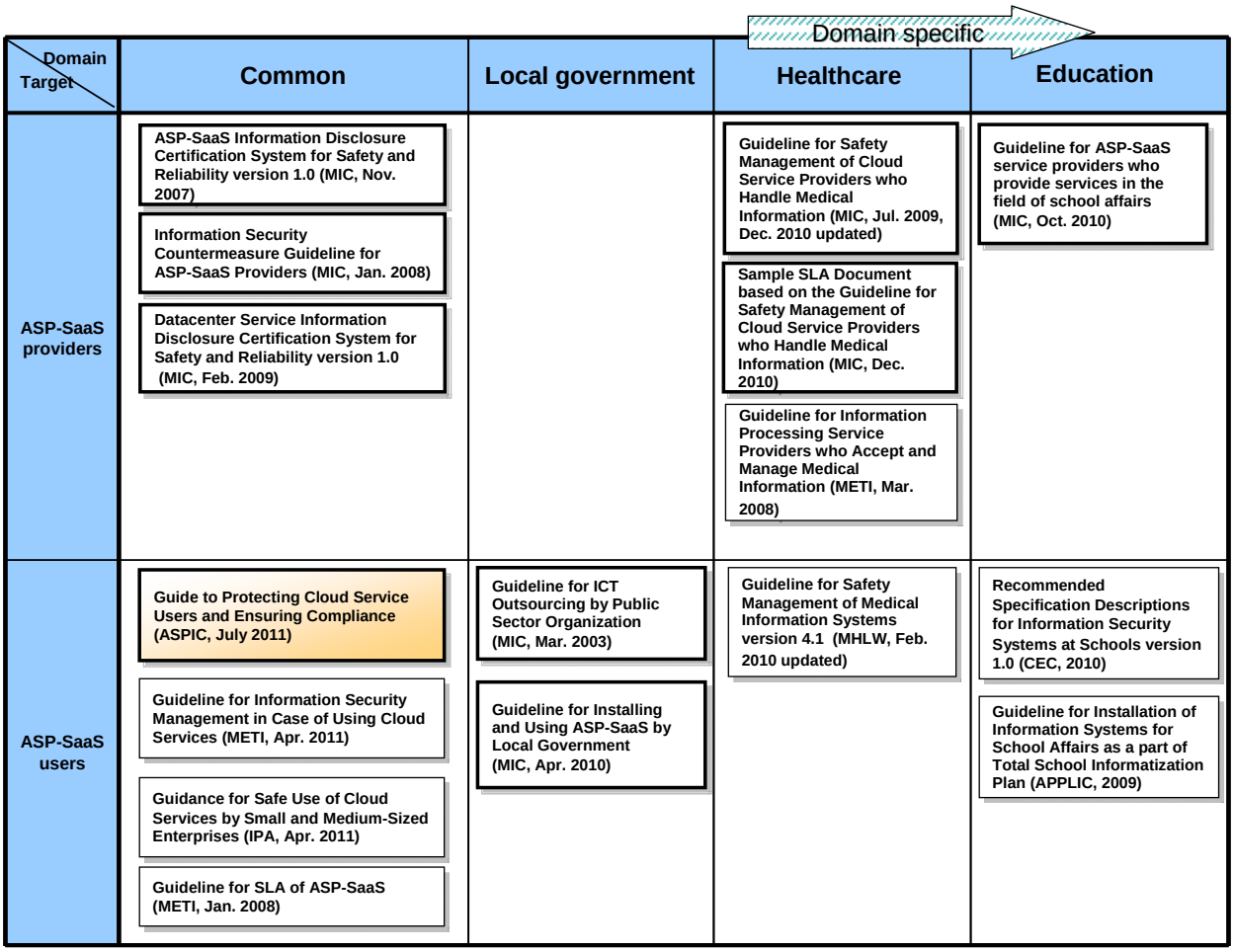
Explanations on important risks related to cloud services

A cloud service is a technically advanced implementation of IT outsourcing. Public cloud services have the following risks because of the black-boxed feature of these services. Especially, risks related to loss of governance, compliance violation, incomplete deletion of users' data upon end of use and risks that emerge when users record their data at overseas datacenters are considered to be important.

Cause of risks	Actual consequence by this risk
Loss of governance	- Loss of fine risk control - Black-boxed operations and resources - Difficult to cope with digital forensics - Difficult to make SLA - Inadequate information disclosure by cloud service providers in case of critical incidents etc.
Compliance violation	- It becomes difficult to manage and control cloud service providers adequately and appropriately to maintain compliance because of the loss of governance over cloud service providers. - It may be hard for cloud service users to verify and prove that they maintain compliance via a third party's audit if cloud service providers do not disclose the necessary information.
Reconsignment	Cloud service providers do not properly manage and control recommissioning service providers.
Sudden termination of services	Cloud services may suddenly be terminated due to bankruptcy of cloud service providers, M&As of cloud service providers, and so on.
Vendor lock-in	Users may be locked in by cloud service providers because of the difficulty of migrating data to other cloud services.
Incomplete deletion of users' data upon end of use	Cloud service providers may not delete users' data completely upon end of use.
Users record their data at overseas datacenters	- It becomes difficult to determine which country's law is applied in order to resolve conflicts between users and cloud service providers. - Unexpected data disclosure by forced producing of evidence or e-disclosure may happen due to foreign country's public power. - Robbery at datacenter's facilities may happen due to a disturbance or coup d'etat. - Technological information may illegally flow out to foreign countries.

Reference 2 Guidelines related to cloud services

Whole picture: This guide is colored.



Guidelines for ASP-SaaS users

1. Guideline for Installing and Using ASP-SaaS by Local Government (MIC): April 2010

This guideline describes points requiring attention when local governments install and use ASP-SaaS.

2. Guideline for SLA of ASP-SaaS (METI): January 2008

This guideline describes important characteristics of ASP-SaaS from the viewpoint of information security management. Such management is necessary for enterprise management and IT division employees to well understand the points of information security requiring attention, establish appropriate agreement and eventually use ASP-SaaS safely. This guideline should help enterprises to better select ASP-SaaS providers and services and appropriately establish SLAs.

Guidelines for cloud service users

1. Guideline for Information Security Management when using Cloud Services (METI): April 2011

This guideline describes the following three issues by assuming that cloud services are extensively used by users:

1. Risk controls that users should implement
2. Service level and security management that users should request to cloud service providers
3. Recommended information security management systems

This Guideline updates risk controls of JIS Q 27002* in order for organizations that use cloud services to smoothly implement adequate information security countermeasures based on this document.
* Code of practice for information security management

2. Guidance for Safe Use of cloud Services by Small and Medium-Sized Enterprise (IPA): April 2011

This Guidance describes recommendations and check items so that small and medium-sized enterprises can easily decide to use cloud services, verify adequacy of terms of service and confirm important reminders related to information security.

Reference 3 Data related to users' rights and compliance

This section indicates guidelines set by government agencies cited in this guide with regard to users' rights and compliance.

Note: This reference does not show comprehensive data of the guidelines formulated by government agencies. If there are any regulations or guidelines that are observed by your company other than those mentioned below, they should be added in your operation.

Guidelines for users' rights

■ METI Protection of trade secrets by Unfair Competition Prevention Act

Name	Announcement and review (latest one only)	Competent authority or issuing party
Trade Secrets Management Guidelines Chapter 2 1. Definition of trade secrets Chapter 3 2. Secret management method recommended to implement management of trade secrets 3. Status of organizational management recommended to implement appropriate functioning of trade secret management	April 2010	METI

* There is no description that clearly refers to the consignment of system services to external parties. If cloud services are used, the focus will be on whether or not the trade secrets preserved on provider's side should satisfy the requirements shown in the definition of trade secrets.

Guidelines for security of users' compliance

- MOJ/FSA Internal governance of large corporations (companies with a board of directors and listed enterprises)

Name	Announcement and review (latest one only)	Competent authority or issuing party
Ordinance for the Enforcement of the Companies Act (System to ensure appropriate operation) Article 100-1	March 2009	MOJ
Standard for evaluation of internal governance and audit for financial reports I. 2. (6) Measures devised to deal with IT	February 2007	FSA
Enforcement standard on evaluation of governance and audit for financial reports II. 3. (3) (e) Evaluation of internal governance by using IT (4) (c) Judgment on effectiveness of internal governance relating to IT	February 2007	FSA

* COSO framework and such like are useful references with respect to the details of IT governance and measures to be taken when consigning to external parties.

- Each government agency

  Guidelines related to protection of private information[3]: Requirements for consignment to external parties are clearly described.

1. Health insurance and welfare

Name	Announcement and review (latest one only)	Competent authority or issuing party
Guidelines for Appropriate Handling of Private information in Health Insurance Associations etc. (Director's notification) III. 4. (3) Handling in the case of consignment of services	December 2004	MHLW
Guidelines for Appropriate Handling of Private information in National Health Insurance Associations etc. (Director's notification) III. 4. (3) Handling in the case of consignment of services	December 2004	MHLW
Guidelines for Appropriate Handling of Private information in the Federation of National Health Insurance Associations etc. (Director's notification) III. 4. (3) Handling in the case of consignment of services	September 2005	MHLW
Guidelines for Appropriate Handling of Private information by Welfare Service Business Providers (Director's notification) III. 4. (3) Handling in the case of consignment of services	November 2004	MHLW

[3] CAA: http://www.caa.go.jp/seikatsu/kojin/gaidorainkentou.html

2. Broadcast and postal area

Name	Announcement and review (latest one only)	Competent authority or issuing party
Guidelines for Protection of Private information of Broadcast Recipients (Notice) (Supervision of data consignees) Article 16, Article 17	September 2009	MIC
Guidelines for Protection of Private information in Postal Business Area (Notice) (Supervision of data consignees) Article 11	March 2008	MIC
Guidelines for Protection of Private information in Correspondence Delivery Business Area (Notice) (Supervision of data consignees) Article 11	March 2008	MIC

3. Economy and industry

Name	Announcement and review (latest one only)	Competent authority or issuing party
Guidelines for Laws on Private information Protection in Economy and Industry Area (Notice) 2-2-3-4. Supervision of data consignees (Related to Article 22)	October 2009	METI

4. Employment management

Name	Announcement and review (latest one only)	Competent authority or issuing party
Guidelines for Countermeasures by Providers to Secure Appropriate Handling of Private information Related to Employment Management (Notice) No. 3 “4. Matters on supervision of data consignees” defined in Articles 22.	July 2004	MHLW

5. Legal issues

Name	Announcement and review (latest one only)	Competent authority or issuing party
Guidelines for Protection of Private information in Operations under Jurisdiction of MOJ (Notice) No. 6 Responsibilities Related to Management of Privacy Data, 4 Supervision of data consignees (Related to Article 22)	September 2009	MOJ
Guideline for Protection of Private information in debt management and collection industry area No. 7 Responsibilities for management of personal data, 4 Supervision of data consignees (Related to Article 22)	March 2010	MOJ

6. Corporate pensions

Name	Announcement and review (latest one only)	Competent authority or issuing party
Handling of Private information Related to Corporate Pension etc. (Director’s notification)	October 2004	MHLW

No. 5 Matters related to supervision of data consignees		

7. Foreign affairs

Name	Announcement and review (latest one only)	Competent authority or issuing party
Guidelines for Protection of Private information Handled by Providers in Services under the Jurisdiction of MOFA (Notice) (Countermeasures for consignment of personal data) Article 11	March 2005	MOFA

8. Financial matters

Name	Announcement and review (latest one only)	Competent authority or issuing party
Guidelines for Protection of Private information in Area under the Jurisdiction of MOF (Notice) (Supervision of data consignees) Article 13	March 2010	MOF

9. Agriculture, forestry and fisheries

Name	Announcement and review (latest one only)	Competent authority or issuing party
Guidelines for Protection of Private information in Agriculture, Forestry and Fisheries area (Notice) No.6 5. Supervision of data consignees (Related to Article 22)	July 2009	MHLW

10. Land and transport

Name	Announcement and review (latest one only)	Competent authority or issuing party
Guidelines for Protection of Private information in Area under the Jurisdiction of MLIT (Notice) (Supervision of data consignees) Article 11	December 2004	MLIT

11. The environment

Name	Announcement and review (the latest only)	Competent authority or issuing party
Guidelines for Protection of Private information in Operations under the Jurisdiction of MOE (Notice) No. 6 “4. Supervision of data consignees” (Related to Article 22)	December 2009	MOE

■ METI　Prevention of outflow of technological information

Name	Announcement and review (latest one only)	Competent authority or issuing party
Guidelines to prevent flow-out of technological information I. 2. (2) “Unintended flow-out of technology” II. 5. Flow-out of technology through flow-out of drawings and knowhow necessary for manufacturing III. 4. 6. Considerations to prevent flow-out of technology through flow-out of drawings and knowhow necessary for manufacturing (p. 22)	March 2003	METI

* See separate table of Export Trade Control Ordinance[4] for the scope of technologies for which flow-out is prohibited.

■ MOF　Preservation of National Tax Records in Electronic Form

Name	Announcement and review (latest one only)	Competent authority or issuing party
Rules for the Enforcement of Corporate Tax “Limitation on place of preservation” (Filing and Preservation for Books and Documents of Consolidated Corporations) Article 8, 3–10 (Filing and Preservation for Books and Documents) Article 59 (Filing and Preservation for Books and Documents etc.) Article 67 * Reference: Law Concerning Preservation of National Tax Records in Electronic Form and Rules for the Enforcement of Law Concerning Preservation of National Tax Records in Electronic Form (MOF) stipulate provisions with regard to preservation of books in electronic form[5].	October 2010	MOF
MFJ Ordinance No.1 dated January 31, 2005: Ordinance for Partial Revision of Rules for the Enforcement of Law Concerning Preservation of National Tax Records in Electronic Form “Presentation of requirements for preservation etc.”	January 2005	MOF

[4] http://www.kyushu.meti.go.jp/seisaku/boueki/bouekikanri/yushutsurei.html
[5] http://www.nta.go.jp/taxanswer/hojin/5930.htm