

**Guide to Safe Use of
Cloud Services**

for

**Small-to-Mid-Sized
Enterprises**

April 2011

**Information-technology Promotion Agency,
Japan (IPA)**

Guide to Safe Use of Cloud Services for SMEs

Introduction

Cloud computing is drawing attention these days. By taking advantage of this technology, enterprises may be able to make use of IT at a lower cost and/or in a more advanced way. Cloud computing holds real promise for advancing the utilization of IT, especially by small-to-mid-sized enterprises (SMEs) that have not been able to utilize IT sufficiently or feel somewhat burdened by owning and operating IT.

However, SMEs may have difficulty in understanding what the cloud is and how to utilize it, and in some cases the negative effects of improper use of the cloud may outweigh the advantages.

This guide is intended to provide support for decision making, defining conditions and checking precautions points regarding the use of cloud, and contains referential explanations and a check list.

It is expected that people in SMEs will make good use of this guide in using the cloud properly and safely, taking the advantage of effective use of IT in corporate management, and improve IT security levels.

Please note the followings when using this guide:

- This guide assumes that enterprises are already utilizing IT to some extent¹.
- The check list assumes the use of Software as a Service (SaaS) as the type of cloud service. Other checks and cautions may be necessary when using PaaS or IaaS. If it is the case, we recommend that the enterprise consults other references and/or an expert (for definitions of SaaS, PaaS, and IaaS, see footnote 2).
- The target audience of this guide is the executive level of SMEs. In case an IT department should be involved, the managers and the staffs can also depend on this guide. While some minor matters can be decided within the IT department without involving executives, it is supposed that corporate executives should be involved in judging the use of cloud.

¹ This guideline basically assumes that the user SME is at Stage 2 in "IT Management Maturity Index" defined by Ministry of Economy, Trade, and Industry (METI), and also supports some of the enterprises at Stage 1 close to Stage 2.

1. Cloud Computing

● Definitions of Cloud Computing and Cloud Services

Cloud computing is a general term that refers to a model in which computing capabilities², provided by a large-scale data center equipped with various technologies such as virtualization, are used freely and flexibly via the Internet. It is drawing attention for its technologies and services that reduce various types of IT-related burdens ranging from development and procurement to operation and maintenance and associated costs compared with the cases that companies and individuals own and use their respective computers and applications.

Cloud services can be defined as a set of IT functions provided to users in a form of services using cloud computing. We shall refer to "services by cloud computing" as "cloud services" throughout this document. Also, we shall refer to those businesses rendering cloud services as "cloud service providers".

● Benefits of Using Cloud Services for SMEs

Cloud services are believed to provide the following benefits by converting the "IT in possession" to "IT in use":

- (a) Elimination or mitigation of IT-related procurement load
 - Finalizing specifications, procurement, installation or configuration of servers, storage devices and network equipment
 - Development and procurement of application software
 - Capacity enhancement to accommodate increased process volume
 - Renewal of facilities and systems
 - Initial cost and capital investment regarding above
- (b) Elimination or mitigation of IT-related operation and maintenance load
 - Operation, periodic maintenance and troubleshooting of IT facilities and systems
 - Updating, patching, troubleshooting, upgrading and license management of operating systems and application programs
 - Onsite support, help desk support and account management of in-house users
 - Communication and negotiation with vendors in relation to

² "Computing capabilities" are provided in variety of levels and forms. IaaS (Infrastructure as a Service) provides information system infrastructure such as hardware, network, and operating systems, PaaS (Platform as a Service) provides running environments for applications, and SaaS (Software as a Service) provides the applications themselves. Besides these, providing an X service via a network is sometimes called as XaaS (X as a Service).

above-mentioned items

(c) Attainment of flexibility and scalability in using IT resources

- IT usage can be scaled up and down aligning to the increase or decrease of process or use volume: In contrast, IT in possession must prepare the capacity enough to handle peak usages. There is virtually no way to shape down to align to decrease in workload.
- Capacity reinforcement can be flexibly implemented to accommodate sharp changes of load (No lead time is required to upscale facilities)

(d) Elimination or mitigation of implementation of IT security measures

- Reduction of burden in setting and changing firewall configurations or in monitoring unauthorized access
- Reduction of burden for servers in implementing antimalware measures, updating operating systems or applying security patches in a timely manner
- Reduction of burden in filtering spam emails and virus-infected emails

• **Elements to be cautious on when Using Cloud Services**

Despite the advantages, there are some elements to be cautious about the use of cloud services.

(a) Limitations that arise from not administering computer systems in-house

- Choice of time for maintenance
- Control of recovery processes in case of failure
- Limited choice of features

(b) Limitations and discomfort about allowing data to be outside corporate control or entrusting data to a third party

- Difficulty in controlling and assuring the integrity and availability of data in case of failure
- Difficulty in imposing controls on subcontractors to conform to the requirements to control subcontractors

(c) Risk of rapid rise in usage fees due to abnormal or unexpected increase in use and process volume

(d) Limitations on customizing provided applications

(e) Limitations or associated cost increases in data correlations between applications

In consideration of these elements to be cautious on, the decision to use cloud services must be made after implementing risk assessments, appropriate countermeasures and preparations, on top of comprehensive evaluation of

current status of the enterprise and the information about the cloud service providers.

2. Examples of Utilization of Cloud Services

Cloud services can be accessed and used via the Internet from highly capable terminals such as PCs and smartphones. Since many services are provided by a variety of cloud service providers, enterprises can choose the services that best match their needs, and utilize them for corporate needs such as business improvement. Fees are generally scaled according to the time or volume used, while some services apply monthly or annual flat rates.

The fastest way to understand cloud services is to actually try them out. Cloud service providers often provide a trial period, a free version for a small number of users, or a limited-feature free edition. Enterprise applications are often difficult to evaluate unless actually used. Therefore, we recommend that enterprises do not hesitate to ask cloud service providers about trial use.

In the following sections, we introduce several types of cloud services as example use cases.

2.1 Email

One that is relatively easy to implement among cloud services is an email service. By not owning in-house email servers, enterprises can mitigate equipment cost, and by outsourcing administration and operation of the service, they can also keep system administration burdens in check. In addition, since security measures such as spam filtering and virus check are often provided at the cloud service side, they can reduce or eliminate the burdens of these types of security measures as well.

Furthermore, as long as Internet access is provided, users can utilize the same email environment from anywhere in the world. This improves work mobility. If local copies are not kept at the local PCs or devices, the risk of data loss or leaks is also mitigated.

2.2 Management Applications

Applications for management tasks such as financial accounting, tax calculation, payrolls, HR management and customer relations management can also be delivered as cloud services. Since cloud services do not need dedicated servers or terminals, or installation and update of software, the initial investment and maintenance costs for such servers and software are eliminated as well. Because cloud application services can be used from Web browsers with easy configuration, applications are accessible from more variety of terminals and locations, and that will improve operational efficiency.

The threshold for IT-based corporate management is expected to become much

lower for those SMEs who used to be prevented from adopting IT to business management tasks because of the burdens of owning or maintaining their own IT systems.

2.3 Office Software

Some cloud services provide features of office software (also called office applications or desktop applications). By introducing such services, employees can simply enjoy the functions of general office applications such as email, word processing, and spreadsheets, or the applications to help automate information sharing and communication in the office such as groupware and sales process management tools, without the need to install applications on local computers.

This eases the workload and cost of installing application software on individual computers or setting up a server to share information. In some cases, it may also result in reduction of software license fees.

Further, updates and security patches are applied at the cloud service side, so users can comfortably and readily use the applications.

Finally, by having files created by office software stored on the cloud, the file sharing and collaboration can be easily accomplished among staffs, and even across divisions.

3. Have you ever encountered with the expectations and challenges as...?

SMEs often have expectations or challenges about utilizing IT in corporate management or facilitating IT-equipped management, which are listed below. Some of them may apply to your enterprise and in such a case they may be realized or solved by employing cloud services.

First let's see what kinds of cloud services are available and what they can do. You can also consult a professional such as a consultant, an IT coordinator, or a systems integrator. When doing so, it is important to explain your expectations and concerns in detail.

<Operation Efficiency>

- Reduce indirect cost by increasing the efficiency of processing by IT
- Aggregate information severally stored across the enterprise to make more effective use of information
- Increase the IT-equipped rate of managerial and indirect works to improve operational efficiency
- Use email and scheduling software from outside the enterprise as well

<IT Cost>

- Reduce cost (human resources and workload) of IT operation, maintenance and administration
- Lighten the operation workload of dedicated in-house servers
- Utilize state-of-the-art IT without hiring dedicated employees
- Maintain and improve information security without extra work
- Use up-to-date software without the need to perform software updates
- Reduce backup workload and cost

<Leveraging IT in the Business>

- Quickly and inexpensively start a new service business exploiting IT
- Enhance and expand the current IT-based business with a small amount of investment
- Make corporate management and business processing equipped with IT

- Introduce IT into order processing, customer relations management, and sales process management (e.g., SCM³, CRM⁴, or SFA⁵)
- Share information between allied enterprises and explore unknown value added and new services

³ Supply Chain Management

⁴ Customer Relationship Management

⁵ Sales Force Automation

4. Let's Check it out Before Introducing a Cloud Service

Introducing a cloud service could change the way IT is used in your enterprise. As a result, the ways to utilize IT in offices, the fashions to handle and store data, or the methods to correlate data between processes could be affected.

Before introducing cloud services consider the various aspects of the service and prepare conditions for effective use. This is necessary to use cloud services safely and effectively.

Prior to introducing cloud services, the effects of the move should be studied by both sides of executive management or those involved in business administration and those in charge of IT who actually will administer the use of cloud services. In this section the minimum items that should be pre-evaluated are listed in the following three areas:

[A] Scope of use of cloud services (four items)

[B] Preparing to use cloud services (four items)

[C] Conditions of cloud services to be provided (six items)

We recommend that enterprises use the check sheet in the appendix to confirm necessary evaluation conferring to the following explanations.

The items of the check sheet that are not marked OK may introduce security or other risks to implementation and utilization of cloud services. Thoroughly evaluate whether the possible risks associated with such items are acceptable or tolerable (whether there is a danger that a severe inefficiency is imposed over corporate management or business operations).

[A] Scope of use of cloud services

No.	Check item	Description
(1)	Clarification of scope of usage	Have you examined what operation and data are to be handled by cloud services? Have you analyzed and set divisions of operations? Have you set operation rules?
(2)	Types and costs of services	Does the cloud service you are considering properly match your operational needs, and have you checked the cost?
(3)	Importance of handled information	Have you checked the level of the information classification handled by the cloud service?

(4)	Integrity with policies and regulations	Will conflicts or inconsistency arise between usage of the cloud service and the security policies?
-----	---	---

(1) Have you examined what operation and data are to be handled by cloud services? Have you analyzed and set divisions of operations? Have you set operation rules?

First you must decide what operations should be migrated to cloud services, and to what extent. Evaluate what workload is occurring in what operations in-house, and compare them with the services and costs examined in item (2) below. Based on this information, decide the scope of the operation that you want to migrate to the cloud service and the types and scope of information that should be handled by the service.

During this step, you must clarify the issues that could arise when a cloud service is introduced. For example, is it possible to extract a specific part of a process handled by IT and transfer it to another system? Will there be any issues regarding interconnections to other existing systems or processes in doing so? Consider the effects of introducing cloud services on existing operations and systems.

It is a good idea to begin using cloud services on a limited scale, such as for email or secure storage. It is worth thinking to limit the use of cloud services to a certain extent so that critical information (personal or secret information) is not entrusted to a third party.

(2) Does the cloud service you are considering properly match your operational needs, and have you checked the cost?

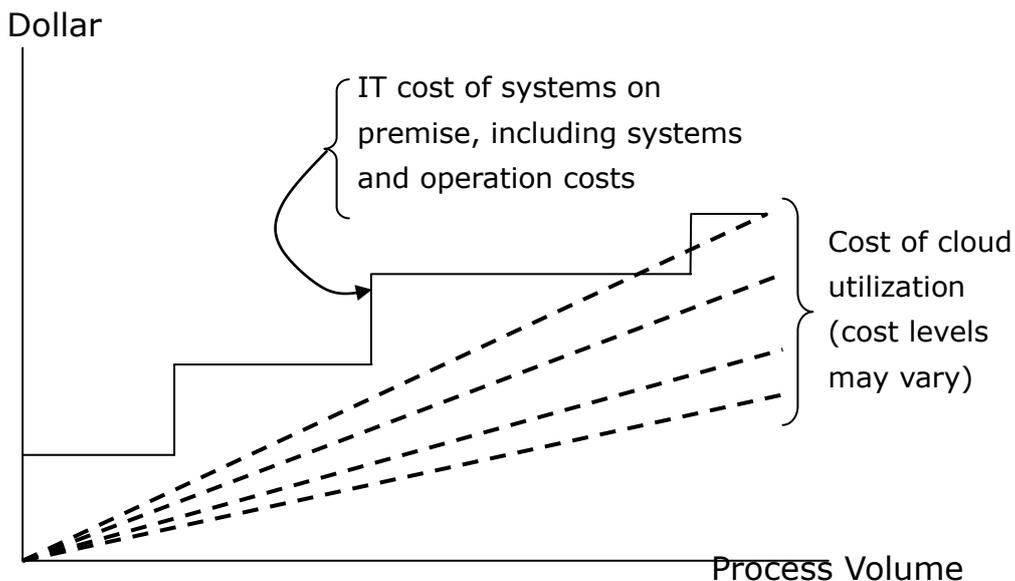
Many services are provided by a variety of cloud service providers. Examine services and features, compare and comprehend them in order to choose the service that is most appropriate for your business.

Examples of Cloud Services
 Financing, accounting, HR management, payroll, tax filings, groupware, security measures, sales management, project management, internet banking, social insurance processes, customer relations management, purchase and inventory management, CAD, data distribution, data management, energy-saving management, email, office applications, etc.

Estimate the cost of introduction and operation of the cloud service and examine the benefits of the cloud. One idea is to compare the required costs of all relevant

elements to obtain the same results. If dedicated or partially-assigned IT administration and operation staff can be eliminated, or IT assets can be eliminated, cost advantages will increase. Another effective method is to migrate to the cloud services when you are due to replace one or more servers.

In addition to the cost of introduction, it is also necessary to consider the monthly operation cost, including indirect expenses. Also, simulate the possible increase in cost that could arise when the scale of use is expanded in the future.



Example of cost simulation for a cloud service

The relationship between on-premises IT cost and cloud utilization cost can be roughly expressed by the model shown in the above figure.

(3) Have you checked the level of the information classification handled by the cloud service?

When handling information related to privacy or trade secrets on a cloud service, appropriate management is required. Examine whether or not there will be an issue in handling the information in a cloud service in view of classification and criticalness of the information.

Examine whether or not the information can be entrusted outside. For example, when handling personal information on a cloud service, under the Personal Information Protection Act of Japan, you may have an obligation to appropriately supervise the subcontractor.

Regarding the criticalness of information, evaluate the potential damage to the

enterprise when the information is lost. The potential damage to enterprise may be as significant to corporate operation as loss of competitiveness, loss of customers, destruction of corporate trust, bank deposit fraud, and loss of operation management information.

(4) Will conflicts or inconsistency arise between usage of the cloud service and the security policies?

If corporate security policies and rules prohibit storing data outside the enterprise premise, or there are limitations on outsourcing, it may be difficult to use cloud services. If your company has policies or rules that consists such prohibition or limitation, but you are confident it is worth utilizing a cloud service even by changing such policies or rules, it is recommended that you review them so that you can entrust data to a cloud service provider and retain the state that there is no conflict between the policies and rules and actual state of IT usage.

When making these kinds of judgment, make sure that the possible disadvantages associated with the use of cloud services are within the acceptable range of your business. Make sure to employ and utilize cloud services only after evaluating the advantages of entrusting data or information processes outside the enterprise in comparison with the acceptable range of risk associated with such use.

[B] Preparing to use cloud services

No.	Check item	Description
(5)	Cloud Use Administrator	Have you secured a cloud use administrator who understands the characteristics of cloud services?
(6)	User Management	Can the user management of cloud services be implemented appropriately?
(7)	Passwords	Can you appropriately perform setting and management of passwords?
(8)	Data backup	Are you prepared to secure in hand and make available important information in case the service is discontinued?

(5) Have you secured a cloud use administrator who understands the characteristics of cloud services?

You will need at least one cloud use administrator, who will be in charge of

operations related to cloud services (the assignment need not be a dedicated one but can be an extra to another task). Secure a cloud use administrator for cloud services within your company (an employee who is familiar with IT utilization is likely to be suitable).

Under the direction and supervision of the IT administration manager, the cloud use administrator is responsible for setting several configurations, which is identical to ordinary IT admin staff, for use of cloud services. The job description will typically include the followings:

- (a) Register and delete user accounts (specify cloud service settings as to who can do what processes of an operation in compliance with corporate policies)
- (b) Prepare operation manuals and provide instruction about using the cloud service
- (c) Serve as a help desk for cloud service users
- (d) Perform regular backup of data stored in cloud services
- (e) Communications and negotiations with the cloud service providers and preparation and implementation of workarounds as needed, in case of cloud service failures
- (f) Adjust service usage per increase/decrease of the process volume under cloud services

It is also recommended to secure a resource to consult⁶ outside the enterprise in case of a difficulty in judgment within the company.

(6) Can the user management of cloud services be implemented appropriately?
--

Appropriate user administration is requisite for the use of cloud services. User administration refers to managing users who utilize the cloud for their businesses, by setting authorizations and other attributes for them. The followings should be implemented and/or set:

- (a) For each cloud service operation, register employees who are permitted to use the service and prevent others from accessing the service (access control).
- (b) For each of the cloud service users, specify what operation or processing on what job or data is allowed (authorization management).
- (c) For each of the cloud service users, prepare a set of ID and password (i.e. user account). (Sharing one account among multiple users should result

⁶ Possible candidates are consultants (such as IT coordinators), professionals (such as tax accountants), and sales representatives of IT or office equipment.

in incidental processing without authorization or ambiguity in accountability tracing.)

To regularly supervise that utilization and operations are done according to the rules, prepare an administrator account as well. Grant the administrator privilege only to the persons who need it.

(7) Can you appropriately perform setting and management of passwords?

Passwords of cloud service users must be those that are not easily guessed or figured out by others. In addition, passwords must be managed appropriately in such way as periodically changing to prevent abuse by someone else with impersonation .

If a user forgets the password, he or she will not be able to access the cloud service. This causes suspension of business or disabled access to required data. For this reason, it is important to provide measures so that passwords are never forgotten or lost⁷, and to prepare a method to recover passwords⁸.

Most cloud service providers are supposed to provide a mechanism to reset passwords in case users happen to be unable to recall passwords. Check in advance whether such a mechanism is provided. If yes, check the details, including who is able to send the password reset request and whom it is to be addressed, how the requester authentication is implemented, and whether the requests are only accepted from the persons duly registered in advance. If anyone can reset passwords, there is a risk of a privilege breach or impersonation.

Another checkpoint is the lead time. For example, if the reset request can only be accepted via a postal mail, the lead time will be longer. In this case, it will be important to provide alternatives or workaround to prevent trouble within that period.

(8) Are you prepared to secure in hand and make available important information in case the service is discontinued?

It is suggested to periodically make a copy of important data stored in the cloud. This work is called "archiving". We recommend duplicating data to a location outside the cloud service at appropriate intervals so that business can continue or

⁷ One idea is to log the passwords based on a certain rule, and assign someone other than the users to store the data in a separate place based on the rule.

⁸ One idea is to generate passwords using a specific method and a specific parameter (such as a combination of specific numbers), and keep the method and the parameter separately.

be quickly resumed should the data stored in the cloud service be lost. For example, upon completion of daily sales processing, sales ledger will be copied to an in-house server, or backed up to tape or DVD and stored in a warehouse. It is suggested to prepare a scheme where data duplication work is appropriately carried out or operated.

Cloud service providers generally provide automated backup as a standard feature. It is supposed that users may not need to perform frequent backups in daily business activities. Subject to certain backup services by cloud service providers to be confirmed, the user backup (creating a local copy, or archiving) effort can be limited to the level to prepare for very occasional cases.

[C] Conditions of cloud services to be provided

No.	Check item	Description
(9)	Reliability of Service Provider	Is the cloud service provider reliable?
(10)	Reliability of Service	Are the service levels indicated in such way of uptime rate of services, frequency of failures and target time to recover in case of failures?
(11)	Security Measures	Are detailed security measures for the cloud service disclosed?
(12)	User Support	Is assistance (help desk support and FAQs) provided when users cannot see how to use the service?
(13)	Securing data at the Term of Use	Check the conditions how the data will be disposed after termination of cloud service use.
(14)	Check Contract Terms	Check general terms of the contract.

(9) Is the cloud service provider reliable?

Check that the management of the cloud service provider is stable, and the service is likely to be provided for the long term. Evaluating corporate management tends to be difficult, but the following information may give some reference to support your judgment.

Note: These items are only meant for reference. It is not a requirement that these conditions be met, and meeting these conditions does not necessarily mean that the provider is reliable. On the other hand, new cloud service providers or new services may enter into market with high

and appreciable value. Having a perspective to make effective and safe use of these services is as important as depending on establishments.

- (a) Is the provider public on stock market? The public enterprises are subject to inspection to its corporate management and are obligated to disclose relevant information periodically.
- (b) How long has the provider been doing business? Running business for a long period of time constitutes indication of stability and continuity.
- (c) Does the service have many users? Being used by many users generally mean higher reliability. It further helps if you can specifically know who are using the service. (If you have a chance to talk to actual users of the cloud service, confirm whether they have a negative valuation on the service in terms of ease of use, effect on investment, occurrence of failures and measures taken in case of failure.)
- (d) Do you frequently hear news about failures? Is the provider taking appropriate measures in case of failure?
- (e) In some cases the service is distributed by a reliable system integrator or IT distributor. If a reliable and proven enterprise recommends and resells the service, it can be assumed to be reliable to some extent.
- (f) Some cloud services are provided on a platform provided by a large cloud service provider. (Computer manufacturers and communication carriers also provide cloud services.) In this case, the security and reliability of the platform cloud service, such as availability and tolerance against attacks, are generally high.

(10) Are the service levels indicated in such way of uptime rate of services, frequency of failures and target time to recover in case of failures?

Cloud services are sometimes suspended due to maintenance or failures, with or without a prior announcement. Policies for, and measures against such service suspensions are often described in a document such as the Service Level Agreement (SLA). Make sure about the followings:

- (a) For service suspension with prior notice, make sure that sufficient lead time of notice is ensured, that manner of notice is sufficient to ensure the notice is given in advance, and that there is no possibility of inconvenience.
- (b) Though it may be difficult to give prior notice or forecast of sudden failures, check with the cloud service provider regarding how the provider will contact you when a trouble occurs in the cloud services. It is

important as well that immediate notice upon a trouble is implemented.

- (c) Regarding unexpected failures, some cloud service providers provide information such as the frequency of faults estimated logically or statistically, and the target time to recover. Such information is often aggregated and shown as "uptime rate guarantee".

If an uptime rate guarantee is provided, check the basis of the rate (typically, it is provided on a monthly basis). If an annual denomination is used, even 0.1% downtime can logically mean 8 hours and 45 minutes of continued service suspension.

Note that the uptime rate guarantee is sometimes simply referred to as an SLA.

- (d) In addition, uptime rate guarantee is generally provided in a manner of commitment to compensate some damage in case the duration of service suspension exceeds the guarantee. It is to be noted that there is no guarantee of service availability as indicated as "uptime rate guarantee." To protect against unexpectedly prolonged service suspension, preparation by implementing a local backup or archiving, as described in item (8) above, is recommended.

- (e) Some cloud service providers provide a screen, often called a dashboard, to provide information about current operation and trouble status of the cloud in real time. It can be expected that such cloud service provider has high level of management to ensure service operation. It is also helpful and comfortable for you to be able to observe operating conditions from time to time.

(11) Are detailed security measures for the cloud service disclosed?

In most cases cloud service providers make explanations on their security measures available on their web sites. They may also publish annual reports (which often takes the form of Information Security Reports or CSR Reports) or security white papers (reports).

Check that the cloud service provider provides explanations on following items of security measures on the website or otherwise:

- (a) Security Controls on the Systems
- Timely application of updates, security patches and service packs on operating systems and application programs
 - Measures to ensure system availability and reliability (such as multiplexing or redundancy of servers, storage, and networks, and automated backups)

- (b) Security Controls on the Data Management
 - Automated encryption or provisioning of encryption features
 - Automatic backup by the cloud service provider (including intervals, generations, recovery steps, term of preservation, etc.)
- (c) Security Controls on the Networks and Communications
 - Measures to protect against viruses and malware, countermeasures against unauthorized access, and remedies for network troubles
 - Measures for monitoring, detection, analysis, and protection against failures or cyber attacks
- (d) Security Features of Data Centers
 - Safeguard equipment, entrance and exit controls, emergency response, monitoring systems, etc.
 - Duplication of power supply and cooling equipment, auxiliary power supply, etc.
- (e) Security Management of the Data Center Operations
 - Employee screening of operators, monitoring of their daily services and operations
 - Management of access controls to systems and administration privileges, monitoring operation logs, etc.

Government and public entities provide variety of information disclosure references and services guidelines. In addition, there are many standards, including from private sectors, about information security and data protection and management. If the cloud service provider performs operation management and information disclosure, and obtains certification and accreditation, based on and under these standards, it is likely you can be confident about the provider's reliability and security management. Examples of these guidelines and standards include the following:

- Ministry of Economy, Trade, and Industry (METI): SLA Guideline for SaaS
- METI: Information Security Report Model
- METI: Information Security Management Guidelines for the Use of Cloud Services
- Ministry of Internal Affairs and Communications (MIC): Information Security Management Guidelines for ASPs and SaaS
- MIC: Information Disclosure Guidelines for the Safety and Reliability of Data Centers
- Information Security Management System (ISMS) Conformity Assessment Scheme

- IT Service Management System (ITSMS) Conformity Assessment Scheme
- Japan Institute for Promotion of Digital Economy and Community (JIPDEC): Privacy Mark System
- Foundation for Multimedia Communications (FMMC): Information Disclosure Certification System for the Safety and Reliability of ASPs and SaaS
- PCI DSS: Payment Card Industry Data Security Standards (Data Security Standards defined by the credit card industry)
- Audit reports regarding internal control, based on SAS 70 Type II Audit defined by AICPA (American Institute of Certified Public Accountants) (in Japan, equivalent to the "Clause 18 Audit" defined by the Japanese Institute of Certified Public Accountants)

(12) Is assistance (help desk support and FAQs) provided when users cannot see how to use the service?

Facilitations for user assistance include FAQs (frequently asked questions) available on the cloud provider's website, manuals in the form of video and other media, and help desk (customer assistance) that accepts questions on usage of services.

Check that these user support facilitations provided by the cloud service provider are substantial and dependable.

For user support contact point, check the following:

- How, where or whom to contact (Ways via telephone, email, and other methods are provided)
- Business hours (check whether the business hours match the usage in your enterprise, and whether you might need to call outside normal business hours)
- Fees (check whether inquiries are included in the monthly fee or an additional fee is required)

It is a good idea to try calling user support and check actual performance and services.

(13) Check the conditions how the data will be disposed after termination of cloud service use.

When for some reason the use of a cloud service ends, the data stored in the cloud

must be restored to the in-house system or moved to another service provider.
Check the following to assure this task is effectively performed without trouble:

- Whether the data is returned at the necessary time (or, as an alternative, whether local copying is possible as needed, and transfer speed is commensurate with data volume)
- Whether the formats of returned data are compatible with other systems
- When use has ended and data is returned, whether remaining data on the cloud system is certainly erased and protected against reuse or abuse by third parties

(14) Check general terms of the contract.

When using a cloud service, the contract terms are generally structured as to take effect when the user clicks a button marked "I agree." This has the same effect as a written and signed contract, so check the contract terms before clicking the "I agree" button.

Generally, in addition to those that constitute the actual contents of the transaction, the following terms should be carefully considered as well:

- Pricing system and applicable conditions
- Sentences constituting price changes (when to notice, how to notice, how to deal with disagreement, etc.)
- Sentences constituting change of service (what to change, how to change, when to notice, how to notice, how to deal with disagreement, etc.)
- Non-disclosure obligations (check vendor side, user side and reciprocal obligations; confirm the non-disclosure obligations of the vendor regarding user information, as well as obligations on the user side)
- Damage compensation rules (whether damage compensation are stipulated for the case of loss of data due to causes attributable to vendors or the consequential damage due to service interruptions, as well as whether or not these rules are sufficient)
- Rules governing expiration and renewal of contract (what is the initial and renewed term, whether there is an automatic renewal provision, and when and how to notice for renewal or expiration of the contract)
- Rules governing termination of the contract (check for stipulations that give the vendor the option to terminate the contract at its sole discretion and whether a penalty is imposed when the contract is

terminated by the user)

- Sentences defining procedures associated with expiration or termination of the contract (whether vendor obligations and user rights are defined for the case the contract is terminated, and whether they are appropriate; also, whether it is clearly specified that user data shall be returned upon termination and remaining user data on the cloud shall be completely erased after the data is returned)

[P1] Definitions of "IT Management Competency Index Stage 2" by METI

Stage 2

- * Management has a grasp of general management issues.
- * Management strategies are not known to everyone.
- * IT is used on a group (organization) basis.
- * Business processes are visualized, but improvements are only done on a per-organization basis.
- * Job duties and powers are defined.
- * System infrastructure is built separately on a per-application basis.
- * Management is involved in planning IT strategy.
- * The effects of IT investment are estimated before the actual investment, but assessment after investment is not performed.
- * Manuals, workshops, and education activities are performed to improve capabilities of management and employees to utilize IT.
- * Management recognizes threats caused by or related to IT, such as information breaches, viruses, and unauthorized access

- * METI, "IT Management Competency Index"

http://www.meti.go.jp/policy/it_policy/it_keiei/about/idea/management.html

Check sheet for Safe Use of Cloud Services by SMEs

No.	Item	Description	Check	Notes/Remarks
[A] Scope of use of cloud services				
(1)	Clarification of scope of usage	Have you examined what operation and data are to be handled by cloud services? Have you analyzed and set divisions of operations? Have you set operation rules?	[]	
(2)	Type and cost of service	Does the cloud service you are considering properly match your operational needs, and have you checked the cost?	[]	
(3)	Importance of handled information	Have you checked the level of the information classification handled by the cloud service?	[]	
(4)	Integrity with policies and regulations	Will conflicts or inconsistency arise between usage of the cloud service and the security policies?	[]	
[B] Preparing to use cloud services				
(5)	Cloud Use Administrator	Have you secured a cloud use administrator who understands the characteristics of cloud services?	[]	
(6)	User Management	Can the user management of cloud services be implemented appropriately?	[]	
(7)	Passwords	Can you appropriately perform setting and management of passwords?	[]	
(8)	Data backup	Are you prepared to secure in hand and make available important information in case the service is discontinued?	[]	

[C] Conditions of cloud services to be provided				
(9)	Reliability of Service Provider	Is the cloud service provider reliable?	[]	
(10)	Reliability of Service	Are the service levels indicated in such way of uptime rate of services, frequency of failures and target time to recover in case of failures?	[]	
(11)	Security Measures	Are detailed security measures for the cloud service disclosed?	[]	
(12)	User Support	Is assistance (help desk support and FAQs) provided when users cannot see how to use the service?	[]	
(13)	Securing data at the Term of Use	Check the conditions how the data will be disposed after termination of cloud service use.	[]	
(14)	Check Contract Terms	Check general terms of the contract.	[]	