Report of the Council of Experts on the Usage of Cloud Computing by Financial Institutions

November 2014

The Center for Financial Industry Information Systems

Contents

Introduction

Cloud computing may seem like a new term but is actually quite old. Eight years have already passed since the term "cloud computing" began to be used in 2006, and cloud computing has become increasingly important as a base for IT services and solutions. Cloud computing is generally recognized to offer benefits such as cost reductions through the sharing of resources and economies of scale, speedy system delivery, and reductions in system management effort. In 2008, the U.S. government, as part of its basic strategy for IT procurement and usage, introduced the Cloud First policy, which mandates the use of the public cloud as the first option in order to sharply consolidate data centers, and many companies around the world have followed this way of thinking. The use of cloud computing has also been growing in Japan. In particular, when the Great East Japan Earthquake struck, the widespread use of cloud computing as the infrastructure for confirming the safety of loved ones and sharing information led to the recognition of the fundamental benefits of cloud computing. As a result, the number of companies introducing cloud computing in various industries has grown sharply in recent years. It can be thought of as a natural course of action for companies to reduce system management effort through the building of IT infrastructure by effectively making use of cloud computing and other outside resources, allowing them to strategically shift human resources to core businesses.

The Center for Financial Industry Information Systems (FISC) began conducting full-scale research of cloud computing in fiscal 2009. By looking at the status of cloud computing usage by financial institutions, organizing the risks and taking other steps, it has periodically released investigative reports.[1] The results show that financial institutions are generally cautious about using cloud computing, especially the "public cloud," in which multiple customers share services. The main reasons cited include concerns about the protection of customer information data and other aspects of information security, service reliability and concerns about laws and regulations. According to tabulated results (Reference Materials "[Figure A] Usage Status of Cloud Computing") that are based on the survey "Study on Trends and Status of Security Measures on Computer Systems for Banking and Related Financial Institutions," which the FISC conducted in fiscal 2014, 16% of all financial institutions are actually using a public cloud, have plans, or are considering to use. A breakdown by type of business reveals that while many large banks and insurance companies are using public clouds, the percentage of usage is low among small and midsize financial institutions.[2]

The use of cloud computing by financial institutions as a whole is growing. Reference Materials [Figure A] shows changes in the overall usage of cloud computing (including those planning and considering adoption), and reveals that the percentage has increased from about 20% in fiscal 2010 to 37% in fiscal 2013. Furthermore, of this number, the use of the public cloud is also growing in many fields, mainly for front-end information systems (sales support systems, e-mail, internal information sharing, e-learning systems, etc.). Separate hearings by FISC found that we are starting to see widespread use of public clouds in operations that deal with customer information, such as customer management (please refer to Reference Materials "[Figure C] Public Cloud Usage Examples").[3]

---

[1] The results of research activities were published as the report "Issues and Outlook for Cloud Computing" in fiscal 2009, the research report "Notes Related to the Usage of the Internet and Cloud Computing During Reconstruction From the Recent Disaster" and the report "Security Assurance and Outsourcing Management for Cloud Computing by Financial Institutions" in fiscal 2011, and the research report "Trends and Issues for Regulation and Supervision of Financial Institutions for Cloud Computing Users" in fiscal 2013.

[2] Please refer to Reference Materials "[Figure B] Results of Hearings by the FISC." Hearings were also conducted on the reasons that cloud computing is not being used, revealing such general issues as the handling of personal information as well as such issues specific to financial institutions as control of cloud service providers, audits and inspections, and the handling of data after it has finished being used.

[3] The effects of using the public cloud, as shown in Reference Materials [Figure C], include benefits of ordinary

Cloud computing technologies and services are constantly advancing, so more financial institutions may actively use cloud computing in an effort to provide better financial services and strengthen competitiveness. In order to promote usage of cloud computing in a sound manner in Japan's financial industry, we believe that the parties concerned, including financial institutions and cloud service providers, must have broad discussions about the benefits and risks of cloud computing as well as appropriate risk management and contract management, leading to a shared recognition and understanding.[4]

Based on awareness of these issues, the FISC established the Council of Experts on the Usage of Cloud Computing by Financial Institutions (hereinafter referred to as the "Council") in accordance with an inquiry by the FISC President. The Council was comprised of members that included academics and officials from financial institutions and cloud service providers as well as observers from government agencies and other organizations. The Council discussed how financial institutions of Japan can make the most of the potential of cloud computing technologies after correctly ascertaining their characteristics and their risks, as well as properly managing these risks. Furthermore, the Council considered what the best security measures would be for supporting such efforts. The conclusions of the Council are outlined in this report.

---

cloud computing -- cost reductions, speedy system introduction, and improved convenience and functionality -- and the strengthening of security, which has been considered a concern.

[4] The FISC conducted a revision (Supplements to the 8th Edition) of the "FISC Security Guidelines on Computer Systems for Banking and Related Financial Institutions" ("FISC Security Guidelines") in March 2013, creating [O-108] as standards for the usage of cloud services (Reference Materials "[Figure D] The Handling of Cloud Services Under the 'FISC Security Guidelines' (Supplements to the 8th Edition)"). However, in this latest revision, this matter was designated as an issue that will continue to be considered, with the document stating: "Cloud services are advancing every day, and while there are such benefits as cost reductions and speedy introduction, cloud services are expected to be used for important operations and are expected to entail risks exclusive to cloud services, therefore this revision shall be considered a provisional document that deals with issues and problems that have become apparent, and is in no way a final document."

I. Characteristics of Cloud Computing

1. Definition of Cloud Computing

While there are various definitions and views of cloud computing, the Council has decided to adopt the definition given by the National Institute of Standards and Technology (NIST) of the U.S., which is shown below ([Figure 1]).[5]

[Figure 1] The Definition of Cloud Computing by the NIST

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Source: NIST "SP 800-145, The NIST Definition of Cloud Computing." Summarized by FISC.

The NIST classifies cloud computing into such deployment models as (1) "private cloud," which is provisioned for exclusive use by a single organization, (2) "public cloud," which is shared by multiple users, and (3) "community cloud," which is shared by a specific group of organizations. Of these, the Council discussed the "public cloud," which has more of a resource-sharing characteristic than the others.[6]

Furthermore, it is natural to regard the use of a public cloud as outsourcing all or part of the administration of information processing necessary for conducting business, i.e., system operation, maintenance and development, to a cloud service provider. Therefore, the Council has concluded that this should be treated as a form of "outsourcing," just as financial supervisors in other countries do.[7] Since financial institutions bear the final responsibility to customers and settlement systems, they would not be able to avoid responsibility if the cloud service provider that provides service to the financial institution causes a problem that results in a negative impact on the customer or others.[8]

[5] Refer to The NIST Definition of Cloud Computing (Special Publication 800-145). (http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf)

[6] As a general rule, the Council did not discuss anything other than the public cloud based on the view that the existing framework for outsourcing management can be applied as is in many cases based on their characteristics - such as the fact that the range of users of resources is limited to individuals or financial institutions - and due to the belief that the results of this Council can also be applied.

[7] The definition of outsourcing under the Financial Services Agency's supervisory guidelines (Reference Materials "[Figure E] Definition of Outsourcing Under the Financial Services Agency's Supervisory Guidelines") also states that it "includes cases in which banks outsource administrative work necessary to conduct their business (including cases in which actual conditions can be considered equivalent to outsourcing despite the absence of an outsourcing contract, and cases in which the outsourced work or other work is conducted overseas)."

[8] Some Council members argued that, "the public cloud can take the form of 'usage' instead of 'outsourcing,' so perhaps risk management should be considered for approaches other than outsourcing." Financial institutions that use cloud services still bear the responsibility for operations as a whole, so appropriate risk management on their part, such as ascertaining the actual conditions of cloud services, will be necessary.

2. Benefits and Risks of Cloud Computing

When considering whether to use cloud computing, it is important for financial institutions to fully understand the benefits and risks.

(1) Benefits

Some of the benefits of cloud computing are shown below in [Figure 2]. The various benefits include: cost reductions, a decrease in system management effort, scalability and flexibility, and the provision of business continuity.

[Figure 2] Benefits of Cloud Computing (Examples)

Cost reductions	System costs can be expected to decrease due to economies of scale under a resource-sharing scheme.
Quicker deliveries and shorter system development periods	The time until service launch and system development periods can be shortened because the time needed for the introduction and configuration of resources can be sharply reduced compared to when the users procure and configure their own IT infrastructure.
Reduction in system operation effort	Users can reduce management effort by outsourcing system maintenance and other operations to service providers.
Scalability/flexibility	Users are able to start small, use systems temporarily, withdraw immediately and have other options, so this may help to reduce opportunity losses and secure first-mover advantages.
On-demand self service	Users can control the usage and stopping of servers and other equipment on their own, eliminating wasted usage of resources.
Improved convenience and functionality	Users can enjoy a drastic improvement in convenience and functionality because new technologies are introduced quickly. Furthermore, cloud computing has a high affinity with mobile devices, social networking services, etc., which facilitates data exchange and information-sharing with those inside and outside the company.
Business continuity	If the service is based on the usage of multiple resources that are geographically dispersed, it would offer high business continuity in case some facilities are affected by disasters or other conditions.

(2) Risks

Risk management specific to cloud computing needs to be considered because of various unique factors, including the fact that cloud computing is a resource-sharing scheme and that depending on the service, the relationship of contracts and responsibility becomes complex since multiple cloud service providers will be involved. Examples of key risks that need to be considered for risk management are shown in [Figure 3] below (Details are outlined in Reference Materials "[Figure F] Risks That Should Be Considered for Usage of Cloud Computing by Financial Institutions").

[Figure 3] Cloud Computing Risks (Examples)

Risk	Category*	Details
Impact of difference in legal systems	Legal system (3)	Differences in demands for the protection of privacy and other factors depending on the country (jurisdiction) could hamper countermeasures in the event that trouble occurs or for the transfer of personal data.
Information leakage risk	Technical (7)	There is a risk of remaining data leaking because of the difficulty of completing data erasure either by physically destroying or degaussing hardware like disk media when the service ends.
	Technical (8)	Unlike an on-premises environment, this framework is based on the transmission of data over the network, which will cause a bigger risk of data leaking during data transmission.
Concerns about real time and availability	Operation (11)	Increased traffic for other users could result in a shortage of resources for processing one's own users, possibly leading to poor response and system shutdown, so the expected level of service may not be guaranteed.
Insufficient incident handling	Governance (18)	Cloud service providers place weight on cost-saving and the quick start of a service, so they may be reluctant to provide more than standardized user support. As a result, they may not disclose information that users need for risk management or sufficiently respond to any incidents.

* The numbers in the "Category" column correspond to the order of these risks in Reference Materials "[Figure F] Risks That Should Be Considered for Usage of Cloud Computing by Financial Institutions."

However, depending on the cloud computing service type, all of the risks listed in Reference Materials [Figure F] do not necessarily apply, and the degree of risk differs. When actually using a cloud, one needs to carefully examine the service details and evaluate whether the risks listed in Reference Materials [Figure F] exist as well as the level of those risks.

Furthermore, cloud technologies are constantly evolving, so while it is possible that some risks may be reduced, new risks could also emerge. Risks related to cloud computing should be re-evaluated in a timely and appropriate manner while keeping in mind that there may be unknown weaknesses related to as-yet unrecognized technologies, new threats, changes in the external environment, including regulations and laws, and other factors.

II. Basic Approach to Risk Management

Making Business Decisions Through a Risk-Based Approach

Cloud computing offers various benefits, as stated earlier, so financial institutions would be able to reduce costs or quickly deliver new systems in line with any changes in business conditions. However, there are risks, such as service shutdown due to system failure and bankruptcy of the cloud service provider as well as the leakage of customer information from the cloud environment, and if these risks materialize, they could have a major impact on many customers and the financial institution itself. For this reason, financial institutions must conduct appropriate risk management by taking the characteristics of cloud computing into consideration. Below is the basic approach to risk management involving cloud computing.

1. Establishment of Policies, Etc. for Cloud Computing Usage and Risk Management

Before a financial institution uses cloud computing, it is important for those involved - the executive or senior management and divisions concerned with the systems, users (business divisions, etc.) and system risk management - to understand and recognize the benefits and risks of cloud computing and then establish policies on a basic cloud computing usage or for risk management, involving executive or senior management.

To that end, the financial institution should first decide the purpose of using cloud computing and the scope of operations and systems that will switch to the cloud. In particular, a financial institution that is considering cloud computing should fully examine internally, for example, (1) what operations and systems to realize with cloud computing based on the company's own IT strategies, etc., (2) how much of those can be concentrated in a particular cloud service provider or cloud service, and (3) how much of the remaining risks can be tolerated; and then decide their appetite for risk and other matters related to cloud computing.

Furthermore, it is important for a company to clearly establish a companywide decision-making process related to the introduction of cloud computing, and then permeate this throughout the company. For example, a situation that should be avoided is for a user division (such as a business division) to introduce cloud computing without the involvement and knowledge of the systems and risk management divisions, which could lead to the saving of important data in locations outside of the company before the situation is noticed.

In addition, since cloud computing takes the form of "outsourcing," it would be preferable to create risk management policies, etc. for cloud computing by taking into account existing policies and standards for outsourcing management. The effectiveness of risk management measures in the risk management system should be reviewed periodically and changes should be made if necessary.

2. Application of the Risk-Based Approach

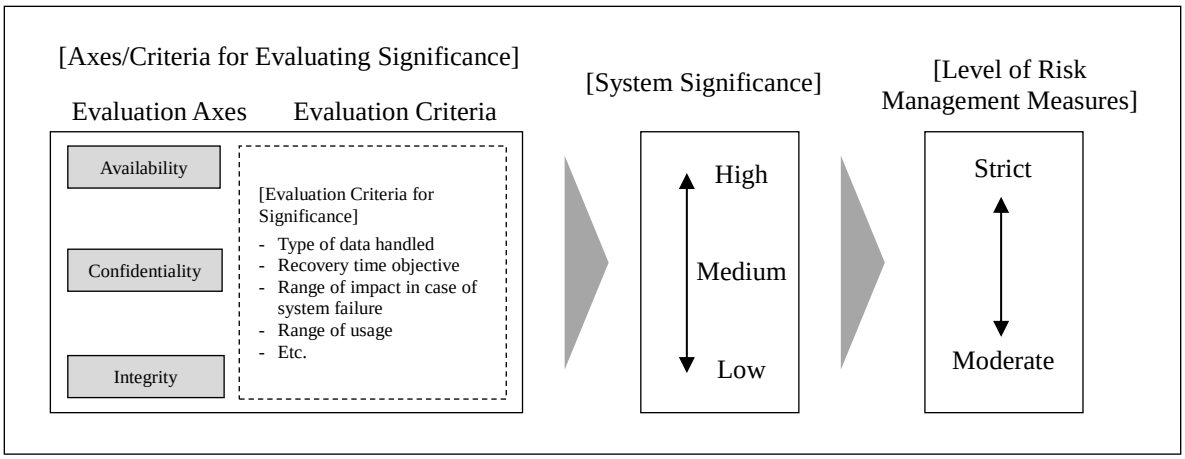
(1) Overview of the Risk-Based Approach

This report's understanding of the "risk-based approach" is as follows.

First, the characteristics and significance of operations that will use cloud computing (including system processing) are analyzed and ascertained based on such criteria as system availability and data confidentiality.[9] In cases that important operations will be implemented by using cloud computing, appropriately strict risk management needs to be implemented, but on the other hand, for relatively less important operations that will use cloud computing, a financial institution could decide to employ moderate risk management depending on the characteristics and significance of those operations. It is important for financial institutions to employ this kind of "risk-based approach" to create appropriate risk management measures based on business decisions. A visual representation of this risk-based approach is shown in [Figure 4].

While there are cases in which the significance of operations and systems are evaluated directly based on such evaluation axes as availability and confidentiality, some financial institutions will evaluate significance based on their own criteria (e.g., the type of data handled, recovery time objective, and the range of impact in case of a system failure), and this could result in the same decision as evaluating significance based on such evaluation axes as availability and confidentiality. Each financial institution needs to decide the axes or criteria for evaluating significance based on their own risk management policy and other factors.

[Figure 4] Overview of a Risk-Based Approach



[9] Criteria other than availability and confidentiality for evaluating the significance and characteristics of operations include data integrity (no altering or loss of data). While it is possible to evaluate significance comprehensively based on multiple criteria, this could result in a highly complicated scheme, so in this chapter we used two criteria to keep the discussion simple.

(2) Examples

1) Deciding Risk Management Measures

Actual examples of how to set the levels of risk management measures based on its significance of systems under a risk-based approach are shown in [Figure 5] below.

Two examples are shown below for setting risk management measures. In the first example, the significance of systems are evaluated based on both availability and confidentiality, which are two axes that the systems require, and then risk management measures are set based on significance. In the second example, the significance of systems is evaluated based on either availability or confidentiality, and then risk management measures are set based on significance.

[Figure 5] Setting Risk Management Measures Using a Risk-Based Approach (Examples)

Example 1: Risk Management Measures Based on a Comprehensive Evaluation of Multiple Axes (Availability & Confidentiality)

System Significance		Level of Risk Management Measures (e.g., audits)
Comprehensive evaluation of availability & confidentiality	High (core IT fields)	Audits, etc. led by the financial institution are necessary
	Medium (semi-core IT fields)	Audits, etc. led by the financial institution are necessary in part
	Low (non-core IT fields)	Audits, etc. led by the cloud service provider are adequate

Example 2: Risk Management Measures Based on an Evaluation of One Axis

System Significance		Level of Risk Management Measures (e.g., SLA for availability and data erasure for confidentiality)
Availability	High	Appropriate SLA that meets the financial Institute requirements on availability and service level is necessary
	Low	Contract based on the standard service agreement presented by the cloud service provider
Confidentiality	High	Upon termination of the agreement, irreversible physical or logical data erasure[10] is necessary
	Low	Data erasure is not necessary

a. Example of Comprehensive Evaluation

In [Figure 5], Example 1 shows cases in which the significance of systems is evaluated comprehensively by combining the availability and confidentiality axes, with the scope and depth of risk management measures changing in accordance with the significance level. In this example, significance was grouped into three grades (high/medium/low) and levels were set for "audits, etc." (on-site audits and monitoring by the client financial institution and third-party audits) based on the significance grade.

b. Example of Individual Evaluation

In Example 2, the significance level of systems (two stages of high/low in this case) is not evaluated comprehensively but rather based on either the availability or confidentiality axis, with the scope and depth of risk management measures changing in accordance with the significance level. In the risk management items, the use of "SLA" is employed as an example for the availability axis and "data erasure" is used for the confidentiality axis.

[10] Regarding "logical data erasure," please refer to "III-1.-(4) [Figure 16] Logical Erasure of Data that Meets Certain Conditions."

The matrix for the system significance levels of the "comprehensive evaluation" described above have been outlined in Reference Materials "[Figure G] Examples of System/Data Classification Based on Significance." Usually, "core IT fields," in which system availability and confidentiality are both high, have the highest significance and require strict risk management. Meanwhile, "non-core IT fields" have low significance, so moderate risk management may be sufficient. "Semi-core IT fields" fall in between the other two. This classification into "core IT fields," "semi-core IT fields" and "non-core IT fields" is not standardized, and they are listed here as reference so that each financial institution can decide system significance and risk management based on its own business characteristics and risk management policies, etc. Therefore, some financial institutions may decide to set even narrower fields. Furthermore, the levels for risk management measures for each field also are not standardized, so financial institutions have discretion to decide these as well.

As examples for risk management measures, "audits, etc." (Example 1) and "SLA/data erasure" (Example 2) were used above, but a more detailed list of ways to set risk management measures is provided in Reference Materials "[Figure H] List of Risk Management Measures (Examples)." In this table, those risk management items that state "comprehensive evaluation" in the "standard" column are items in which risk management measures are set based on a comprehensive evaluation as described in a. above. Furthermore, those that state "confidentiality" or "availability" in the "standard" column are those that set risk management measures based on an individual evaluation as described in b. above.

2) About Availability and Confidentiality

Systems that require high availability (high-availability systems) are assumed to be systems that affect customers or transactions, such as core-banking systems and fund-settlement systems.

Furthermore, data that requires high confidentiality (high-confidentiality data) likely includes information that could have a large effect on business if leaked and trade secrets that must be strictly managed under law (for specific examples, please refer to Reference Materials "[Figure I] High-Confidentiality Data (Examples)"). Based on the risk-based approach, systems that handle "high-confidentiality data" could have some latitude in the level of risk management required. Systems that include personal information would have high confidentiality, but uniform risk management may not be required because of differences in the data characteristics, data volume, the environment in which the data is handled, the expected impact of a data leak and other factors.

For example, a conference room reservation system may record the names of customers, which are regarded to be confidential information. But one may be able to decide not to employ strict risk management for that system based on the impact caused by leakage of that data, considering that the data is fragmentary.

Email systems also record names, but since this data is stored in a database and because emails can contain personal information and other important information, a decision to require strict risk management would be appropriate. However, if the user financial institution had implemented rules prohibiting the entry of highly confidential information, including insider information and credit card data in the bodies of emails and in attachments, and if these rules are being properly managed, then it may be possible to simplify the management level required for the system provided by the cloud service provider, based on the view that a large portion of the risks are being managed by the financial institution side. Naturally, it may be possible for a large portion of the risk management for email systems to be entrusted to cloud service providers, and for cloud service providers to implement risk management measures such as those based on

encryption technologies, which are mentioned later, with the financial institutions to examine whether those measures are appropriate.

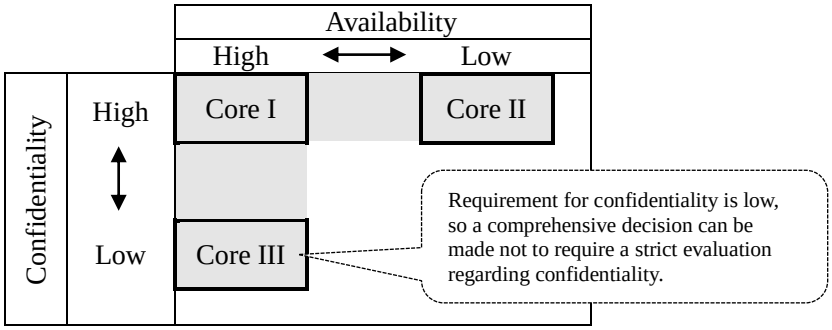
In this way, it is important to consider the risk management level by taking into consideration in a comprehensive manner the risks associated with the data itself, internal management by the financial institution side, and measures implemented by the cloud service provider side.

3) Points to Consider

As stated above, Reference Materials [Figure G] shows examples of system significance levels, or three fields (core IT fields, semi-core IT fields and non-core IT fields) in which significance was determined based on the two axes of availability and confidentiality. Risk management levels will usually differ between fields, as mentioned earlier, but one should also keep in mind that risk management levels required within the same field are not determined uniformly.

For example, [Figure 6] is a simplified version of Reference Materials [Figure G], with the shaded areas basically considered "core IT fields." Among the core IT fields, "Core I" is a field in which high risk management for both availability and confidentiality is required, "Core II" is a field in which high risk management is required for only confidentiality (requirement for availability is relatively low), and "Core III" is a field in which high risk management is required for only availability (requirement for confidentiality is relatively low).

[Figure 6] Differences in Risk Management Levels within the "Core IT Field"



Management levels for each risk management item should be evaluated independently. For example, systems defined as "Core III" in [Figure 6] are defined as core IT fields, but of the risk management items in Reference Materials [Figure H], all the items for which a comprehensive evaluation should be conducted based on both availability and confidentiality do not necessarily require the most strict management (furthest on the left in the table) uniformly. In another example, in the Due diligence of Cloud Service Provider at the use examination in Reference Materials [Figure H], the necessity for disclosure of detailed information regarding evaluation items related to confidentiality is not that high.

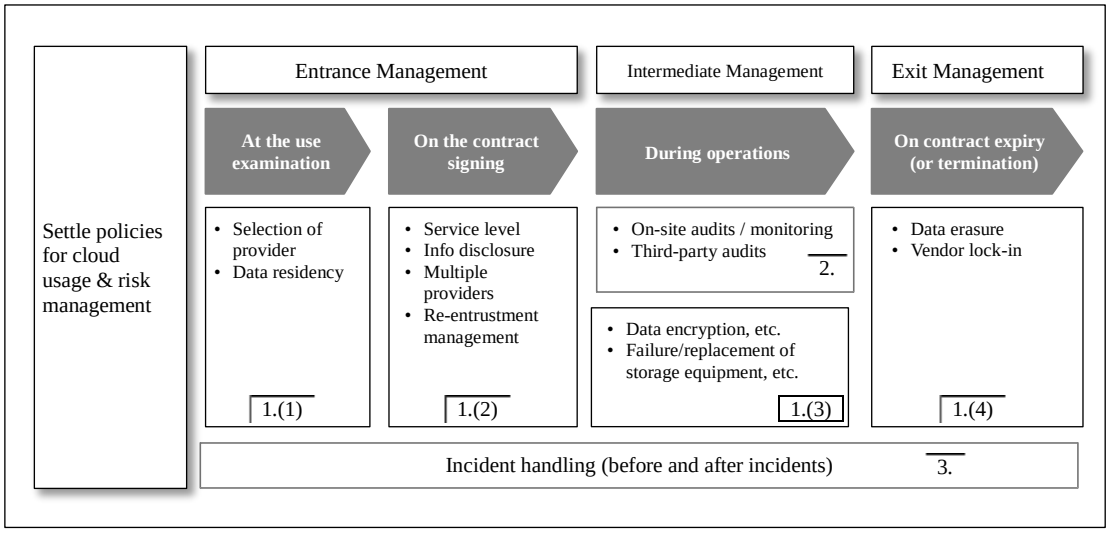
Please note that Reference Materials [Figure G] and Reference Materials [Figure H] are just examples of standards to employ when setting the ranges for simplifying risk management based on the risk-based approach. Financial institutions should consider risk management measures by using these reference materials and other information just as a reference.

III. Specific Risk Management Measures

This chapter summarizes risk management measures from three viewpoints: (1) risk management measures for the selection of cloud service providers and the ascertaining of actual conditions for their systems and data, in addition to other activities, (2) verification of whether cloud service providers are conducting effective management/operation in accordance with contracts, SLA, etc. (through audits, etc. of cloud service providers), and (3) incident handling.

Regarding each risk management measure, the section "a. Management Measures" shows examples of the application of strict, high-level risk management that is thought to be necessary for processing extremely important operations (i.e., operations that require high availability or confidentiality) via the public cloud. The section "b. Moderate Risk Management" lists approaches for simplifying risk management based on the significance of systems and operations.[11]

[Figure 7] Overview of Risk Management Measures



1. Risk Management Measures

When using cloud computing, systems and data are placed outside the company, so the range and depth of information that can be ascertained directly by the user is narrow compared to systems configured on-premise, which means that they are less likely to come under internal governance. For this reason, when financial institutions use the cloud for very important businesses, they should ascertain the actual conditions of cloud computing from various viewpoints - e.g., the cloud service provider's job performance capabilities and risk management system, the contents and level of services offered, and data residency - so that as much as possible no portion remains as a "black box".

Below are details of risk management measures for each phase: (1) At the Use Examination, (2) On the Contract Signing, (3) during operations of cloud services, and (4) On Contract Expiry (or Termination).

[11] In Reference Materials [Figure G], the examples for risk management measures for "core IT fields" are believed to correspond to "a. Management Measures" while those for "semi-core IT fields" and "non-core IT fields" are believed to correspond to "b. Moderate Risk Management."

(1) At the Use Examination

1) Selection of Provider (Due Diligence on Cloud service provider)

A public cloud service is a resource-sharing service based on the concept of "multiple users enjoying cost benefits by using common functions," so if the actual functions and service levels are not what the financial institution had expected before introducing the service, then it would be very difficult to make changes later. For this reason, it is important for those considering the introduction of cloud services to pay close attention and perform due diligence.

a. Management Measures

Risks should be analyzed and recognized from the viewpoint of such factors as the availability and confidentiality required of operations that will be moved to Cloud and also from the viewpoint of company management. Then, after considering the risk management levels required for those operations, a cloud service provider with sufficient ability to carry out the relevant services properly should be selected. At that time, it is necessary to perform due diligence based on information about the cloud service provider's qualifications and job performance capabilities, internal controls, and the status of risk management ([Figure 8]).[12]

Some cloud service providers are reluctant to disclose information before the signing of contracts, but one should consider seeking disclosure by signing a nondisclosure agreement in advance if necessary.

Furthermore, since cloud computing is a relatively new technology, it may be difficult to acquire trustworthy information based on business histories, but it is important to evaluate a cloud service provider from various angles by looking at such factors as service reputation and track record.

[Figure 8] Important Evaluation Items When Performing Due Diligence (Examples)

1. Track record and technological prowess involving operations expected to use cloud computing[13]
2. Business continuity (corporate strength/profitability, human resource base, CEO's capability/business strategy, and BCM/data backup in case of disasters)
3. Service availability, data security (protection of confidentiality), and integrity
4. Status of internal controls, risk management, etc. within the cloud service provider (including re-entrustment management), and whether the cloud service provider has received external audits and acquired various certificates
5. Stance regarding information disclosure
6. Policy towards acceptance of on-site audits
7. Data Residency (place where the data is stored or may be stored)
8. Ease of linking with existing systems, data migration to new systems, etc.
9. Support structure (support desk, response in case of failure [securing traceability, etc.])
10. Balance between expected damage (direct damage & indirect damage) in case an incident occurs and the maximum compensation for damages offered by the cloud service provider
11. How the cloud service provider deals with the ending of usage (vendor lock-in risks, data erasure, etc.)
12. When signing a contract that spells out that all or part of the handling of personal data will be done by the cloud service provider, compliance with the "Standards for Selecting Outsourcing Contractors Concerning the Protection of Personal Information" (please refer to Reference Materials [Figure J]) as defined in section III of the "Practical Guidance on Safety Management Measures for the Guidelines on Personal Information Protection in the Financial Industry."

Note: The evaluation items listed above should be examined by fully taking into consideration the details and conditions stated in "III. Specific Risk Management Measures."

[12] In the case of a public cloud, which is a resource-sharing service, a cloud service provider may not comply with requests from individual customers for changes to the contents of standard contracts, SLA, etc. Financial institutions should confirm in advance if they will be able to negotiate such change requests for especially important matters.

[13] Technological prowess would include such evaluation items as the cloud service provider's specialty regarding the operations that will be outsourced by the financial institution and whether the cloud service provider conducts stable development/operations related to its business.

b. Moderate Risk Management

When the significance of operations that will use cloud computing is not necessarily high, the financial institution may decide to simply conduct an objective evaluation by looking at a cloud service provider's public information, reputation within the industry, track record, etc.

2) Data Residency

Some cloud service providers conduct operations and manage data using multiple data centers located around the world. Depending on their policies, cloud service providers may be reluctant to disclose the location of their data centers, but financial institutions need to take into account such factors as which country's laws would be applied in case of a dispute, or whether business continuity would be affected in the event that local authorities seize data for their investigation. In particular, ascertaining the location of data stored/being proceeded is even more important when outsourcing important operations.

a. Management Measures

(a) During Normal Times

When conducting operations that require high availability or when processing/ accumulating/storing highly confidential customer information, the client financial institution needs to ascertain the region (country, state, etc.) to the extent that it can identify the laws that will be applied to the cloud service, by taking into consideration the possibility that local authorities will browse data, or order submission of data, etc. Even in cases where the data is dispersed, it is necessary to ascertain in which country or region the data may be stored, for the same reason.[14]

(b) When an Incident Occurs or There is an On-Site Audit

When an incident such as an information leak occurs, the specific location of data centers or other facilities will naturally become necessary for inspections of those facilities. The same holds true in cases in which the client financial institution needs to conduct an on-site audit.

(c) When Data is Stored Overseas

When data is stored overseas, costs and communication methods for on-site audits should be considered as shown in [Figure 9].

[Figure 9] Points to Consider When Data is Stored Overseas

Time/costs for on-site audits of data centers	On-site audits could take a long time and personnel costs could become high. For this reason, there may be many cases in which audits are outsourced to local auditing firms.
Communication methods when dealing with failure	In cases that a financial institution's personnel for dealing with failure have insufficient local language skills, then it becomes necessary to clarify in the contract such matters as Japanese-language support and whether the cloud service provider will set up a failure-support desk at its Japanese branch.

b. Moderate Risk Management

Differences may arise in the necessity to ascertain location data and required detail of such data depending on the characteristics and significance of operations that use cloud computing. From the viewpoint of risk profiles, when outsourcing operations that are not deemed important, information about the data residency is not that important.

[14] For mission-critical systems that require high availability and confidentiality, such as core-banking systems, the exact locations of data centers should be confirmed in order to ascertain their location status and other factors.

(2) On the Contract Signing

1) Agreement on the Service Level

A contract with a cloud service provider usually includes an SLA,[15] but many standard SLAs only offer a reduction of service usage fees if the actual uptime is lower than the specified standard monthly uptime, for example. For this reason, the signing of contracts that include standard SLAs may be insufficient for systems that require high uptime, such as online processing for core-banking systems.

Cloud service providers have as clients not only financial institutions but companies from various other industries as well. Cloud service providers can therefore sometimes be reluctant to sign separate SLAs based on the view that preparing contracts with different content for each client company is not efficient. Meanwhile, when financial institutions outsource especially important operations, a high service level is required in light of the significance of the operations to society. A financial institution may need to examine the contents of the contract, SLA and SLO[16] with the cloud service provider and request additional content depending on the profile of the operations that will use cloud computing, in order to ensure sufficient service level and risk management.

a. Management Measures

Contracts[17] as well as SLAs/SLOs that are signed as necessary are recommended to include the items listed in [Figure 10]. Naturally, financial institutions should consider adding or changing items instead of simply using [Figure 10] as is, based on the profiles of their operations.

[15] Service Level Agreement: an agreement between the service provider and the client financial institution regarding the details and scope of the service provided as well as the required quality level (standard value or guaranteed minimum value) or a document or contract that defines these matters. If the required quality level is not met, the service provider may be liable to pay damages for incomplete fulfillment or nonfulfillment of its obligations.

[16] Service Level Objective: a target set by the service provider for the quality of service. Target levels and target values are set for performance, availability, data management, operations systems, support systems, security, etc. for services provided as well as systems, equipment, etc. that comprise the service, and these targets are presented to the client. If the targets are not achieved, the service provider is not immediately liable to pay damages like a contract or SLA, but the service provider will be obliged to make efforts and improvements to achieve target levels and target values. If the service provider does not meet these obligations appropriately, it may be liable to pay damages for incomplete fulfillment or nonfulfillment of its obligations.

[17] Includes appendices and supplementary documents that are attached to the main contract.

[Figure 10] Items That Should Be Included in Contracts, SLAs and SLOs (Examples)

1	Ordinary contract clauses (definition of terms, division of roles, areas of responsibilities, scope of liability to pay damages in case of nonfulfillment of obligations, applicable law, court with jurisdiction, etc.)
2	Individual contract conditions (service contents, fees, duration, etc.), service specifications (resource allocation, etc. [necessary time for restricting or changing specifications, etc.]), and management measures for data protection (data encryption, etc.)
3	Service level items (1) System operations: availability,[18] reliability, performance and scalability (2) Support: response to failure and response to inquiries (3) Data management: Mention of security of user data (4) Control environment: Re-entrustment management (including further outsourcing), protection of confidential information, and obligation to maintain a favorable control environment
4	Response in case service level is not attained
5	Scope of information disclosure; obligation to cooperate with inspections, etc. by supervisors, etc.; acceptance of audits by financial institutions; operating rules for reporting, communication, etc. between service provider and user; and incident response
6	Assurance that there are no connections with anti-social forces and terrorist organizations
7	Return to original condition at end of use; obligation to cooperate with transfer to any new system; and data return, erasure, etc.
8	Damages and compensation
9	Holder of intellectual property rights for products created while using applications running on the cloud service provider's resources (or percentage of ownership)

Note: The items listed above should be included in contracts/SLAs/SLOs by fully taking into account the contents and conditions described in "III. Specific Risk Management Measures."

b. Moderate Risk Management

The items listed in [Figure 10] are just an example of items that should be covered when outsourcing important operations to a cloud service provider. The contents and standard values for each item could change depending on the significance and risk characteristics of the operations that will be outsourced, and the necessity of each item could change as well. For example, when outsourcing operations that are not important, all of the items above are not necessarily needed, and the standard SLA that the cloud service provider usually presents to clients other than financial institutions may suffice. Or, it may be possible to sign just a standard contract and not sign an SLA at all.

[18] The evaluation of availability should cover (1) times the system shuts down due to failure, etc. and (2) scheduled shutdowns for system upgrades/maintenance (including emergency security patches) and for improving the quality/security of the system, including the addition of new services. A point that should be noted is that for the second item, if the service is a public cloud offering global service, then scheduled shutdowns to implement emergency security measures may not be implemented in accordance with an individual user's requests (work time, etc.) because precedence is given to the security of users as a whole. For this reason, it is important to confirm a cloud service provider's policies and standards for scheduled shutdowns and emergency security measures.

2) Information Disclosure by the Cloud service provider

A financial institution bears important social responsibilities due to its operations, so in cases where information is being (successively) entrusted, it needs to ensure the soundness and appropriateness of the operations. For this reason, when outsourcing operations, the financial institution needs to acquire information about whether the cloud service provider can perform tasks appropriately and the contents of its security management system before or even after signing the contract, and then evaluate the cloud service provider appropriately based on that information, in order to manage the cloud service provider. Meanwhile, it is expected that when a cloud service provider agrees to provide service to a financial institution, it takes into consideration the important social responsibilities of the client and becomes accountable by complying with requests for the supply of information.

a. Management Measures

(a) Specification of the Contents of Standard Information Disclosure in Normal Times

When a cloud service provider receives requests to disclose all sorts of information from multiple client financial institutions, it could face an increased burden to respond to these requests. For this reason, it is recommended to reduce the burden on the cloud service provider by deciding in advance the scope of standard information disclosure through the contract, SLA, etc., which would make it easier for the cloud service provider to comply with requests for information disclosure from financial institutions. Some cloud service providers may be reluctant to supply information beyond what is normally disclosed because it needs to protect the confidentiality of the information. But the contract needs to state that if a financial institution requests the disclosure of information and provides a rational explanation why that information is necessary, the cloud service provider will supply the information after discussing the matter with the financial institution. If the information being requested is highly confidential, then the two sides will need to sign a nondisclosure agreement before the information is supplied.

(b) Information Disclosure When Risks Become Apparent

The contract or SLA should state that the cloud service provider will disclose information in compliance with requests from the financial institution regardless of whether the conditions in section (a) above apply, in such cases as the occurrence of risk phenomena, when the risk of information leakage has increased based on various materials, and when the cloud service provider's internal controls have worsened.

(c) Dealing with Refusals to Disclose Information

There is a possibility that a cloud service provider will refuse a request for information disclosure because information such as the architecture and specifications of cloud services is likely confidential information of paramount significance to the cloud service provider. A financial institution needs to fully ascertain items that are connected directly with risk management ([Figure 11]), so it needs to carefully consider whether to sign a contract with a cloud service provider unwilling to disclose such information.

[Figure 11] Items Connected Directly with Risk Management

(1) The flow from data input to storage, processing, backup, and output
(2) Encryption format, and which areas are encrypted and not encrypted
(3) Acquisition scope, acquisition frequency and retention period for system logs
(4) Acquisition content, storage location, and retention period for data copies (including backups)

b. Moderate Risk Management

If a determination is made that operations outsourced by a financial institution are not important, then there may not be a need to strictly request that a cloud service provider provide detailed information about items connected directly with risk management. In this case, the contents of standard information disclosure by the cloud service provider would be sufficient, so it would not be necessary to request additional information.

3) Outsourcing to Multiple Cloud service providers

Cloud services are sometimes provided by multiple cloud service providers. In this case, one should keep in mind that a performance bottleneck or failure in resources overseen by a particular cloud service provider has a major impact on the quality of the entire cloud service. What should be avoided is a situation in which when an incident occurs, each cloud service provider does not assume responsibility and blames the other, resulting in delays in ascertaining the status of the failure and implementing recovery measures.

a. Management Measures

In order to deal quickly with failures, it is necessary to decide on a business operator (hereinafter referred to as "main contractor") that acts as the single point of contact and handles coordination between the cloud service providers, to clarify the responsibilities of the client financial institution and cloud service providers, depending on the management capability of the client financial institution. If the client financial institution is able to handle this role, a main contractor could be optional.

b. Moderate Risk Management

A main contractor may not be necessary if a risk analysis concludes that a failure would only have a limited impact or if a determination is made that a delayed recovery would have only a negligible impact.

4) Re-Entrusting Management

In order to ensure stable service and protection of information, it is important for a financial institution to ascertain actual conditions and conduct appropriate risk management not just for the cloud service provider to which it outsources operations directly but also providers to which the cloud service provider re-entrusts ("sub-contractors").

a. Management Measures

Management measures described in [Figure 12] should be taken to ensure the sound operations of sub-contractors.

[Figure 12] Management Measures for Sub-Contractors

Appropriate advance screening of sub-contractors	• When outsourced operations are re-entrusted, it is necessary to conduct appropriate advance screening of sub-contractors to ascertain the status of re-entrustment and to exclude any inappropriate service provider.[19] • If the cloud service provider's screening or management process of sub-contractors are believed to be more effective than the financial institution's, then the cloud service provider's advance screening[20] could be the best option. Note: When re-entrustment operations that are especially important (core-banking systems, systems that store highly confidential customer data, etc.), then the financial institution should conduct the advance screening itself.
Clarification of responsibilities, including liability for damages	Clarify that if a sub-contractor causes a problem, it is responsible for a prompt recovery in addition to being liable for damages within the limits of the clause defining the cloud service provider's maximum liability for damages.
Clarification of the obligations of the sub-contractor	The contract between the financial institution and cloud service provider should clearly state that any contract between the cloud service provider and sub-contractor should include clauses specifying that the sub-contractor bears the same obligations, including those for reporting and ensuring internal controls, that the cloud service provider has to the financial institution.
Halting of re-entrustment	It is recommended to clearly state in the contract that the financial institution can ask the cloud service provider to stop re-entrustment if, based on various reports and other materials, there is reason to question the job performance capabilities of the sub-contractor. If the cloud service provider does not comply with the cancelation request, then the financial institution should consider terminating service with the cloud service provider.

b. Moderate Risk Management

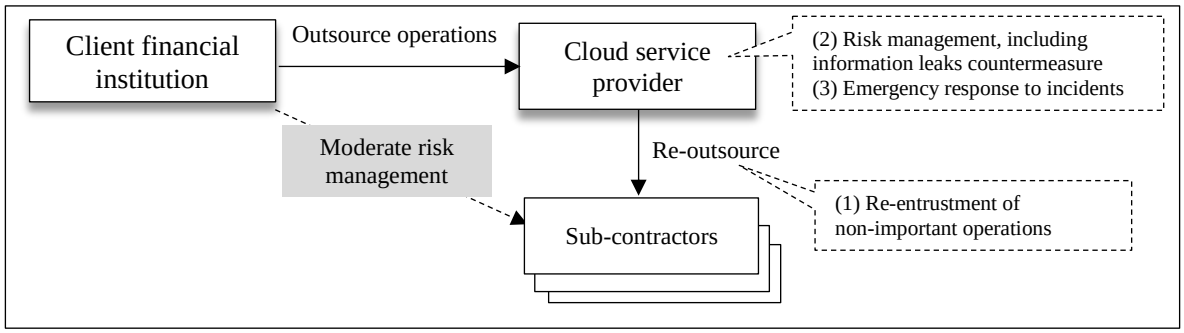
Depending on the operations that are re-entrusted, the client financial institution may be able to simplify the risk management, including advance screening and everyday monitoring, for the sub-contractor.[21] This case could apply if the following conditions are met: (1) the operations re-entrusted are not important, (2) the cloud service provider handles risk management, including measures to fight cyberattacks and measures to deal with information leaks caused by a malicious insider, and (3) the cloud service provider handles emergency measures when an incident occurs, including the acquisition and analysis of logs ([Figure 13]).

[19] In cases that the financial institution conducts the advance screening itself, a possible scheme for improving the efficiency of the advance screening would be for candidate service providers for re-entrustment to be screened in advance under an agreement between the cloud service provider and financial institution.

[20] If a cloud service provider conducts advance screening of sub-contractors, this should be equal or greater in scope and depth than a screening conducted by the financial institution itself, based on the financial institution's risk management policy, etc. If these conditions are met, then advance reporting and approval of individual sub-contractors (existing providers, addition of new providers and changes) are not necessarily needed.

[21] The simplifying of risk management could include, for example, reducing the frequency and depth of check items (however, keep in mind that society demands strict handling of anti-social forces, etc.).

[Figure 13] Simplifying of Risk Management for Sub-contractors



The items "a. Management Measures" and "b. Moderate Risk Management" above can be reorganized as [Figure 14] below.

[Figure 14] Relationship between the Significance of Operations That Are Re-Entrusted and the Party Conducting Advance Screening/Screening Level

	"a. Management Measures"		"b. Moderate Risk Management"
	Important operations	Especially important operations	Non-important operations
Party conducting advance screening	Financial institution or cloud service provider	Financial institution	Financial institution or cloud service provider
Screening level	Strict		Moderate

(3) During Operations of Cloud Services

This section will explain data encryption and management in the event of failure of storage devices, etc., from the viewpoint of data management during operations of cloud services. During operations, there is also a need to conduct monitoring and audits to check if the cloud service provider is providing appropriate service, implementing appropriate risk management, etc., based on the contract or SLA, but those issues[22] will be discussed in "2. Audits, Etc. of the Cloud service provider."

1) Data Encryption, Etc.

The "FISC Security Guidelines" state that important data are recommended to be encrypted, and that particularly in the case when personal data are stored, encryption, password setting, and other proper precautions should be taken to protect data contents from being read out even if files are copied illicitly or stolen. In light of this description and the fact that overseas regulations strongly recommend encryption,[23] there is a need to consider more effective data protection measures. Furthermore, while encryption is one management measure, technological advances could lead to the emergence of management measures that offer stronger data

[22] The issues discussed will mainly be monitoring and on-site audits; such issues as the contents and methods of monitoring and audits (monitoring of uptime, receipt, verification, etc. of periodic operations reports) will not be covered.

[23] For example, a law in the U.S. state of California (Senate Bill 1386: SB1386) and other laws require companies to notify consumers if they believe there is a possibility that consumers' personal information has been leaked. However, they are exempted from this obligation if the "personal data" in question was encrypted. So while the "encryption of personal data" is not mandatory, companies face tough information disclosure measures if data is not encrypted.

protection, so employing these new measures as an alternative should also be considered.

a. Management Measures

Data protection, including encryption, should include the management measures described in [Figure 15] below.

[Figure 15] Management Measures for Data Protection

Encryption of stored/transmitted data	Such management measures as encryption should be employed for data that includes highly confidential personal data or other sensitive information. To ascertain the risk of data being observed at parts where encryption is impossible due to specification restrictions (parts processed as plaintext), financial institutions should ascertain the specifications of encryption ((1) which parts are encrypted and which parts are not encrypted during processing, (2) the encryption format, (3) management of the encryption key, etc.) and decide whether they match their own risk management policies.
Party managing the encryption key	The encryption key does not necessarily have to be managed by the financial institution, but the measures[24] defined in [O-43] of the "FISC Security Guidelines" are necessary. When management of the encryption key is entrusted to the cloud service provider, the financial institution should fully ascertain the gist of the cloud service provider's risk management and determine if that matches its own risk management policy. Technologies are now being offered that allow the client financial institution to store and manage the encryption key. The use of solutions that are based on such technologies would be effective to improve risk management.
Alternatives to encryption	Although encryption is an effective management measure, there are some concerns, such as (1) the issue of management of encryption keys, as noted above, (2) concerns about putting the original data on the cloud, and (3) concerns of performance degradation due to the need to repeatedly encrypt and decrypt data as part of work processing through cloud computing. For example, such technologies as tokenization -- in which the financial institution holds the original data and token, and the data on the cloud is replaced with random numbers, effectively rendering the data meaningless -- may become an alternative to encryption. However, if tokenization is employed as a management measure, then proper management measures would have to be taken for management of the token mapping table by the financial institution. Note: Measures to prevent data from being read out following illicitly copied or stolen are not limited to encryption and tokenization.

b. Moderate Risk Management

Encryption and tokenization are among management measures to protect customer data and other important data, so if data is not determined to be "important data" based on the confidentiality of the information and risk profile, then the necessity for such management measures as encryption and tokenization may be low.

2) Failure/Replacement of Storage Equipment, Etc.

When using cloud services, the cloud service provider sometimes will replace equipment or parts due to the failure, etc. of storage equipment. In that case, the storage equipment, etc. being replaced may still contain highly confidential information, such as information about the financial institution or its customers. The financial institution should conduct proper management for those storage equipment, etc., as well, including the erasure of data.

[24] [O-43] states: "Clarify the operation management method for the use of encryption keys."

a. Management Measures

The following are management measures that could be taken for the failure and replacement of storage equipment, etc.

(i) Physical erasure (degaussing) or logical erasure (in case logical erasure cannot be performed due to a failure of the moving parts, logic circuits, etc., then physical erasure shall be performed) of data on the storage media that may have stored the data in any storage equipment, etc. that was replaced.

Note: Regarding logical erasure, please refer to "(4) On Contract Expiry (or Termination) 1) Data Erasure" below.

(ii) Properly perform physical erasure before the equipment is moved outside of the cloud service provider's facility.

(iii) The contract, SLA, etc. clearly states that equipment is moved outside only after irreversible erasure is performed.

Unlike steps taken at the end of the cloud service contract, which is mentioned later, the failure/replacement of storage equipment, etc. during the contract period means that the financial institution can verify the effectiveness of the erasure/destruction process by requesting information from the cloud service provider and through audits, etc. Considering this fact, the issuance and acquisition of data erasure completion certificates may not necessarily be cost-effective.

b. Moderate Risk Management

When important data is not handled, erasure/destruction of data may not be necessary when replacing storage equipment, etc.

(4) On Contract Expiry (or Termination)

1) Data Erasure

On the cloud service contract expiry, the data entrusted by the financial institution should be erased in an appropriate manner and at an appropriate time. Management measures to ensure that data is erased for certain should be implemented.

a. Management Measures

When the storage of confidential data is entrusted, the various system resources of the cloud services are usually the assets of the cloud service provider, so it will likely be difficult for the financial institution itself to erase the data. In this case, one possibility would be for the cloud service provider to perform the data erasure and issue data erasure completion certificate, etc. Data erasure in this context refers to physical erasure or, logical erasure satisfying predetermined (predescribed) conditions ([Figure 16]). Furthermore, in order to reduce the burden of issuing and acquiring separate data erasure completion certificates, the contract could specify that the cloud service provider will perform data erasure, including logical erasure, on the cloud service contract expiry, and verification of the appropriateness of the erasure process by a third party could eliminate the need for data erasure completion certificates.

However, at present, logical erasure cannot be used to make the restoration of personal information "impossible" (it can only make the restoration of information "extremely difficult"), so from the viewpoint of further reducing information leak risks, the contract should clearly state that the cloud service provider will perform "physical erasure" when replacing or removing hardware in the future.

It is recommended that the timing of the data erasure be discussed with the cloud service provider and clearly stated in the contract, given the possibility that even after the end of the contract, the data entrusted to the cloud service provider will be used (as backup data) to deal with such incidents as data leaks.

[Figure 16] Conditions under Which Logical Erasure of Data Would Be Allowable

Fragmented data	Fragmented data is stored in the data storage area, and restoring personal information and information about the client financial institution would be extremely difficult from fragmented data alone. In this case, the information that links the data management area and data storage area should be severed irreversibly.
Full overwriting of the data storage area	A complete overwriting of the data storage area (with intentionally meaningless data or other user's data).
Destruction of the encryption key	If the stored data is encrypted, the encryption key should be destroyed.

b. Moderate Risk Management

If operations that do not handle customer data or other confidential information are entrusted to the cloud service provider, then no data would be subject to the requirements for physical/logical erasure. In this case, the data erasure process at the end of the cloud service contract may be simplified or unnecessary, and a data erasure completion certificate will not be necessary.

2) Vendor Lock-In

If the programming language, services, etc. provided by the cloud service provider are fixed, then it may be extremely difficult for the user to configure the cloud environment freely. The

financial institution is recommended to take steps in advance so that it can quickly switch to an alternative cloud service, to an ordinary outsourcing arrangement, or to an on-premises environment in the event that the cloud service provider violates the SLA or has difficulty continuing the service contract due to any change in policy of the cloud service provider or financial institution.

a. Management Measures

The client financial institution is recommended to make preparations for a system transfer due to suspension or ending of the contract. The management measures for that situation are described in [Figure 17] below.

[Figure 17] Management Measures to Reduce Vendor Lock-In Risks

Duty of cooperation of Cloud Service Provider	Include the following in the contract. • The cloud service provider shall provide the client financial institution with a method for extracting data that will be transferred to the new cloud service provider or existing in-house system. • The cloud service provider shall cooperate with the actual transfer work.
Advance knowledge of transfer work	The client financial institution shall acquire knowledge of the method of transfer data extraction and details of the actual transfer work before using the cloud service.
Sharing of expense	The bearing of expenses for the transfer work should be specified in the contract by envisioning various cases, including the cloud contract being canceled by the financial institution or by the cloud service provider.

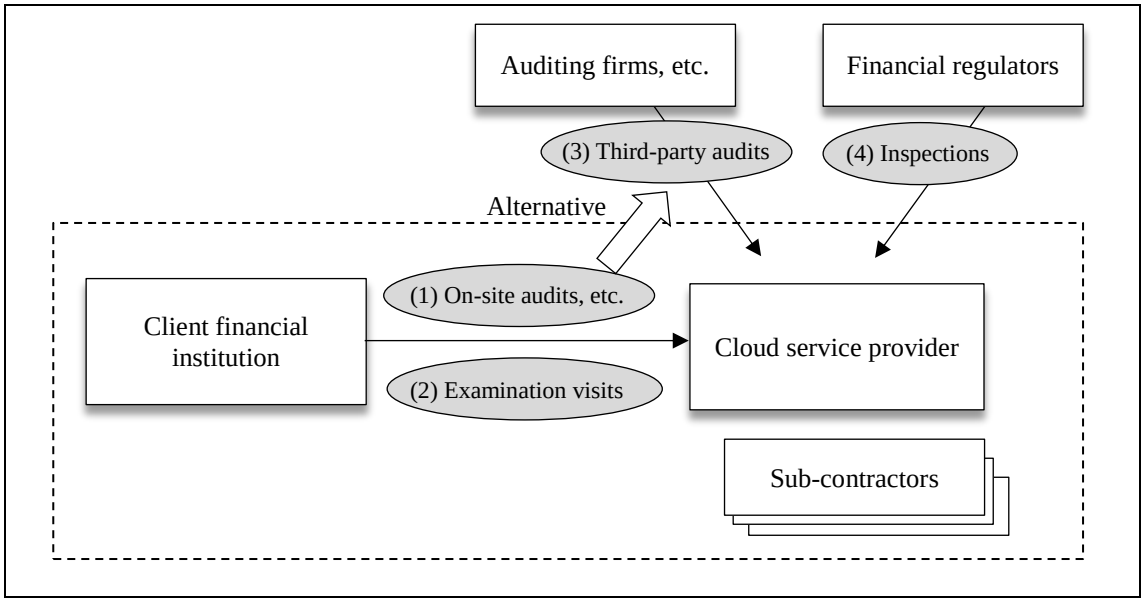
b. Moderate Risk Management

Measures to reduce vendor lock-in risks are recommended to be taken when transferring important systems to the cloud, but in cases in which operations with low significance are outsourced, then it may be sufficient for the financial institution to make preparations to switch to an alternative provider without the cooperation of the initial cloud service provider. For example, in the case of an IaaS (Infrastructure as a Service), in which only the computing resources are outsourced, it may be possible to switch to another cloud service relatively easily without the cooperation of the initial cloud service provider.

2. Audits, Etc. of Cloud service providers

The financial institution's management team even bears responsibility for the use of a cloud service in which information that is used as a base for financial operations and the processes that handle such information are entrusted to an outside company. For this reason, the effectiveness of risk management systems, etc. needs to be verified for cloud service providers, since they are not easily managed directly with internal controls ([Figure 18]).

[Figure 18] Overview of Issues Regarding Audits, Etc. of Cloud service providers



(1) On-Site Audits and Monitoring by the Client Financial Institution

Since financial institutions are responsible for conducting proper job processing and need to appropriately manage customer data and other important information, when they outsource work, they need to verify that the work being outsourced is being done appropriately. In cases that the appropriateness of outsourced work cannot be sufficiently verified with information submission requests alone, then the appropriateness should be confirmed by conducting on-site audits, monitoring and other actions ("on-site audits, etc.") of the offices and data centers of the cloud service provider.[25]

a. Management Measures (Operation Method)

The operation method for onsite audits, etc. by the client financial institution is described in [Figure 19] below.

[25] Some believe that allowing monitors and other personnel of the client financial institution to enter into the facilities of the cloud service provider causes security issues and other issues for the many other client companies that use the same cloud service provider, so there is a risk that this could negatively impact the safety and security of job processing. However, many believe that rather than avoiding those risks, there is a stronger need to accept such verification by users or their agents to confirm the soundness of job processing as a whole.

[Figure 19] Operation of On-Site Audits, Etc. by Client Financial Institutions

Specification of the right to conduct on-site audits, etc.	The business consignment contract (Cloud Service Contract) should clearly state that the client financial institution has the right to conduct on-site audits, etc.
Alternative methods for on-site audits, etc.	The financial institution should be able to ask a third party skilled in conducting on-site audits, etc. to inspect the cloud service provider during normal times instead of the client financial institution conducting on-site audits, etc. directly. The conditions for this case are described later in "(3) Third-Party Audits."
Exercising the right to conduct on-site audits (Trigger and Conditions)	When taking the operation format in which on-site inspections, etc. are conducted only when a third-party audit which is a substitute for on-site audits, etc. cannot be conducted, or when it is determined that a third-party audit cannot be depended upon, then the conditions for exercising the right to on-site audits, etc. may be put in writing if necessary so that both the client financial institution and cloud service provider can share an understanding on this matter.
Expenses for receiving on-site audits, etc.	The client financial institution and cloud service provider need to discuss in advance how the expenses will be covered for the cloud service provider receiving on-site audits, etc.
On-site audits, etc. of sub-contractors	When important operations are re-entrusted, the contract between the client financial institution and cloud service provider should clearly state that the financial institution has the right to conduct on-site audits, etc. of sub-contractors.
Handling of issues pointed out in on-site-audits, etc.	The contract should clearly state that regarding issues pointed out in on-site audits, etc., the client financial institution and cloud service provider will discuss countermeasures, including whether to implement them, as well as a reasonable time period for implementing them.

b. Moderate Risk Management

When non-important operations are outsourced, then it may be possible to make use of "third-party certification"[26] reports that cover the items of on-site audits, etc. that are appropriate for the specific operations instead of on-site audits, etc. by the client financial institution (or "third-party audits" mentioned later). Depending on the significance of the operations, possible management measures include "third-party certification" reports prepared by the cloud service provider and security white papers.

(2) The Client Financial Institution Entering the Cloud service provider's Facilities

There are instances in which the client financial institution needs to enter the facilities of the cloud service provider other than those listed in "(1) On-Site Audits and Monitoring by the Client Financial Institution" above.

a. Management Measures (Operation Method)

(a) Visits to the Cloud service provider's Facilities before Signing the Contract or Starting Service

[26] Certifications of such standards as information security systems and privacy protection systems of companies by certified public accountant institutes, industry groups and other organizations of various countries. Some well-known ones include ISMS (ISO27001), PCI DSS Level 1, SOC1, SOC2, Auditing and Assurance Practice Committee Practical Guidelines No. 86, IT Committee Practical Guidelines No. 7, and PrivacyMark.

A client financial institution has the need to seek on-site confirmation of processing and data storage facilities as well as interviews with administrators to secure communication channels for the future. The main purpose of these on-site studies is not to point out flaws in internal control at data centers and other facilities. Whether these visits are allowed will depend on the cloud service provider's policies, but a client financial institution conducting due diligence to select a cloud service provider may take into consideration the cloud service provider's stance on allowing visits and information disclosure.

(b) On-site Inspections When Incidents Occur

When incidents[27] such as information leaks occur, or when they are suspected to have occurred, the cloud service provider should cooperate with the client financial institution's investigation in order to determine whether damage has occurred and, if damage has occurred, to fully ascertain the incident situation and specify a leak source or leak route. In cases that users and others conduct on-site audits to investigate serious incidents, cloud service providers are recommended to comply with requests to submit evidence.

In cases that the cloud service provider fails to supply information, the client financial institution judges that the cloud service provider was too slow to supply information, or there are questions over the completeness of the information supplied, then an on-site audit by the client financial institution itself or by a security firm or digital forensics firm designated by the client financial institution will be necessary, and the cloud service provider should accept this. Furthermore, it is recommended to clearly state it in the contract. In this investigation, the on-site inspector or the cloud service provider's operator acting under the instructions of the on-site inspector will operate the equipment to collect and analyze evidence (logs).

If the cloud service provider, due to its own policies, wishes to avoid receiving an investigation in which the client financial institution's on-site inspector or personnel from the security firm or digital forensics firm operates their equipment, then a tool will be necessary that will make it possible for the facilities of the client financial institution, cloud service provider or others to extract information needed for analysis, in order to ensure traceability. In this case, an independent third party will need to verify that this extraction tool works properly.

This kind of data extraction function may be supplied to the user as a part of their applications, but if it is not supplied or there is a problem with the completeness of the tool, then an extraction tool will need to be developed and verified separately. In this case, the client financial institution needs to agree with the cloud service provider at the time of contract signing regarding the range of evidence collection (including evidence that normally cannot be disclosed to the client financial institution because it involves the cloud service provider's other clients) and the bearing of expenses for the development and verification of an extraction tool.

(c) When There Are Concerns That the Cloud service provider May Collapse

The contract should clearly state that when there are concerns that the cloud service provider may collapse, then the client financial institution or a specialist that it designates can enter the cloud service provider's facilities if necessary to protect customer data or related works and products.

b. Moderate Risk Management

Regarding operations that the financial institution determines are relatively less important, management measures considered cost-effective can be implemented. Entering the cloud service provider's facilities may not be necessary if it is decided that risk management is possible without doing so, such as when the cloud service provider prepared and supplied a data

[27] In this case, "incidents" refer to incidents involving the operations that the client financial institution outsourced. In the event that an incident occurred in portions involving other clients of the cloud service provider, depending on the situation, this could be considered a case in which "an incident is suspected to have occurred in operations outsourced to the cloud service provider."

extraction tool.

(3) Third-Party Audits

a. Management Measures (Operation Method)

Assuming that there may be cases in which the client financial institution's on-site audits, etc. will not be effective, it needs to consider conducting third-party audits instead. Below is a summary of the three conditions that would be required for third-party audits: "verification items," "verifying party" and "verification flexibility."

(a) Verification Items

If a third-party audit is conducted instead of on-site audits, etc. by the client financial institution, then the verification items should include not just items typically related to system risks, but also take into consideration the cloud risk profile and meet the inspection needs of the client financial institution.

Furthermore, if an audit of a cloud service provider is to be conducted after the client financial institution has signed an audit contract with a third-party auditor on its own or jointly with other financial institutions, the effective method would be to first examine the results of audits already conducted on the cloud service provider and then conduct an on-site examination of the cloud service provider by focusing on points of uncertainty and missing verification items.

(Audit Guidelines Related to Cloud Usage by the Financial Industry)

Risk management ought to be conducted by financial institutions on their own volition, and each financial institution should draw up audit guidelines and standards on its own by being innovative and creative. But efforts to share and standardize audit viewpoints would help to improve the effectiveness of cloud-related audits. Under these circumstances, the FISC plans to revise the FISC Security Guidelines and the FISC Information System Audit Guidelines for Banking and Related Financial Institutions based on this report. It is expected that these audit guidelines will be used by members of the industry, including third-party auditors.

(b) Verifying Party

Taking into consideration the view that the client financial institution ought to take responsibility for conducting and leading audits, the measures described in [Figure 20] below may help to ensure the independence of the cloud service provider or third-party auditor, or to prevent a decline in effectiveness due to the involvement of a third-party auditor whose verification capabilities are not sufficient.

[Figure 20] Measures to Ensure the Independence of the Verifying Party and Prevent a Decline in Effectiveness

Ensuring independence	The client financial institution should be able to choose how to conduct an audit of the cloud service provider by clearly prescribing in a contract, either by itself or jointly with others, with a third-party auditor for audits of the cloud service provider.
	The client financial institution should shift to a system in which it bears (or partly bears) the expenses for third-party audits.
	To avoid questions over the appearance of independence if the same auditor were to conduct audits over an extended period, it would be preferable to change auditors after an appropriate period.
Preventing a decline in effectiveness	An effective way to improve the quality of audits would be to make use of an auditing scheme in which the liability for damages of the auditor is clearly stated in the contract, as exemplified by SOC 2.[28]
	To guarantee the competency of the third-party auditor, the auditor (auditing firm) should prepare and operate an appropriate quality management system based on the guidance and guidelines of the Japanese Institute of Certified Public Accountants and others.
Ensuring efficiency	An effective way to improve the efficiency of third-party audits would be for multiple financial institutions to jointly entrust audits to a third party.

(c) Verification Flexibility

It should be possible to conduct an emergency third-party audit to confirm the effect on the client financial institution after such events as: (1) serious vulnerability related to cloud computing technologies becomes apparent, (2) an incident occurs at the cloud service provider in an area related to another client, and (3) when an incident occurs at a different cloud service provider.

b. Moderate Risk Management

Similar to moderate risk management described in "III.-2.- (1) On-Site Audits and Monitoring by the Client Financial Institution," when non-important operations are outsourced, it may be possible to make use of "third-party certification" reports that cover the items of on-site audits, etc. that are appropriate for the operations instead of third-party audits. Depending on the significance of the operations, possible management measures include "third-party certification" reports prepared by the cloud service provider and security white papers.

(4) Inspections, Etc. by Financial Regulators[29]

Acting in the public interest, financial regulators examine the soundness of operations of financial institutions, including outsourced operations. The cloud service provider has a legal obligation to accept on-site inspections, etc. if requested by regulators. The items required of the client financial institution and cloud service provider in regards to on-site inspections, etc. by regulators are described in [Figure 21] below.

[28] A report on compliance and internal controls for business operations that mainly covers a service provider's security, availability, processing integrity, confidentiality or privacy.

[29] Includes requests for the submission of reports and materials.

[Figure 21] Items Required of the Client Financial Institution and Cloud service provider

Obligation to cooperate with inspections, etc. by regulators	In order to ensure that on-site inspections, etc. by regulators go smoothly, the contract between the client financial institution and cloud service provider should clearly state that the cloud service provider has an obligation to cooperate with on-site inspections, etc. by regulators.
On-site inspection, etc. of sub-contractors	The contract between the client financial institution and subcontractor should clearly state that sub-contractors (including service providers to which operations are outsourced further) have an obligation to cooperate with on-site inspections, etc. by regulators.
Handling of issues pointed out due to on-site inspections, etc.	The contract should clearly state that improvement measures should be taken promptly to address issues pointed out due to on-site inspections, etc. by regulators.

3. Dealing with Incidents

(1) Pre-Incident and Post-Incident Measures

Unlike incidents involving on-premises systems, anticipated incidents involving cloud computing include assets and data that are not under the full control of the financial institution, so the countermeasures that should be taken will differ, depending on the situation. From the viewpoint of risk management, preparations (backups, arranging alternative service, etc.) should be made in advance for dealing with expected incidents, and when an incident does actually occur, measures such as detection and separation, data collection and analysis for incident event analysis, elimination of the cause and a quick recovery, and drawing up measures to prevent recurrences are important.

(2) Ensuring Traceability

Because a cloud is a virtualized and dynamically changing environment, if an incident such as a failure or information leak should occur, it is possible that the work to identify the leaked or damaged data or to investigate the cause could become more complicated. For this reason, the financial institution needs to make preparations to ensure traceability.

When an incident occurs, the financial institution bears the responsibility to extract the necessary data, analyze it, and implement measures (or have others implement them). If it is unable to conduct the analysis on its own, then a security firm or digital forensics firm will do so on its behalf, and in this case there will be a need to enter the relevant facilities if necessary (regarding on-site investigations, please refer to "III.-2.-(2) The Client Financial Institution Entering the Cloud service provider's Facilities" mentioned earlier).

Closing Remark

The environment surrounding financial institutions in Japan is changing at an unprecedented pace, as exemplified by the diversification of products and services due to deregulation as well as consolidation and realignment among financial institutions. Under these circumstances, financial institutions need to reform their operations and make business decisions more quickly, such as understanding the needs of customers promptly and offering new financial services and products to differentiate themselves from other financial institutions. To do this, they need to be able to offer new products and services, enter or withdraw from businesses, or expand or downsize operations at low cost and speedily, and it is expected that cloud computing can be an effective tool to realize these objectives.

The Council discussed risk management for the public cloud, which has more of a resource-sharing characteristic than other types of cloud computing. Risk management will be based on the significance and risk profiles of operations and systems that will use cloud computing, and this report presents some examples and criteria for risk management measures. It is also expected that the barriers preventing the use of cloud computing will be lowered by having financial institutions properly ascertain risks and implement appropriate risk management measures based on the conclusions of the discussions by the Council.

Furthermore, in order for cloud computing to be used more effectively in the financial industry, it will be important for the various stakeholders - including financial institutions, cloud service providers and financial supervisors - to organically coordinate.

For financial institutions, as mentioned earlier, cloud computing is an effective tool for realizing quick reforms of operations and speedy management, so it is important for them to consider the use of cloud computing. Financial institutions looking to expand the use of cloud computing will work to improve risk management through such steps as creating systems that allows them to deal flexibly with new risks that may emerge due to the constant advances in cloud computing technology.

As for cloud service providers, they are expected to cooperate as much as possible with the financial institutions that outsource operations, such as by ensuring its auditability, disclosing information to improve risk management, providing information related to traceability to prepare for incidents, and supporting the work of financial institutions.

As for regulators and organizations that create voluntary rules and guidelines, it is expected that they will sequentially draw up regulations and guidelines that reflect actual conditions for cloud computing in line with the evolution of cloud computing technologies and changes in the legal system.

The Council wishes that this report will help Japan's financial institutions create or revise policies regarding cloud computing usage and risk management, and that it will help cloud service providers draw up and implement the risk management measures necessary to provide services to financial institutions.

--END--

List of Members and Observers of the "Council of Experts on the Usage of Cloud Computing by Financial Institutions"

(Honorific titles omitted)

Chairperson	*Masaru Kitsuregawa*	Director General, National Institute of Informatics, Research Organization of Information and Systems Professor, Campuswide Computing Research Division, Institute of Industrial Science, The University of Tokyo
Members	*Etsuya Shibayama*	Professor, Information Technology Center, The University of Tokyo
	Jiro Kokuryo	Vice President, Keio University Professor of Faculty of Policy Management, Keio University
	Hiroshi Kamiyama	Patent Attorney, Attorney-At-Law, Hibiya Park Law Offices
	Katsunori Tanizaki	Managing Director, Sumitomo Mitsui Banking Corporation
	Hiroki Yonezawa	Manager, Systems Division, Bank of Kyoto, Ltd. (Until the 3rd meeting)
	Nobuaki Nanchi	Tokyo Branch Manager/Tokyo Office Manager, Managing Executive Officer, The Senshu Ikeda Bank, Ltd. (Starting from the 4th meeting)
	Tetsuya Koide	General Manager, Group Management Headquarters Group, IT Business Process Unit, IT Business Process Planning Dept., The Dai-ichi Life Insurance Co., Ltd.
	Satoshi Iitoyo	Manager, IT Strategy Planning Dept./Executive Officer, Sompo Japan Nipponkoa Insurance Inc. (formerly Sompo Japan Insurance Inc.) (Until the 3rd meeting)
	Shinji Nishiwaki	General Manager, IT Strategy Planning Dept., Sompo Japan Nipponkoa Insurance, Inc. (Starting from the 4th meeting)
	Keiji Sakagami	Managing Director, IT Governance & Corporate Security Dept., Nomura Holdings, Inc.
	Akira Iwasaki	Chief Customer Officer, Salesforce.com Co., Ltd.
	Hiroyoshi Watanabe	Director and Head of Public Policy Japan, Amazon Japan K.K.
	Hiroyuki Koike	Vice President, GTS Cloud, IBM Japan, Ltd.
	Koichi Furukawa	Member of the Board of Directors, Executive Vice President/Solution Services, NTT Communications Corp. (Until the 3rd meeting)
	Motoo Tanaka	Senior Vice President, Cloud Services, NTT Communications Corp. (Starting from 4th meeting)
	Akira Maeda	Senior Manager Chief Consultant, General System Department Financial Project Management Unit, Hitachi, Ltd.
	Motohiko Nakamura	Certified Public Accountant Executive Board Member Information Technology, The Japanese Institute of Certified Public Accountants
Observers	*Makoto Koriyama*	Supervising Inspector, Head of Information Technology Monitoring, Inspection Coordination Division, Inspection Bureau, Financial Services Agency
	Hidekazu Shimura	Director, Head of Computer System Risk and Business Continuity Group, Examination Planning Division, Financial System and Bank Examination Department, Bank of Japan
	Shinsuke Akasaka	Director, ICT Security Office, Promotion for Content Distribution Division, Information and Communications Bureau, Ministry of Internal Affairs and Communications
	Masahiro Uemura	Director, Office for IT Security Policy, Commerce and Information Policy Bureau, Ministry of Economy, Trade and Industry

(The Center for Financial Industry Information Systems)

President		*Tatsuo Watanabe*
Executive Director		*Tomoo Yoshida* (Starting from the 4th meeting)
Executive Director		*Tadashi Nunami* (Until the 3rd meeting)
Planning Dept.	Director General	*Masao Yoneyama* (Starting from the 4th meeting)
Research Dept.	Director General	*Takashi Arai* (Until the 4th meeting)
Research Dept.	Director General	*Yasuo Sakurai*
Security & Audit Research Dept.	Director General	*Toshinobu Nishimura*
General Affairs Dept.	Director General	*Akinobu Saka* (Starting from the 2nd meeting)
General Affairs Dept.	Director General	*Haruhiko Nakata* (At the 1st meeting)

◆ Administrative Staff

Ryuji Enoki,
So Ozawa (Until the 5th meeting),
Takeya Miyahara,
Shoichi Okada,
Koji Shinbayashi,
Shinichi Honda (Until the 3rd meeting)

(REFERENCE) Dates of Council Meetings

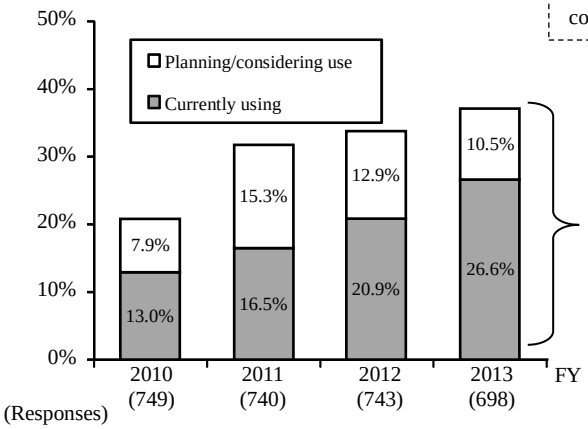
1st meeting: April 14, 2014;
2nd meeting: May 16, 2014;
3rd meeting: June 16, 2014;
4th meeting: July 7, 2014;
5th meeting: Sept. 30, 2014;
6th meeting: Oct. 20, 2014

Reference Materials

[Figure A] Usage Status of Cloud Computing

- Created based on results of the "Study on Trends and Status of Security Measures on Computer Systems for Banking and Related Financial Institutions" by the FISC
- Study base date: March 31, 2014
- Valid responses: 698

(1) Change in Cloud Computing Usage (Overall, Including Public, Community and Private)



* The study did not differentiate between "planning/considering use" and "currently using" for "public cloud".

[FY2013 Cloud Computing Usage]

	Overall Cloud	Public Cloud
Planning/considering use	73	*
Currently using	186	
Total	259	112
Percentage	37.1%	16.0%
(FY2012)	(33.8%)	(13.5%)

(2) Cloud Computing Usage Environment (Based on responses from 259 companies that indicated either "currently using" or "planning/considering use" [multiple responses allowed])

- In descending order for "public cloud" usage

		Public cloud	Community cloud	Private cloud	Total
1	Sales Support system	35	8	38	81
2	Email	33	11	29	73
3	Intracompany information sharing	29	9	39	77
4	E-learning system	23	7	16	46
5	Website structuring	22	4	14	40
6	Schedule management	18	8	23	49
7	Server	17	8	32	57
8	Attendance management system	17	4	15	36
9	Personnel system	10	4	16	30
10	Accounting system	9	4	13	26
11	Welfare system	9	5	8	22
12	Backup system	7	7	20	34
13	General affairs system	7	6	9	22
14	Asset management system	6	5	17	28
15	System development management	6	2	9	17
16	Core business system	3	10	22	35
17	OA	3	3	18	24

(3) Cloud Usage by Business Type (Ratio)

[Overall, Including Public, Community and Private] (Unit: %)

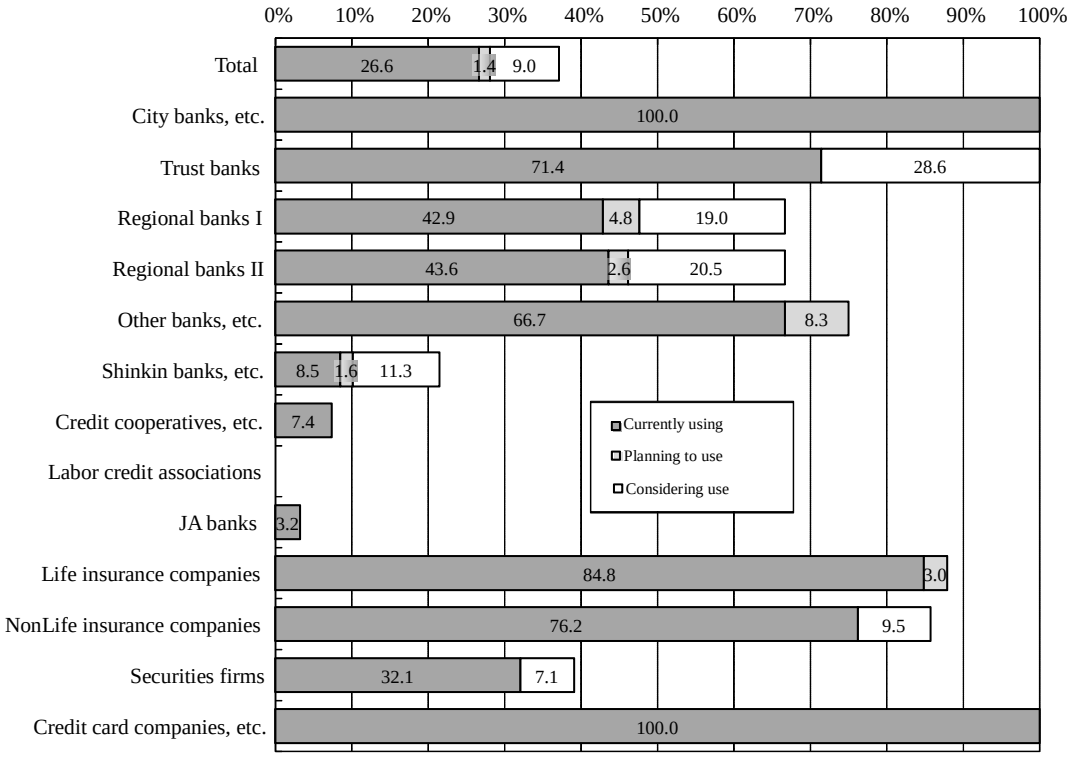
	Business type	Valid responses (companies)	Using	Currently using	Plan/consider use	No plan to use/consider use	No response
	Total	698	37.1	(26.6)	(10.4)	60.2	2.7
1	City banks, etc.	5	100.0	(100.0)	(-)	-	-
2	Trust banks	7	100.0	(71.4)	(28.6)	-	-
3	Regional banks I	63	66.7	(42.9)	(23.8)	33.3	-
4	Regional banks II	39	66.7	(43.6)	(23.1)	33.3	-
5	Other banks, etc.	12	75.0	(66.7)	(8.3)	25.0	-
6	Shinkin banks, etc.	247	21.5	(8.5)	(13.0)	77.7	0.8
7	Credit cooperatives, etc.	68	7.4	(7.4)	(-)	91.2	1.5
8	Labor credit associations	13	-	(-)	(-)	100.0	-
9	JA banks	31	3.2	(3.2)	(-)	80.6	16.1
10	Life insurance companies	33	87.9	(84.8)	(3.0)	9.1	3.0
11	NonLife insurance companies	21	85.7	(76.2)	(9.5)	9.5	4.8
12	Securities firms	156	39.1	(32.1)	(7.1)	55.1	5.8
13	Credit card companies, etc.	3	100.0	(100.0)	(-)	-	-

[Public Cloud] (Unit: %)

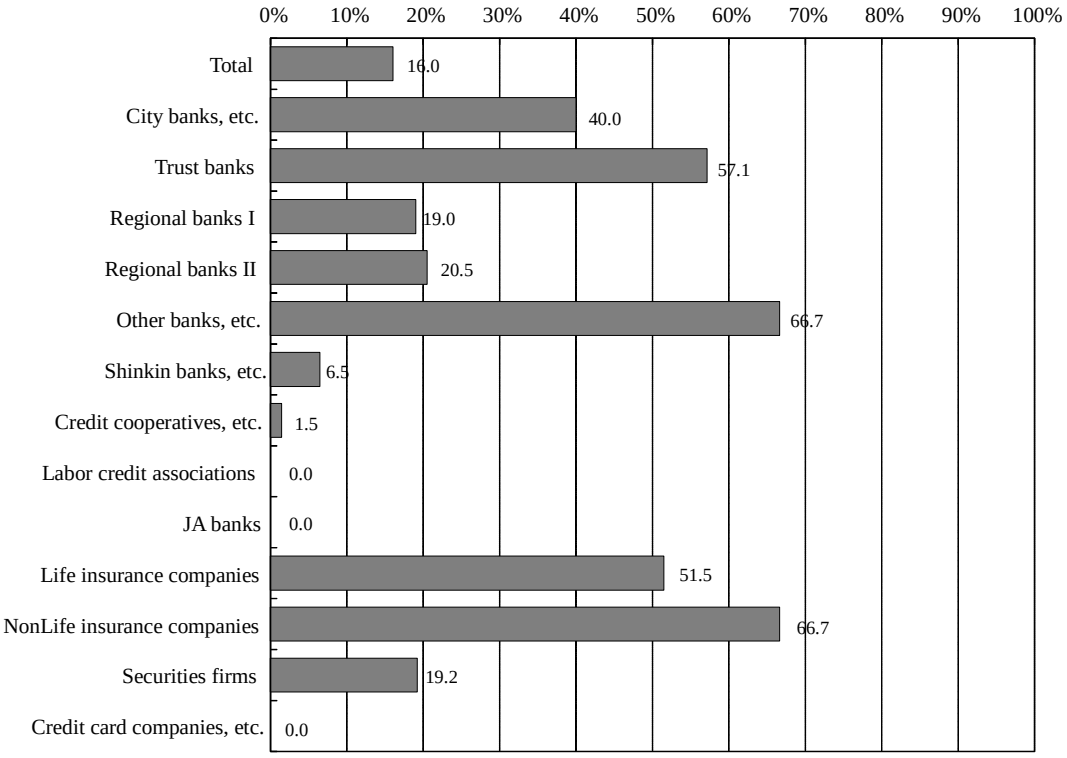
	Business type	Valid responses (companies)	Currently using, plan to use & considering using	No plan to use/consider use	No response
	Total	698	16.0	81.2	2.7
1	City banks, etc.	5	40.0	60.0	-
2	Trust banks	7	57.1	42.9	-
3	Regional banks I	63	19.0	81.0	-
4	Regional banks II	39	20.5	79.5	-
5	Other banks, etc.	12	66.7	33.3	-
6	Shinkin banks, etc.	247	6.5	92.7	0.8
7	Credit cooperatives, etc.	68	1.5	97.1	1.5
8	Labor credit associations	13	-	100.0	-
9	JA banks	31	-	83.9	16.1
10	Life insurance companies	33	51.5	45.5	3.0
11	NonLife insurance companies	21	66.7	28.6	4.8
12	Securities firms	156	19.2	75.0	5.8
13	Credit card companies, etc.	3	-	100.0	-

[REFERENCE] Graph of Cloud Usage by Business Type (Ratio)

[Overall, Including Public, Community and Private]

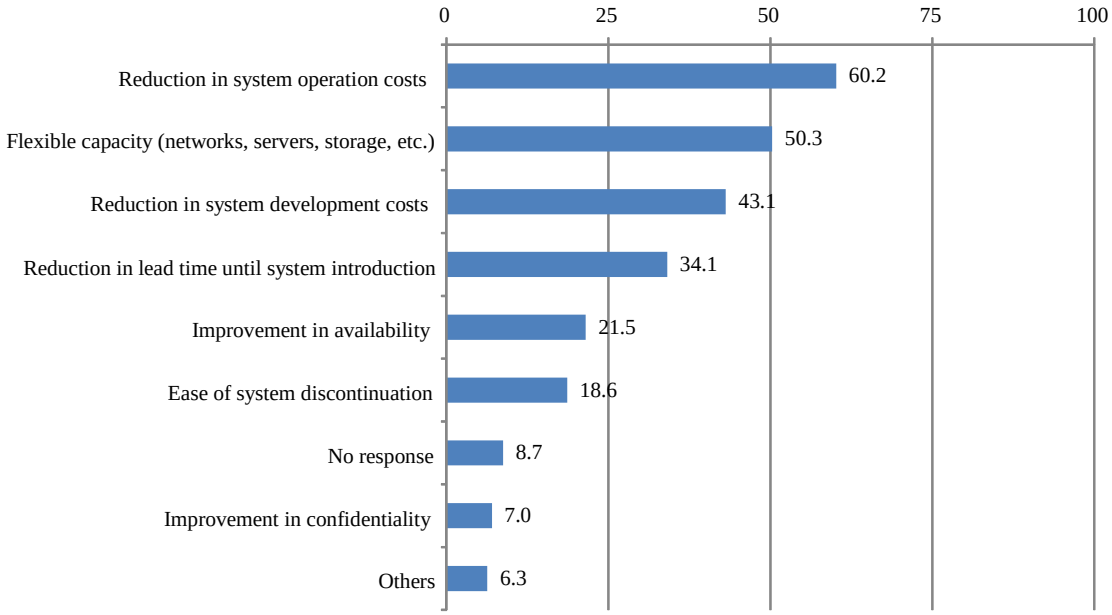


[Public Cloud] (Sum of "Using," "Planning to Use" & "Considering Use")



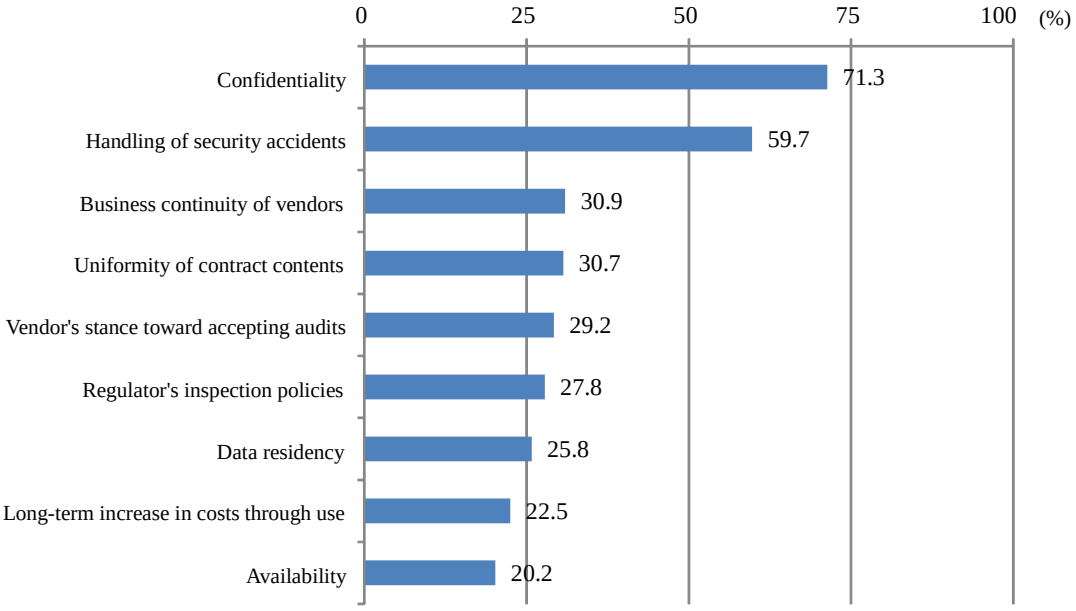
(4) Expected Benefits from Using Cloud Computing

— All financial institutions were asked what they expect the benefits of cloud computing will be. A "reduction in system operation costs" was mentioned by 60.2% of the respondents, the highest number, followed by 50.3% that cited "flexible capacity." (Total of 698 respondents; multiple replies allowed.)



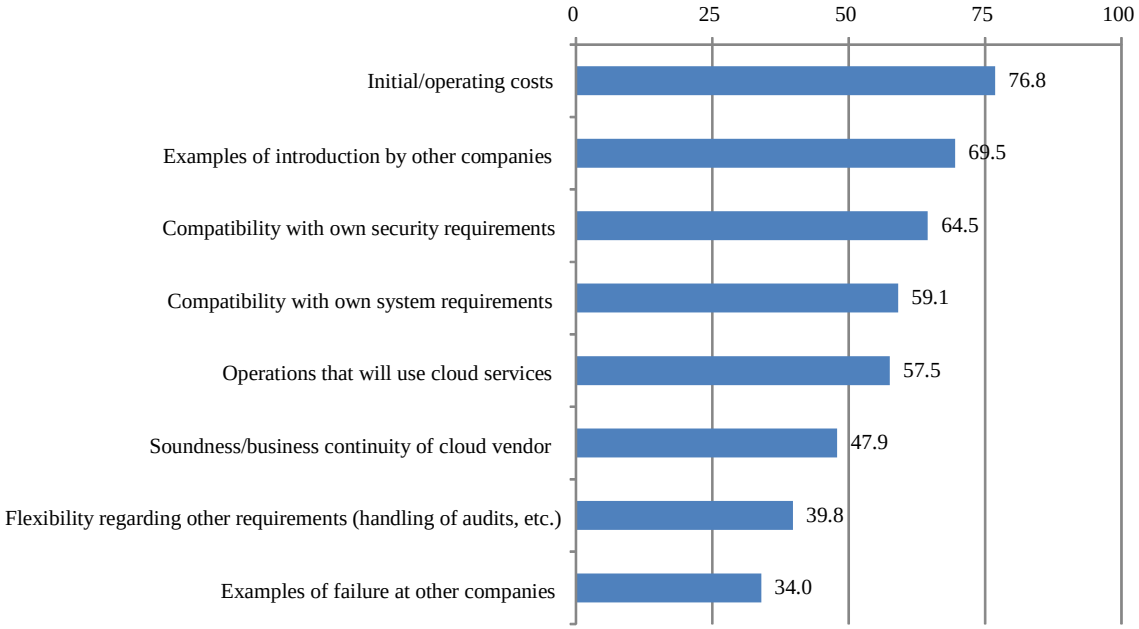
(5) Concerns About Cloud Computing Use

— All financial institutions were asked what concerns they have about using cloud computing. Concerns about "confidentiality (access management, encryption management, etc.)" were mentioned by 71.3% of the respondents, the highest number, followed by "handling of security accidents," which was cited by 59.7%. (Total of 698 respondents; multiple replies allowed.)



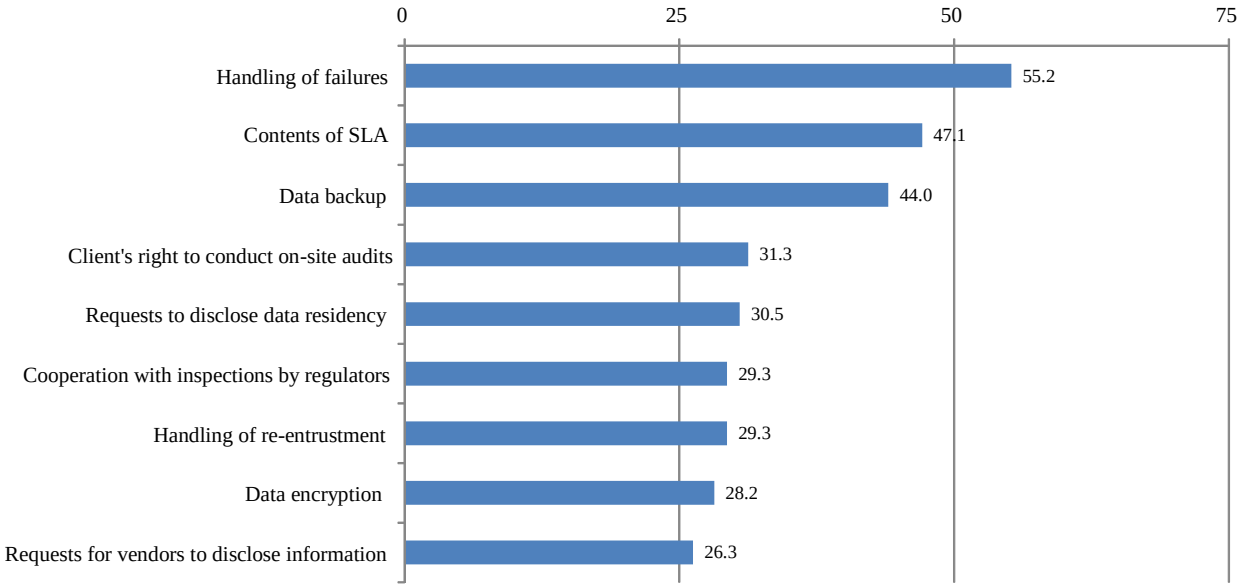
(6) Items that Financial Institutions Collected Information on as They Used or Planned Use of Cloud Computing

—— Financial institutions using or planning to use cloud computing were asked what items they are collecting information on. Many items were mentioned by a large percentage of respondents, including "initial/operating costs" and "examples of introduction by other companies." (Total of 259 respondents; multiple replies allowed.)



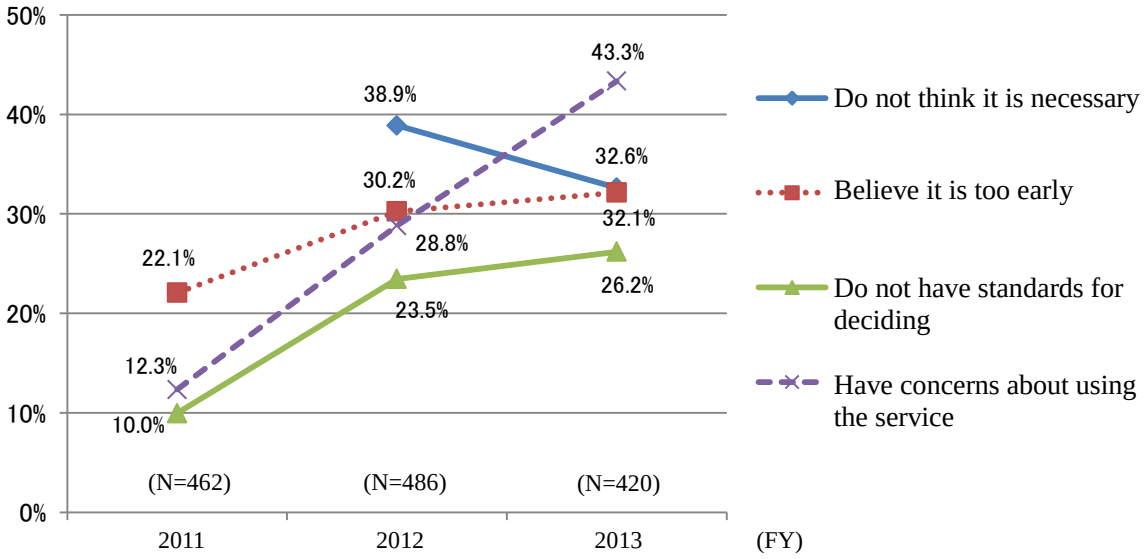
(7) Items that Financial Institutions Coordinated with Vendors as They Used or Planned Use of Cloud Computing

—— Financial institutions using or planning to use cloud computing were asked what items they coordinated with vendors. "Handling of system failures" was mentioned by the highest percentage of respondents, followed by "contents of SLA" and "data backup," showing that there was a lot of coordination over service quality. Other items cited by many respondents included "client's right to conduct on-site audits" and "requests to disclose data residency." (Total of 259 respondents; multiple replies allowed.)



(8) Reasons for Not Using/Considering Cloud Computing Use (Overall, Including Public, Community and Private)

—— Financial institutions that are not considering or planning to use cloud computing were asked the reasons why. "Concerns over using the service" was the reason that received the most responses, and the percentage giving that response grew from the previous fiscal year. (Total of 420 respondents in fiscal 2013; multiple replies allowed.)



[Figure B] Results of Hearings by the FISC

▽ Issues that are Unique to Financial Institutions

(1)	We have been taking sufficient security measures on-premise, and the system configured in-house has been sufficiently cost-effective, so there are few benefits to using cloud computing at the current point in time.
(2)	Specific standards for security measures and system auditing guidelines for cloud computing use do not exist or are insufficient.
(3)	Financial institutions bear responsibility to conduct risk management even if operations are outsourced to a cloud service provider, but we are unable to sufficiently control the cloud service provider because we have no choice but to accept the contract template presented by the cloud service provider.
(4)	It is not clear if they will erase the data for sure when ending service. Also, there are uncertainties over whether the cloud service provider will cooperate with the work of transferring to a new system.
(5)	It is not clear if the cloud service provider will cooperate with inspections of its facilities by the Financial Services Agency under the Banking Act.
(6)	The cloud service provider will not comply with on-site audits. Also, regarding the results of third-party certification that were presented as an alternative to on-site audits, the audit items are standard ones decided in talks between the cloud service provider and the auditing firm, and there is little room to include items that the client financial institution would like to have checked.
(7)	Cannot use cloud computing for core-banking systems because the SLA for the cloud service does not guarantee 24 hours/365 days availability.

▽ Ordinary Issues

(8)	It is not clear how personal data (or encrypted or fragmented personal data information) that exists in the cloud environment will be handled under the Act on the Protection of Personal Information.
(9)	There is a possibility that important data, including personal information, will be viewed by domestic and foreign authorities.
(10)	Cloud service providers' stance on the disclosure of information is insufficient. More than a few cloud service providers refuse to disclose information other than the prescribed items by citing anti-terrorism measures and the protection of intellectual property.
(11)	When considering use of the cloud to manage data, including personal information, we asked about the specific encryption specifications and details about access control from the viewpoint of checking whether the confidentiality of the data is properly secured, but the cloud service provider refused to reply.
(12)	Many of the documents are in English. Also, there are many cases in which the Japanese branch does not have the authority to reply to inquiries and requests, so we are concerned whether the cloud service provider will properly deal with any problems that may arise.

[Figure C] Public Cloud Usage Examples

—— Created using information provided by members of the Council

(Domestic)

(1) Sales Support Systems

Business type		SaaS, PaaS or IaaS	Details of operations	Type of data in the cloud	Effects of introduction				
					Cost reduction	Speedy introduction	Improved convenience/ functionality	More efficient operations	Notes
1	Bank	S	Corporate CRM	Borrower info, Item info, Activity log		○	○	○	
2	Bank	S	Retail CRM	Customer info, Inquiry info, Product application info	○	○		○	
3	Securities	S	Ops for institutional investors, Global CRM	Customer info, Negotiation records	○	○			Improved customer service
4	Bank	S	Corporate sales compliance management	Borrower info, Negotiation records		○			Stronger compliance
5	Securities	S	Management of sales to affluent clients	Customer info, Item info, Activity info			○		Stronger sales, flexible customization
6	Nonlife insurance	P	Agent management control	Agent management info, Solicitor info				○	Paperless
7	Life insurance	P	Prospective customer integrated database, New corporate customer development using face-to-face/Web channels	Customer info	○			○	
8	Life insurance	S P	Customer management, Corporate sales support, etc.	Customer info, etc.		○			Improved productivity/ security by handling in the system fields that were not handled in a system before
9	Credit cards	P	Partner card applications, Portal site building	Customer info		○			

(2) Contact Centers & Help Desks

Business type		SaaS, PaaS or IaaS	Details of operations	Type of data in the cloud	Effects of introduction				
					Cost reduction	Speedy introduction	Improved convenience/ functionality	More efficient operations	Notes
1	Bank	S	Contact center operations	Customer info, Inquiry info		○		○	
2	Bank	S	Call center operations	Customer response history, Customer info	○	○	○		
3	Life insurance	S	Outbound call center operations	Customer info	○			○	Used to integrate prospective customer databases and linking information with outbound call center
4	Nonlife insurance	S P	Call center, Sales activity management, Sales support back office, etc.	Contact history, Materials request info, Phone log, etc.	○	○			IT staff able to concentrate on main business
5	Nonlife insurance	S	Agent system help desk	Agent info, Solicitor info	○	○			

(3) In-House Information Sharing Systems

Business type		SaaS, PaaS or IaaS	Details of operations	Type of data in the cloud	Effects of introduction				
					Cost reduction	Speedy introduction	Improved convenience/ functionality	More efficient operations	Notes
1	Bank	S	Enterprise SNS	Comments on SNS			○		Stimulated exchanges within bank
2	Bank	I	Info sharing system	n/a	○	○			Disaster measures
3	Securities	S	Enterprise SNS	(No customer info on cloud)				○	
4	Securities	S	Enterprise case management, Fault management	Employee info, Internal rules, Item info, Fault management, Various inquiry info	○				Stimulated communication within company
5	Nonlife insurance	P	Enterprise info sharing, Various application workflows, schedules, etc.	Employee info, Various documents, Customer info	○	○			Stronger security
6	Nonlife insurance	S	Email, Calendars	Email data, Activity schedules	○				IT staff able to concentrate on main business

(4) Others

Business type		SaaS, PaaS or IaaS	Details of operations	Type of data in the cloud	Effects of introduction				
					Cost reduction	Speedy introduction	Improved convenience/ functionality	More efficient operations	Notes
1	Bank	I	Workflow system, Document management, Integrated monitoring, Campaign sites, etc.	n/a	○	○		○	Roughly 37% reduction in costs
2	Bank	P	Investment trust application management, Info sharing between banks	Customer info, Product info		○			Development of partner financial institutions
3	Bank	S	Uncollateralized loan screening applications	Customer info, Credit info (Number of loans/balance at other companies)		○		○	Quick launch of application management site
4	Bank	S	Social listening	SNS, Blog			○		Confirmed reviews of own products/services, Measured effects of promotions, Improved product planning
5	Bank	P	Management of budgets with IT vendors	Item info, Budget info			○	○	Broke free from Excel-based management, More efficient information sharing
6	Bank	S	Market integration solutions	n/a	○	○	○		Ensured security, BCP measures
7	Bank	P	Management of loss incidents for operational risks, Tabulation by category	Operational risk info, including administrative risks, system risks, lawsuit risks	○	○			Cost reduction from existing system (on-premises)
8	Life insurance	I	Risk calculation system	n/a	○	○			Easy verification of optimal system configuration
9	Bank	I	Investment trust info providing system	n/a	○	○			Released in 2 months, including app development
10	Securities	I	Stock price delivery system	n/a	○	○	○		
11	Securities	I	Website load balancing and video distribution	n/a		○			Configuration completed in 2 days
12	Life insurance	P	Public web server	Corporate info, Product info, etc.	○				Stronger security, Disaster measures
13	Life insurance	S	Real estate management	n/a	○			○	
14	Bank	P	Project/budget management for systems segment	Project info, Various documents	○	○			
15	Bank	P	Access control, Intradepartmental business support	Employee info, Investment internal memo info				○	Development productivity, Paperless
16	Insurance	S P	New-graduate recruitment management, Company vehicle management, asset management	Various info, including customer info		○		○	Improved security
17	Nonlife insurance	S	Development environment service	n/a	○	○			Built development environment depending on need, information sharing within projects, etc.

(Overseas)

(1) Sales Support Systems

Business type		SaaS, PaaS or IaaS	Details of operations	Type of data in the cloud	Effects of introduction				
					Cost reduction	Speedy introduction	Improved convenience/ functionality	More efficient operations	Notes
1	Bank (Europe)	I	Backup/recovery solutions for front-office CRM service	CRM info, etc.		○			Ensured solid security, Ensured business continuity
2	Bank (Europe)	I	B2B transaction support base, Use social functions to find new borrowers and support business promotion	Customer info, Transaction info	○	○			Solid security, Ensure 24 hrs/365 days availability & performance
3	Bank (N America)	S	Business process management	Data related to wholesale banking processes				○	Improved efficiency of business processes (Target: 10% increase in 1-2 years)
4	Bank (N America)	S P	Customer management, Info sharing, Item transfer/tracking, etc.	Customer info, Employee info, Corporate info		○		○	Raised level of sales activities while covering compliance and security, Released apps at incredible speed, Improved customer acquisition rate by managing leads and referrals, Improved efficiency of management level, Ensured and improved security level
5	Bank (N America)	S P	Monitor/manage social communications	Customer info			○	○	Established social banking hub, Real time responses
6	Bank (Asia)	S P	Multi-channel services, Fusion of sales and services (cross-selling/up-selling)	Customer info, Employee info			○		Contributed to profit growth, Used advanced CRM, Promoted smartphone banking, Strengthened asset management
7	Bank (Australia)	I	More than 30% of applications owned by the Company	n/a	○				
8	Bank (N America)	P	Loan origination	Customer info, Employee info, Corporate info				○	Signed contracts at quadruple the speed of industry average, Expanded to small/midsize companies, retail

(1) Sales Support Systems (continued)

Business type		SaaS, PaaS or IaaS	Details of operations	Type of data in the cloud	Effects of introduction				
					Cost reduction	Speedy introduction	Improved convenience/ functionality	More efficient operations	Notes
9	Insurance (N America)	S P	Integrated portal, Tracking customers' social activities	Customer info, Corporate info			○		Realized integrated portal for 10,000 independent advisors
10	Bank (N America)	S P	Analyze trends of online customers	Customer info, Corporate info				○	Realized linking of offers. leads and products, Offered end-to-end comprehensive process that spans business segments
11	Bank (N America)	S P	CRM	Customer info, Corporate info			○	○	Standardized sales techniques, Full linking with core system
12	Bank (N America)	S P	CRM, Banking platform centering on end-to-end and customers	Customer info, Corporate info		○			Achieved front office reform in 10 months, Completed account opening in 10 minutes instead of 1 hour
13	Bank (Australia)	S P	Put info collected via phone and Web into the cloud	Customer info, Corporate info	○		○		Access from multiple regions, Cost reductions, Legal compliance
14	Bank (N America)	S P	Mortgages	Customer info				○	More efficient operations, Improved customer satisfaction, Develop prospective customers
15	Bank (N America)	S P	Integrated customer management (wholesale), Social communication, Social marketing	(Customer info), Employee info, Corporate info, Social info			○		Improved customer service by being constantly connected with customers via multiple channels and social, Better speed and response to change
16	Insurance (Europe)	S P	Customer management, Agent management, in-house communication	Customer info, Employee info, Corporate info				○	Built system that allows better connections with customers, Full use of iPads, Improved customer service, Smoother in-house communication
17	Securities (N America)	S P	Investment customer management, Customer management, Mobile	Investment customer info, Customer info, Corporate info			○	○	Unification of customer service through investment advisory ops, Customer service using mobile
18	Life insurance (N America)	I	Insurance purchase application system	Personal info	○				Configured system in the cloud while complying with such regulations and security requirements as GLBA and PCI DSS

(2) Contact Centers & Help Desks

Business type		SaaS, PaaS or IaaS	Details of operations	Type of data in the cloud	Effects of introduction				
					Cost reduction	Speedy introduction	Improved convenience/ functionality	More efficient operations	Notes
1	Bank (U.S.)	I	Analytic solutions for the service desk	Info on service desk tickets		○		○	Reduction in call volume & incident tickets, Improved self-help capability of end users
2	Bank (N America)	S P	Unification of contact point for inquiries through integrated customer portal, Mortgage portfolio management	Customer info, Regulation info, Corporate info		○		○	Unification of 17 types of systems, Improved work efficiency of 20,000 core employees, Smooth compliance with regulations, Introduction in 120 days
3	Bank (N America)	S	CRM, Call center	Customer info, Employee info, Corporate info	○		○		Building a system that unifies and shares customer service info allowing cyclic tracking from initial lead, to contract conclusion, to the next business (standardization of sales process)

(3) Others

Business type		SaaS, PaaS or IaaS	Details of operations	Type of data in the cloud	Effects of introduction				
					Cost reduction	Speedy introduction	Improved convenience/ functionality	More efficient operations	Notes
1	Bank (Australia)	I	Transfer of more than 2,000 applications, including mission-critical ones	n/a		○	○		
2	Bank (Australia)	I	Re-construction of website	n/a	○				Cost reduction of more than 60%
3	Bank (Europe)	I	Risk simulation system	n/a	○			○	Shortening of calculation time (from 23 hours to 20 minutes), Flexible resource use, Server purchase became unnecessary

[Figure D] The Handling of Cloud Services Under the "FISC Security Guidelines" (Supplements to the 8th Edition)

[O-108] Risks should be managed appropriately when using cloud services.

1. When using cloud services, appropriate risk management is necessary in accordance with the approach toward outsourcing management.

2. The following are some of the items that should be managed.
(1) Clarification of the purpose, scope, etc. when using cloud services [O-87]
(2) Clarification of the procedures for selecting the cloud service provider [O-87-1]
(3) Sign a contract that includes items related to security measures, regardless of the outsourcing format [O-88]
The contract should include agreements on the boundaries of management and responsibilities with the cloud service provider.
The following are some of the items that should be agreed upon.
1) Security management methods and framework [O-1 & 3]
2) Frameworks for system, data management for system, data management and network management [O-4-6]
3) Creation of manuals to deal with failures & disasters, recovery procedures and education/training [O-15, 63 & 83]
4) Backup of data for using cloud services [O-27]
5) Erasure of data when canceling or ending use of cloud services [O-75]*
Furthermore, a "risk management contract" may have to be signed separately from a "service usage contract," if necessary.
* For cloud services, system resources are usually the assets of the cloud service provider, so it may be difficult for the financial institution, etc. to erase data on its own. In that case, the cloud service provider may conduct the data erasure and provide a certificate, etc. that states it has done so.
(4) The laws that apply in the event of a dispute with the cloud service provider, and a risk assessment if the court with jurisdiction is in another country.
The following are some of the risks that should be assessed.
1) Ascertainment and analysis of local laws and regulations as well as judicial systems
2) Securing of attorneys qualified to practice locally
3) Economic and human resource costs for conducting meetings, appearing in court and other activities in unfamiliar, remote locations
4) Dealing with all of the above in a foreign language
…Etc.

3. There is a need to conduct system audits of the cloud service being used to ascertain and evaluate its effectiveness, efficiency, reliability, compliance and security.
Please refer to [O-90 & 91] regarding system audits.

4. Regarding equipment standards, technological standards and operating standards in addition to those for outsourcing management that are referred to in these guideline items, please refer to those standards when necessary.

5. When the standards being referenced include the term "outsourcing contract," this should be replaced with a "service usage contract," such as "usage contract" and "terms of service" when referencing the documents.

[Figure E] Definition of Outsourcing Under the Financial Services Agency's Supervisory Guidelines

When a bank outsources its operations to a third party (hereinafter referred to as "outsourcing"), it may be able to not only improve the efficiency of its operations, but also to deal with the diverse needs of its customers and respond quickly to rapid technological innovations, for example, by outsourcing operations to a more specialized party. However, since a bank that outsources needs to protect its customers while ensuring sound and appropriate operations, including appropriate management of the risks that accompany outsourcing, banks are legally required to take measures to ensure appropriate execution of outsourced operations (Article 12-2, Clause 2 of the Law; Article 13-6, Clause 8 of the Enforcement Regulations).

...

(Note 1) Outsourcing includes a bank outsourcing any administrative work necessary to conduct its operations to a third party (including cases in which an outsourcing contract was not officially signed but the actual conditions can be considered outsourcing, or when the outsourced operations are conducted overseas).

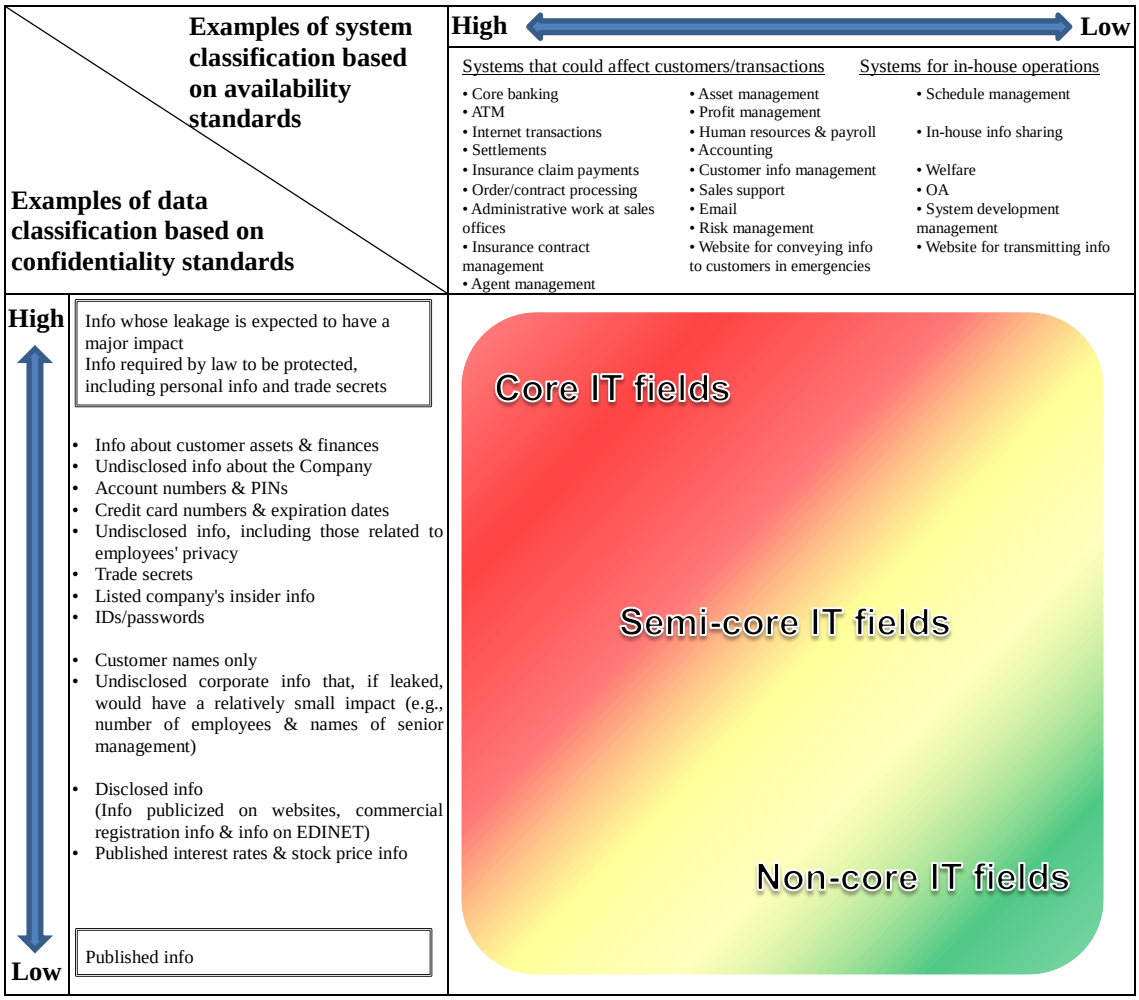
<*The rest is omitted*>

[Figure F] Risks That Should Be Considered for Usage of Cloud Computing by Financial Institutions

No.	Class	Risk	Details
(1)	Risks related to legal systems	The effect of authorities intercepting communications or taking enforcement action against other users	• In the unlikely event that enforcement action is taken against another user, there is a possibility that authorities will prohibit changes to hardware in which the client financial institution's own data is stored or seize that hardware, preventing the client financial institution from processing the data or resulting in the contents of the data becoming known to authorities. • Similarly, if domestic or foreign authorities conduct operations to intercept the communications or browse the data of another user, then information related to the client financial institution's data processing could be subject to interception and other actions.
(2)		Impediment to on-site audits by the client financial institution and inspections by Japanese authorities	• On-site audits and inspections are difficult due to travel expenses, time needed, etc. • Foreign clients or foreign regulators may have difficulty conducting audits and inspections.
(3)		Impact of difference in legal systems	• Differences in demands for the protection of privacy and other factors depending on the country (jurisdiction) could hamper countermeasures in the event that problems occur, or for the transfer of personal data. • If processing is dispersed across multiple countries (jurisdictions), the laws that apply may not be clear (privacy laws and financial regulations are compulsory provisions, so it may be difficult to designate the applicable laws through the contract). In this case, in order to avoid legal risks, responses should be made by assuming that the laws of the country (jurisdiction) with the toughest rules will apply.
(4)		Intelligence activities or data browsing by foreign authorities	• Foreign governments may intercept communications lines or browse data within their jurisdictions for the purpose of fighting terrorism, maintaining security or preventing tax evasion.
(5)	Risks related to technology	Effects of attacks from the outside	• Since data center facilities, processors, storage and networks are shared among multiple users, attacks against others users that share the infrastructure could have an effect on the client financial institution.
(6)		Effects of inappropriate activities by other users	• Unauthorized actions or operational mistakes by other users that share the system could have an effect on the client financial institution.
(7)		Effects of difficulties in physical erasure of data	• There is a risk of any remaining data leaking because of the difficulty of complete data erasure by physically destroying or degaussing hardware when the service ends.
(8)		Data leakage from transmission routes	• Unlike on-premises environments, this framework is based on the transmission of data over the network, which will cause a bigger risk of data leaking during data transmission.
(9)		Ease of probing from the outside	• The fact that many components that comprise the system exist on the network means that probing from the outside using specialized technologies is relatively easy, so outsiders may be able to easily ascertain the full picture of the system configuration.

No.	Class	Risk	Details
(10)		Effects of the network connection becoming interrupted	• Unlike when hosting in one's own building, the client financial institution cannot receive the service if the network connection is interrupted.
(11)	Risks related to operations	Concerns about real time and availability	• Increased traffic for other users could result in a shortage of resources for processing one's own users, possibly leading to poor response and system shutdown, so the expected level of service may not be guaranteed.
(12)		Effects of outsiders entering data centers	• On-site audits by the client financial institution or inspections by regulators could be affected if they take place at the same time as on-site audits by other companies or inspections by regulators. • The client financial institution's operations could be affected if there are problems with on-site audits by other companies.
(13)		Problems with the cloud service provider's processing of jobs straddling its service area	• The cloud service provider could have problems with processing jobs that straddle its service area due to requirement inconsistencies, insufficient coupling tests, etc.
(14)		Poor handling of incidents	• In case an incident occurs, cloud service providers may shift the responsibility among each other, for example, hampering the ascertainment of the current status and recovery.
(15)		Difficulty in viewing items necessary for risk management	• The cloud service provider may be reluctant to disclose information because it is using new technologies. • The system structure may be highly complex due to redundancy and dispersion of resources.
(16)		Vendor lock-in	• Sufficient consideration may not have been taken for the smooth transfer of data and systems at the end of service.
(17)	Risks related to governance	Inappropriate control environment at sub-contractors	• Users may have difficulty exerting direct control over sub-contractors to which cloud service providers outsource operations because sub-contractors have not signed contracts directly with the user. As a result, users may not be able to ensure a sufficient control environment at sub-contractors.
(18)		Difficulty in responding to individual needs regarding risk management	• Cloud service providers place weight on cost-saving and starting services, so they may be reluctant to provide more than standardized user support. As a result, they may not disclose information that users need for risk management or to handle incidents sufficiently.
(19)		Effect of specification restrictions for risk management	• Depending on the cloud service, there are cases in which not enough consideration is given to "measures to deal with information leakage risks," which is something that the financial industry is very interested in.

[Figure G] Examples of System/Data Classification Based on Significance



[Figure H] List of Risk Management Measures (Examples)

Risk management items		Standard*	Strict management ←——→ Moderate management		
At the use examination	Cloud service provider selection	Comprehensive evaluation	• Evaluation of risk management status based not only on disclosed info but also by asking the cloud service provider to disclose undisclosed info	• Evaluation based not only on disclosed info but also on reputation & track record of the cloud service provider	• Evaluation based mainly on disclosed info
	Data residency	Confidentiality	• Location region (country, state, etc.) should be ascertained, specific enough so that the laws that will be applied to the cloud service will be known • Location should be ascertained in cases that on-site access will be necessary due to an incident occurring	• Data residency is unnecessary if important data is not stored or processed	
On the contract signing	Service level	Availability	• Items necessary for risk management should be included in the outsourcing contract or SLA/SLO • Customization of the standard agreement presented by the cloud service provider to match the financial institution's own security policy	• Customization of the standard agreement presented by the cloud service provider is not necessary	
	Information disclosure	Comprehensive evaluation	• Request that the cloud service provider disclose info in addition to the cloud service provider's standard info disclosure to match the financial institution's own security policy • Request disclosure of information about architecture as necessary for risk management	• Not necessary to request disclosure of information in addition to the cloud service provider's standard info disclosure	
	Outsourcing to multiple service providers	Comprehensive evaluation	• Clarification of the main contractor is necessary	• Clarification of the main contractor would be recommended	• Clarification of the main contractor is not necessary
	Sub-contractor management	Comprehensive evaluation	• Strict advance screening & monitoring is necessary	• When re-entrustment operations that are not important, strict advance screening is not necessary • Sub-contractors should be checked & monitored as needed	
			• If the cloud service provider's advance screening is more effective, then that can be used instead of the financial institution's (The financial institution itself should conduct advance screening if especially important operations will be re-entrusted)		
During operations	Data encryption, etc.	Confidentiality	• Such measures as encryption are necessary to protect highly confidential info, including personal data, that is stored/transmitted • Storage & management of the encryption key by the financial institution would be recommended	• For highly confidential info other than personal data, such measures as encryption to protect the storage/transmission of data would be recommended	• Protection using encryption, etc. is unnecessary when important data is not being handled
	Failure/ replacement of storage equipment, etc.	Confidentiality	• Physical/logical erasure of data stored on the storage media • Contract or SLA should clearly indicate that any storage equipment will be turned into a state incapable of being restored before it is moved outside of the facility	• Physical/logical erasure is unnecessary if important data such as confidential personal info is not being handled	
On contract expiry(or termination)	Data erasure	Confidentiality	• Physical erasure or irreversible logical erasure should be conducted for important data, such as highly confidential personal info • Although the issuance of a data erasure completion certificate would be recommended, this could be omitted if the contract states that the data will be erased and the effectiveness of that action can be confirmed through a third-party audit	• Physical/logical erasure is unnecessary if important data, such as confidential personal data, will not be handled • A data erasure completion certificate would also be unnecessary	
	Vendor lock-in	Comprehensive evaluation	• Request cooperation in extracting data that needs to be transferred to the new service provider or to an in-house system	• Confirmation of existence of a method of extracting data for transfer • Work to be done by the client financial institution	• Select potential alternative cloud service providers in advance
On-site audits & monitoring by the client financial institution		Comprehensive evaluation	• The outsourcing contract should clearly state that the client financial institution has the right to conduct on-site audits to verify appropriate management of the outsourced operations • Under agreement, the contents of limited operation of such audits should be put in writing	• The outsourcing contract should clearly state that the client financial institution has the right to conduct on-site audits • On-site audits, etc. could be replaced by using the results of third-party certification and adding the financial institution's risk profile	• Clearly stating the right to conduct on-site audits, etc. is not necessary • The results of third-party certification or security white papers could replace on-site audits, etc.
Entering of the cloud service provider's facilities by the client financial institution		Comprehensive evaluation	• An on-site investigation is necessary when an incident occurs • When the cloud service provider is at risk of going bankrupt, its facilities should be entered to protect data, etc.	• Request that the cloud service provider promptly present log info necessary for analysis when an incident occurs, or have it prepare a tool for extracting the necessary logs • When the cloud service provider is at risk of going bankrupt or if the steps outlined above are not possible, then it will be necessary to protect data through such steps as entering the cloud service provider's facilities	• On-site investigation or the protection of data when the cloud service provider is at risk of going bankrupt are not necessary
Third-party audits		Comprehensive evaluation	• Audit led by financial institution is necessary • Third-party audits can be conducted if the conditions of "verification items," "verifying party" and "verification flexibility" are met.	• The use of third-party certification is possible if the verification contents are sufficient based on the client financial institution's risk profile	• Third-party certification, security white papers, etc. can be used instead

* The main management axis that should be considered when deciding the appropriate level for risk management measures for each risk management item.
Availability: Risk levels should be decided mainly based on whether availability is high or low
Confidentiality: Risk levels should be decided mainly based on whether confidentiality is high or low
Comprehensive evaluation: A decision should be made by looking at both availability and confidentiality comprehensively

[Figure I] High-Confidentiality Data (Examples)

Class	Data examples
Personal information	• Name, date of birth, sex and address • An individual's credit information • An individual's "sensitive information," such as illness history, religion and legal domicile • Account number/PIN, credit card number/expiration date and transaction data
Corporate information	• Information regarding a company's creditworthiness • Insider information about a listed company, etc. Note: Information that can be acquired by viewing a company's registration, such as company name and capital, should be treated as "public information."
Information about the client financial institution	• Undisclosed information that, if leaked to the outside, could have an impact on confidence in the client financial institution
Information provided by public institutions, etc. on the understanding that it would be kept secret	• Information that, if leaked to the outside, could hurt the public interest (inspection results by regulators, information about anti-social forces, etc.)

[Figure J] Practical Guidance on Safety Management Measures for the Guidelines on Personal Information Protection in the Financial Industry

III. "Supervision of Subcontractors" Under Article 12 of the Guidelines on Personal Information Protection in the Financial Industry

Under Article 12, Clause 3 of the Guidelines, companies that handle personal information in the financial industry must, when outsourcing the handling of personal data, select a subcontractor that can be recognized to handle personal data appropriately and ensure that the subcontractor is taking security control measures for that personal data.

(Standards for Selecting Subcontractors in Regards to Protection of Personal Data)

5-1. When a company that handles personal information in the financial industry outsources the handling of personal data, based on Article 12, Clause 3-1 of the Guidelines, it must set the items below as standards for selecting the subcontractor, select the subcontractor in accordance with the standards, and periodically review the standards.

(1) Creation of basic policies, handling rules, etc. regarding security control of personal data at subcontractors
(2) Creation of an implementation system for security control of personal data at subcontractors
(3) Confidence in security control of personal data at subcontractors based on track record, etc.
(4) Soundness in management of subcontractors

5-1-1. Standards for the selection of subcontractors must include the following items as part of "Creation of basic policies, handling rules, etc. regarding security control of personal data at subcontractors."

(1) Creation of basic policies regarding security control of personal data at subcontractors
(2) Creation of handling rules regarding security control of personal data at subcontractors
(3) Creation of rules regarding the inspection and audit of the status of handling of personal data at subcontractors
(4) Creation of rules regarding outsourcing by subcontractors

5-1-2. The standards for the selection of subcontractors, as part of the "Creation of an implementation system for security control of personal data at subcontractors," must include systematic security control measures under I.-(2)-1), human security control under 2) of the same clause, and technical security control under 3) of the same clause. Furthermore, when the subcontractor outsources operations, then standards must be set regarding the status of implementation systems for security control at the sub-contractors.

5-2. Companies that handle personal information in the financial industry must, based on 5-3, periodically or whenever the need arises, confirm compliance to the items set in the standards for subcontractor selection after the outsourcing contract is signed, and if the subcontractor is not meeting the standards, provide supervision so that the subcontractor meets the standards.

(Items Regarding Security Control that Should be Included in Outsourcing Contracts)

5-3. Companies that handle personal information in the financial industry must include in any outsourcing contracts the items related to security control shown below.

(1) Authority regarding supervision and auditing of subcontractors as well as the seeking of reports
(2) Prohibition of the leakage, theft, alteration or unauthorized use of personal data by subcontractors
(3) Conditions for re-entrustment
(4) Accountability of subcontractors in the event that information leaks, etc. occur

5-4. Companies that handle personal information in the financial industry must, based on 5-3, periodically or whenever the need arises, confirm that the subcontractor is complying with security control measures, and if the subcontractor is not meeting the requirements stated in the contract, provide supervision so that the subcontractor meets the requirements stated in the contract. Furthermore, companies that handle personal information in the financial industry must periodically review the security control measures included in the outsourcing contract.

Report of the Council of Experts on the Usage of Cloud Computing by Financial Institutions

Published March 2015
Edited & Published: The Center for Financial Industry Information Systems

4th Floor, Sumitomo Irifune Bldg.,
2-1-1 Irifune, Chuo-ku, Tokyo 104-0042
JAPAN

Phone: +81-3-5542-6060
Fax: +81-3-5566-1052
URL: https://www.fisc.or.jp/
E-mail: infofisc@fisc.or.jp

© This report may not be reproduced or copied in any form, in whole in part, without permission from the publisher.