Report of the Council of Experts on FinTech in Financial Institutions

June 2017

The Center for Financial Industry Information Systems

Table of contents

Introduction

In recent years, efforts to deliver innovative financial services through use of information technology (IT), referred to generally as FinTech, have been advancing rapidly among Financial Institutions, industry organizations, regulators, and others. (See References, Reference 1)

Amid expectations that FinTech will see widespread use in the future as a result of the advancement of such efforts, the Center for Financial Industry Information Systems ("FISC" hereinafter) is expected to consider in advance the ideal forms of security measures related to FinTech, in tempo with developments among Banking and Related Financial Institutions.

Already, the FISC Council of Experts on Outsourcing in Financial Institutions ("Outsourcing Council" hereinafter), which completed its activities in June of last year, has proposed the new frameworks of a risk-based approach and IT governance and effected considerable progress in thinking on security measures in financial information systems, reflecting consideration of matters including developments in the leading Western nations.

The Council of Experts on FinTech in Financial Institutions ("FinTech Council" hereinafter) was established to identify explicit, practical guidelines regarding the ideal form of security measures for FinTech in Japanese Financial Institutions, based on such findings of the Outsourcing Council.

Participants in this the Council included academic experts, Financial Institutions, IT solution providers, and others as committee members, along with observers from regulators and others. The Council's deliberations were intended to enable Financial Institutions in Japan to enjoy the maximum benefits of FinTech innovations suited to customer needs while maintaining system security. These deliberations are summarized in this report.

Accordingly, the content of this Report is useful for reference by a wide range of parties involved in IT governance and IT management at Financial Institutions, including not only the system risk management sections but also top management, management, sections responsible for systems, system auditing sections, and others. It also is hoped that it will be referred to by not only Financial Institutions but all parties involved in financial information systems, such as IT solution providers (including Cloud solution providers) and firms involved in FinTech.

I. Consideration of security measures related to FinTech

1. Steps employed in consideration

First of all, since the operations related to financial services known generally as FinTech ("FinTech operations" hereinafter) are broad ranging, there is a need for guidelines to use in determining whether or not the information systems handling such operations are (or should be) subject to the Security Guidelines[1].

Next, what kinds of additional consideration should be conducted in applying the Security Guidelines to the information systems that handle FinTech operations subject to such guidelines needs to be considered.

(See References, Reference 2)

If an information system handling FinTech operations qualifies as one such as an information system with critical externalities or an information system containing sensitive information ("critical information system" hereinafter), then in accordance with the basic principles of security measures the high Security Guidelines must be applied when setting the goals to be achieved by such security measures, from a social and public perspective. For this reason, if they have new properties that have not been included among the assumptions of the Security Guidelines through now, then the technologies and other aspects of FinTech used in critical information systems must reflect the high Security Guidelines.

At the same time, if an information system handling FinTech operations is one other than a critical information system ("general information system" hereinafter), then a Financial Institution employing a fully risk-based approach would be able to decide on security measures on its own, and thus regarding such cases there is no need for any particular additional consideration in the Council of matters such as goals to be achieved.

However, it is anticipated that at a Financial Institution employing a simplified risk-based approach, under which the minimum necessary Security Guidelines are identified as the goals to be achieved by security measures[2], the high Security Guidelines would need to be applied since the handling of the Security Guidelines is not defined clearly in light of the projected appearance of wide-ranging FinTech operations in the future.

In this way, there is a need to make clear in advance the issues involved in connection with matters such as application of the Security Guidelines with regard to FinTech and the ideal form of security measures, after first making clear the assumptions such as matters assumed in existing the Security Guidelines and those not necessarily envisioned by existing the Security Guidelines, so that application of the Security Guidelines to information systems handling FinTech operations will not be a mere formality.

2. Guidelines for identification of information systems subject to the Security Guidelines

[1] This stands for the FISC Security Guidelines on Computer Systems for Banking and Related Financial Institutions. As used here, this refers not only to the current Version 8 and Version 8 after additions and amendments but also includes the outcome of the FISC Report of the Council of Experts on Outsourcing in Financial Institutions.

[2] With regard to the simplified risk management measures that are a precondition of minimum necessary Security Guidelines, the Council of Experts has made recommendations based on the state of security measures in each of the cases of use of cloud services and outsourcing, and efforts have advanced to ensure that high Security Guidelines are not applied uniformly.

Ever since the first edition of the Security Guidelines was formulated more than 30 years ago, the guidelines have applied to the "computer systems of Banking and Related Financial Institutions"[3]. Computer systems of Banking and Related Financial Institutions refers to information systems that handle financial operations, and for which the Banking and Related Financial Institutions bear responsibility for system security. Accordingly, information systems handling FinTech operations identified as being subject to the Security Guidelines are those that handle FinTech operations that qualify as financial operations and for which the Banking and Related Financial Institutions bear responsibility for system security.

Financial operations refer to operations related to the financial services that Banking and Related Financial Institutions provide to their customers under industry laws and other considerations. Accordingly, since information systems handling e-commerce operations intended to sell products or other merchandise, even if such services are provided to customers, would not be considered to be information systems handling operations related to financial services, they would not be subject to the Security Guidelines. Also, information systems used only within Banking and Related Financial Institutions (e.g., HR and payroll systems or management information systems) are not subject to the Security Guidelines[4].

At the same time, FinTech operations conducted by businesses other than Banking and Related Financial Institutions solely as service users, unrelated to Banking and Related Financial Institutions or the customers of Banking and Related Financial Institutions are not subject to the Security Guidelines because they do not involve any responsibility on the part of Banking and Related Financial Institutions to implement security measures.

3. Handling of technologies etc. related to FinTech used in critical information systems

Conceivable technologies etc. related to FinTech expected to be used in critical information systems include block-chain technologies and AI[5]. In considering these, since it is conceivable that cases of use (use cases) of such factor technologies may be broad ranging, there is a need to move forward with consideration while focusing on technological properties suited to each use case. Since, indeed, under current conditions no use cases in critical information systems have appeared yet, instead of considering such cases immediately, the timing at which consideration would be feasible will be identified while observing matters such as the state of appearance of use cases in the future.

[3] Since the first version of the Security Guidelines (December 1985), these have been referred to as "companies in the industry conducting financial operations, including finance, insurance, securities, and credit."

[4] The first edition of the Security Guidelines stated, "These guidelines assume application to systems related to services provided by Banking and Related Financial Institutions to their customers. For this reason, they also include portions that may be referred to regarding guidelines for security measures for internal systems used by Banking and Related Financial Institutions." The same thinking basically holds today.

[5] Artificial intelligence

4. Assumptions in consideration of ideal forms of security measures related to FinTech

(1) The appearance of FinTech firms as new related parties in implementing security measures

Security Guidelines have been formulated with the following two parties considered related parties in implementing security measures in financial information systems: Financial Institutions themselves and IT solution providers serving as outsourcees performing technical roles in development and operation of information systems[6].

However, companies handling FinTech operations involve technological properties similar to those of IT solution providers along with business properties involving matters such as planning of business models for financial services, and it is not necessarily the case that existing the Security Guidelines clearly envisioned their application to related parties possessing such technological and business properties simultaneously[7].

Accordingly, when making clear the issues inherent to application of the Security Guidelines to FinTech operations, it would be beneficial to consider the roles related to security measures that should be fulfilled by newly appearing FinTech firms and other parties after first categorizing and sorting out the three related parties of Financial Institutions, IT solution providers, and FinTech firms.

(2) The appearance of business forms in which Financial Institutions would not necessarily occupy positions of leadership

The Security Guidelines have assumed that Financial Institutions would bear responsibility to their customers for security measures for information systems handling operations related to financial services provided by Financial Institutions to customers. This is a natural conclusion under conditions in which Financial Institutions take leadership in all decision-making regarding the financial services that they provide to their customers.

At the same time, in recent years FinTech firms have arisen as intermediaries between customers and Financial Institutions[8]. These include some service providers that are provided by customers with the IDs, passwords, and other information needed to use the services of Financial Institutions and, as a result, provide financial-related services to customers directly themselves after obtaining customer-related data from the Financial Institutions and adding their own value to the data thus obtained. While based on data obtained from the Financial Institutions, the services of such FinTech firms add elements such as innovative user experiences unavailable from the services provided by Financial Institutions to their

[6] In addition to "IT solution providers," the Security Guidelines also user terms such as "vendors" and "computer makers." This document refers to parties of a technical nature collectively as "IT solution providers." It also uses IT solution providers in a sense that includes "Cloud service providers."

[7] The FISC Report of the Council of Experts on Outsourcing in Financial Institutions identifies, under II. IT Governance and IT Management: 2 (3) User Roles and Responsibilities, the following as the main roles and responsibilities of related parties having a business nature in security measures" (i) Planning business models with consideration for security measures, (ii) Achieving results of investment, and (iii) Providing business requirements.

[8] FinTech firms serving as intermediaries between customers and Financial Institutions may include, in addition to those discussed here, those using open data such as branch locations and interest rates provide on Financial Institutions' websites.

customers, and as such these services are well received by customers and their use is advancing[9].

In some cases, the services that such FinTech firms provide directly to their customers are decided on entirely under the leadership of the FinTech firms, and they are able to obtain customer-related data from the Financial Institutions in a unidirectional manner without negotiating with the Financial Institutions in any way. In such a case in which the Financial Institution employs a fully passive stance, it is understood that the Financial Institution bears no responsibility for security measures to its customers, since it has no means of governance. Accordingly, it would be proper to understand such services not to be subject to the Security Guidelines even if they are financial services provided to customers of the Financial Institutions[10].

On the other hand, there also are cases in which even though the services are provided to the customers directly by the FinTech firms, negotiation has taken place between the FinTech firms and the Financial Institutions, and as a result the Financial Institutions can decide on the data that they provide to the FinTech firms. Also, it is conceivable that in some cases the Financial Institutions may decide which data they will receive from FinTech firms. In such cases in which the Financial Institution has the right to decide which customer-related data[11] it will provide or receive, the Financial Institution can be considered to be demonstrating leadership, if only in part, and thus it would be proper to understand the Financial Institution to bear some responsibility for security measures.

For these reasons, even when a Financial Institution bears only partial responsibility for security measures for information systems in services provided by FinTech firms it will need to consider the ideal form of security measures, as a case subject to the Security Guidelines[12].

Such partial responsibility for security measures on the part of Financial Institutions comes from the fact that originally the Financial Institutions are—even with their customers' consent—providing to third parties customer-related data that they are responsible for managing, or updating customer-related data in accordance with data received from third parties. For this reason, they must focus on the risk properties of such data provided or received and consider the ideal forms of security measures accordingly. In doing so, based on a risk-based approach it would be appropriate regarding data provision to focus on the degree of sensitivity, which is one risk property of the data, in addition to the volume of data. The degree of sensitivity refers to the degree of damages that a customer would be expected to incur in a case such as if the data were to be used by the FinTech firm beyond the extent to which the individual concerned has consented, or were to be leaked by the FinTech firm[13].

---

[9] The Financial System Council's Financial System Working Group Report (published December 27, 2016) states, "In recent years, increasing numbers of businesses have been engaged in settlement as entrusted by customers, by communicating settlement instructions using IT means or obtaining or providing to customers information on accounts with Financial Institutions, as intermediaries between Financial Institutions and customers.

[10] The British Open Banking Standard (February 8, 2016) addresses "screen-scraping," identifying as issues in unilaterally obtaining customer-related data from Financial Institutions "Access to the host system is uncontrolled and unregulated" and "Consumers are uncertain about the procedure and have little recourse to their bank in case something goes wrong." It also must be noted that screen-scraping is not immediately identifiable as a problem and involves obtaining data without negotiating with Financial Institutions.

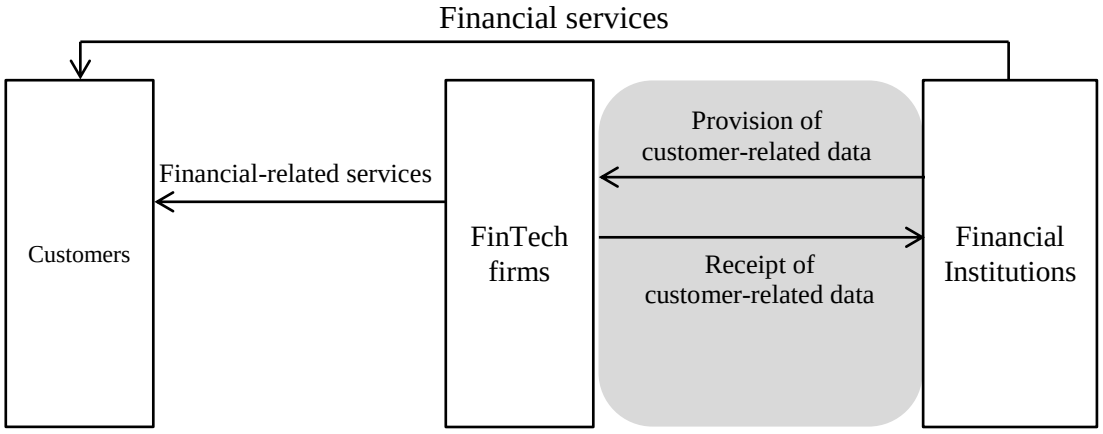
[11] The data provided by Financial Institutions to FinTech firms may include, for example, customer transaction histories. Data that Financial Institutions obtain from FinTech firms may include, for example, settlement instructions.

[12] Under Operation 90-1, the Security Guidelines include guidelines on use of services, which differs from outsourcing, as a case in which Financial Institutions do not play a leading role. Noting that "Financial Institutions find it difficult or inefficient to choose from multiple service providers or conduct risk management on their own, similarly to the case of outsourcing management," under these guidelines the degree of responsibility borne by Financial Institutions for security measures should be understood in a more limited way than in the case of general outsourcing. However, they cover "mutual system networks between Financial Institutions," not the customer services considered here.

[13] The FISC Report of the Council of Experts on Outsourcing in Financial Institutions identifies as highly sensitive information personal information for which the highest objective of security measures should be set, noting, "Since leakage of sensitive information without the consent of the person concerned could lead not only to economic damages but also to broad-ranging damage such as infringement on fundamental human rights, its handling has an inherent social and public nature.

With regard to receiving data as well, in addition to the scale of updating of data in accordance with such data received, it would be appropriate to focus on the method by which the FinTech firm confirms customer identity—i.e., whether it confirms properly that the data received from the FinTech firm are based on customer instructions.

Fig. 1. Business forms in which Financial Institutions would not necessarily occupy positions of leadership

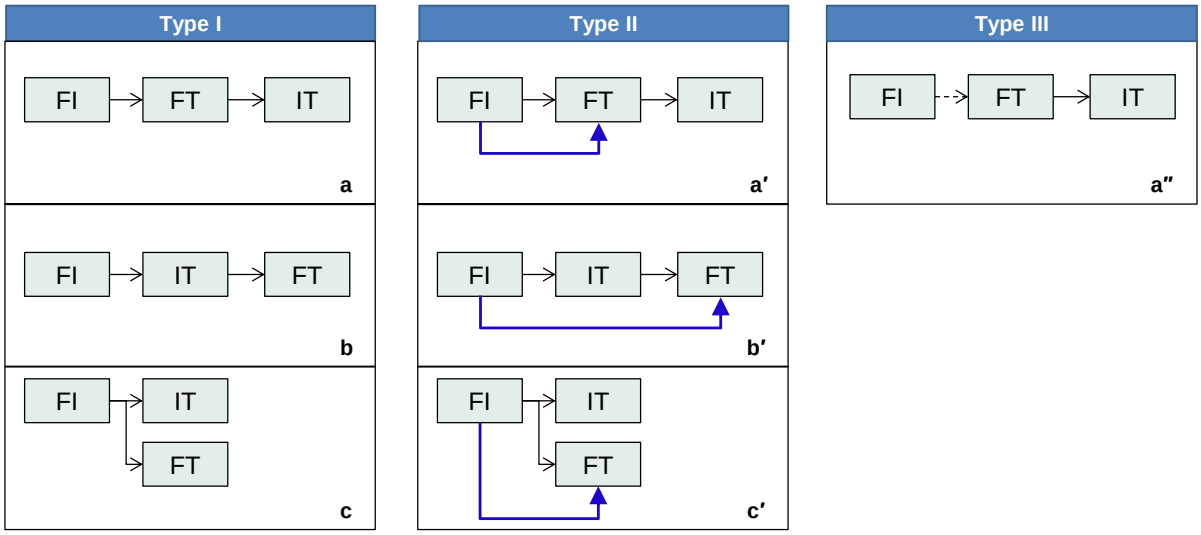


Financial Institutions are understood to bear responsibility to their customers for security measures in the areas in which they have decision-making authority (i.e., demonstrate leadership).

(3) Types of FinTech operations

Based on the appearance of new related parties and forms of business as outlined above, the patterns of FinTech operations by type that should be considered the assumptions of this examination are as shown in Fig. 2. (See References, Reference 3)

Fig. 2. Types of related parties for security measures in FinTech operations



Type I involves three basic patterns of outsourcing relations, in each of which the Financial Institution bears full responsibility for security measures. Type II is a derivative of Type I in which responsibility for subsidiaries has been added. While Type III resembles Type I, in it the Financial Institution bears only partial responsibility for security measures.

In this Report, practical consideration will be given to the presence or absence of any inherent issues in a case in which existing the Security Guidelines are applied to the above seven patterns in three types.

(4) Perspectives that should be considered in examining security measures in FinTech operations

In clearly identifying the location of issues, it would be beneficial to share in advance the perspectives from which issues will be considered.

First of all, consideration should be conducted based on the perspective stated in the Council's guiding principles of "Aiming to enable Japan's Financial Institutions to adapt to customer needs and enjoy the benefits of innovation to the maximum extent, while maintaining system security."

Then, in implementing FinTech operations, since it is expected that a wide range of types will be deployed there is a need to take care to ensure that the effects of the Security Guidelines will not, for example, be restricted when employing a specific type. Security Guidelines are the basis of security measures for information systems, and that fact itself must not harm the diversity of business models that Financial Institutions may employ. If there were to be any

strains that would have a restrictive effect on adoption of a specific type, then that would need to be addressed as an issue (i.e., one regarding the neutrality of the Security Guidelines).

On the other hand, as long as Financial Institutions bear responsibility under security measures then in order to fulfill this responsibility then in implementing security measures their feasibility—that is, their ability to control outsourcees and subcontractors when outsourcing—needs to be secured fully. However, if there are cases in which amid the wide range of types of FinTech operations Financial Institutions' control capabilities as necessary to fulfill such responsibilities under security measures do not necessarily function fully, then that would need to be addressed as an issue (i.e., one regarding the efficacy of the Security Guidelines).

Next, since the above perspectives of the neutrality and efficacy of the Security Guidelines may not necessarily be achieved together in a well-balanced way, it is conceivable that which of these perspectives to prioritize should be considered in advance.

While prioritizing neutrality would contribute to realizing maximization of enterprise value by enjoying the benefits of innovation without harming the diversity of business models, it also would lead to the concern that Financial Institutions might not necessarily fulfill their responsibilities to customers under security measures. On the other hand, if prioritizing efficacy then it would be anticipated that FinTech firms or IT solution providers would need to bear burdens specific to their businesses, or that the freedom of their businesses could be restricted, and as a result the innovative nature of FinTech firms could be harmed.

Since it is conceivable that this issue of a tradeoff between neutrality and efficacy could arise under diverse conditions, it also is conceivable that it could be difficult to make a judgment in advance on which to prioritize, leading to the need to make such judgments on a case-by-case basis in light of individual circumstances.

Under a simplified risk-based approach in particular, probably it would be appropriate to consider whether it would be valid to prioritize neutrality or efficacy in formulating simplified risk-control measures and other matters after first making clear the individual issues that would arise when applying existing the Security Guidelines.

(5) Relationship to open APIs

One method of realizing Type III is that known generally as an "open API."[14] Under an open API, information systems are connected to each other based on agreement between FinTech firms and Financial Institutions. This enables FinTech firms to combine diverse information and implement harmonized security measures with Financial Institutions, making it possible to provide customers with highly convenient and secure services.

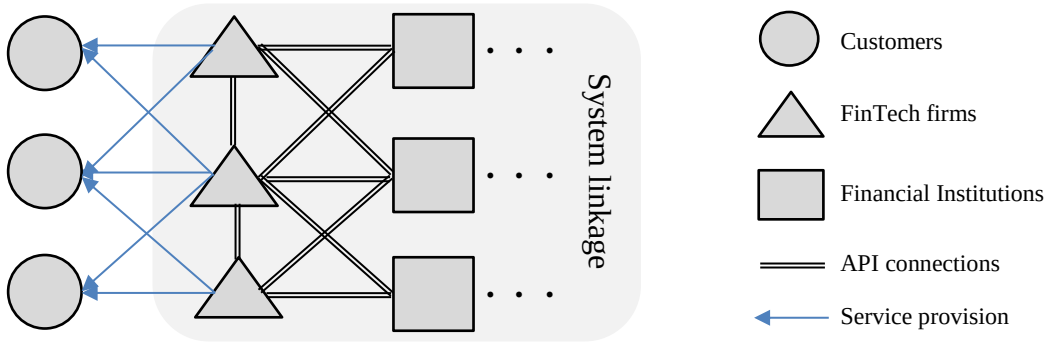
Technologically, multilayered linkage of IT systems among businesses, from a many-to-many and multistage approach, is possible using an API. For this reason, if the opening of Financial Institutions' APIs involves diverse related parties in linkage of financial information systems, then the types of information combinations will be diverse as well, and this diversity would

[14] The Financial System Council's Financial System Working Group Report (released December 27, 2016) states, "As used here, API refers to an interface that enables parties other than a bank to connect to the bank's IT systems and use their functions. Of these, an open API refers to an API provided by a bank to FinTech firms and others and permitting it to access the bank's systems, subject to customers' consent." http://www.fsa.go.jp/singi/singi_kinyu/tosin/20161227-1.html

open up the possibilities for innovative services[15]. Society expects the cultivation of an environment that would enable such open innovation.

On the other hand, when a large number of related parties is involved in system linkage, it is conceivable that there would be an increased possibility of the manifestation of unforeseen risks within the interactions among such parties[16]. For this reason, to address such interactions and similar matters, it is important to collect together related parties and consider security measures from a multifaceted approach ("collective consideration" hereinafter) (Fig. 3).

Fig. 3. Linkage relationships through an open API



As one example of collective consideration of thinking on security under an open API, in October 2016 the Review Committee on Open APIs, in which the Japanese Bankers Association ("JBA" hereinafter) serves as secretariat and members include Financial Institutions, IT-related firms, and financial regulators ("Bank API Committee" hereinafter), was established[17]. FISC also is a member of this Council, and the Council refers to the deliberations of the Bank API Committee[18] in its own studies[19].

[15] Regarding the mechanism by which in a networked age open technologies stimulate innovation, refer to Ryojiro Kuni, Open Architecture Strategies: Cooperation Models for the Networked Age (1999).

[16] Ryojiro Kuni, in Social Capitalism: The Management Strategy of Connections (2013), notes, "By definition, emergent phenomena arising from the combination of information communicated by diverse actors cannot be controlled fully. Attempts at such control will prevent the emergent phenomena themselves from occurring." He also notes, "One must be prepared for the possibility that chaos and accidents could arise amid unanticipated interactions, particularly when linking numerous systems to each other. Thinking continually about countermeasures for these will help to minimize damage when an accident occurs."

[17] https://www.zenginkyo.or.jp/news/detail/nid/6752/

[18] https://www.zenginkyo.or.jp/news/detail/nid/7670/ The Report of Review Committee on Open APIs: Promoting Open Innovation (Interim Summary [Draft]) is referred to hereinafter as the "Bank API Report."

[19] In addition, in March 2017 the Ministry of Economy, Trade and Industry launched the Study Group for API-based Collaboration Involving Credit Card Utilization, with the participation of credit card issuers, FinTech industry representatives, and others, which is considering topics including what kinds of guidelines would prove satisfactory to both credit card issuers and FinTech firms from security and other perspectives.

II. Topics in application of FinTech-related the Security Guidelines and ideal forms of security measures

1. Matters that it would be beneficial to clarify in advance in consideration of topics

(1) Effects of security measures that should be targeted

While consideration of information systems handling FinTech operations subject to the Security Guidelines is based on the assumption of a tripartite relationship involving FinTech firms in addition to Financial Institutions and IT solution providers, it would be beneficial to make clear in advance the degree of effects of security measures aimed for.

The effects of security measures expected by society for financial information systems were given concrete form for the first time through the formulation of the Security Guidelines 30 years ago, when it was common for businesses to provide their own IT resources. Since then, while the effects of security measures given concrete form in the Security Guidelines have reflected changes in society's expectations for Financial Institutions, they can be considered to have been maintained within the bipartite relationship between Financial Institutions and IT solution providers without being affected by the change in Financial Institutions' circumstances as seen in their rising dependency on IT solution providers.

Accordingly, as Financial Institutions aim to enjoy the benefits of innovation, even when the new related party of FinTech firms has appeared on the scene it is important to take care to ensure that the effects of security measures remain equivalent to those of security measures realized under existing the Security Guidelines in a bipartite relationship ("principle of equivalency" hereinafter).

In addition, when aiming to realize equivalent effects of security measures in both a bipartite and a tripartite relationship, from the perspectives of neutrality and efficacy it is important that adjustments to existing the Security Guidelines be kept within the extent necessary. That is, it is important to take care to ensure that the burdens on Financial Institutions, IT solution providers, and others will not increase beyond the necessary extent as a result of such adjustments.

(2) Domains subject to consideration in the Security Guidelines

The existing the Security Guidelines consist of guidelines that apply to "things," including equipment guidelines that cover the buildings and equipment that contain computer systems, and those similar to technical guidelines, which cover hardware and software, as well as those that apply to "people," similar to operation guidelines that cover hardware, software, and other subjects. It would be beneficial first of all to make clear which of these guidelines should be the main subject of consideration.

In a situation in which a diverse range of FinTech technologies is expected to appear in the future, it is difficult for equipment guidelines and technical guidelines covering things[20] to identify practical security measures premised on specific individual technologies, and it would not be appropriate to establish final individual security measures while the FinTech environment is changing. For this reason, with regard to equipment guidelines and technical

[20] It must be noted that the technical guidelines include portions highly susceptible to the effects of technological changes and those that are not.

guidelines it is sufficient if Financial Institutions decide on their own on security measures suited to the risk properties of individual FinTech operations and employ IT governance in accordance with the basic principles of security measures[21].

At the same time, since it is conceivable that operation guidelines applying to people would be applicable even in the event of the appearance of a diverse range of FinTech technologies without being impacted by such varied and diverse technologies or other matters, in this consideration it would be appropriate to consider such operation guidelines as a main subject.

In addition, since FinTech operations may be realized in the form of outsourcing from Financial Institutions to FinTech firms, among such operation guidelines it would be appropriate to consider guidelines related to outsourcing as a main subject.

(3) Nature of simplified risk management measures

In considering simplified risk management measures, it is beneficial to make clear in advance the nature thereof.

First of all, simplified risk management measures are based on the precondition that that controls have been established for critical information systems. Such controls are derived through easing for general information systems. At the same time, as indicated by the expression "minimum necessary guidelines[22]," the also are binding to the extent that they indicate the minimum level that must be implemented.

For this reason, if establishment of simplified risk management measures is inappropriate, then the results would be not only to detract from neutrality and efficacy but also to bring about chronically excessive or insufficient security measures. For this reason, in consideration of such matters it also is important both to take care to reflect accurately an awareness of the issues related to security measures faced by FinTech firms and other related parties in the fields in which individual information systems are used and to carry out such consideration carefully.

(4) Handling of the Security Guidelines related to use of cloud services

It is said that among IT solution providers, many FinTech firms entrust operational information systems to Cloud service providers. For this reason, it would be beneficial to confirm in advance the positioning of guidelines on use of cloud services within the Security Guidelines.

First of all, the Security Guidelines consider cloud services to be a form of outsourcing[23]. Furthermore, the Security Guidelines related to use of cloud services, minus content specific to cloud services alone, are referenced as guidelines for outsourcing as a whole[24]. Since such

[21] This refers to the four principles based on a risk-based approach proposed in the FISC Report of the Council of Experts on Outsourcing in Financial Institutions .

[22] Under "the significance of minimum necessary Security Guidelines," the FISC Report of the Council of Experts on Outsourcing in Financial Institutions notes, "'simplified risk management measures' refer in general to security measures for relatively low-risk information systems, which are similar in nature to the categories for which the Security Guidelines indicate 'Acceptable.'" It also notes, "These should be established within a scope intended to reduce the uncertainty of security measures."

[23] The Security Guidelines' operation guideline (XIV) Use of Cloud Services notes, "When using cloud services, . . . appropriate risk management needs to be employed in accordance with the thinking on outsourcing management." In addition, the FISC Report of the Council of Experts on Outsourcing in Financial Institutions includes the Cloud within the scope of outsourcing in the overview of part 5. Outsourcing.

[24] Footnote 31 to the FISC Report of the Council of Experts on Outsourcing in Financial Institutions notes, "Among the guidelines for cloud services, those applicable to outsourcing as a whole should be referred to, while those specified to the Cloud should not be used as general guidelines for outsourcing."

revisions to the Security Guidelines are conducted based on the findings of the Outsourcing Council and the Council[25], it must be noted at this point in time that no final version yet exists of the Security Guidelines for outsourcing (including cloud services) following such adjustment.

For this reason, tentatively the Council needs to make clear an overview of guidelines related to outsourcing within existing the Security Guidelines, to the extent needed for its consideration.

Next, since it is not necessarily the case that the FISC Report of the Council of Experts on the Usage of Cloud Computing by Financial Institutions ("Cloud Council" hereinafter), which serves as the preconditions for the Security Guidelines related to use of cloud services, reflects the significance of critical information systems proposed in the report of its successor, the Outsourcing Council, at present some uncertainty remains with regard to whether or not the risk management measures of the Cloud Council report are applicable unchanged to critical information systems.

In light of the fact that simplified risk management measures are derived based on the management measures for critical information system by easing the degree of their controls, it would be recommended to take note of such circumstances.

To resolve the above matters deserving of note, the Council will consider supplemental management measures for cases in which cloud services are used, based on the findings of the Report of the Council of Experts on Outsourcing in Financial Institutions. Doing so would make clear the relevant assumptions even when FinTech use cases involving use of cloud services in critical information systems (e.g., block chain, AI) arise.

[25] The FISC Report of the Council of Experts on Outsourcing in Financial Institutions states, "Revisions to the Security Guidelines etc. will be conducted after completion of the work of the FinTech Council, taking into account the outputs of both the outsourcing and FinTech councils."

2. Duties of related parties under existing the Security Guidelines

(1) Duties of related parties

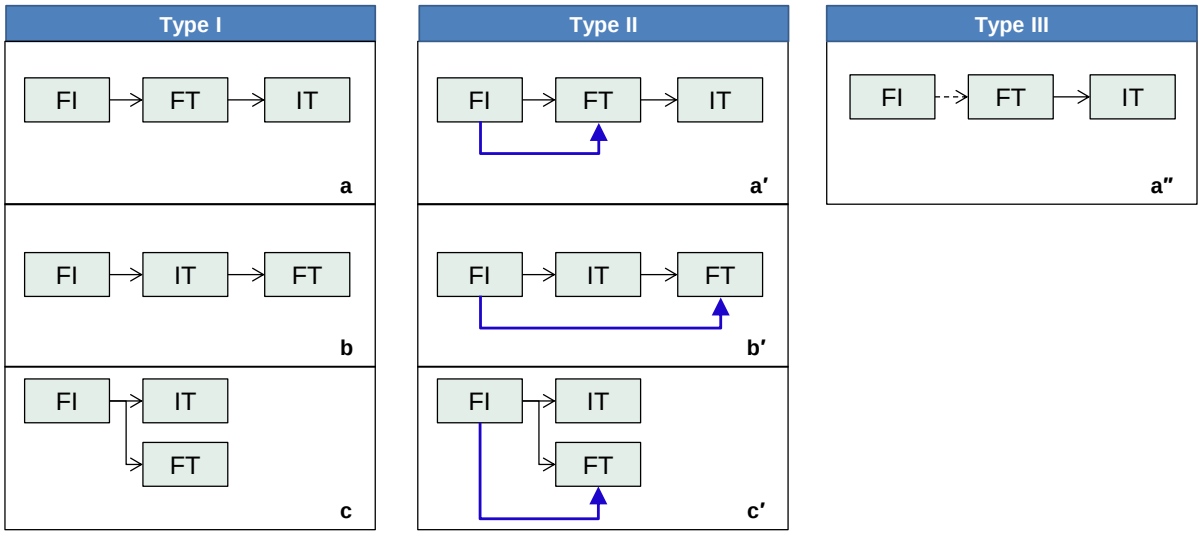
First of all, in considering inherent issues, the "Overview of Existing Security Guidelines (Outsourcing)" was sorted under the tripartite relationship in Type I. (See References, Reference 4)

This involved categorizing the duties of each of the parties implementing security measures as shown below.

- Duties of Financial Institutions when using outsourcing: Duties A
- Duties of primary outsourcees: Duties B
  Duties borne as Financial Institutions' primary outsourcees: Duties B-1
  Duties borne by Financial Institutions' subcontractors: Duties B-2
- Duties borne as Financial Institutions' subcontractors: Duties C

While the efficacy of security measures can be realized in FinTech as well through the appropriate performance by related parties of the above duties, since the inherent issues in such a case are recognized in practical terms by the FinTech firms serving as new related parties, patterns sorted by types (a), (b), and (c) under Fig. 4 with a focus on the duties of FinTech firms are as shown in Fig. 5.

Fig. 4. Patterns of related parties in implementing security measures in FinTech operations



FI: Financial Institution; FT: FinTech firm; IT: IT solution provider (including Cloud solution provider)
→: Full responsibility for security measures ⇢: Partial responsibility for security measures
→: Responsibility for subsidiaries

Fig. 5. Examples of duties of FinTech firms

Pattern (a)

Duties B-1: Main duties borne as Financial Institutions' primary outsourcees		Note
a. When considering use	Duty to provide to Financial Institutions the information they need for purposes of making objective evaluations	3
	Duty to provide to Financial Institutions information on the locations of data	7
b. When concluding the contract	Duty to conclude contracts with Financial Institutions on matters such as protection of confidential information and performance of safe operations	11
	Duty to clearly describe Financial Institutions' auditing authority vis-a-vis subcontractors	14
	Duty to respond to prior review by Financial Institutions of subcontractors	25
d. During operation	Duty to take measures to prevent leakage when entrusted with data management by Financial Institutions	28
	Duty to employ sufficient management, including data deletion, when replacing machines and components due to failure of storage devices or other reasons	29
	Duty to undergo everyday auditing by Financial Institutions	30
	Duty to accept general auditing and evaluation of systems by Financial Institutions	31
Duties B-2: Main duties borne by Financial Institutions' subcontractors		**Note**
a. When considering use	Duty to evaluate Financial Institutions' subcontractors objectively (Simplified) Evaluation may be conducted based on public information, industry reputation and business performance, etc.	3
	Duty to ascertain locations of data (Simplified) Ascertaining locations of data may be omitted	7
b. When concluding the contract	Duty to conclude contracts with Financial Institutions' subcontractors on matters such as protection of confidential information and performance of safe operations	11
	Duty to clearly describe Financial Institutions' auditing authority vis-a-vis subcontractors (Simplified) Not requiring clear description of auditing authority is possible	14
	Duty to conduct appropriate prior screening of subcontractors	25
d. During operation	Duty to take measures to prevent leakage when entrusting management of Financial Institutions' data to subcontractors	28
	Duty to ensure sufficient management, including data deletion, is employed when replacing machines and components due to failure of storage devices or other reasons (Simplified) Verification of efficacy of deletion/destruction process may be used instead	29
	Duty to conduct everyday monitoring of subcontractors	30
	Duty to conduct general auditing and evaluation of subcontractors' systems (Simplified) Third-party certification or similar means may be used instead	31

Pattern (b)

Duties C: Main duties borne as Financial Institutions' subcontractors		Note
a. When considering use	Duty to provide to IT solution providers the information they need to implement objective evaluation	3
b. When concluding the contract	Duty to conclude contracts with IT solution providers on matters such as protection of confidential information and performance of safe operations	11
	Duty to clearly describe Financial Institutions' auditing authority	14
d. During operation	Duty to undergo everyday auditing by IT solution providers	30
	Duty to accept general auditing and evaluation of systems by IT solution providers	31

Pattern (c)

Duties B-1: Main duties borne as Financial Institutions' primary outsourcees		Note
a. When considering use	Duty to provide to Financial Institutions the information they need for purposes of making objective evaluations	3
b. When concluding the contract	Duty to conclude contracts with Financial Institutions on matters such as protection of confidential information and performance of safe operations	11
d. During operation	Duty to undergo everyday auditing by Financial Institutions	30
	Duty to accept general auditing and evaluation of systems by Financial Institutions	31

(Simplified): Simplified risk-management measure already formulated;
Note: Indicates no. on References, Reference 4

(2) Approaches to inherent issues

Based on the above sorting out of the issues, consideration by type based on the following approach will be employed when considering inherent issues when applying existing the Security Guidelines (i.e., those related to outsourcing) to FinTech operations.

- Would there be any problem with application of existing the Security Guidelines in the case of Type I?
- Would it be appropriate to apply existing the Security Guidelines originally in the case of Type III?

Type II will be considered separately since it is a type in which different responsibilities are assigned than for Type I.

3. Issues inherent under Type I and the ideal form of security measures

Under Type I, FinTech firms bear responsibility for Duties B or Duties C. Since originally the existing the Security Guidelines were formulated with the two parties of Financial Institutions and IT solution providers in mind, Duties B or Duties C were formulated with IT solution providers' ability to execute security measures in mind.

For this reason, when FinTech firms are responsible for Duties B or Duties C, the inherent issue is involved of the possibility of a lack of balance vis-a-vis FinTech firms' abilities to execute security measures[26] (e.g., the management resources that they possess).

Accordingly, when formally demanding of FinTech firms that they apply the Security Guidelines similar to those demanded of IT solution providers, the result would be an excessive burden of security measures borne by FinTech firms who do not have the same ability to implement such measures as IT solution providers, leading to an incentive to avoid such a burden. This could introduce strains on FinTech firms' choice of business models as a result (from the perspective of neutrality). Alternatively, FinTech firms could prioritize allocation of their internal management resources to security measures in an attempt to bear such excessive security measures, harming innovation as a result (from the perspective of enjoying the benefits of innovation).

At the same time, even in the case of a tripartite relationship to which FinTech firms have been added, based on the concept that the effects of such security measures should be equivalent to those of security measures in a traditional bipartite relationship (i.e., the principle of equivalency), if Financial Institutions were simply to tolerate residual risk as being adequate in light of the ability of FinTech firms to execute such security measures or to adjust risk-management measures to match the ability of FinTech firms to execute security measures would not be effective solutions to the issue (from the perspective of efficacy).

Originally, Financial Institutions engage in outsourcing in order to employ the innovative nature of FinTech firms in their own business operations, aiming to maximize their enterprise value. They do not necessarily engage in outsourcing in order to replace completely the roles performed by IT solution providers with those of FinTech firms.

Accordingly, Financial Institutions should first confirm the abilities of FinTech firms to execute security measures, and if the duties involved are beyond the abilities of FinTech firms then it would be recommended to employ consideration for Financial Institutions and IT solution providers dividing such responsibilities so that the efficacy of security measures can be achieved without losing the innovative nature of FinTech firms.

In other words, to resolve this issue it would be appropriate to authorize explicitly the reasonable redistribution of the roles of the types of the three parties and their abilities to execute security measures (e.g., management resources in their possession), while maintaining the aggregate total of the duties required under existing the Security Guidelines based on a bipartite relationship.

[26] A basic part of the ability to execute security measures is the ability to ensure that internal controls related to security measures function effectively. An example would be the ability to identify on one's own a problem with security measures if it were to arise, to address it on one's own, and to implement continually on one's own improvement activities through identifying the source of the problem and addressing it (i.e., the ability to run through the PDCA cycle fully for security measures). This basic part of the ability to execute security measures also should be demanded, at a minimum, from FinTech firms handling financial-related services. Accordingly, this ability to execute security measures does not necessarily refer to a state that can be confirmed formally by checking to see whether individual security measures have been completed at any point in time.

In redistribution of duties, if there are multiple related parties capable of bearing duties then from the perspective of minimizing the social costs of security measures it is recommended to reallocate duties to a party that would bear fewer additional costs[27].

(Rules for redistribution) (See References, Reference 5)

Based on tripartite agreement among Financial Institutions, IT solution providers, and FinTech firms, outsourcing duties under the existing the Security Guidelines may be redistributed[28] among the three parties[29].

In such redistribution, in accordance with the principle of equivalency there is a need to take care to ensure that the burden on any related party does not increase beyond the necessary scope. Redistribution of duties to related parties who would incur lower levels of additional costs contributes to minimization of the social costs of security measures.

The above rules also represent a valid way of thinking regarding types other than Type I as well as critical information systems.

4. Issues inherent to Type III and the ideal forms of security measures

(1) Financial Institutions' responsibilities under security measures

Type III represents a pattern in which FinTech firms play a leading role in financial-related services. The relationships between Financial Institutions and FinTech firms may take various diverse forms that will not necessarily fit within the forms characterized as outsourcing. For this reason, with regard to Type III there is a need to consider the ideal forms of security measures to enable flexible adaptation to a wide range of forms of the relationships between Financial Institutions and FinTech firms, ranging beyond the scope of outsourcing alone.

On this subject, regardless of the form of the relationship between the Financial Institution and the FinTech firm there is a high likelihood that a look at the actual content of FinTech operations from the Financial Institution's point of view would show some elements in common with outsourcing. On the other hand, while under existing the Security Guidelines the guidelines related to outsourcing have been revised and supplemented in accordance with environmental changes and other developments, it is not necessarily the case that explicit guidelines exist for other forms. Accordingly, the ideal form of security measures under Type III basically would be that of applying mutatis mutandis the guidelines for outsourcing, and in

[27] If a FinTech firm were to choose to minimize the costs it must bear, then it is clear that Financial Institutions would bear duties instead of the FinTech firm, and it is possible that if the FinTech were to bear no duties under security measures, it might be expected that the Financial Institutions would bear them. At the same time, if a Financial Institution were to choose to minimize the costs it must bear, then the FinTech firm might understate its ability to execute security measures to claim that it would not be able to bear any more costs if asked to, in an attempt to avoid being asked to bear such costs. Accordingly, from a social perspective it is recommended that related parties cooperate to consider ways to minimize the sum total of costs borne. Also, it is conceivable that agreement might be reached in advance on schemes for providing returns to related parties suitable to the duties they bore, to ensure cooperation through means such as appropriate disclosure of information.

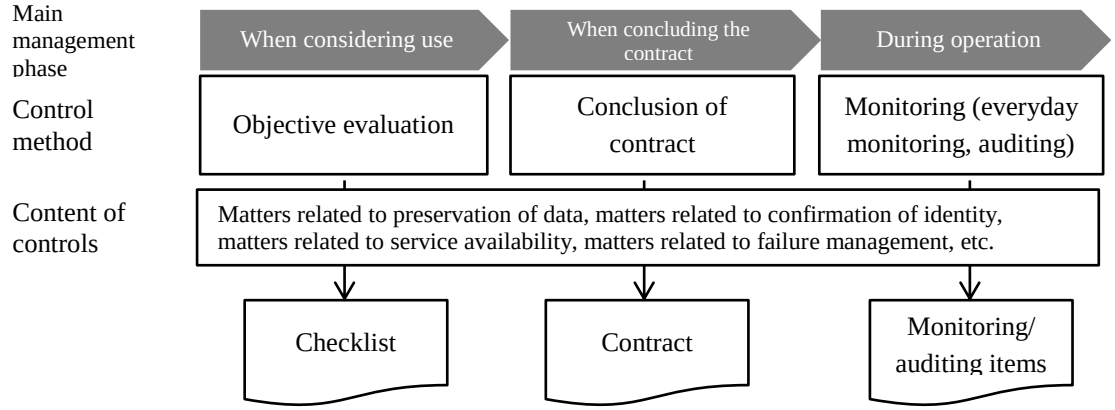
[28] For example, It is considered that Financial Institutions would control IT solution providers directly by taking on the responsibility of a part of Duties B-2 instead of FinTech firms based on tripartite agreement.

[29] Since FinTech companies vary widely in size and types of businesses, it would not be appropriate to specify in advance fixed content for the redistribution of duties. It would be sufficient for Financial Institutions to decide on the content of such distribution in a reasonable manner for each category, in accordance with the state of the FinTech firms and IT solution providers that they use in outsourcing. They also might want to hold training sessions and provide other support so that FinTech firms can fulfill their duties regarding security measures instead of relying on revising the content of distribution.

the event of individual circumstances that cannot be handled under such measures it would be appropriate to revise them as necessary.

Next, when considering mutatis mutandis application of outsourcing guidelines there is a need to note that originally outsourcing guidelines consist of guidelines on methods of control, through implementation of objective evaluation and monitoring in management phases such as when considering use and during operation, and guidelines on the content of controls, through use of encryption as a measure for preventing leakage of data (Fig. 6).

Fig. 6. Control methods and content



First of all, regarding methods of controls in mutatis mutandis application of these guidelines, as long as the Financial Institutions bear some responsibility under security measures, then it can be considered that they should be implemented in the same way as with outsourcing, although with a difference in degree.

Fig. 7. Examples of items of interest to Financial Institutions under Type III

a. When considering use	Implementation of objective evaluation
	Should FinTech firms bear the same degree of responsibilities as the management responsibilities borne by Financial Institutions under security measures? Alternatively, should Financial Institutions bear the management responsibilities required of FinTech firms? For example, do FinTech firms possesses the ability to execute security measures needed for such measures (e.g., the management resources they possess)?
b. When concluding the contract	Conclusion of contracts that include security measures
	Do FinTech firms conclude with Financial Institutions contracts that include security measures? Also, do FinTech firms conclude contracts that include security measures with IT solution providers (e.g., provisions regarding notification of leakage of data and compensation for damages)?
d. During operation	Everyday monitoring
	Is it possible for FinTech firms to report to Financial Institutions on the status of implementing security measures?
	Development of a structure for auditing IT systems
	Do FinTech firms undergo auditing and evaluation?

On the other hand, it could be considered sufficient regarding the content of controls if only the portions leading to responsibilities under security measures are implemented. If FinTech firms play a leading role in financial-related services, then Financial Institutions' partial responsibility for security measures comes from the provision or receipt of customer-related

data. For this reason, the content of Financial Institutions' controls is concentrated on whether the data provided by FinTech firms is managed properly or whether FinTech firms properly confirm that the data received from FinTech firms is based on customer instructions.

As described above, the duties borne by Financial Institutions when providing data to FinTech firms, or receiving data from them, under Type III can be understood to be limited to portions related to preservation for customer-related data or confirmation of identity. For this reason, if it can be verified that FinTech firms implement effective security measures and realize the effects thereof with regard to these portions, then Financial Institutions' risk-management measures can be considered to be sufficient.

Under Type III, matters other than the portions related to preservation of customer-related data or confirmation of identity (e.g., stable operation of IT systems) are outside the scope of interest of Financial Institutions, and from the standpoint of Financial Institutions there is no need for any particular controls for these. However, it must be noted that in the event that the degree of system controls that should be carried out by FinTech firms overall were to decrease due to the fact that they were not subjects of interest to the Financial Institutions and, as a result, the effects of security measures related to data preservation or confirmation of identity were to be harmed, then the Financial Institutions would need to implement some kind of additional controls on FinTech firms for such matters beyond their scope of interest as well.

(Rules on mutatis mutandis application of outsourcing guidelines)

Under Type III, Financial Institutions can apply mutatis mutandis existing outsourcing guidelines. In such a case, the duties of Financial Institutions are limited to portions related to preservation for customer-related data or confirmation of identity at FinTech firms.

If it is not possible to enjoy the benefits of security measures for portions subject to the duties of Financial Institutions arising from portions for which Financial Institutions are not responsible, then additional security measures will need to be taken for the portions not subject to the duties of Financial Institutions.

(2) Responsibility for security measures remaining with FinTech firms

Under Type III, it is general practice for FinTech firms to entrust operation of information systems to IT solution providers such as Cloud service providers. Accordingly, from the perspective of applying mutatis mutandis outsourcing guidelines society expects FinTech firms to bear some part of Duties A in a form inseparable from the duties demanded of Financial Institutions.

Furthermore, since FinTech firms themselves play a leading role in providing financial-related services, they can be understood to bear chief responsibility to customers for security measures.

Accordingly, FinTech firms are expected to play an active role in advancing efforts related to security measures, through means such as formulating autonomous industry guidelines that conform to the Security Guidelines. (This is covered in detail under "III. Handling of FinTech operations not subject to the Security Guidelines.")

(3) Handling of cases in which Financial Institutions do not bear responsibility

In cases of financial-related services in which Financial Institutions have a completely passive approach, such as those in which FinTech firms play leading roles and obtain customer-related data from Financial Institutions in a unidirectional manner without any negotiation with the Financial Institutions, Financial Institutions can be understood to bear no responsibility for security measures.

However, since from the customer's point of view this means that they would not be able to rely on the Financial Institutions for assistance in the event that some kind of problem were to arise when using such financial-related services, it is recommended that the Financial Institutions advise their customers in advance of the fact that they are using financial-related services in which customer-related data are obtained from the Financial Institutions in a unidirectional manner.

5. Cooperation among related parties

As is clear from the considerations above, in implementation of appropriate security measures in FinTech operations close cooperation among the three parties of Financial Institutions, IT solution providers, and FinTech firms is essential, and if this is lacking then users could be exposed to unforeseen damages.

The most pivotal part of such cooperation is appropriate disclosure of information (including that concerning system risks) by FinTech firms to Financial Institutions in each management phase, such as when considering use and in the event of an incident. At the same time, if this were to be demanded of FinTech firms to an extent beyond the necessary scope, then it could be detrimental to innovation on the part of FinTech firms by forcing excessive burdens on them.

Accordingly, to enable cooperation and appropriate disclosure of information concerning security measures, it is recommended that the three parties reach a consensus in advance (principle of cooperation).

Also, utilizing a Checklist[30] for use in evaluation of outsourcees is recommended as a means of such cooperation. For this reason, it is conceivable that the Checklist used ordinarily would be considered a means of sharing information to promote cooperation, and that its content could be revised—including simplification—as appropriate.

As seen above, under any pattern the three parties involved in FinTech operations—Financial Institutions, IT solution providers, and FinTech firms—must balance the securing of IT system security and enjoyment of the benefits of innovation, and need to take on security measures through close cooperation.

[30] The existing Security Guidelines call for "objective evaluation of outsourcees" when considering use of outsourcing. In actual evaluation, it is common for Financial Institutions to use general checklists to evaluate the risks of outsourcing overall, including system risk. Possible methods of using these include handing the checklists to outsourcees and asking them to conduct self-checks before interviewing them concerning the results of these self-checks.

6. Supplementary consideration based on the properties of Type II

Based on the above consideration, the derivative form of Type II will be considered individually below with regard to the types of properties it involves in light of security measures and what kind of supplementation is necessary as a result.

(1) Properties of Type II

In general, Financial Institutions manage and control their subsidiaries based on individual management contracts concluded with them, in accordance with each subsidiary's position and role within the financial group or its size or other matters. For example, a Financial Institution might provide constant advice and guidance through means such as monitoring of risk-management status, or it might ascertain information in a timely and appropriate manner through means such as establishment of an obligation to report on material facts in a timely and appropriate manner. For this reason, under Type II, in which FinTech firms also bear responsibility to such subsidiaries, in addition to controls for outsourcees controls for such subsidiaries are added as well.

As a result, in the area of controls Type II may involve more points of contact on controls than other types, while also securing effective disclosure of information, and as a result it can be considered to facilitate the implementation of appropriate security measures through cooperation among related parties—which should be an aim of FinTech operations—to a greater extent than other types, for both Financial Institutions and FinTech firms.

On the other hand, in the area of allocation of management resources, in a case in which the results of objective evaluation show that FinTech firms lack full abilities to execute security measures and also lack management resources that can be allocated additionally to security measures, then under Type II the choice could be made to reinforce FinTech firms' management resources through means such as increasing capital or dispatching personnel, not just the method of reallocation of duties.

For the above reasons, from the perspectives of both controls and allocation of management resources Type II can be considered a type that offers a possible solution for Financial Institutions and FinTech firms vis-a-vis the objective of enjoying the benefits of innovation while ensuring IT system security.

(2) Supplemental information

In some cases, business administration and outsourcing management are handled using different contact sections, management items, and management cycles within Financial Institutions (see Fig. 8[31]). For this reason, it is anticipated that FinTech firms may need to employ individual handling for separate cases even when they involve the same Financial Institution. Since this is expected to lead to a burden on the part of FinTech firms, if there is a case that such a burden could be detrimental to innovation then it is recommended that the sections handling business administration and outsourcing management cooperate in taking care to ensure that no excessive burden will be imposed on FinTech firms[32].

[31] Here, Fig 8 looks at the example of an IT subsidiary. However, it is not the case that an IT subsidiary and a FinTech firm would require completely identical business administration or outsourcing management. A FinTech firm would be subject to management by Financial Institutions by category, in accordance with actual conditions such as its positioning within the financial group.

[32] Financial Institutions conduct business administration and outsourcing management from different points of view. They cannot omit one or the other of these. Also, as shown in Fig. 8, already a variety of efforts are underway to improve the efficiency of management.

Fig. 8. Fact-finding survey on business administration and outsourcing management (in the case of an IT subsidiary)[1]

Business administration			Outsourcing management		
Contact section	Examples of management items	Management frequency	Contact section	Examples of management items	Management frequency
Business administration section / IT planning section	Prior approval of decisions on important matters ・Changes in shareholders and executives ・Large-scale IT investment etc. Ascertain state of implementing business plans Ascertaining state of risk management ・Risk-management rules ・Large-scale IT system failures etc.	*2	Risk-management section / IT section	Ascertaining state of subcontractor management ・Prior review of new subcontractors ・Ascertaining state of subcontractor management etc. Ascertaining state of implementing subcontracting ・Work performance ・Performance on use of production data etc. Ascertaining state of IT risk management ・Results of IT risk evaluation ・System failures and analysis results etc.	*2

*1 Multiple banks with IT subsidiaries were surveyed.
*2 While management is implemented as needed or periodically depending on the management item, these are not necessarily handled the same way in both business administration and outsourcing management.

【Efforts to increase the efficacy and efficiency of management】

Parent company and subsidiary occupying the same building

Parent company providing training

Omitting periodic reporting for subcontractors located on site

Sharing of rules between parent company and subsidiary

Sharing of email and other systems with parent company

etc.

7. Treatment of information systems handling FinTech operations in terms of security measures

At first, the Council considered information systems handling FinTech operations based on the assumption that in most cases these would be general information systems. However, in a case in which the manifestation of a risk in an information system handling FinTech operations would have a serious impact on a service provided by a critical information system[33], the information system handling FinTech operations is considered a part of the critical information system, and as such it needs to be handled in accordance with security measures.

At the same time, since the scope subject to an individual information system is decided on by the Financial Institution independently, there also is a possibility that an information system handling FinTech operations could be handled under security measures as part of a critical information system even though it would not have a serious impact on a service provided by the critical information system.

In such a case, while there is a possibility that the judgment could be made that high Security Guidelines must be applied to the information system handling FinTech operations as well, by following the precedent of the higher-risk system, doing so would involve concerns that it could result in restraining Financial Institutions' efforts in the area of FinTech operations.

From the perspective of enjoying the benefits of innovation, it is recommended to address such issues in advance. For this purpose, it is conceivable that information systems that satisfy all of the following conditions could be identified clearly as separable subsystems that could be treated independently.

(1) Separability of the impact of risk manifestation
It is possible to ensure that the impact of manifestation of risks such as system failure occurring inside a subsystem will not affect other services provided by the system as a whole.

(2) Separability of risk properties
The properties of risks to the subsystem differ markedly in nature[34] from those of the system as a whole.

(3) Separability of risk management
It is possible to implement risk management—i.e., risk evaluation, security measures, and follow-up measures after manifestation of a risk—entirely within the relevant subsystem.

It is recommended that Financial Institutions consider handling of security measures for information systems handling FinTech operations with the above concepts in mind.

[33] For example, if a Financial Institution has no branch offices and no means of receiving settlement instructions other than through API connection with a FinTech firm, then if the system handling API connection were down then even if the accounting backbone system is not down the institution's settlement services themselves would be suspended as a result.

[34] For example, cases are conceivable in which although the system as a whole does contain customer information, the relevant subsystem does not.

III. Handling of FinTech operations not subject to the Security Guidelines

1. Handling of traditional subjects of the Security Guidelines

Information systems subject to the Security Guidelines are those that handle financial operations and for which Banking and Related Financial Institutions bear responsibility for such security measures. Simply put, this refers to information systems handling the financial operations conducted by Financial Institutions. Accordingly, the Security Guidelines do not apply directly to information systems that handle non-financial operations conducted by Financial Institutions, financial operations conducted by non-Financial Institutions, or non-financial operations conducted by non-Financial Institutions.

However, since it is anticipated that in many cases information systems handling non-financial operations conducted by Financial Institutions are information systems operated by those same Financial Institutions and subject to common security measures under policies related to security measures, even if it would not be appropriate to apply fully to them unchanged the Security Guidelines that assume the nature of financial operations, it is recommended that the beneficial portions of security measures for information systems handling non-financial operations included in the Security Guidelines be referred to—that is, that they be incorporated as appropriate in ways suited to the actual conditions of Financial Institutions' operations[35].

On the other hand, the thinking employed traditionally regarding financial operations conducted by non-Financial Institutions (such as prepayment methods and funds transfers conducted by non-Financial Institutions under the Payment Services Act) is that even though they involve elements that are similar in functional terms to financial operations conducted by Financial Institutions, and as such it cannot be denied that the security measures under the Security Guidelines would be beneficial in part for such operations, for the following reasons information systems handling such operations are not subject.

- Security Guidelines are voluntary guidelines formulated by FISC members. In general, voluntary guidelines differ from laws clearly established by a national or other government and enforceable through means such as courts of law (hard law) in that they are a type of arrangement reached privately (soft law)[36], and as such their socially normative nature is understood to apply only to the parties who explicitly took part in the process of formulation of such voluntary guidelines. The Security Guidelines were formulated mainly by Financial Institutions among the members involved in handling of financial information systems[37], and parties such as representatives of non-Financial Institutions conducting financial operations did not necessarily participate explicitly in the formulation process[38]. For this reason, it would not be reasonable to apply the Security Guidelines unilaterally to such non-Financial Institutions.
- While in fact the Security Guidelines are applicable beyond the framework of FISC members to Financial Institutions regulated by the Financial Service Agency since they are

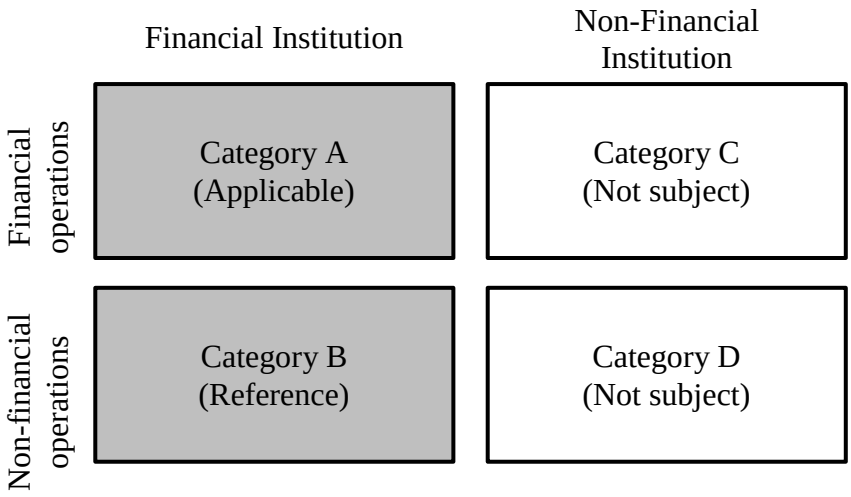
[35] See Footnote 4
[36] The description concerning soft law and hard law is cited from Hiroyuki Seshita, "Soft Law and hard Law," in Chapter 1, Part 3 of Nobuhiro Nakayama, editor in chief, Basic Theory of Soft Law (2008).
[37] As of the end of March 2017, Financial Institutions accounted for 542 of 644 FISC member companies, or 84%.
[38] The Security Guidelines were established through consideration by the Specialized Committee on Security measures and its subsidiary organization, the Study Group on Revisions to the Security Guidelines, whose members consist mainly of FISC member representatives, and then seeking the opinions of members.

mentioned in its inspection manual and other documents, it would be unreasonable to apply them beyond this scope to non-Financial Institutions not regulated by the Financial Service Agency.

Information systems handling non-financial operations conducted by non-Financial Institutions have never been considered subject to the Security Guidelines.

Fig. 9 presents the thinking outlined above in visual form.

Fig. 9. Handling of the traditional scope of the Security Guidelines



Note: Grey areas indicate those where Security Guidelines have normative application.

2. Courses of action on handling of FinTech operations not subject to the Security Guidelines

The financial-related services generally referred to as FinTech are broad ranging and new technologies or new business models are expected to appear in the future, and under such conditions it is expected that the Council sort out in advance the handling of FinTech operations under the Security Guidelines.

It is thought that while generally Financial Institutions and non-Financial Institutions are identified by the legal system through industry laws and other laws that make the subjects relatively clear, the financial-related services referred to in general as FinTech should be approached by clearly demarcating the boundaries between financial and non-financial operations through means such as focusing on functional aspects and identifying specific operations clearly, since the boundaries between such operations tend to be relatively ambiguous[39] in the case of FinTech.

However, even under such an approach it is difficult to identify individual operations in advance under conditions in which a wide range of services will appear, and even if such boundaries were made clear, handling under the Security Guidelines would vary even though

[39] For example, FinTech Law (2016), by Masakazu Masujima and Takane Hori, states, "The reorganization of the industry and changes to business models effected by FinTech are dissolving not only the barriers between financial businesses but also those between finance and non-financial industries."

in functional terms operations did not differ very much. There are concerns that doubts could arise regarding the appropriateness of such handling of FinTech operations.

It is thought that traditionally users expect appropriate security measures to be implemented in a seamless and inseparable way across FinTech operations as a whole, regardless of whether they are conducted by Financial Institutions or non-Financial Institutions, and that whether or not operations qualify as financial operations is not of primary importance to users.

Accordingly, in order to meet such social expectations it would be beneficial first of all for Financial Institutions in Japan to be able to obtain in FinTech operations a degree of trust in society similar to that which they have built up in their traditional operations. In particular, since the Security Guidelines, as rules agreed to in society, have played a role in the formation of such trust in society regarding information systems, when assuming as given the fact of diverse FinTech operations, it would be beneficial to sort out the degree to which the Security Guidelines have a socially normative nature among the parties handling such operations, regardless of whether they are Financial Institutions or non-Financial Institutions.

(1) Courses of action on handling of category B

In this category, the Security Guidelines long have been referred to in the form of reference. Under the actual conditions of Financial Institutions, in many cases the Security Guidelines and other FISC guidelines are incorporated into security policies and security standards, and security measures are implemented uniformly for both financial and non-financial operations[40].

Accordingly, even when FinTech operations include some that are considered non-financial operations, if Security Guidelines regarding FinTech are in place then security measures would continue to be implemented in reference to these guidelines, and there would be no particular issues that need to be considered.

(2) Courses of action on handling of categories C and D

This category includes FinTech operations conducted as financial operations by non-Financial Institutions, including financial-related services such as individual asset management in which FinTech firms play leading roles and P2P lending as conducted in the United States.

In considering handling of the Security Guidelines in this category, if we do not assume systemic changes by regulators then a normative nature of the Security Guidelines vis-a-vis non-Financial Institutions as well would be expected for purposes including earning users' trust in security measures.

Next, such a normative nature could arise through the following two methods:

(i) Direct normative nature
Non-Financial Institution FinTech firms become members of FISC individually. They participate explicitly in the process of formulation of the Security Guidelines and

[40] Part I, "Thinking on Security Guidelines,' of the Security Guidelines, states, "A security policy must be formulated to enable unified handling of information companywide." In addition, it also states, "Each Financial Institution or other organization needs to formulate and implement security standards suited to its usage of computer systems, the type and size of risks it faces, the importance of information it must protect, and the size and properties of its own company (internal Security Guidelines), in accordance with its own security policies and with reference to these guidelines."

contribute to formulation of guidelines from a FinTech perspective, as well as complying with the Security Guidelines.

(ii) Indirect normative nature

FinTech firms' industry organizations become members of FISC. As representatives of the industry, they participate explicitly in the process of formulation of the Security Guidelines and contribute to formulation of guidelines from a FinTech industry perspective. They also formulate voluntary guidelines for the FinTech that are consisted with the Security Guidelines, and members of the industry organizations comply with these.

With regard to method (i) above, FISC members already include some FinTech firms, and it is expect that they will take part in the process of formulation of the Security Guidelines in the future. Regarding method (ii), FISC membership also already includes some industry organizations, and some such organizations participate in consideration as members of the Council as well. Furthermore, these industry organizations plan to formulate voluntary guidelines regarding security measures, and at present consideration is underway while referring to the Security Guidelines and reflecting points of view corresponding to the distinctive properties of the industry organizations.

If as a result of progress on such initiatives the normative property of the Security Guidelines also impacts FISC-member FinTech firms and industry organizations, then as a result it can be expected that appropriate security measures would be implemented in a seamless and inseparable way in general for the financial-related services known as FinTech, by both Financial Institutions and non-Financial Institutions.

However, since ultimately the consideration of the industry organizations themselves must be relied on with regard to whether or not the content of these voluntary guidelines is consistent with the Security Guidelines and not all FinTech firms and industry organizations are necessarily FISC members, it would be appropriate for the Council to issue some kind of opinion on this topic.

3. Statement of opinion on security measures in FinTech operations

In light of the above points, the following opinion is offered concerning security measures in FinTech operations as a whole.

Statement of opinion

The FISC Council of Experts on FinTech in Financial Institutions is highly interested in the ideal form of security measures in information systems handling FinTech operations, whether such FinTech operations are implemented by Financial Institutions or others. For this reason, businesses involved in FinTech operations are expected to implement appropriate security measures that reflect the following Principles Applicable to Businesses Involved in Provision of Financial-Related Services[41], formulated by the Council.

(1) Businesses involved in provision of financial-related services shall implement appropriate security measures for information systems for which they are responsible for management, with the goal of ensuring that their users may use such services with peace of mind.

(2) In implementing security measures, businesses involved in provision of financial-related services shall give consideration both to ensuring that the results of innovation contribute to increased convenience for users and to promoting cooperation in security measures so that Financial Institutions and other businesses can utilize their own individual advantages.

(3) In implementing security measures in cooperation with each other, businesses involved in provision of financial-related services shall strive to form socially agreed-upon rules with regard to security measures, including the FISC Security Guidelines.

(1)

It is anticipated that businesses involved in provision of financial-related services would include a wide range of businesses, including not only Financial Institutions and IT solution providers but also FinTech firms. Since ensuring that users can use financial-related services with peace of mind is of utmost importance for purposes of maximizing enterprise value, it would not be appropriate if such businesses failed to implement any security measures for the information system needed to provide such services.

(2)

As seen in FinTech, innovations in financial-related services are taking place at a remarkable pace, contributing in particular to improvements in user convenience through providing innovative user experiences. Use of such services is advancing as a result. Accordingly, in implementing security measures care should be taken to avoid impeding innovation.

In addition, as open innovation advances among Financial Institutions it is expected that to a greater extent than before multiple businesses will be involved, in multilayered ways and at multiple stages, in provision of financial-related services. Even as relations among businesses

[41] While the "basic principles of security measures" recommended in the FISC Report of the Council of Experts on Outsourcing in Financial Institutions are basic principles applying mainly to FISC members, the "principles applicable to businesses involved in provision of financial-related services," while based on the "basic principles of security measures," apply more broadly to businesses involved in provision of financial-related services in general.

grow more complex in this way, it is possible to secure mutual advantages through involvement in services through cooperation among multiple businesses. Accordingly, business should cooperate with each other in implementing security measures as well.

(3)

Socially agreed-upon rules have been established with regard to security measures for financial information systems. These include the FISC Security Guidelines on Computer Systems for Banking and Related Financial Institutions issued by the Center for Financial Industry Information Systems, a voluntary guideline adopted by Banking and Related Financial Institutions. Distinctive characteristics of these include the fact that in the process of formulation of the Security Guidelines related parties with specialized and technical knowledge, including representatives of industries involved in financial operations and information systems, were involved, and related parties who bear responsibility for security measures in financial information systems and handle the field operations in which security measures are implemented participate voluntarily in planning (See References, Reference 6).

It is recommended that businesses involved in financial-related services both strive toward the formation of socially agreed-upon rules and implement security measures that conform to such rules.

4. FISC's role in working toward formation of socially agreed-upon rules

Traditionally, the main related parties in financial information systems have consisted of Banking and Related Financial Institutions as well as IT solution providers, and since most of these are FISC members it is possible for the Security Guidelines to reflect sufficiently the intents and properties of providers of financial information systems. As a result, most of the security measures needed for financial information systems can be checked using the Security Guidelines.

However, under conditions in which it is anticipated that with advances in open innovation even more businesses will be involved in provision of financial-related services in the future, it can be expected that businesses other than FISC members might become involved, and in such a case it probably would not be as easy to ensure that the Security Guidelines reflect sufficiently the intents and properties of all businesses involved.

In addition, since it is conceivable that individual businesses would formulate their own voluntary guidelines if voluntary guidelines completely unrelated to the Security Guidelines were to be formulated, then different rules would be applied and used among financial-related services.

FISC needs to fulfill its role in society to address such issues that might arise in the future. For example, if industry organizations of businesses involved in provision of financial-related services were to consider their own voluntary guidelines, then FISC would participate in such consideration and provide support as needed to form socially agreed-upon rules, striving to secure mutual consistency among such guidelines[42].

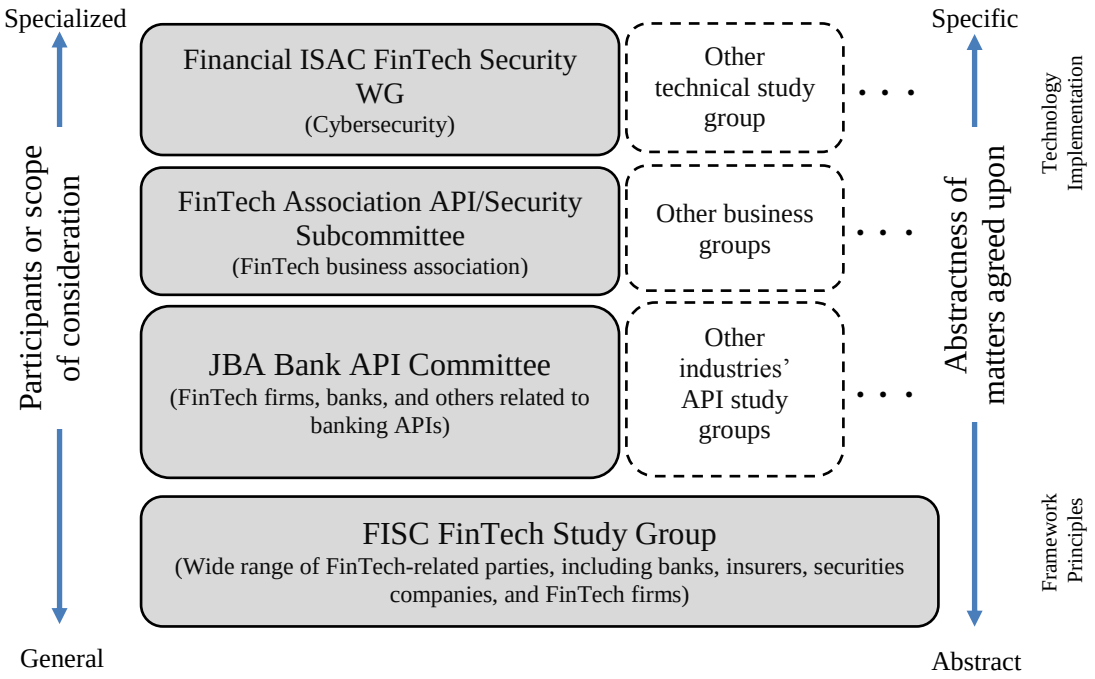
In formation of socially agreed-upon rules, it would be beneficial to focus on the minimum necessary Security Guidelines that FISC plans to formulate. Formulated as the minimal level

[42] An example of formulation of voluntary guidelines already underway is the establishment of the Review Committee on Open APIs , for which the JBA serves as secretariat, in the banking industry. It is studying independent guidelines reflecting the intents and nature of the banking industry. FISC both participates in this council and serves as secretariat in supporting the API Connection Checklist (tentative name) that it recommends. Also, the FinTech Association of Japan, a FinTech industry organization, is making progress on formulating its own voluntary guidelines. FISC participates in its studies and provides support through means including explanation of the Security Guidelines.

of guidelines that should be implement for information systems handling financial operations, these minimum necessary Security Guidelines can be considered to be guidelines that should be taken into consideration not only by FISC members but by other businesses involved in provision of financial-related services as well.

With regard to security measures in FinTech operations, collective consideration is underway by a wide range of organizations, including various industry organizations, and the interrelations among these, based on a look at the natures of the participants in such organizations and the scope of the matters they are considering, can be seen as shown in Fig. 10. From the perspective of ensuring consistency among the subjects of consideration by each of these organizations, it is expected that efforts would advance based on collective consideration, reflecting a consciousness of the interrelations among these.

Fig. 10. Examples of interrelations between organizations considering FinTech-related security measures



IV. Supplemental consideration of risk-management measures when using cloud services

Supplemental consideration centered on use of critical information systems

1. Perspectives of supplemental consideration

It would be beneficial to consider in a supplemental manner the Report of the Council of Experts on the Usage of Cloud Computing by Financial Institutions ("Cloud Council" hereinafter), and the Security Guidelines for cloud services formulated in supplemental revision 8 to the Security Guidelines based on that report ("Cloud Guidelines" hereinafter), from the following perspectives.

(1) Reflecting conditions after formulation of the Cloud Guidelines

After formulation of the Cloud Guidelines, together with advancing use of Cloud computing at Financial Institutions[43], Financial Institutions' FinTech efforts have rapidly increased in activity. Since cloud services often are used under such conditions in FinTech operations, it is expected that use of cloud service would increase further in the future. At the same time, through the Outsourcing Council's activities such as clarification of the meaning of critical information systems, deliberation on the risk-based approach proposed by the Cloud Council has intensified. In light of such conditions following formulation of the Cloud Guidelines, it is anticipated that in some cases Cloud Guidelines will be applied to critical information systems (e.g., block chains and AI as FinTech use cases), and in order further to increase the efficacy of Cloud Guidelines, it would be beneficial to carry out supplemental consideration of matter such as whether there are any points on which Cloud Guidelines should be made clearer. It also would be beneficial to identify the properties specific to cloud services in order to make clear the perspectives of risk-management measures that should be supplemented[44].

(2) Trends among other developed countries

Since formulation of guidelines on use of cloud services advanced in other developed countries around the same time the Cloud Council met, it would be beneficial to refer to such guidelines and other materials (References, Reference 8).

While the guidelines of other developed countries share many points of commonality with Japan's Cloud Guidelines, some examples of their distinctive features are provided below.

- Financial Institutions must have effective access to data related to outsourced operations. As used here, data includes not only Financial Institutions' data, customer data, and transaction-history data but also data related to systems and procedures[45], and it is thought that it would not be appropriate to narrow the scope of subject data. In addition, while based on this way of thinking the business facilities subject to such access are interpreted broadly to include headquarters and administrative centers, it is conceivable that in some

[43] In FY2013, immediately before the launching of the Cloud Council, 26.7% of Banking and Related Financial Institutions used the Cloud. In contrast, in FY2015 this percentage had increased to 36.4%. (See References, Reference 7)

[44] Identification of properties specific to cloud services is beneficial for differentiating in the future which Cloud Guidelines are applicable to outsourcing in general and which are specific to the Cloud. For details, see Footnote 31 to the FISC Report of the Council of Experts on Outsourcing in Financial Institutions.

[45] For example, procedures for investigating staff identity and system audit traceability also are included.

cases access to data centers would not necessarily be required. Furthermore, with regard to jurisdiction contracts with Cloud service providers are de facto subject to the jurisdiction of domestic law. This is intended to increase the efficacy of data access. These can be understood as explicit requirements focused on access to data needed for control purposes in light of the fact that in use of cloud services the degree of controls implemented by Financial Institutions in general tends to be low.

- The purpose of establishment of requirements is identified as "to identify appropriately and encourage management of operational risks involved in use by Financial Institutions of outsourcees," and based on this, there is a need to "ensure that operational risk to Financial Institutions does not increase." Most requirements are centered on matters related to general control methods such as risk management and supervision and do not touch on the content of controls related to equipment and other technologies. While clearly identifying the basic concept that the level of controls should be identical regardless of whether or not outsourcing is employed (i.e., that the effects of security measures should be identical), it is understood that if these are understood sufficiently then the various individual technical risk-mitigation measures that may be taken in light of factors such as the properties and sizes of Financial Institutions should be entrusted primarily to the Financial Institutions themselves.

In light of the above matters, properties specific to cloud services will be discussed in detail first, and then supplemental consideration will be conducted centered on cases in which cloud services are used in critical information systems.

2. Properties specific to cloud services

The Cloud Council determined that it would be appropriate to treat cloud services as a form of outsourcing. As used here, outsourcing is a term used to refer to the source from which IT system resources are procured. Thus it would be appropriate here to summarize the nature of cloud services, a form of outsourcing, from the perspective of procurement of IT system resources.

At the time at which the Security Guidelines first were formulated, methods of procuring IT system resources were not as diverse as they are today. In general, resources such as buildings, power supplies, air-conditioning, and water-cooling equipment, as well as the staff required in development of business software applications and operation of information systems, basically were arranged by Financial Institutions themselves, while procurement from outside suppliers was limited more or less to hardware such as host computers and tape storage equipment, basic software such as operating systems and database systems, and some development and operation staff[46].

Later, for purposes including to reduce costs and put advanced technologies to use, outsourcing, thorough procurement from outside suppliers of resources related to operation of information systems, gradually advanced, and as a result today more than 90% of Financial Institutions employ outsourcing for accounting backbone systems. At the same time, this means that Financial Institutions need to shift the focus of their controls from internal to external subjects, while also maintaining the effects of security measures at the same level as

[46]For this reason, since the internal organizations of Financial Institutions are the main subject of controls under security measures, of the 113 guidelines in the first edition of the Security Guidelines two concerned outsourcing.

when procuring such resources on their own, even as the focus of controls shifts in this way. This had led to the need to implement additional security measures[47].

Cloud services appeared amid these changes in methods of procuring IT system resources and in the focus of controls. Since in procurement of IT system resources cloud services enables more flexible procurement in accordance with user needs than does traditional outsourcing[48], it is anticipated that use of cloud services will advance further as Financial Institutions incorporate FinTech across a wide range of areas.

At the same time, it is anticipated that the status of cloud services as being subject to controls would increase more and more at Financial Institutions, and in light of the state of cloud services in recent years their specific natures will be summarized below, together with making clear the perspectives on which supplemental consideration is needed.

(1) Anonymous joint use

While cloud services involve the nature of joint use in which multiple businesses entrust services to the same Cloud service provider, this is anonymous joint use in that no communication takes place among users.

For this reason, the main role in decision-making on security measures in cloud services is played not by individual users but by the Cloud service providers. For example, there is a tendency to take a passive approach toward audit requests or improvement requests from individual users, and this could lead to a refusal to grant access to data centers as needed for auditing purposes, due to security concerns. Accordingly, there is an inherent possibility that controls by Financial Institutions might not function fully at Cloud service providers, and as a result risk evaluation and risk mitigation measures might not be able to be implemented appropriately.

While for general information systems it would be sufficient to choose Cloud service providers appropriately with consideration for such possibilities and for Financial Institutions to make decisions on the degree of controls in accordance with the risks involved, for critical information systems the social impact of an incident could be massive, and particularly in an emergency Financial Institutions need to demonstrate fully their control capabilities with regard to Cloud service providers, to the same degree as in traditional outsourcing of critical information systems[49]. While in considering controls it is conceivable that risk-management measures could be considered based on the control perspective employed at shared system centers[50], which involve a similar nature of joint use, it also must be noted that cloud services differ from shared system centers, to which specific outsourcees entrust operations

[47] The most recent supplemented and revised Version 8 of the Security Guidelines includes nine additional guidelines on outsourcing (including five on cloud services). It is thought that in future revisions to the Security Guidelines it will be necessary to reflect appropriately, for example in the structure of the Security Guidelines, the fact that the focal point of controls is shifting from an internal to an external one.

[48] Conceivable characteristics of flexible procurement include economical costs, immediacy of procurement, simplicity of procurement procedures, and efficiency of system management. Economical costs refer to the ability to enjoy economies of scale in the form of relatively lower costs since the scale of information processing is so large. Immediacy of procurement refers to the relative shortness of the period from the decision to use a service to the time it enters service. Simplicity of procurement procedures refers to cases such as the ability to configure system usage conditions easily on the Internet. Efficiency of system management refers to, for example, the lack of a need for individual management of hardware. It also has been pointed out regarding these characteristics of security measures that the amount of investment in security is higher than for Financial Institutions (some Cloud service providers invest billions of yen per year in security) and the high degree of service continuity since information processing covers a wide area.

[49] While the Cloud Guidelines mention the option of use of third-party auditing as an effective and efficient means of monitoring during operation, intended to demonstrate control capabilities during normal times, the May 2016 FISC System Audit Guidelines (Additions to Revision 3 ("Audit Guidelines" hereinafter) provide specific recommendations on methods of joint auditing using third-party auditors, as key points of cloud service auditing including the processes thereof and points to consider.

[50] A shared system center is a center to which multiple Financial Institutions jointly entrust tasks such as operation of critical information systems. It is similar to cloud services in that multiple users enjoy the benefits of security measures.

comprehensively, in that Cloud service providers may be entrusted with partial operations, such as information systems' hardware or basic software.

For the above reasons, in supplemental consideration related to critical information systems decisions are made on the scope of controls and their content based on an understanding of the demarcation of responsibilities with Cloud service providers while referring to the risk-management measures applicable to shared system centers[51] with regard to this nature of joint use[52]. It also would be appropriate to clarify risk-management measures to make up for the decrease in controls accompanying the nature of anonymity[53].

(2) Broad range of information processing

Since users of cloud services are broad ranging, business facilities including those where information is processed may cover a broad geographical range that includes multiple countries. This differs from traditional outsourcing in which the bulk of business facilities tends to be located domestically, and users may want, for example, to know in advance the location of the facility where they can access the data they need to effect recovery and investigate the cause in the event of an incident. Also, to ensure that recovery, investigation of causes, and subsequent measures to prevent reoccurrence can be conducted effectively, they would like it to be stated clearly in the contract who is the auditing authority for the business facility where they can access such data, or that the laws and regulations of their own country apply to that business facility.

While in the case of general information systems it is sufficient for Financial Institutions to respond to incidents individually, deciding themselves on the degree of controls in accordance with risks, since in the case of critical information systems the social impact of an incident could be massive Financial Institutions also need to consider risk-management measures from the perspective of the business facilities at which data can be accessed.

For the above reasons, in supplemental consideration related to critical information systems it would be appropriate to clarify risk-management measures related to the business facilities where it is possible to access the data needed for control purposes, including recovery from incidents and investigating their causes[54].

(3) Technical advancement

Cloud services are undergoing remarkable technological advances, particularly in the areas of software such as virtualization technology that makes it possible for multiple users to use resources efficiently and technologies to conceal data better so that it cannot be accessed or used by other than the authorized users. For this reason, in some cases it is possible to achieve

---

[51] The FISC Report of the Council of Experts on Outsourcing in Financial Institutions addresses the issue of timeliness in responding to an emergency in particular as a form of risk management at a shared system center. While since in cloud services there is no communication among users, in a sense this means that the issue of achieving a shared understanding among users does not arise. However, since Cloud service providers consider the impact on all users as a whole, it might take some time for them to respond to emergencies. Accordingly, the issue of timeliness in responding to an emergency concerns use of cloud services as well, and for this reason the "IT governance specific to shared system centers (risk management measures)" proposed in the FISC Report of the Council of Experts on Outsourcing in Financial Institutions should be referred to.

[52] The Security Guidelines (Operation 109) identify as one basic matter that should be considered when concluding contracts with Cloud service providers "arrangements regrading demarcation of management and divisions of responsibilities with Cloud service providers (including cases when serves are entrusted to multiple Cloud service providers)."

[53] Auditing is one way to improve control capabilities. Regarding auditing, the Cloud Guidelines state, "System auditing and monitoring are required." On auditing authority, they state that "clearly stating the right to implement on-site auditing etc." is "recommended."

[54] Under the Cloud Guidelines, it is anticipated that data for which the location should be confirmed would be Financial Institutions' data. For this reason, the location needs to be ascertained from the perspective of business continuity. Also, regarding jurisdiction, the guidelines state, "There is a need to give sufficient consideration to . . . which country's laws would apply in the event of a dispute."

effects equal to those of physical security measures such as those achieved through equipment and hardware using software technology alone[55], and in other cases more effective software technology itself is appearing, redrawing the existing technological map. Accordingly, it might not necessarily be appropriate to identify technical security measures such as equipment guidelines and technical guidelines uniformly in advance.

In light of such conditions, under existing the Security Guidelines ways of thinking about mutual handling of operation guidelines, equipment guidelines, and technical guidelines are not necessarily identified clearly. For this reason, current conditions involve uncertainties when equipment guidelines and technical guidelines, which are highly susceptible to the effects of technological changes, are used exactly as defined without reflecting the conditions of technological changes as evaluation items in (for example) objective evaluation when choosing a Cloud service provider[56]. As a result, when viewed from the perspective of the results of security measures overall, there is a risk that controls formally could be extended to areas in which Financial Institutions should not implement controls individually, leading to excessive security measures.

In addition, although in light of the advanced nature of technologies employed auditors need to have full knowledge of the details of technologies employed in cloud services, if the IT staff and IT system auditing staff available to Financial Institutions internally are limited, then there is a risk that audits will not necessarily be effective.

While for general information systems if handling of Security Guidelines is defined clearly then it is sufficient for Financial Institutions to make risk-based decisions accordingly, in the case of critical information systems Financial Institutions need to employ consideration from the perspective of securing efficacy while assuming that auditing will be conducted.

In light of the above matters, it would be appropriate for additional consideration to clarify the handling of Security Guidelines of a technical nature, such as equipment guidelines and technical guidelines, and to clarify risk-management measures related to human resources, such as auditing, for critical information systems[57].

3. Thinking on controls for outsourcees handling critical information systems

In light of the specific nature of cloud services, it would be beneficial for additional consideration of risk-management measures to make clear the way of thinking on controls for outsourcees handling critical information systems.

First of all, "critical information systems" refers to information systems involving serious externalities or those handing sensitive information (including personal information that must

[55] For example, from the perspective of the principle of equivalency, if the effects of the security measures can be increased through means such as data encryption and distribution of data across multiple data centers, then the physical security measures conducted in a single data center might not need to be as strong as usual.

[56] For example, the equipment guidelines include Equipment 47: "Measures must be taken to prevent damage due to rodents. While this does exist as a risk, among the data centers used by Cloud service providers there are cases in which this risk is not high enough to require explicit confirmation by Financial Institutions. For this reason, whether or not to apply this guideline should be determined through consideration of the actual situation of the Cloud service provider. Also, the technical guidelines include Technical 28, 29: "Measures must be taken to prevent leakage of data." This guideline states, "Encryption is recommended," providing an example of technical measures. However, since such technology is advancing rapidly from day to day, if the example provided in the technical guidelines were to be stuck to in a formal manner, then there is a risk of a failure to evaluate properly superior technologies adopted by Cloud service providers.

[57] To increase the efficacy of auditing, the Cloud Guidelines state, "It is acceptable to substitute auditing by a third party in cases such as when it would not be effective for an outsourcer Financial Institution to conduct an on-site audit" and "It is effective to verify the content of results of auditing already undergone by the Cloud service provider and conduct spot verification of the Cloud service providers concerning chiefly problems and matters on which the audit results were inadequate."

be given special consideration[58]). In the event of a large-scale system failure involving one of the former systems, the impact would not be limited to internal matters such as customers but also could affect the financial infrastructure or stable economic management, while a case of leakage of sensitive personal information involving one of the latter systems could lead to credit instability that could develop into a situation that could impact the survival of Financial Institutions themselves. Since responsibility for responding to incidents in information systems with such a social and public nature rests primarily with the Financial Institutions, because it derives from the nature of financial operations, even when using outsourcing such responsibility is not borne by the outsourcees, who handle only technical aspects. Accordingly, in the event of an incident the Financial Institutions are responsible for minimizing its impact as well as effecting swift recovery of the information systems and ensuring business continuity, and they need to make adequate arrangements in advance to implement the same degree of controls for outsourcees as they would for internal systems.

To enable effective controls in the event of such incidents, it is necessary both to monitor the status of operation of IT systems on an everyday basis in normal times for reasons including to ensure that no irregularities will be overlooked and to check periodically on the state of internal controls on the part of outsourcees, encouraging them to resolve any issues that could affect responses in the event of an incident.

The points above also apply to cloud services, as a form of outsourcing, and when Financial Institutions use cloud services as critical information systems, in light of the demarcation of responsibilities of Cloud service providers they need to implement effective controls while keeping in mind the positioning of Cloud services in business continuity[59].

4. Supplemental consideration of risk-management measures

In light of the above matters, the following supplemental proposals are offered concerning risk-management measures for implementing effective controls when using cloud services.

(1) Ascertaining Cloud facilities subject to controls

When using cloud services for critical information systems, during selection of Cloud service providers Financial Institutions must ascertain the business facilities subject to effective controls[60] ("Cloud facilities subject to controls" hereinafter), such as information processing

[58] As used here, sensitive information refers to such information as stipulated in the Financial Service Agency's Guidelines on Protection of Personal Information in the Financial Sector. This includes personal information for which consideration is required under the amended Personal Information Protection Act. (Article 5, Paragraph 1 of the Guidelines [enacted May 30, 2017] identifies as sensitive information "personal information requiring consideration pursuant to Article 2, Paragraph 3 of the Act as well as information concerning labor union membership, family status, legal domicile, health, and sexual lifestyle." Article 2, Paragraph 3 of the amended Personal Information Protection Act states, "Personal information requiring consideration refers to personal information identified in laws, regulations, etc. requiring particular consideration in handling to avoid inappropriate discrimination or bias against the individual, such as his or her ethnicity, creed, social status, medical history, criminal record, or status as a victim of crime.")

[59] While Financial Institutions need first of all to ensure business continuity in an emergency, keeping the effect of the emergency to a minimum, this does not mean that all Financial Institutions need to apply uniform risk-management measures to Cloud service providers. For example, if the business continuity plan includes use of a standby system in an emergency without waiting for recovery of the cloud service, then clearly the risk-management measures for Cloud service providers would differ from those in a case in which the business continuity plan assumes recovery of cloud services. Also, as pointed out in the FISC Report of the Council of Experts on Outsourcing in Financial Institutions, if as a result of fractionalization of outsourced operations the risk of operations outsourced to Cloud service providers can be judged to be sufficiently low, then risk-management measures may differ. Accordingly, for critical information systems Financial Institutions should decide on specific risk-management measures in light of the positioning of the cloud service and how it is used.

[60] While Cloud facilities subject to controls may include the head offices, sales offices, data centers, operation centers, and a variety of other facilities of Cloud service providers, in fact these may be specified by Financial Institutions individually in accordance with matters such as the content of cloud services used and the state of internal controls of Cloud service providers. Accordingly, it is not absolutely necessary to include data centers in Cloud facilities subject to controls.

facilities where data necessary for control purposes ("necessary data" hereinafter) can be accessed.

Also, Cloud facilities subject to controls need to be located in regions (countries, states, etc.) where controls effectively are feasible.

(2) Clear description of auditing authority etc.

When using cloud services for critical information systems, Financial Institutions must make clear in contracts concluded with Cloud service providers or through other means the rights that they require (e.g., auditing authority) in order to implement effective controls over the Cloud facilities subject to controls, to secure such rights.

(3) Implementing audits

In auditing Cloud service providers, in light of the advanced nature of the technologies involved it is recommended that Financial Institutions use guaranteed audit reports from auditors entrusted by the Cloud service providers themselves. Also, in such a case it is recommended that reports be used that verify consistency with the Security Guidelines, so that controls function fully and effectively[61].

When using cloud services for critical information systems, Financial Institutions must implement periodic auditing to ensure that effective controls function fully and effectively.

(4) Assignment of auditors and other monitoring staff

When using cloud services for critical information systems, Financial Institutions' top management must assign human resources who possess the capabilities needed effectively to implement auditing and other monitoring of the Cloud service providers, based on an understanding of the advanced nature of the technologies employed in cloud services. In addition, if it is not easy to train such human resources inside the Financial Institutions, use of specialized third-party auditors and similar parties is recommended.

(5) Points to note when implementing objective evaluation

While the Cloud Guidelines state that Financial Institutions "need to conduct evaluation based on information related to the qualities and business execution capabilities of Cloud service providers and on matters such as the states of the Cloud service providers' internal controls and risk management" when selecting Cloud service providers, it must be noted that this does not necessarily mean that the evaluation items used when implementing objective evaluation must include the equipment guidelines or technical guidelines of the Security Guidelines.

[61] In addition, it is conceivable that Cloud service providers could provide services such as audit tracing to users via the Internet or other methods as means of effective and efficient auditing.

V. Ideal form of security measures for open APIs based on collective consideration

1. Control-related issues in open APIs

Since an open API is one means of realizing Type III, Financial Institutions publishing APIs apply mutatis mutandis outsourcing guidelines and implement controls for FinTech firms connecting via these APIs through the methods of objective evaluation and monitoring[62].(Rules on mutatis mutandis application of outsourcing guidelines)

Accordingly, if in the future regulators, industry organizations, and others were to develop an open API environment, then API-based connections between Financial Institutions and FinTech firms would increase in number, and as a result FinTech firms would be subject to controls by multiple Financial Institutions.

If in doing so it were to be the case that multiple Financial Institutions would formally implement individual controls, then there would be a concern that the burden of responding to these would be excessive for FinTech firms, and this could be detrimental to innovation.

Since originally the controls implemented by Financial Institutions are conducted in accordance with the Security Guidelines etc., it is conceivable that the methods and content of controls would involve commonalities among Financial Institutions in numerous areas. If parties involved in API connections were to study these commonalities in controls jointly and implement related efforts with the goal of lessening the burden on FinTech firms, then Financial Institutions would be able to enjoy the benefits of innovation.

2. Ideal form of security measures in open APIs

Controls can be divided into their content—e.g., data preservation, confirmation of identity, service availability, and failure management—and their methods—e.g., objective evaluation, conclusion of contracts, and monitoring. Each of these involves numerous points of commonality among Financial Institutions.

First of all, in general Financial Institutions decide on the content of controls as independent items added to the rules agreed upon by society, such as the Security Guidelines and voluntary guidelines of industry organizations. Accordingly, it is conceivable that at first Financial Institutions and FinTech firms would come together to consider and build consensus on the content of controls—that is, items on Checklists used for objective evaluation—at the entry stage of considering use, based on socially agreed-upon rules related to open APIs[63]. If agreement has been reached in advance on the parts in common of the Checklist, then it will be possible to reflect these in the contract, monitoring and auditing items, etc. as the content of controls conducted later, when concluding the contract and during operation. This would result in lessening the burden of reaching consensus individually between Financial Institutions and FinTech firms on security measures.

Next, with regard to the methods of controls, traditionally it has been common practice at Financial Institutions to implement control methods such as monitoring jointly. Controls have

[62] The Bank API Report states, "Before connecting with the APIs of other businesses there is a need to review the suitability of such APIs from security and other perspectives," and "The security suitability of API connections needs to be checked periodically or as needed."

[63] The Bank API Report states, "To lessen the burden of review on companies connected to multiple banks through APIs, it is expected that the bank will prepare an API connection checklist (tentative name) for use in reviewing the suitability of API connections." For this reason, the API Connection Checklist (Tentative Name) Working Group was established with FISC serving as its secretariat, and it handles tasks including consideration of commonalities in the content of controls. See References, Reference 9 for details.

been made more efficient through multiple Financial Institutions reaching agreement and having a selected lead Banking and Related Financial Institution (or a third-party auditor entrusted by the Banking and Related Financial Institutions) implement controls as their representative, sharing the results. Accordingly, under an open API too it would be possible for Financial Institutions to implement controls jointly of parties connected to using a common API. For example, use by other Financial Institutions of the results of objective evaluation, contracts concluded, and audit results of such a lead Banking and Related Financial Institution[64] would lessen the burden on FinTech firms compared to dealing with each Financial Institution individually.

As seen above, it is possible when Financial Institutions conduct controls as a group in accordance with content agreed upon in advance among related parties to lessen the burden further if FinTech firms are able to respond to controls as a group.

As regulators, industry organizations, and others make progress on environmental improvements, a movement can be seen toward the establishment of groups of businesses participating in open APIs, as an effort toward forming groups of FinTech firms[65]. If such a group of businesses has been established, then it would be possible both to formulate voluntary guidelines on security measures based on the content of controls agreed upon in advance among related parties and to provide guidance and recommendations to members as necessary based on the results of verification of the state of compliance of individual members with such voluntary guidelines, for example through auditing by internal auditors (including third-party auditors entrusted by such groups of businesses)[66].

As seen above, if efforts based on collective consideration are expected to advance at FinTech firms, then it would be expected that groups of Financial Institutions would begin consultation with groups of FinTech firms concerning security measures, and both sides would cooperate in advancing efforts aimed at minimizing the burdens on related parties while securing overall security[67].

[64] The Bank API Report states, "Prior review may refer to the results of prior review by other banks in order to standardize the level of such review and lessen the burden on companies connected to multiple banks through APIs, with the bank taking responsibility for entrusting such review to another bank." It also states, "Monitoring may refer to the results of monitoring by other banks in order to standardize the level of such monitoring and lessen the burden on companies connected to multiple banks through APIs, with the bank taking responsibility for entrusting such monitoring to another bank." Regarding joint auditing methods, refer to the "Key points of joint system audits" and "Key points of cloud service audits" in the audit guidelines.

[65] On March 3, 2017, the FinTech Association of Japan released a document titled "Toward a certified e-settlement agency business association," calling for "Preparation by multiple businesses for . . . establishment of a certified e-settlement agency business association as called for in the proposed amended Banking Act" and noting, "The new association plans to consider improved APIs for Financial Institutions in addition to providing the operations stipulated for such an association in the amended Banking Act, such as establishment of the necessary rules and handling complaints."

[66] For example, the act on partial revisions to the Banking Act (passed May 26, 2017) included under Article 52-61-20, as duties of an association of certified e-settlement agency businesses "establishment of rules as necessary to ensure the propriety of e-settlement and other businesses conducted by members and the appropriate handling and security of information handled" and "guiding and advising members and other activities intended to ensure compliance with rules."

[67] For example, if a FinTech business association were to verify members' state of compliance with voluntary guidelines as part of its guidance and advising of members, then even though the party conducting this task would differ from that of verification by an association of Financial Institutions of FinTech businesses during objective evaluation and monitoring, effectively there are likely to be many areas of overlap, and so a joint implementation scheme might be considered in order to minimize the burden on related parties.

VI. Thinking on future revisions to the Security Guidelines etc.

After those of the Council, FISC will receive recommendations from the Outsourcing Council and the FinTech Council and proceed with revisions to the Security Guidelines and other guidelines. In doing so, it is expected that such revisions will be based on the content of the reports from both councils, including that outlined below, and that an understanding centered on thinking on security measures will be attained among a diverse range of parties related to security measures in financial information systems.

1. Adoption of the basic principles of security measures

Basic principles based on a risk-based approach shall be adopted as the thinking on security measures.

2. Clarification of the Security Guidelines

(1) Clarification of the subjects of the Security Guidelines

Financial information systems subject to application of the Security Guidelines shall be defined clearly as information systems used in the financial operations conducted by Financial Institutions, and the relationship between other information systems and the Security Guidelines shall be made clear.

(2) Clarification of the definitions and positioning of the high Security Guidelines and minimum necessary Security Guidelines

The high Security Guidelines shall be defined and their subjects identified clearly as information systems involving serious externalities and information systems containing sensitive information. In addition, minimum necessary Security Guidelines shall be defined and the fact made clear that they should be established within the scope of the objective of reducing uncertainty in security measures.

(3) Clarification of the positioning of technical guidelines

It shall be made clear that under conditions characterized by rapid technological progress, technical guidelines and other guidelines should be handled in different ways. It shall be made clear that the former should not be applied literally to all information systems but rather that Financial Institutions should determine whether or not to apply them based on the latest technological trends and other factors, while taking into consideration the high Security Guidelines and minimum necessary Security Guidelines.

3. Enhancement of external control guidelines

(1) Reflecting shifts in the focus of controls

Financial Institutions' dependency on outsourcing is increasing in backbone accounting systems and other areas. Based on the fact of this shift of the focus of controls from internal to

external resources, control guidelines applicable to external parties under the Security Guidelines shall be made clear.

(2) Consolidation of control guidelines in light of diverse forms

Guidelines and related matters shall be consolidated in accordance with the ideal forms of controls based on the diverse forms of related matters such as shared system centers, cloud services, and FinTech and in accordance with the nature of each.

Conclusions

In addressing the theme of FinTech, the Council began its consideration by first making clear the form taken by FinTech. This resulted in recommendations unlike those made elsewhere in the world, through classifying FinTech by type based on the perspective of controls by Financial Institutions. This has made it possible to identify the issues logically and appropriately, and to draw out effective and practical countermeasures for them.

In addition, even though FinTech is a broad-ranging theme, this report was prepared over a short period of just nine months, through a total of six meetings, in order to keep pace with the movements of Financial Institutions, industry organizations, regulators, and other related parties. This was possible in large part thanks to the sufficient groundwork that had been laid for collective consideration by parties related to financial information systems in Japan through the process of the FISC's maintenance of the Security Guidelines for more than 30 years. That is, when considering FinTech in Japan there was no need to gather related parties together anew and deliberate on new guidelines, since it was sufficient to consider, through an existing system for collective consideration, additional issues arising when applying existing the Security Guidelines to FinTech. This groundwork laid by the FISC will enable efficiently and flexibly addressing various issues related to financial information systems that may arise in the future—not just FinTech—in ways in which Japan can either lead the world or keep pace with other countries.

At the same time, the Council's consideration builds on the groundwork of the recommendations of the Outsourcing Council. For example, while the Outsourcing Council added maximizing enterprise value to ensuring system security as part of the thinking behind the Security Guidelines, the Council, by focusing on enjoyment of the benefits of innovation through FinTech initiatives, proposes practical methods for maximizing enterprise value in the form of principles and rules. In addition, while the Outsourcing Council proposed application of the Security Guidelines from a risk-based approach, the Council deepens this further to consider the fundamental issues of what should be subject to the Security Guidelines to begin with and how FISC should address matters not subject to application of the Security Guidelines, expressing its opinion based on such consideration. Furthermore, since the Outsourcing Council made clear the meaning of "critical information systems," the Council considered cases in which cloud services are used as critical information systems, shining light on a subject not necessarily addressed sufficiently in previous consideration by the Cloud Council, and thus serving to supplement the content of its recommendations. Through the process of such consideration, the Council has reviewed the history of procurement of IT system resources and, building on this, both made clear the historical significance of cloud services to Financial Institutions and offered advanced opinions unlike any seen before in the world, by making clear the distinctive properties of cloud services that differ from those of traditional information systems.

In this way, as a result of deliberation of uniform depth through both councils on outsourcing and FinTech, it has been possible to offer broad-ranging and mutually consistent opinions from individual risk-management measures to the fundamental principles of thinking on the Security Guidelines as well as the ideal form the FISC should take.

This final report is the fruit of passionate and diligent deliberation on the part of the Chair Iwahara, Assistant Chair Fuchizaki, and other members of both councils, including experts and representatives of Financial Institutions, FinTech firms, IT solution providers, and Cloud service providers, as well as the observers from government agencies and the central bank.

In the future, revisions to the Security Guidelines will be advanced through a permanent specialized committee on security measures organized by the FISC, based on the content of the recommendations of both councils. In doing so, plans call for employing discussions from perspectives that will be easy for those involved in the field in financial information systems to understand and use, while not deviating from the fundamental principles of the recommendations of the Council of Experts. In addition, since they will reflect the fundamental and broad-ranging recommendations of both councils, plans call for implementing the most thoroughgoing, large-scale reforms to the Security Guidelines since their first edition was formulated in 1985.

It is expected that through these revisions, the thinking on new security measures to serve in central roles in the coming age, as recommended by both councils of experts, will be reflected appropriately in the Security Guidelines, and that as a result Financial Institutions will be able to aim to maximize their enterprise value while also ensuring the security of their IT systems even as they respond appropriately to future environmental changes.

List of Members and Observers of the Council of Experts on FinTech in Financial Institutions
(As of June 21, 2017)

(Honorifics omitted)

Chair	Shinsaku Iwahara	Professor of Law, Waseda Law School
Assistant Chair	Masahiro Fuchizaki	Representative Director, President & CEO, the Japan Research Institute, Limited
Members	Kiyoshi Yasutomi	Professor emeritus, Keio University Visiting Professor of Law School and director, Legal Education Center,Kyoto Sangyo University Attorney (Atsumi & Sakai)
	Jiro Kokuryo	Vice President/Professor of Faculty of Policy Management, Keio University
	Hiroshi Kamiyama	Attorney-at-law, Partner, Hibiya Park Law Offices
	Hideaki Tanaka	Head of Information Tehcnology Risk Management Department, IT & Systems Planning Division, Mizuho Financial Group, Inc. (through fourth meeting)
	Kohtaro Mochida	General Manager, IT & Planning Dept., System Risk Planning Dept., Sumitomo Mitsui Banking Corporation (starting with fifth meeting)
	Mitsuru Yamada	General Manager, IT Systems Division, The Nanto Bank, Ltd.
	Norifumi Yoshimoto	General Manager, FinTech Business Planning Dept., SBI Sumishin Net Bank, Ltd.
	Hironori Sanada	General Manager In Charge of Information Systems Dept., Sumitomo Life Insurance Co.
	Toshitsugu Hisai	Associate Director, IT Planning Dept., Tokio Marine & Nichido Fire Insurance Co., Ltd. (through fourth meeting)
	Koji Kuroyama	General Manager, IT Planning Dept., Tokio Marine & Nichido Fire Insurance Co., Ltd. (starting with fifth meeting)
	Motohiro Uemura	Deputy Managing Director CIO Office (Executive Director), Nomura Holdings, Inc.
	Mark Makdad	Director, Fintech Association of Japan
	Toshio Taki	Director and Executive Officer, Head of the Money Forward Fintech Research Institute

	Hironobu Todoroki	Head of Corporate Management,General Counsel, Liquid Inc.
	Takashi Murakami	Senior Specialist, Business Development Group, Planning Department, Fourth Financial Sector, NTT DATA Corporation
	Toshiya Cho	Senior Vice president, Financial Innovation Center, Business Planning Unit, Hitachi, Ltd., Financial Information Systems Sales Management Division
	Daichi Iwata	Senior Manager, FinTech Business Development Office, Corporate Business Developent Division, NEC Corporation
	Akihiro Umegai	AWS Security Assurance, AWS Security Assurance Lead - Japan/APAC, Amazon Web Services Japan K.K.
	Kappei Uchida	General Manager, Financial Industry, Cloud & Solution Business Division, Microsoft Japan Co., Ltd. (through second meeting)
	Kunihisa Hirahara	Senior Industry Marketing Development Manager, Financial Service Industry, Industry Sales Group 1, Microsoft Japan Co., Ltd. (starting with third meeting)
	Yasuyuki Ogyu	Director, Deloitte Tohmatsu Consulting LLC
Observers	Junichi Kanda	Director, Credit System Office, Planning and Coordination Bureau, Financial Services Agency
	Sayuri Katayose	Head of Information Technology Monitoring team, Inspection Coordination Division,Inspection Bureau, Financial Services Agency
	Daisuke Nakai	Director, Deputy Head of Computer System Risk and Business Continuity Group, Examination Planning Division, Financial System and Bank Examination Department, Bank of Japan
	Akihiko Morota	Director, Cybersecurity Division, List of officials of Commerce and Information Policy Bureau, Ministry of Economy, Trade and Industry
	Kazuaki Omori	Counselor for Cybersecurity Strategy, Global ICT Strategy Bureau, Ministry of Internal Affairs and Communications

(Secretariat of the Center for Financial Industry Information Systems)

President		Tatsuo Watanabe
Executive Director		Norikazu Takahashi
Planning Div.	General Manager	Jutaro Kobayashi
Planning Div.	Deputy General Manager	Akira Fujinaga
Planning Div.	Lead Researcher	Hideki Osawa (starting with second meeting)
Research Div.	General Manager	Yasushi Nakayama
Security&Audit/ Research Div.	General Manager	Toshinobu Nishimura (through fourth meeting)
Security&Audit/ Research Div.	General Manager	Masaaki Wada (starting with fifth meeting)
General Affairs Div.	General Manager	Kouichiro Mizuno
General Affairs Div.	Special Managing Researcher	Makoto Koriyama

◆ Secretariat staff

Akihiro Shibata, Fuminori Nakahodo (through fourth meeting), Kazuma Okamoto (through first meeting), Satoshi Miura, Tian Hao

Reference: Council schedule

First meeting: October 5, 2016; second meeting: December 1, 2016; third meeting: February 2, 2017; fourth meeting: March 23, 2017; fifth meeting: May 15, 2017; sixth meeting: June 13, 2017

VII. References

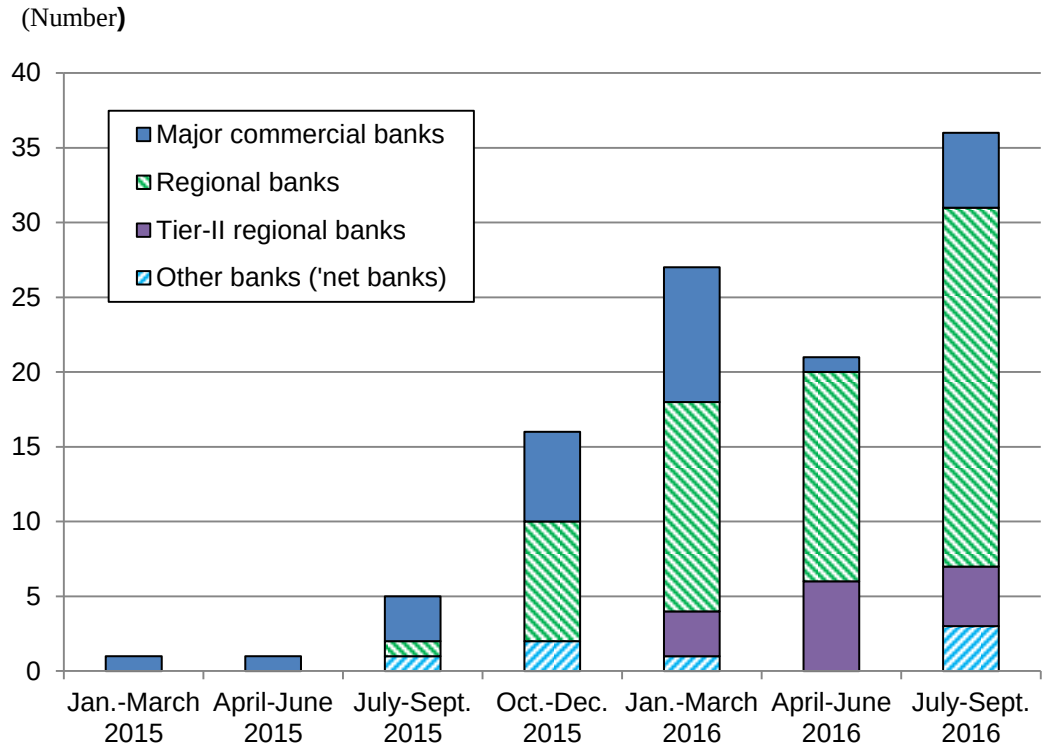
Reference 1. FinTech-related trends among Banking and Related Financial Institutions

1. Trends among domestic Financial Institutions

Since 2015, domestic Financial Institutions, centered on major commercial banks and regional banks, have issued increasing numbers of press releases in which "FinTech" appears as a keyword. Their main content is outlined below.

January 2015:	Major commercial bank holds FinTech competition
July 2015:	Increasing number of press releases from regional banks (e.g., establishment of sections to promote FinTech)
January 2016:	Major commercial banks and regional banks begin feasibility studies on new technologies
	Regional bank enters into an alliance with a FinTech firm
July 2016:	Major commercial bank begins feasibility study on domestic remittances using block chain technology

Numbers of press releases from domestic Financial Institutions concerning FinTech



Source: Prepared by FISC based on press releases from Financial Institutions

2. Sample definitions of FinTech from regulators and others

Japan Revitalization Strategy 2016 (June 2, 2016 Cabinet decision)
In recent years, progress has been made toward fusing finance and IT, under the name FinTech, and this is bringing about transformations in the financial business and markets.
Financial System Council, "Report of the Working Group on Advances in Settlement Operations etc." (December 22, 2015)
FinTech is a word made by combining finance with technology. It refers mainly to innovative financial services using IT. In particular, there have been active moves toward provision of financial services not provided by traditional banks by IT startups using IT technology, chiefly overseas.
Ministry of Economy, Trade and Industry, "About the Industry/Finance/IT Research Group (FinTech Research Group)" First Release (October 6, 2015)
Recent years have seen the appearance of startup ventures providing innovative financial services using IT, known as FinTech, and around the world a movement is apparent toward companies from businesses other than traditional financial businesses, such as retailers, offering new financial services.
Bank of Japan, "Settlement Systems Report" (March 2016)
FinTech is a word formed by combining finance with technology. It has rapidly started to attract attention in recent years. While the definition of FinTech is not necessarily clear, and in many cases its meaning may vary among speakers, in general it often refers to new types of financial services incorporating new technologies such as information and communication technologies, or to the movement toward proactively providing such financial services.

3. Trends among Japanese regulators and others

(1) Amendments to the Banking Act etc.

The Banking Act and other laws were amended in May 2016, making it possible for Financial Institutions (or financial groups) to invest in "companies operating in businesses that contribute, or are expected to contribute, to advancing the banking business or increasing convenience to users" as subsidiaries, subject to individual approval by regulators. As a result, cases of Financial Institutions (or financial groups) making FinTech firms into subsidiaries in participating in FinTech businesses are expected to appear in the future.

(2) The report of the Financial System Working Group and amendments to the Banking Act etc.

The Financial System Council's Financial System Working Group began meeting on July 28, 2016 to discuss the ideal forms of regulations targeting intermediaries. It issued a report on its deliberations on December 27, 2016. That report included recommendations for a systemic framework for business handling e-commerce settlement and other activities, to encourage open innovation. Based on this report and other factors, an act on partial amendment of the Banking Act and other acts was promulgated on March 6, 2017 and passed on May 26 of the same year.

(3) JBA initiatives

On August 4, 2016 the JBA held the first meetings of its Open API Research Group and its Research Group on Feasibility of Block-chain Technologies and Related Issues to consider matters relate dot promotion of financial innovations through FinTech based on the results of surveys of individual banks. Each of these groups issued a report in March 2017. (FISC also participated in both research groups and the Council.)

The JBA survey included the following comment on FISC: "Guidelines such as FISC Security Guidelines on Computer Systems for Banking and Related Financial Institutions can be expected both to encourage standardization of security measures and to reduce study time and cost requirements, by identifying the security measures and other steps that banks should take."

(4) The Financial System Council's report on advances in settlement operations etc.

The Financial System Council has reported the following matters concerning issues related to information security and other subjects in the interim report of its Study Group on Advances in Settlement Operations etc. (issued April 2015)[68] and its Report of the Working Group on Advances in Settlement Operations etc. (issued December 2015)[69].

[68] http://www.fsa.go.jp/singi/singi_kinyu/tosin/20150428-1.html
[69] http://www.fsa.go.jp/singi/singi_kinyu/tosin/20151222-2.html

Interim report of the Study Group on Advances in Settlement Operations etc.

Chapter 4: Security of Settlement Systems and Information Security;
2. Information Security

(2) Future topics

Through now, information security in banking has been addressed basically through reducing the risk of intrusions by limiting external connections mainly to parties within the financial industry and having service providers bear responsibility for damages in the event of a problem.

On the other hand, against a backdrop of developments including advances in IT, settlement interfaces are expanding to outside of banks, as seen in the examples of services such as 'net banking and mobile remittances, and at the same time unbundling is underway in banking services centered on settlement. Under such conditions, increasingly diverse players are becoming involved in settlement information processes.

Under such conditions, there are concerns that the traditional methods of having service providers bear responsibility for information security measures and achieving information security by blocking out external networks might not enable sufficient measures.

In light of these facts, in the future it will be important to implement information security measures compatible with adoption of open networks. For this reason, it is thought that for now there is a need to proceed with consideration of matters such as the following.

- While efforts have been implemented with regard to banks' net banking and similar services such as establishment of supervisory guidelines and FISC Security Guidelines, when diverse players are involved in the settlement information process it is important to improve information security among such diverse players, not just banks alone. From this point of view, measures to establish rules and information security guidelines on which such diverse players can base their measures, and to secure their efficacy, are important.
- To carry out effective information security measures for open networks, it is essential to implement measures under which banks, other diverse players, and users each bear certain responsibilities. For this reason, it is expected that responsibilities and damages in the event of a problem will be divided and, as necessary, certain reasonable rules will be formed.
- To raise the level of security across open networks as a whole, including outside of Financial Institutions, information security measures on the part of users of services as well—not just service providers—are important. From this perspective, it is important to implement measures to promote information security efforts by a broad range of related parties, including increasing user literacy, while also giving consideration to convenience.

Chapter 6: Continual Efforts to Advance Settlement

There is a need to shift toward steady activities to advance settlement operations etc., in accordance with the courses of action discussed above. At the same time, in light of the possibilities of changes and advances in settlement environments and settlement services, there is a need to implement continuous strategic initiatives based on the basic courses of action discussed in this Report.

For this reason, together with following up on the state of progress on efforts toward advancement of settlement, there is a need to identify issues and actions continually and shift toward implementation of these through public-private partnership, while reflecting international trends, the state of innovation related to advancement of settlement, and other considerations. It is expected that the Financial Service Agency will implement efforts toward development of structures for these purposes. Also, in doing so it is important to take care to respond appropriately to the issues of stability of the settlement system and information security.

4. Trends in other developed countries

(1) United States

At the end of March 2016, the U.S. Office of the Comptroller of the Currency (OCC) published and requested opinions on the document *Supporting Responsible Innovation in the Federal Banking System: An OCC Perspective*[70].

Noting that national banks have driven innovation for more than 150 years, this document describes the expectation that they will continue to serve as a source of national strength by demonstrating their advantages in financial innovation, even as FinTech leads to a breakdown of traditional ways of doing business in the banking industry.

- *Innovation has been a hallmark of the national banking system since its founding in 1863 by President Lincoln. That innovative spirit has been especially evident in recent decades as national banks and federal savings associations have led the way in developing and adapting products, services, and technology to meet the changing needs of their customers.*
- *While banks continue to innovate, rapid and dramatic advances in financial technology (fintech) are beginning to disrupt the way traditional banks do business. As the prudential regulator of the federal banking system, we want national banks and federal savings associations to thrive in this environment and to continue fulfilling their vital role of providing financial services to consumers, businesses, and their communities.*

For this purpose, the OCC identifies eight principles for preparing a regulatory framework to support responsible innovation among federally authorized Financial Institutions.

1. *Support responsible innovation.*
2. *Foster an internal culture receptive to responsible innovation.*
3. *Leverage agency experience and expertise.*
4. *Encourage responsible innovation that provides fair access to financial services and fair treatment of consumers.*
5. *Further safe and sound operations through effective risk management.*
6. *Encourage banks of all sizes to integrate responsible innovation into their strategic planning.*
7. *Promote ongoing dialogue through formal outreach.*
8. *Collaborate with other regulators.*

It also recommends a relationship of mutual collaboration between national banks and FinTech firms, utilizing the advantages of each.

- *By employing their respective advantages, banks and nonbank innovators can benefit from collaboration. Through strategic and prudent collaboration, banks can gain access to new technologies, and nonbank innovators can gain access to funding sources and large customer bases.*

Furthermore, effective risk management is identified as a necessary condition.

[70] https://www.occ.treas.gov/news-issuances/news-releases/2016/nr-occ-2016-39.html

- *Innovation is not free from risk, but when managed appropriately, risk should not impede progress. Indeed, effective risk management is essential to responsible innovation. Banks and regulators must strike the right balance between risk and innovation.*
- *As we learned in the financial crisis, not all innovation is positive. . . . The OCC will support innovation that is consistent with safety and soundness, compliant with applicable laws and regulations, and protective of consumers' rights.*

Later, in December 2016, the OCC announced a proposal to grant special-purpose national bank licenses to some FinTech firms[71].

(2) United Kingdom

The British Financial Conduct Authority (FCA) launched Project Innovate in October 2014, intended to promote more effective competition in financial services through fostering autonomous innovation. As part of these efforts, implementation plans for a "regulatory sandbox" under which innovative ideas can be tested with real-world users were released in December 2015.

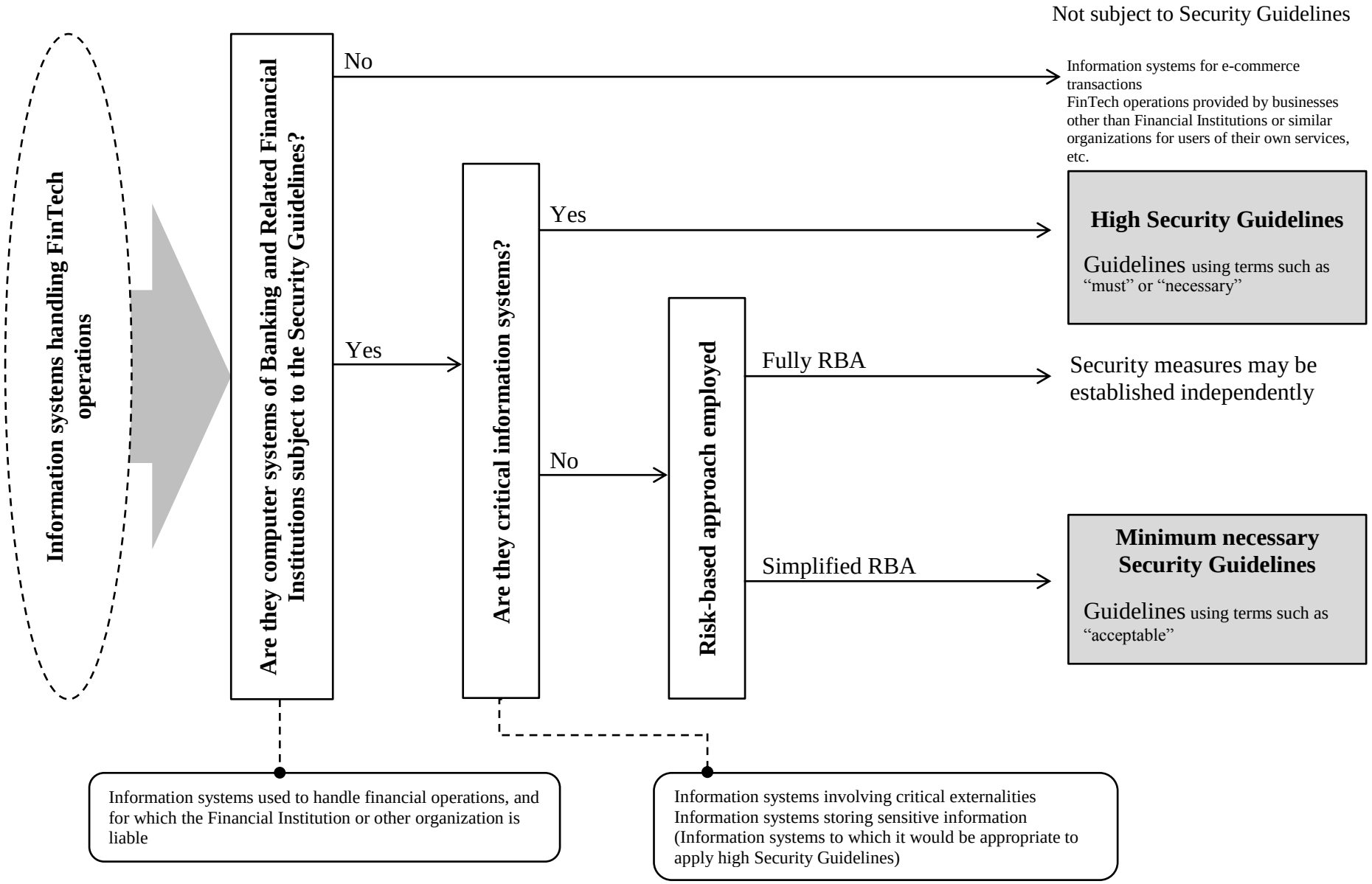
At the same time, as requested by Her Majesty's Treasury an Open Banking Working Group was established in September 2015, beginning studies toward promotion of open standards for APIs used in Britain's banking industry. As a result of such studies, on February 8, 2016 the Open Banking Standard[72] was announced. This report includes a detailed framework for promoting the Open Banking Standard in the U.K., intended to enable the nation to secure a position of international leadership in this field and remain an economic and industrial powerhouse in the new century.

- *Leadership in this area will set UK banking apart. It will also set precedents across many sectors: a strong data infrastructure will be as important to the UK's economy today as roads have been to our success in the industrial economy for over a century.*

(Underlining added by FISC.)

[71] https://www.occ.treas.gov/news-issuances/news-releases/2016/nr-occ-2016-152.html
[72] https://theodi.org/open-banking-standard

Reference 2. Procedures for application of the Security Guidelines

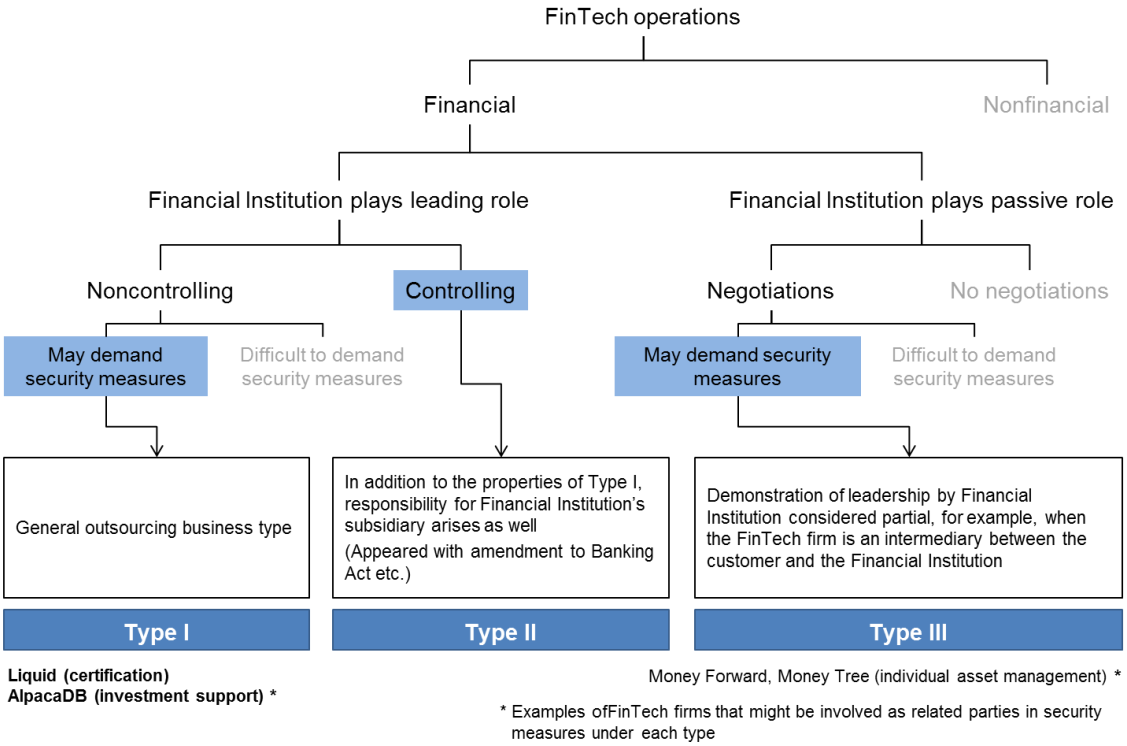


Reference 3. Thinking on types of FinTech operations

1. Types of FinTech operations subject to consideration

Based on the guidelines for determining information systems subject to the Security Guidelines and the business forms in which Financial Institutions would not necessarily occupy positions of leadership, the FinTech operations subject to consideration by the Council can be grouped into the following three types.

Types of FinTech operations that should be subject to the Security Guidelines



Type I corresponds to the basic type in which outsourcing is addressed under the existing Security Guidelines. Type II is a type used in consideration of responsibilities under security measures when Financial Institutions make FinTech firms subsidiaries under the above May 2016 amendments to the Banking Act and other acts, since responsibilities for subsidiaries arise in addition to those under security measures[73]. Type III is a type in which, unlike under Type I and Type II, Financial Institutions' responsibilities under security measures is partial.

2. Basic patterns of related parties when implementing security measures in FinTech operations

In looking at the tripartite relationship in FinTech operations, it would be beneficial to refer to the thinking on the basic pattern of a bipartite relationship. In a bipartite relationship, one party may consist of a single or multiple businesses. The singular case is one pattern. The

[73] In the amendments to the Banking Act and other acts in May 2016, the functions that should be performed by a holding company were clarified in order to enhance business administration in financial groups. Also, Shinsaku Iwahara, Group Governance in Financial Holding Companies: Interactions between the Banking Act and the Companies Act (3) notes, "Many financial holding companies . . . have concluded business administration contracts with subsidiaries calling for them to provide advice and guidance on business administration."

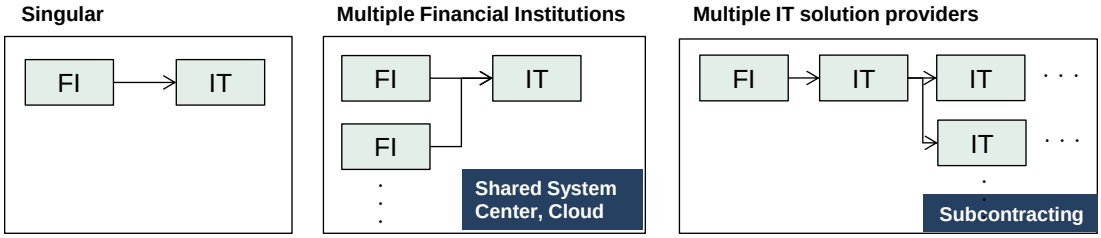
multiple cases may involve either multiple Financial Institutions or multiple IT solution providers.

In the former case, subject patterns in which distinctive properties are considered to arise in security measures are those of shared system centers and cloud services. The former makes it possible to improve the efficiency of security measures and other resources, with the results enjoyed by multiple Financial Institutions (joint nature), while the issue remains of some uncertainty with regard to whether or not the same degree of swift and smooth decision-making can be achieved as in the case of a single Financial Institution (issue of timeliness). While the latter does have a joint nature and does not require mutual agreement among the outsourcers since they are independent of each other (anonymity), it requires specific care under security measures with regard to control methods such as ascertaining where data are stored.

In the latter case, if there are multiple outsourcees of Financial Institutions then controls are feasible directly. For this reason, no distinctive properties arise, and there is no difference from the singular case. If there are multiple stages of indirect outsourcees due to subcontracting, then it would be more difficult for Financial Institutions to implement controls on subcontractors, and for this reason such a pattern will involve some distinctive properties. (See the Report of the Council of Experts on Outsourcing in Financial Institutions for more details.)

The above points are summarized below.

Basic types of bipartite relationships



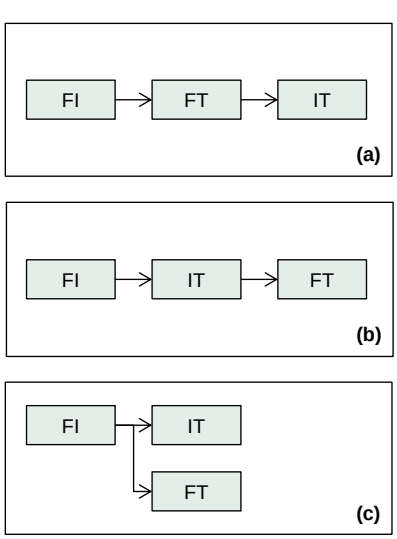
FI: Financial Institution; FT: FinTech firm; IT: IT solution provider (including Cloud solution provider) →: Outsourcing responsibility

In light of the above, types are considered with regard to a tripartite relationship. However, there is no need to consider patterns for bipartite relationships among the three parties. This is because naturally information systems are required when Financial Institutions implement FinTech operations with FinTech firms, and it is considered common practice that Financial Institutions and FinTech firms would provide external resources for development and operation of the information systems needed for this purpose. That is, they would outsource these to IT solution providers. (Particularly with regard to FinTech firms that have only just begun operations, it is said to be common practice to entrust such resources to Cloud service providers among IT solution providers[74].)

[74] According to the Bank of Japan's supplement to its Financial System Report, "New possibilities of financial services arising form IT advances, and cybersecurity" (March 2016), one point on which FinTech differs from the financial services provided by Financial Institutions through now is the fact that "proactive use of external resources and services such as cloud services and open-source software shortens preparatory periods and serves as a strength enabling dynamic service provision." In addition, the FISC Cloud Council Report notes that the Cloud offers benefits including scalability and flexibility suited to a small start, the speed of adoption of new technology, and a high affinity to mobile devices and social medial resulting in increased convenience and functionality.

Accordingly, it can be considered sufficient to consider singular and multiple relations among the three partiers of Financial Institutions, FinTech firms, and IT solution providers[75]. First of all, if any one of the three parties is singular, then since the Financial Institutions always will be the outsourcers, it would seem appropriate to consider the following three types in accordance with the combinations of the other two parties.

Conceivable types when the three parties are singular



Examples

FI provides to its customers, as its own service, a service that the FT subcontracts to the IT, etc.

FI adds to some financial services for its customers provided using the IT a new service from the FT, etc.

FI receives software and services from the FT, operated by an IT chosen by the FI, etc.

FI: Financial Institution; FT: FinTech firm; IT: IT solution provider (including Cloud solution providers) →: Outsourcing responsibility

The next subject to be addressed is whether or not there is a basic pattern that should be employed when any of the three parties under the above patterns consist of more than one business. First of all, if there are multiple IT solution providers then under the assumption that the thinking of the basic bipartite relationship will be employed there would seem to be no need to envision a new pattern. That is, if there are multiple IT solution providers, who serve as outsourcees to Financial Institutions, then no unique properties would arise because Financial Institutions can implement controls directly. On the other hand, with regard to a case of subcontracting to multiple IT solution providers through IT solution providers or FinTech firms, since the Outsourcing Council already has completed comprehensive consideration of types that have their own distinctive properties, there would seem to be no need for individual consideration in the Council.

Next, if there are multiple FinTech firms involved, then since it is conceivable based on a focus on the business properties of FinTech firms that Financial Institutions or solution providers could decide on individual business roles for multiple FinTech firms, no distinctive properties such as a joint nature will arise. Also, when focusing on the technical properties of FinTech firms, no difference arises when there are multiple IT solution providers. Accordingly, even if there are multiple FinTech firms there would seem to be no need for individual consideration.

[75] If the business and technical properties of a FinTech firm can be separated, then theoretically it should be possible to break down into the bipartite relationship. However, since the internal conditions of FinTech firms are diverse it is thought to be difficult to separate these properties clearly.

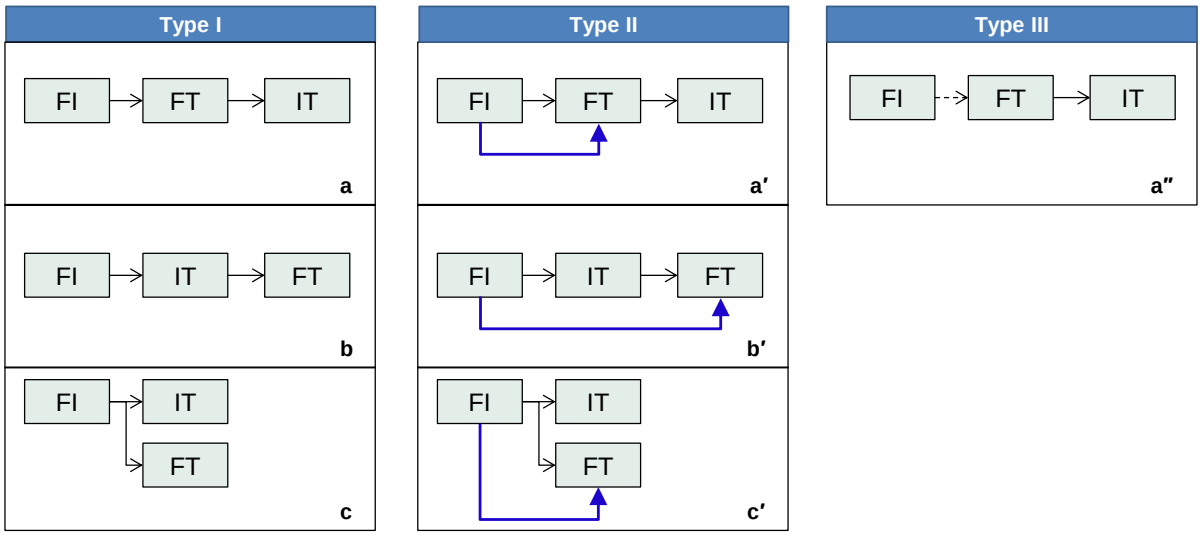
Lastly, when multiple Financial Institutions are involved, it would appear that no distinctive properties would apply other than the joint nature already sorted out through the thinking on the basic patterns in a bipartite relationship.

For the above reasons, no separate consideration is thought to be necessary when any of the three parties consists of multiple businesses.

3. Patterns of FinTech operations by type

The patterns of FinTech operations by type on which this consideration should be based are presented below as a summary of the above points.

Patterns of FinTech operations by type of related party implementing security measures



FI: Financial Institution; FT: FinTech firm; IT: IT solution provider (including Cloud solution provider)
→: Full responsibility for security measures ⇢: Partial responsibility for security measures
➔: Responsibility for subsidiaries

Reference 4. Overview of existing Security Guidelines (related to outsourcing)

Management phase	No.	Theme	Strength of controls	Security Guidelines section no. etc.	Duties of Financial Institutions when using outsourcing (Duties A) (Note 1)	Duties borne as Financial Institutions' primary outsourcees (Duties B-1)	Duties borne by Financial Institutions subcontractors (Duties B-2)	Duties borne as Financial Institutions' subcontractors (Duties C)
a. When considering use	1	Clarification of purpose and scope of outsourcing	Required	Operation 87 1. 2.	When using outsourcing, the objectives, scope, etc. must be made clear in advance.	-	-	-
			Required	Operation 108 1. 2.				
	2	Clarification of selection procedures	Required	Operation 87-1 1.	When selecting outsourcees, the selection procedures must be made clear. (This includes establishing in advance the conditions for selection of subcontractors.)	-	-	-
			Required	Operation 108 1.				
			Required	Outsourcing Council of Experts IV.4.(1)				
	3	Objective evaluation	Required	Operation 87-1 2.	Outsourcees must be evaluated objectively. Only outsourcees capable of realizing the outsourced operations may be selected, based on consideration of the required risk-management levels. In doing so, it is required that evaluation be conducted based on evaluating matters such as the properties and business execution capabilities of the outsourcees and the states of their internal controls and risk management.	There is a duty to provide to Financial Institutions the information needed for Financial Institutions to implement objective evaluation.	There is a duty to evaluate Financial Institutions' subcontractors objectively.	There is a duty to provide to primary outsourcees the information needed for primary outsourcees to implement objective evaluation.
			Required	Operation 108 3.				
	4	Prior conclusion of NDA	recommended	Operation 108 3.	In conducting such evaluation, it is recommended to conclude a nondisclosure agreement in advance as needed.	-	-	-
	5	(If the outsourced operations are not of high importance) Objective evaluation based on disclosed information, judgments, performance, etc.	Acceptable	Operation 108 3.	When there is a possibility that the outsourced operations might be judged to be not of high importance based on sufficient consideration of their properties in Banking and Related Financial Institutions, it must be possible to make objective evaluations based on matters such as public information and industry evaluations and business performance.	-	When it has been determined that the outsourced operations are not of high importance to Banking and Related Financial Institutions, it must be possible to make objective evaluations based on matters such as public information and industry evaluations and business performance of Financial Institutions' subcontractors.	-
	6	Prior ascertaining of migration tasks for contract suspension or termination	recommended	Operation 108 3.(11)	It is recommended to ascertain system migration work involved in suspension or termination of the outsourcing contract (methods of extracting data to be migrated and content of actual migration work) prior to starting to use a service.	-	-	-

Management phase	No.	Theme	Strength of controls	Security Guidelines section no. etc.	Duties of Financial Institutions when using outsourcing (Duties A) (Note 1)	Duties borne as Financial Institutions' primary outsourcees (Duties B-1)	Duties borne by Financial Institutions' subcontractors (Duties B-2)	Duties borne as Financial Institutions' subcontractors (Duties C)
a. When considering use	7	Ascertaining locations of data	Required	Operation 108 4.	When processing operations that require a high degree of availability or processing, collecting, or storing highly confidential customer information, it is required to ascertain the region (country, state, etc.) in which the cloud service is located, to an extent that makes it possible to identify what laws and regulations apply.	When processing operations that require a high degree of availability or processing, collecting, or storing highly confidential customer information, there is a duty to provide to Financial Institutions information on the region (country, state, etc.) in which the cloud service is located, to an extent that makes it possible to identify what laws and regulations apply.	When processing operations that require a high degree of availability or processing, collecting, or storing highly confidential customer information, there is a duty to ascertain the region (country, state, etc.) in which the cloud service is located, to an extent that makes it possible to identify what laws and regulations apply.	When processing operations that require a high degree of availability or processing, collecting, or storing highly confidential customer information, there is a duty to provide to primary outsourcees information on the region (country, state, etc.) in which the cloud service is located, to an extent that makes it possible to identify what laws and regulations apply.
			Required	Operation 108 4.	For systems that require extremely high levels of availability or reliability, such as accounting backbone systems, it is required to ascertain detailed location information in order to ascertain the conditions of data-center locations and other matters.	For systems that require extremely high levels of availability or reliability, such as accounting backbone systems, there is a duty to provide to Banking and Related Financial Institutions detailed location information so that they can ascertain the conditions of data-center locations and other matters.	For systems that require extremely high levels of availability or reliability, such as accounting backbone systems, there is a duty to ascertain detailed location information in order to ascertain the conditions of data-center locations and other matters.	For systems that require extremely high levels of availability or reliability, such as accounting backbone systems, there is a duty to provide to primary outsourcees detailed location information so that they can ascertain the conditions of data-center locations and other matters.
			Required	Operation 108 4.	It is required to ascertain specific locations in cases such as when admission to a data center is needed in response to an incident or when conducting an on-site audit.	There is a duty to provide to Financial Institutions specific location information in cases such as when they require entry to a data-center in response to an incident or when conducting an on-site audit.	There is a duty to ascertain specific locations in cases such as when entry to a data-center is needed in response to an incident or when conducting an on-site audit.	There is a duty to provide to primary outsourcees specific location information in cases such as when they require entry to a data-center in response to an incident or when conducting an on-site audit.
		(If the outsourced operations are not of high importance) Requirement to ascertain locations of data	Acceptable	Operation 108 4.	When Banking and Related Financial Institutions may determine, based on sufficient consideration of the properties of the operations, that the outsourced operations are not of high importance, it is acceptable to omit the ascertaining of information on the locations of data.	-	When Banking and Related Financial Institutions may determine, based on sufficient consideration of the properties of the operations, that the outsourced operations are not of high importance, it is acceptable to omit the ascertaining of information on the locations of data.	-
	8	Risks to be evaluated in anticipation of possible disputes overseas	Required	Operation 108 5.	If the applicable law for disputes with outsourcees is foreign law or the court with jurisdiction is a foreign court, risk evaluation must be conducted when selecting outsourcees.	-	-	-

Management phase	No.	Theme	Strength of controls	Security Guidelines section no. etc.	Duties of Financial Institutions when using outsourcing (Duties A) (Note 1)	Duties borne as Financial Institutions' primary outsourcees (Duties B-1)	Duties borne by Financial Institutions' subcontractors (Duties B-2)	Duties borne as Financial Institutions' subcontractors (Duties C)
a. When considering use	9	Approval by person responsible of selection of service provider	Required	Operation 87-13.	The approval of the responsible person must be obtained ultimately for decisions on outsourcees.	-	-	-
			Required	Operation 1086.				
	10	(When adopting software packages) Development of an evaluation structure and clarification of the operation and management structures	Required	Operation 87-14.	Refer to Operations 72, Operations 73 concerning adoption of applications, services, etc. owned by outsourcees.	When adopting software packages, there is a duty to provide to Financial Institutions the information needed for their evaluation of the packages and similar tasks.	When adopting software packages, there is a duty to establish structures for evaluation of matters such as the efficacy, reliability, and productivity of the packages. There also is a duty to make clear the structures for package operation and management.	When adopting software packages, there is a duty to provide to primary outsourcees the information needed for their evaluation of the packages and similar tasks.
			Recommended	Operation 1087.	Refer to Operations 72, Operations 73 as necessary when adopting software packages.			
b. When concluding the contract	11	Concluding contracts including security measures	Required	Operation 881.	To ensure that outsourced operations are performed securely, contracts must be concluded with outsourcees concerning nondisclosure, secure operation, etc.	To ensure that operations outsourced by Financial Institutions are performed securely, there is a duty to conclude contracts with Financial Institutions concerning nondisclosure, secure operation, etc.	To ensure that outsourced operations are performed securely, there is a duty to conclude contracts with Financial Institutions' subcontractors concerning nondisclosure, secure operation, etc.	To ensure that operations outsourced by primary outsourcees are performed securely, there is a duty to conclude contracts with primary outsourcees concerning nondisclosure, secure operation, etc.
			Required	Operation 1091.				
	12	Disclosure of information from businesses	Required (Note 2)	Operation 1091.(9)	It must be stated clearly in the contract that Cloud service providers shall provide the necessary information based on consultation between Financial Institutions and Cloud service providers.	There is a duty to state clearly in the contract with Financial Institutions provisions regarding provision of the information needed by Financial Institutions.	There is a duty to state clearly in the contract that Financial Institutions' subcontractors shall provide the necessary information based on consultation with Financial Institutions' subcontractors.	There is a duty to state clearly in the contract with primary outsourcees provisions regarding provision of the information needed by primary outsourcees.
			Required (Note 2)	Operation 1091.(9)	If the information subject to a request for disclosure is of a highly confidential nature, it must be provided after first concluding a nondisclosure agreement between both parties.	If the information subject to a request for disclosure is of a highly confidential nature, there is a duty to provide it only after first concluding a nondisclosure agreement between both parties (Financial Institutions and primary outsourcees).	If the information subject to a request for disclosure is of a highly confidential nature, there is a duty to provide it only after first concluding a nondisclosure agreement between both parties (primary outsourcees and Financial Institutions' subcontractors).	If the information subject to a request for disclosure is of a highly confidential nature, there is a duty to provide it only after first concluding a nondisclosure agreement between both parties (primary outsourcees and Financial Institutions' subcontractors).

Management phase	No.	Theme	Strength of controls	Security Guidelines section no. etc.	Duties of Financial Institutions when using outsourcing (Duties A) (Note 1)	Duties borne as Financial Institutions' primary outsourcees (Duties B-1)	Duties borne by Financial Institutions' subcontractors (Duties B-2)	Duties borne as Financial Institutions' subcontractors (Duties C)
b. When concluding the contract	12	Disclosure of information from businesses	Required (Note 2)	Operation 109 1.(9)	It must be stated in the contract or SLA that in the event that a risk event has occurred, or when it has been determined for example that the risk of information leakage through various documents has increased or that the state of internal controls by the Cloud service provider has worsened, then notwithstanding the standard assumptions of information disclosure in normal times when a request for disclosure has been received from the Financial Institution the subject information must be disclosed.	There is a duty to state in the contract or SLA with the Financial Institution that in the event that a risk event has occurred, or when it has been determined for example that the risk of information leakage through various documents has increased or that the state of internal controls by the Financial Institutions' subcontractors has worsened, then notwithstanding the standard assumptions of information disclosure in normal times when a request for disclosure has been received from the Financial Institution the subject information must be disclosed.	There is a duty to state in the contract or SLA with the Financial Institutions' subcontractors that in the event that a risk event has occurred, or when it has been determined for example that the risk of information leakage through various documents has increased or that the state of internal controls by the Financial Institutions' subcontractors has worsened, then notwithstanding the standard assumptions of information disclosure in normal times when a request for disclosure has been received from the Financial Institutions' subcontractors the subject information must be disclosed.	There is a duty to state in the contract or SLA with the primary outsourcees that in the event that a risk event has occurred, or when it has been determined for example that the risk of information leakage through various documents has increased or that the state of internal controls by the Financial Institutions' subcontractors has worsened, then notwithstanding the standard assumptions of information disclosure in normal times when a request for disclosure has been received from the primary outsourcees the subject information must be disclosed.
		(If the outsourced operations are not of high importance) Detailed and strict disclosure of information from businesses	Acceptable	Operation 109 1.(9)	When Banking and Related Financial Institutions have determined, through sufficient consideration of the priorities of the operations, that the outsourced operations are not of high importance, it is acceptable not to issue detailed and strict demands to outsourcees for information such as matters directly related to risk management.	-	WhenBanking and Related Financial Institutions have determined that the outsourced operations are not of high importance, it is acceptable not to issue detailed and strict demands to Financial Institutions' subcontractors for information such as matters directly related to risk management.	-
	13	(When outsourcing to multiple businesses) Prior decision on a business to coordinate among multiple businesses	Required (Note 2)	Operation 109 1.(10)	To ensure swift responses in cases such as failures, the relationships of responsibility between outsourcer Financial Institutions and outsourcees must be made clear, based on the management capabilities of the outsourcer Financial Institutions, and businesses serving as centralized contact points and in coordinating roles among outsourcees must be decided on in advance. If the outsourcer Financial Institutions can fulfill this role, appointing a business to handle coordination on the outsourcees' side is not required.	-	-	-
		(If the outsourced operations are not of high importance) Requirement to decide on a business to coordinate among multiple businesses	Acceptable	Operation 109 1.(10)	When, based on sufficient consideration of the properties of the business,Banking and Related Financial Institutions may determine that the outsourced operations are not of high importance, and results of risk analysis show that the scope of the impact of a failure would be limited or that the impact can be mitigated even if recovery is delayed, it is acceptable not to appoint a business to handle the coordination role.	-	-	-

Management phase	No.	Theme	Strength of controls	Security Guidelines section no. etc.	Duties of Financial Institutions when using outsourcing (Duties A) (Note 1)	Duties borne as Financial Institutions' primary outsourcees (Duties B-1)	Duties borne by Financial Institutions' subcontractors (Duties B-2)	Duties borne as Financial Institutions' subcontractors (Duties C)
b. When concluding the contract	14	Clear statement of authority to audit outsourcees	Required	Operation 88 4.(15)	It is required to conclude a contract with consideration for the right to audit security measures in accordance with the type and scope of outsourced operations (e.g., the right to audit outsourcees or the right to have outside specialized agencies conduct auditing).	There is a duty to conclude a contract with Financial Institutions with consideration for the right to audit security measures in accordance with the type and scope of operations outsourced by Financial Institutions (e.g., the right to audit outsourcees or the right to have outside specialized agencies conduct auditing).	There is a duty to conclude a contract with Financial Institutions' subcontractors with consideration for the right to audit security measures in accordance with the type and scope of outsourced operations (e.g., the right to audit Financial Institutions' subcontractors or the right to have outside specialized agencies conduct auditing).	There is a duty to conclude a contract with primary outsourcees with consideration for the right to audit security measures in accordance with the type and scope of operations outsourced by primary outsourcees (e.g., the right to audit outsourcees or the right to have outside specialized agencies conduct auditing).
			Required	Outsourcing Council of Experts IV 4.(2)	When concluding an outsourcing contract with the outsourcee in outsourcing of critical information systems, the authority of Banking and Related Financial Institutions to audit subcontractors must be stated clearly, to ensure a system for checking on subcontractors.	When concluding an outsourcing contract with Financial Institutions in acceptance of outsourcing of critical information systems, the authority of Banking and Related Financial Institutions to audit subcontractors must be stated clearly, to ensure a system for checking on Financial Institutions' subcontractors.	When concluding an outsourcing contract with Financial Institutions' subcontractors in outsourcing of critical information systems to Financial Institutions' subcontractors, the authority of Banking and Related Financial Institutions to audit subcontractors must be stated clearly, to ensure a system for checking on Financial Institutions' subcontractors.	When concluding an outsourcing contract with primary outsourcees in acceptance of outsourcing of critical information systems, the authority of Banking and Related Financial Institutions to audit subcontractors must be stated clearly, to ensure a system for checking on Financial Institutions' subcontractors.
			Acceptable	Outsourcing Council of Experts IV 4.(2)	It is possible to entrust auditing to an appropriate auditor instead of conducting it oneself.	-	It is possible to entrust auditing to an appropriate auditor instead of conducting it oneself.	-
			Acceptable	Outsourcing Council of Experts IV 4.(2)	When outsourcing information systems other than critical information systems, it is acceptable not to state clearly the auditing authority of Banking and Related Financial Institutions vis-a-vis subcontractors when concluding a contract with an outsourcee.	-	When Financial Institutions outsource information systems other than critical information systems and do not state clearly their auditing authority vis-a-vis Financial Institutions' subcontractors, it is acceptable not to state clearly the auditing authority of Banking and Related Financial Institutions vis-a-vis subcontractors when concluding a contract with a Financial Institutions' subcontractor.	-

Management phase	No.	Theme	Strength of controls	Security Guidelines section no. etc.	Duties of Financial Institutions when using outsourcing (Duties A) (Note 1)	Duties borne as Financial Institutions' primary outsourcees (Duties B-1)	Duties borne by Financial Institutions' subcontractors (Duties B-2)	Duties borne as Financial Institutions' subcontractors (Duties C)
b. When concluding the contract	14	Clear statement of authority to audit outsourcees	Acceptable	Outsourcing Council of Experts IV 4.(2)	Even when outsourcing critical information systems, the above simplified procedures may be used if the outsourced operations are subdivided among subcontractors and the relevant subcontracted operations can be determined to involve sufficiently low risk levels.	-	When Financial Institutions outsource critical information systems and employ simplified procedures because subcontracted operations have been determined to involve sufficiently low risk levels, the above simplified procedures may be used if the relevant subcontracted operations can be determined to involve sufficiently low risk levels.	-
	15	Clear statement of right to conduct on-site auditing etc.	Required (Note 2)	Operation 109 1.(12)	The outsourcing contract must state clearly the right of outsourcer Banking and Related Financial Institutions to conduct on-site auditing and similar activities.	There is a duty to state clearly in outsourcing contracts with Financial Institutions that Banking and Related Financial Institutions have the right to conduct on-site auditing and similar activities.	There is a duty to state clearly in outsourcing contracts with Financial Institutions' subcontractors that primary outsourcees have the right to conduct on-site auditing and similar activities vis-a-vis subcontractors.	There is a duty to state clearly in outsourcing contracts with primary outsourcees the right to conduct on-site auditing and similar activities vis-a-vis primary outsourcees and others.
	16	Clear statement of substitute measures instead of on-site auditing etc.	Required (Note 2)	Operation 109 1.(12)	Instead of conducting direct on-site inspections, client Financial Institutions may substitute verification by independent third parties who possess the skills for on-site inspections and other tasks during normal times.	Instead of conducting direct on-site inspections, Banking and Related Financial Institutions may substitute verification by independent third parties who possess the skills for on-site inspections and other tasks during normal times.	There is a duty to enable primary outsourcees to substitute verification by independent third parties who possess the skills for on-site inspections and other tasks during normal times for direct on-site inspections of Financial Institutions' subcontractors.	Instead of conducting direct on-site inspections, primary outsourcees and others may substitute verification by independent third parties who possess the skills for on-site inspections and other tasks during normal times.
	17	Clear statement of right to conduct on-site auditing etc.	Required (Note 2)	Operation 109 1.(12)	In cases such as when a serious vulnerability related to Cloud technologies has been identified, when an incident has arisen in another customer-related domain at the Cloud service provider, or when an incident has arisen at another business, it must be possible to conduct extraordinary third-party audits to confirm the impact on client Financial Institutions.	There is a duty to enable extraordinary third-party audits to confirm the impact on Banking and Related Financial Institutions in cases such as when a serious vulnerability related to Cloud technologies has been identified, when an incident has arisen in another customer-related domain at the Financial Institutions' subcontractor, or when an incident has arisen at another business.	There is a duty to enable extraordinary third-party audits to confirm the impact on Banking and Related Financial Institutions in cases such as when a serious vulnerability related to Cloud technologies has been identified, when an incident has arisen in another customer-related domain at the Financial Institutions' subcontractor, or when an incident has arisen at another business.	There is a duty to enable extraordinary third-party audits to confirm the impact on primary outsourcees and others in cases such as when a serious vulnerability related to Cloud technologies has been identified, when an incident has arisen in another customer-related domain at the company, or when an incident has arisen at another business.

Management phase	No.	Theme	Strength of controls	Security Guidelines section no. etc.	Duties of Financial Institutions when using outsourcing (Duties A) (Note 1)	Duties borne as Financial Institutions' primary outsourcees (Duties B-1)	Duties borne by Financial Institutions' subcontractors (Duties B-2)	Duties borne as Financial Institutions' subcontractors (Duties C)
b. When concluding the contract	17	(When on-site auditing etc. is limited) Shared understanding of conditions for exercise of right to on-site auditing etc.	Acceptable	Operation 109 1.(12)	Conditions for exercise of the right to conduct on-site auditing and similar activities are documented as necessary and both outsourcer Financial Institutions and Cloud service providers may have a shared understanding of the matter when conducting on-site auditing or similar activities only if it is not possible to use third-party auditing instead of such activities, or if it has been determined that such third-party auditing could not be relied upon.	-	Conditions for exercise of the right to conduct on-site auditing and similar activities are documented as necessary and both primary outsourcees and Financial Institutions' subcontractors may have a shared understanding of the matter when conducting on-site auditing or similar activities only if it is not possible to use third-party auditing instead of such activities, or if it has been determined by the Financial Institutions that such third-party auditing could not be relied upon.	-
	18	Clear statement regarding costs of accepting on-site auditing etc.	Required (Note 2)	Operation 109 1.(12)	Both parties must consult in advance on whether the outsourcer Financial Institutions or Cloud service providers would bear the costs of acceptance by the Cloud service providers of on-site inspections.	There is a duty for both parties to consult in advance on whether the Financial Institutions or primary outsourcees would bear the costs of acceptance by the primary outsourcees of on-site inspections.	There is a duty for both parties to consult in advance on whether the primary outsourcees or Financial Institutions' subcontractors would bear the costs of acceptance by the Financial Institutions' subcontractors of on-site inspections.	There is a duty for both parties to consult in advance on whether the primary outsourcees or Financial Institutions' subcontractors would bear the costs of acceptance by the Financial Institutions' subcontractors of on-site inspections.
	19	Clear statement of authority to audit subcontractors	Required (Note 2)	Operation 109 1.(12)	It must be stated clearly in the contract between the outsourcer Financial Institution and the Cloud service provider that the Financial Institution has the right to conduct on-site auditing of subcontractors when the operations subcontracted are important ones.	There is a duty for the Financial Institution to state clearly in the contract between the Financial Institution and the primary outsourcee that the Financial Institution has the right to conduct on-site auditing of Financial Institutions' subcontractors and other subcontractors when the operations subcontracted are important ones.	There is a duty for the Financial Institution to state clearly in the contract between the primary outsourcee and the Financial Institutions' subcontractors that the Financial Institution has the right to conduct on-site auditing of Financial Institutions' subcontractors and other subcontractors when the operations subcontracted are important ones.	There is a duty for the Financial Institution to state clearly in the contract between the primary outsourcee and the Financial Institutions' subcontractors that the Financial Institution has the right to conduct on-site auditing of Financial Institutions' subcontractors and other subcontractors when the operations subcontracted are important ones.
	20	Clear statement on handing of matters identified in on-site auditing etc.	Required (Note 2)	Operation 109 1.(12)	It must be stated clearly in the contract that for matters identified in on-site auditing and similar activities a reasonable deadline for response, including correction, shall be established through consultation between the outsourcer Financial Institution and the Cloud service provider and responses shall be completed by that deadline.	There is a duty to state clearly in the contract that for matters identified in on-site auditing and similar activities a reasonable deadline for response, including correction, shall be established through consultation between the Financial Institution and the primary outsourcee and responses shall be completed by that deadline.	There is a duty to state clearly in the contract that for matters identified in on-site auditing and similar activities a reasonable deadline for response, including correction, shall be established through consultation between the primary outsourcee and Financial Institutions' subcontractors and responses shall be completed by that deadline.	There is a duty to state clearly in the contract that for matters identified in on-site auditing and similar activities a reasonable deadline for response, including correction, shall be established through consultation between the primary outsourcee and Financial Institutions' subcontractors and responses shall be completed by that deadline.

Management phase	No.	Theme	Strength of controls	Security Guidelines section no. etc.	Duties of Financial Institutions when using outsourcing (Duties A) (Note 1)	Duties borne as Financial Institutions' primary outsourcees (Duties B-1)	Duties borne by Financial Institutions' subcontractors (Duties B-2)	Duties borne as Financial Institutions' subcontractors (Duties C)
b. When concluding the contract	21	Clear statement concerning inspections etc. by financial regulators	Required (Note 2)	Operation 109 1.(13)	To facilitate smooth on-site inspections by regulators and similar activities, outsourcees' duty to cooperate in on-site inspections by regulators and similar activities must be stated clearly in contracts between outsourcer Financial Institutions and outsourcees.	To facilitate smooth on-site inspections by regulators and similar activities, there is a duty to state primary outsourcees' duty to cooperate in on-site inspections by regulators and similar activities in contracts between Financial Institutions and primary outsourcees.	To facilitate smooth on-site inspections by regulators and similar activities, there is a duty to state Financial Institutions' subcontractors' duty to cooperate in on-site inspections by regulators and similar activities in contracts between primary outsourcees and Financial Institutions' subcontractors.	To facilitate smooth on-site inspections by regulators and similar activities, there is a duty to state primary outsourcees' duty to cooperate in on-site inspections by regulators and similar activities in contracts between primary outsourcees and Financial Institutions' subcontractors.
			Required (Note 2)	Operation 109 1.(13)	The duty of subcontractors (including sub-subcontractors) to cooperate in on-site inspections by regulators and similar activities must be stated clearly in contracts between Financial Institutions and lead subcontractors as well.	There is a duty to state clearly the duty of subcontractors (including sub-subcontractors) to cooperate in on-site inspections by regulators and similar activities in contracts between Financial Institutions and primary outsourcees.	There is a duty to state clearly the duty of subcontractors (including sub-subcontractors) to cooperate in on-site inspections by regulators and similar activities in contracts between primary outsourcees and Financial Institutions' subcontractors.	There is a duty to state clearly the duty of subcontractors (including sub-subcontractors) to cooperate in on-site inspections by regulators and similar activities in contracts between primary outsourcees and Financial Institutions' subcontractors.
			Required (Note 2)	Operation 109 1.(13)	Provisions must be stated clearly in the contract regarding prompt rectification of any matters pointed out in inspections by regulators and similar activities.	There is a duty to state clearly provisions regarding prompt rectification of any matters pointed out in inspections by regulators and similar activities in contracts between Financial Institutions and primary outsourcees.	There is a duty to state clearly provisions regarding prompt rectification of any matters pointed out in inspections by regulators and similar activities in contracts between primary outsourcees and Financial Institutions' subcontractors.	There is a duty to state clearly provisions regarding prompt rectification of any matters pointed out in inspections by regulators and similar activities in contracts between primary outsourcees and Financial Institutions' subcontractors.
	22	Clear statement concerning on-site investigation upon an incident	Required (Note 2)	Operation 109 1.(14)	It must state clearly in the contract that if a Financial Institution has determined that the Cloud service provider has failed to submit information or that there are problems with the speed of such provision in a case such as when an incident such as leakage of information has arisen or there are concerns that such an incident has arisen, or if there are doubts about the comprehensiveness of the information submitted, the client Financial Institution itself or a security vendor or data forensics vendor specified by the Financial Institution may conduct an on-site investigation.	There is a duty to state clearly in the contract that if the Financial Institution has determined that the Financial Institutions' subcontractor has failed to submit information or that there are problems with the speed of such provision in a case such as when an incident such as leakage of information has arisen or there are concerns that such an incident has arisen, or if there are doubts about the comprehensiveness of the information submitted, the Financial Institution itself or a security vendor or data forensics vendor specified by the Financial Institution may conduct an on-site investigation.	There is a duty to state clearly in the contract that if the primary outsourcee has determined that the Financial Institutions' subcontractor has failed to submit information or that there are problems with the speed of such provision in a case such as when an incident such as leakage of information has arisen or there are concerns that such an incident has arisen, or if there are doubts about the comprehensiveness of the information submitted, the primary outsourcee itself or a security vendor or data forensics vendor specified by the primary outsourcee may conduct an on-site investigation.	There is a duty to state clearly in the contract that if the primary outsourcee has determined that the Financial Institutions' subcontractor has failed to submit information or that there are problems with the speed of such provision in a case such as when an incident such as leakage of information has arisen or there are concerns that such an incident has arisen, or if there are doubts about the comprehensiveness of the information submitted, the primary outsourcee itself or a security vendor or data forensics vendor specified by the primary outsourcee may conduct an on-site investigation.

Management phase	No.	Theme	Strength of controls	Security Guidelines section no. etc.	Duties of Financial Institutions when using outsourcing (Duties A) (Note 1)	Duties borne as Financial Institutions' primary outsourcees (Duties B-1)	Duties borne by Financial Institutions' subcontractors (Duties B-2)	Duties borne as Financial Institutions' subcontractors (Duties C)
b. When concluding the contract	22	Clear statement concerning on-site investigation upon an incident	Required (Note 2)	Operation 109 1.(14)	Agreement must be reached when concluding the contract on the scope of evidence subject to collection during investigation and the bearing of costs as required for purposes of development of extraction tools and verification.	There is a duty to reach agreement with Financial Institutions when concluding the contract on the scope of evidence subject to collection during investigation and the bearing of costs as required for purposes of development of extraction tools and verification.	There is a duty to reach agreement with Financial Institutions' subcontractors when concluding the contract on the scope of evidence subject to collection during investigation and the bearing of costs as required for purposes of development of extraction tools and verification.	There is a duty to reach agreement with primary outsourcees when concluding the contract on the scope of evidence subject to collection during investigation and the bearing of costs as required for purposes of development of extraction tools and verification.
			Required (Note 2)	Operation 109 1.(14)	The contract must state clearly that when management instability has arisen on the part of a Cloud service provider, then as necessary the client Financial Institution itself or a specialized vendor designated by it is permitted to enter the facilities of the Cloud service provider to preserve customer data and related works or deliverables.	There is a duty to state clearly in the contract that when management instability has arisen on the part of a Financial Institutions' subcontractor, then as necessary it will cooperate in the client Financial Institution itself or a specialized vendor designated by it entering the facilities of the Financial Institutions' subcontractor to preserve customer data and related works or deliverables.	There is a duty to state clearly in the contract that when management instability has arisen on the part of a Financial Institutions' subcontractor, then as necessary the primary outsourcee itself or a specialized vendor designated by it is permitted to enter the facilities of the Financial Institutions' subcontractor to preserve customer data and related works or deliverables.	There is a duty to state clearly in the contract that when management instability has arisen on the part of the company itself, then as necessary it will cooperate in the primary outsourcee itself or a specialized vendor designated by it entering company facilities to preserve customer data and related works or deliverables.
	23	(When storing data overseas) Clear statement concerning Japanese-language support and setting up a failure contact point	Required (Note 2)	Operation 109 1.(16)	It must be stated clearly that if the staff responding to failures at Financial Institutions do not have sufficient local language abilities then support in Japanese or a contact point for responding to failures at a Japanese subsidiary of the outsourcee shall be established.	There is a duty to provide information to Financial Institutions on provision of support in Japanese or establishment of a contact point for responding to failures at a Japanese subsidiary of the primary outsourcee if the staff responding to failures at Financial Institutions do not have sufficient local language abilities.	It must be made clear that support will be provided in Japanese or a contact point established for responding to failures at a Japanese subsidiary of the Financial Institutions' subcontractor if the staff responding to failures at primary outsourcees do not have sufficient local language abilities.	There is a duty to provide information to primary outsourcees on provision of support in Japanese or establishment of a contact point for responding to failures at a Japanese subsidiary of the primary outsourcee if the staff responding to failures at Financial Institutions do not have sufficient local language abilities.
	24	Preparing to secure traceability	Required (Note 2)	Operation 109 1.(17)	Since it is anticipated that in the event of an incident such as a failure or information leakage, tasks conducted to identify leaked or damaged data and identify causes could become increasingly complex, measures must be prepared for securing traceability.	There is a duty to prepare measures for securing traceability as requested by Financial Institutions in the event of an incident such as a failure or information leakage.	There is a duty for Financial Institutions' subcontractors to take measures for securing traceability at them as requested by Financial Institutions in the event of an incident such as a failure or information leakage.	There is a duty to prepare measures for securing traceability as requested by primary outsourcees in the event of an incident such as a failure or information leakage.

Management phase	No.	Theme	Strength of controls	Security Guidelines section no. etc.	Duties of Financial Institutions when using outsourcing (Duties A) (Note 1)	Duties borne as Financial Institutions' primary outsourcees (Duties B-1)	Duties borne by Financial Institutions' subcontractors (Duties B-2)	Duties borne as Financial Institutions' subcontractors (Duties C)
b. When concluding the contract	25	Clear statement concerning prior review of subcontractors	Required (Note 2)	Operation 109 1.(11)	To ascertain the state of outsourcing and eliminate the involvement of inappropriate subcontractors, when subcontracting outsourced operations appropriate prior review of the subcontractors must be conducted. When outsourcing particularly important operations such as those involving accounting systems or systems containing highly confidential customer data, Banking and Related Financial Institutions must conduct the prior review themselves.	So that Financial Institutions can ascertain the state of outsourcing and eliminate the involvement of inappropriate subcontractors, there is a duty for Financial Institutions' subcontractors to respond to appropriate prior review when Financial Institutions subcontract outsourced operations.	So that Financial Institutions can ascertain the state of outsourcing and eliminate the involvement of inappropriate subcontractors, there is a duty for primary outsourcees to conduct appropriate prior review of subcontractors when subcontracting to Financial Institutions' subcontractors.	So that Financial Institutions can ascertain the state of outsourcing and eliminate the involvement of inappropriate subcontractors, there is a duty to respond to appropriate prior review of Financial Institutions' subcontractors conducted by primary outsourcees when Financial Institutions subcontract outsourced operations.
			Required	Outsourcing Council of Experts IV 4.(1)				
		(When outsourcing an information system other than a critical information system) Substitution for prior review of subcontractors	Acceptable	Outsourcing Council of Experts IV 4.(1)	When outsourcing an information system other than a critical information system, if a process of review and management by outsourcees of subcontractors is considered to be at least as effective as that of Banking and Related Financial Institutions, then it is acceptable to replace prior review of individual subcontractors with confirmation of the results of verification of the appropriateness of the state of development and operation of outsourcees' review and management processes by Banking and Related Financial Institutions in advance.	-	-	-
		(If the outsourced operations are not of high importance) Omission of prior review of subcontractors	Acceptable	Operation 109 1.(11)	If Banking and Related Financial Institutions have determined that outsourced operations are not highly important based on sufficient consideration of their properties, then risk-management measures such as prior review and everyday monitoring of subcontractors by client Financial Institutions may be simplified.	-	-	-
	26	SLA	Recommended	Operation 88 5.	It is recommended to reach agreement on service levels through conclusion of an SLA and confirmation of SLO.	There is a duty to reach agreement with Financial Institutions on service levels through conclusion of an SLA and confirmation of SLO.	There is a duty to reach agreement with Financial Institutions' subcontractors on service levels through conclusion of an SLA and confirmation of SLO.	There is a duty to reach agreement with primary outsourcees on service levels through conclusion of an SLA and confirmation of SLO.
			Recommended	Operation 109 2.				

Management phase	No.	Theme	Strength of controls	Security Guidelines section no. etc.	Duties of Financial Institutions when using outsourcing (Duties A) (Note 1)	Duties borne as Financial Institutions' primary outsourcees (Duties B-1)	Duties borne by Financial Institutions' subcontractors (Duties B-2)	Duties borne as Financial Institutions' subcontractors (Duties C)
b. When concluding the contract	26	(If the outsourced operations are not of high importance) Omission of concluding an SLA	Acceptable	Operation 109 3.	If Banking and Related Financial Institutions have, based on sufficient consideration of the properties of the operations, determined that the outsourced operations are not highly important, it is acceptable to conclude only a standard SLA provided by the Cloud service provider or to omit conclusion of an SLA through concluding only a general contract.	-	If Banking and Related Financial Institutions have determined that the outsourced operations are not highly important and have concluded only a standard SLA provided by the Financial Institutions' subcontractors or omitted conclusion of an SLA through concluding only a general contract, then it is acceptable to conclude only a standard SLA provided by the Financial Institutions' subcontractors or to omit conclusion of an SLA through concluding only a general contract.	-
	27	Prior preparations for migration to substitute services etc.	Recommended	Operation 109 4.	To enable continuity of operations even when it would be difficult to continue the contract with the Cloud service provider due to violation of the SLA or a change in policy by the Cloud service provider or the Financial Institution, it is recommended to take steps in advance to enable migration to substitute cloud services or general outsourcing or migration to an on-premises environment.	-	-	-
		(If the outsourced operations are not of high importance) System migration plans not assuming the cooperation of outsourcees	Acceptable	Operation 109 4.	If Banking and Related Financial Institutions could, based on sufficient consideration of the properties of the operations, determine that the outsourced operations are not highly important, then it is acceptable to make preparations in advance for migration to other outsourcees instead of assuming the cooperation of the current outsourcees.	-	-	-
c. Development	Outsourcing of development may be subject to the minimum necessary Security Guidelines (Note 3).							

Management phase	No.	Theme	Strength of controls	Security Guidelines section no. etc.	Duties of Financial Institutions when using outsourcing (Duties A) (Note 1)	Duties borne as Financial Institutions' primary outsourcees (Duties B-1)	Duties borne by Financial Institutions' subcontractors (Duties B-2)	Duties borne as Financial Institutions' subcontractors (Duties C)
d. During operation	28	Measures to prevent leakage when outsourcing data management	Required	Operation 110 1.	When entrusting data management to outsourcees, measures must be taken to prevent leakage.	When entrusted with data management from Financial Institutions, there is a duty to take measures to prevent leakage as requested by the Financial Institutions.	When entrusting data management to Financial Institutions' subcontractors, there is a duty for the Financial Institutions' subcontractors to take measures to prevent leakage as requested by the Financial Institutions.	When entrusted with data management from primary outsourcees, there is a duty to take measures to prevent leakage as requested by the primary outsourcees.
		Encryption of data collected/transmitted	Required	Operation 110 1.(1)	Data-management measures such as encryption must be taken for data that include highly confidential information such as personal data. To ascertain the risk of unauthorized access to data for which encryption is not possible due to the limitations of specifications (i.e., data processed as plain text), it is required to ascertain encryption specifications and determine whether or not they conform to the company's own risk-management policies.	There is a duty to take data-management measures such as encryption for data that include highly confidential information such as personal data. There also is a duty to provide Financial Institutions with information related to encryption specifications so that they can determine whether or not they conform to risk-management policies.	There is a duty for Financial Institutions' subcontractors to take data-management measures such as encryption for data that include highly confidential information such as personal data. To ascertain the risk of unauthorized access to data for which encryption is not possible due to the limitations of specifications (i.e., data processed as plain text), there is a duty to ascertain encryption specifications and determine whether or not they conform to the company's own risk-management policies.	There is a duty to take data-management measures such as encryption for data that include highly confidential information such as personal data. There also is a duty to provide primary outsourcees with information related to encryption specifications so that they can determine whether or not they conform to risk-management policies.
		Checking propriety of managers of encryption keys	Required	Operation 110 1.(2)	When entrusting Cloud service providers with management of encryption keys, it is required to ascertain sufficiently an overview of the management measures employed and determine whether they conform to the company's own risk-management policies.	When entrusting Financial Institutions' subcontractors with management of encryption keys, there is a duty to provide Financial Institutions with information related to encryption specifications so that they can ascertain sufficiently an overview of the management measures employed and determine whether or not they conform to their risk-management policies.	When entrusting Financial Institutions' subcontractors with management of encryption keys, there is a duty to ascertain sufficiently an overview of the management measures employed and determine whether they conform to the company's own risk-management policies.	When entrusting Financial Institutions' subcontractors with management of encryption keys, there is a duty to provide primary outsourcees with information related to encryption specifications so that they can ascertain sufficiently an overview of the management measures employed and determine whether or not they conform to their risk-management policies.
		Substitute measures instead of encryption	Required	Operation 110 1.(3)	It is acceptable to employ token technology that renders data in the Cloud environment essentially meaningless by replacing it with random numbers, with the original data and token maintained on the Financial Institutions' side. However, when employing tokens as a management method, suitable management measures such as token mapping are required on the part of the Financial Institution.	-	-	-

Management phase	No.	Theme	Strength of controls	Security Guidelines section no. etc.	Duties of Financial Institutions when using outsourcing (Duties A) (Note 1)	Duties borne as Financial Institutions' primary outsourcees (Duties B-1)	Duties borne by Financial Institutions' subcontractors (Duties B-2)	Duties borne as Financial Institutions' subcontractors (Duties C)
d. During operation	29	Data deletion upon failure or replacement of storage devices	Required	Operation 110 2.	When replacing devices or components due to causes such as failure of an outsourcee's storage device, it is required to employ sufficient management, including data deletion, for such storage devices since there is a possibility that their devices or components could still contain highly confidential data concerning Banking and Related Financial Institutions or their customers.	When replacing devices or components due to causes such as failure of a primary outsourcee's storage device, there is a duty to employ sufficient management, including data deletion, for such storage devices as requested by the Financial Institution.	When replacing devices or components due to causes such as failure of a Financial Institutions' subcontractor's storage device, there is a duty for Financial Institutions' subcontractors to employ sufficient management, including data deletion, for such storage devices as requested by the Financial Institution.	When replacing devices or components due to causes such as failure of a Financial Institutions' subcontractor's storage device, there is a duty to employ sufficient management, including data deletion, for such storage devices as requested by the primary outsourcee.
		Substitute measures instead of a certificate of data deletion upon failure or replacement of storage devices	Acceptable	Operation 110 2.	The contract may stipulate that verification of the efficacy of the data deletion and destruction process through a request for provision of information made to the Cloud service providers, auditing, or similar method may substitute for the issue and obtaining of a certificate of deletion in the event of damage or replacement of storage devices.	-	The contract may stipulate that verification of the efficacy of the data deletion and destruction process through a request for provision of information made to the Financial Institutions' subcontractors, auditing, or similar method may substitute for the issue and obtaining of a certificate of deletion in the event of damage or replacement of storage devices.	-
		(When not handling important data) Requirement for data deletion or destruction	Acceptable	Operation 110 2.	When outsourcees do not handle important data, they may not need to be required to delete or destroy data when replacing storage devices etc.	-	-	-
	30	Everyday monitoring of outsourced operations	Required	Operation 89 1. 2. 3.	From the perspective of smooth and appropriate management of outsourcing operations, it is required that the scope of outsourcees' operations and their responsibilities and rules that outsourcees' staff must follow be made clear and monitored on an everyday basis.	There is a duty to undergo everyday monitoring by Financial Institutions.	From the perspective of smooth and appropriate management of outsourcing operations, there is a duty to ensure that the scope of Financial Institutions' subcontractors' operations and their responsibilities and rules that subcontractors'' staff must follow be made clear and monitored on an everyday basis.	There is a duty to undergo everyday monitoring by primary outsourcees.
			Required	Operation 90 1. 2. 3.				
			Required	Operation 112 1. 2.				

Management phase	No.	Theme	Strength of controls	Security Guidelines section no. etc.	Duties of Financial Institutions when using outsourcing (Duties A) (Note 1)	Duties borne as Financial Institutions' primary outsourcees (Duties B-1)	Duties borne by Financial Institutions' subcontractors (Duties B-2)	Duties borne as Financial Institutions' subcontractors (Duties C)
d. During operation	31	Preparation of a system auditing structure	Required	Operation 91 1. 2. 3. 4. 5. 6.	To ensure the efficacy, efficiency, reliability, compliance, and security of operation, development, changes, etc. regarding computer systems related to outsourcing, it is required that a system be established under which independent auditors conduct general auditing and evaluation of the computer systems and report the results of such auditing to top management.	There is a duty to undergo general auditing and evaluation of computer systems conducted by an independent auditor regarding matters such as operation, development, and changes regarding computer systems related to the outsourced operations.	There is a duty to undergo general auditing and evaluation of computer systems conducted by an independent auditor to ensure the efficacy, efficiency, reliability, compliance, and security of operation, development, changes, etc. regarding computer systems related to outsourcing.	There is a duty to undergo general auditing and evaluation of computer systems conducted by an independent auditor regarding matters such as operation, development, and changes regarding computer systems related to the outsourced operations.
		On-site auditing	Required	Operation 112 2.	When a request for provision of information alone is not sufficient for verifying the appropriateness of outsourced operations, it is required to check matters through means such as on-site auditing and monitoring of Cloud service providers' offices, data centers, etc.	When a request for provision of information alone is not sufficient for verifying the appropriateness of outsourced operations, there is a duty to undergo checking of matters through means such as on-site auditing and monitoring by Financial Institutions of the company's own offices, data centers, etc.	When a request for provision of information alone is not sufficient for verifying the appropriateness of outsourced operations, there is a duty to check matters through means such as on-site auditing and monitoring of Financial Institutions' subcontractors' offices, data centers, etc.	When a request for provision of information alone is not sufficient for verifying the appropriateness of outsourced operations, there is a duty to undergo checking of matters through means such as on-site auditing and monitoring of the company's own offices, data centers, etc.
		Third-party auditing	Acceptable	Operation 112 3.	In cases such as when on-site monitoring of outsourcees would not be effective, it may be replaced by third-party auditing.	-	In cases such as when on-site monitoring of Financial Institutions' subcontractors would not be effective, it may be replaced by third-party auditing.	-
			Required	Outsourcing Council of Experts Footnote 40 (Note 4)	It is required to choose an audit firm with no external appearances that would lead to suspicions of a conflict of interest with Cloud service providers from an independent, third-party point of view.	As requested by Financial Institutions, there is a duty to choose an audit firm with no external appearances that would lead to suspicions of a conflict of interest with Financial Institutions from an independent, third-party point of view.	As requested by Financial Institutions, there is a duty for Financial Institutions' subcontractors to choose an audit firm with no external appearances that would lead to suspicions of a conflict of interest with Financial Institutions' subcontractors from an independent, third-party point of view.	As requested by primary outsourcees, there is a duty to choose an audit firm with no external appearances that would lead to suspicions of a conflict of interest with primary outsourcees from an independent, third-party point of view.

Management phase	No.	Theme	Strength of controls	Security Guidelines section no. etc.	Duties of Financial Institutions when using outsourcing (Duties A) (Note 1)	Duties borne as Financial Institutions' primary outsourcees (Duties B-1)	Duties borne by Financial Institutions' subcontractors (Duties B-2)	Duties borne as Financial Institutions' subcontractors (Duties C)
d. During operation	31	(If the outsourced operations are not of high importance) Management measures based on cost-benefit analysis	Acceptable	Operation 112 4.	When the importance of outsourced operations is not very high, means such as third-party certification may be used instead of on-site auditing based on a cost-benefits perspective.	-	When Banking and Related Financial Institutions have determined that the importance of outsourced operations is not very high, means such as third-party certification of operations outsourced to Financial Institutions' subcontractors may be used instead of on-site auditing based on a cost-benefits perspective.	-
e. Termination	32	Measures for nondisclosure, privacy, and fraud prevention upon termination of the contract	Required	Operation 111 1.	Upon the end of the outsourcing contract, it is required to take measures to protect confidential information, protect privacy, and prevent improprieties, in order to prevent leakage of data.	Upon the end of the outsourcing contract, there is a duty to take measures to protect confidential information, protect privacy, and prevent improprieties as requested by Financial Institutions.	Upon the end of the outsourcing contract, there is a duty for Financial Institutions' subcontractors to take measures to protect confidential information, protect privacy, and prevent improprieties as requested by Financial Institutions.	Upon the end of the outsourcing contract, there is a duty to take measures to protect confidential information, protect privacy, and prevent improprieties as requested by primary outsourcees.
		Types of data deletion methods	Required	Operation 111 2.	Conceivable means of data deletion are physical deletion and logical deletion. Physical deletion is recommended in cases of future hardware upgrades and removal. Note: Use of logical deletion only also is acceptable.	There is a duty to conduct logical deletion of data as requested by Financial Institutions.	There is a duty for Financial Institutions' subcontractors to conduct logical deletion of data as requested by Financial Institutions.	There is a duty to conduct logical deletion of data as requested by primary outsourcees.
		Receipt of certificate of deletion	recommended	Operation 111 3.	It is recommended to obtain a certificate of deletion when outsourcees delete data.	There is a duty to submit a certificate of deletion to the Financial Institution when deleting data.	There is a duty to obtain a certificate of deletion when Financial Institutions' subcontractors delete data.	There is a duty to submit a certificate of deletion to the primary outsourcee when deleting data.
		Substitute measures instead of certificate of deletion	Acceptable	Operation 111 3.	Instead of requiring the issue and obtaining of a certificate of deletion, the contract may stipulate that outsourcees delete data, including logical deletion, and have the appropriateness of the deletion process verified through means such as auditing by an independent third party.	-	Instead of requiring the issue and obtaining of a certificate of deletion, the contract may stipulate that Financial Institutions' subcontractors delete data, including logical deletion, and have the appropriateness of the deletion process verified through means such as auditing by an independent third party.	-

Management phase	No.	Theme	Strength of controls	Security Guidelines section no. etc.	Duties of Financial Institutions when using outsourcing (Duties A) (Note 1)	Duties borne as Financial Institutions' primary outsourcees (Duties B-1)	Duties borne by Financial Institutions' subcontractors (Duties B-2)	Duties borne as Financial Institutions' subcontractors (Duties C)
e. Termination	32	(Outsourcing that does not involve handling of confidential information) Simplification of data deletion process etc.	Acceptable	Operation 111 4.	When entrusting to outsourcees operations that do not involve handling of confidential information such as customer data, it is conceivable that the data deletion process upon the end of the contract could be simplified or unnecessary, and a certificate of deletion might be unnecessary as well.	-	-	-
f. Upon an incident	33	(Important systems) Emergency responses including subcontractors	Required	Outsourcing Council of Experts IV 4.(3)	When outsourcing critical information systems, formulation of a CP including outsourcees or subcontractors is required.	When entrusted by a Financial Institution with a critical information system, there is a duty to formulate the company's own CP so that it includes Financial Institutions and Financial Institutions' subcontractors.	When outsourcing critical information systems to a Financial Institution's subcontractor, there is a duty to formulate the Financial Institution's subcontractor's CP so that it includes the Financial Institution and the Financial Institution's primary outsourcees.	When entrusted by a primary outsourcee with a critical information system, there is a duty to formulate the company's own CP so that it includes Financial Institutions and primary outsourcees.
			Required	Outsourcing Council of Experts IV 4.(3)	When outsourcees and others prepare CPs individually, their content must be fully consistent and complementary with that of the CPs of individual Banking and Related Financial Institutions.	When Banking and Related Financial Institutions prepare CPs individually, there is a duty for their content to be fully consistent and complementary with that of the company's own CP.	When Financial Institutions' subcontractors and other organizations prepare CPs individually, there is a duty for their content to be fully consistent and complementary with that of the CP of each primary outsourcee.	When primary outsourcees and other organizations prepare CPs individually, there is a duty for their content to be fully consistent and complementary with that of the company's own CP.
			Required	Outsourcing Council of Experts IV 4.(3)	During normal times, Banking and Related Financial Institutions must conduct periodic drills jointly with outsourcees and subcontractors, based on the CPs concluded with outsourcees and others.	During normal times, there is a duty to conduct periodic drills jointly with Banking and Related Financial Institutions' subcontractors, based on the CPs concluded with Banking and Related Financial Institutions.	During normal times, there is a duty to participate in periodic drills conducted jointly with Financial Institutions and Financial Institutions' subcontractors, based on the CPs concluded with Financial Institutions' subcontractors and others.	During normal times, there is a duty to conduct periodic drills jointly with Financial Institutions and primary outsourcees, based on the CPs concluded with primary outsourcees and others.
		Implementation of risk management (Note 5)		Operation 90-1				

(Note 1) Duties of Financial Institutions when using outsourcing (Duties A)
Applicable content reproduced from FISC Security Guidelines on Computer Systems for Banking and Related Financial Institutions (Ver. 8), Security Guidelines on Computer Systems for Banking and Related Financial Institutions(Ver. 8, supplemented and revised), and the Report of the Council of Experts on Outsourcing in Financial Institutions

(Note 2) p. 22, Security Guidelines on Computer Systems for Banking and Related Financial Institutions (Ver. 8, supplemented and revised)
Items for which it is noted as “Required” to state matters clearly in contracts in the Cloud Report are ones that can be considered related to outsourcing in on-premises and shared system center forms. For this reason, in this table these are indicated as “Recommended.”

(Note 3) p. 43, Report of the Council of Experts on Outsourcing in Financial Institutions
Outsourcing of development of important information systems (including not only that conducted during development but also that conducted during consideration of use, when concluding the contract, and upon termination) may be subject to the minimum necessary Security Guidelines stipulated within the extent of the purposes of reducing uncertainty of security measures.

(Note 4) Footnote 40, Report of the Council of Experts on Outsourcing in Financial Institutions
The FISC System Audit Guidelines for Banking and Related Financial Institutions(Rv. 3, supplemented) states under Part 1; Chapter III; 5. Key Points of Auditing Cloud Services; (1) Consideration of Joint Auditing of Cloud Service Providers Using Third-Party Auditing that in selection of an auditor, “As a Financial Institution bearing responsibilities to its customers, there is a need to select an auditor that from the view of a third party would not appear to involve any concerns of conflict of interest with the cloud service provider. For this reason, the outsourcer Financial Institution needs to select for joint auditing an auditor not involved in the account auditing of the cloud service provider. Also, if selecting an auditor that is involved in SOC2 or IT7 guarantees for the cloud service provider, there is a need to select auditing staff not involved in SOC2 or IT7 guarantees for the cloud service provider.

(Note 5) Footnote 12, FinTech Council Report
For cases in which the Financial Institution does not play a leading role, under Operation 90-1 the Security Guidelines include guidelines on service use that differ from those on outsourcing. These guidelines state, “As with management of outsourcing, in many cases it is difficult or inefficient for a Financial Institution to select a service provider from multiple options and conduct risk management itself,” indicating that the degree of responsibility borne by Financial Institutions in security measures should be understood to be more limited than in the case of general outsourcing. However, these guidelines apply to systems and networks linking Financial Institutions and not to the customer services considered herein.

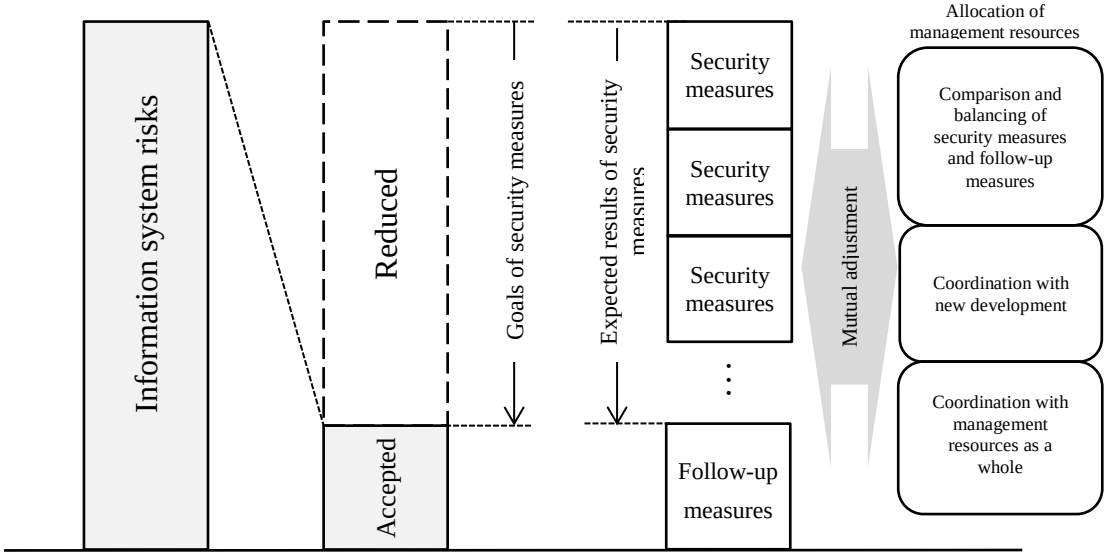
Reference 5. Thinking on the principle of equivalency

The principle of equivalency refers to the concept of ensuring that the effects of security measures for information systems handling financial operations are equivalent regardless of which related parties are involved in such security measures. This principle is explained below, while touching on the relationship between the principle of equivalency and redistribution rules and perusing the processes from risk evaluation through decision on and implementation of security measures.

1. Processes through implementation of security measures in accordance with the basic principles thereof

(1) Risk evaluation and decision-making by top management

First of all, goals to be achieved by security measures and individual security measures themselves are derived based on IT governance in accordance with the basic principles of security measures.



Financial Institutions ascertain the properties of risks through risk evaluation of information systems. Top management decides on the degrees to which to reduce risks or to which to tolerate risks[76] in accordance with the risks of information systems. They also decide on the goals to be achieved by security measures as means of reducing risks. Decisions are made on the goals to be achieved by security measures and individual security measures themselves in accordance with the properties of the related risks, while referring to the Security Guidelines.

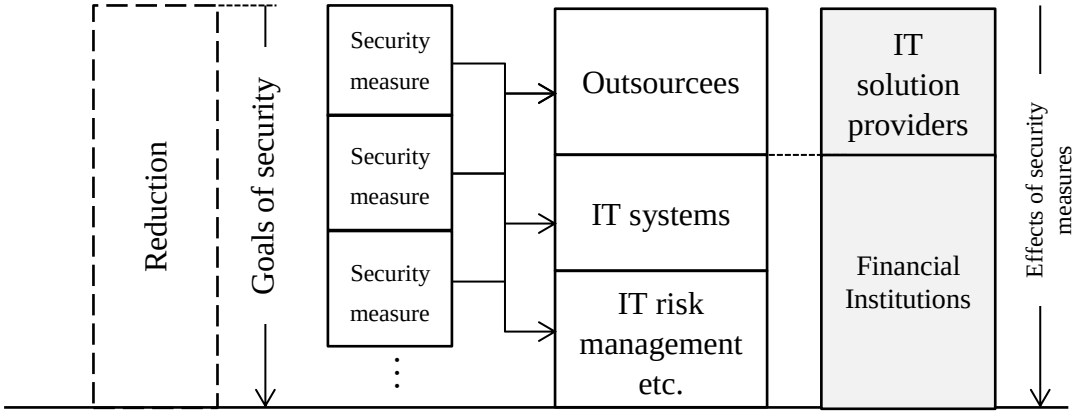
Top management makes decisions on allocation of resources to security measures with the goal of maximizing. enterprise value though measures taken such as adjustment of allocation of management resources as a whole. In doing so, the goals to be achieved are mutually adjusted while comparing and balancing the costs of security measures taken to reduce risks and the subsequent costs that might arise if not implementing the security measures. Next,

[76] Aside from reduction and tolerance, other options include transfer, through insuring against damages in the event a risk occurs, and avoidance, by not using information systems for which such management responsibilities would arise.

adjustments are made with other areas to which resources could be allocated, such as investment in new development, within the information systems budget. Lastly, allocation of management resources as a whole is adjusted, above and beyond the information systems budget.

(2) Allocation of duties related to security measures and achievement of related results

Next, the duties related to security measures derived are allocated among related parties and security measures are implemented.



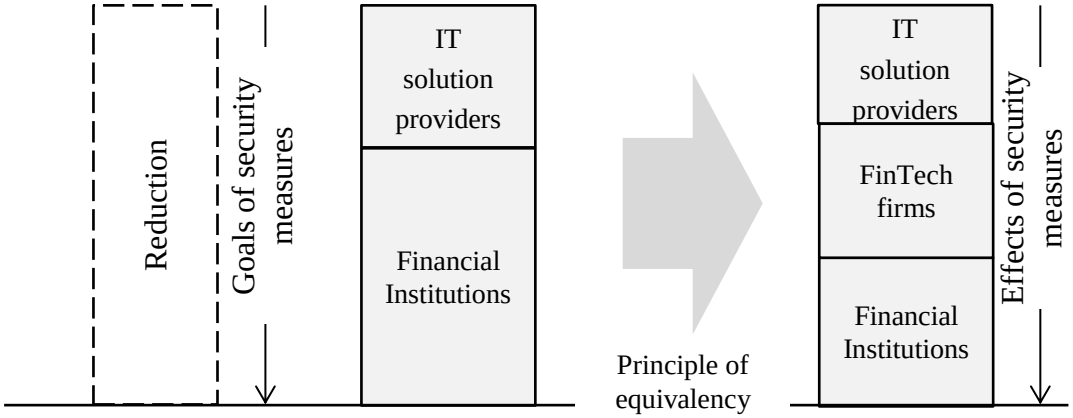
After top management has made decisions on the goals to be achieved by security measures and allocation of management resources, security measures are implemented under management by multiple related parties (e.g., IT risk-management sections, IT sections, and outsourcees). In implementing these, roles (duties) are identified (allocated) among related parties in accordance with individual security measures.

In general, duties related to security measures are allocated to the two parties of outsourcees responsible for the technical aspects of security measures and Financial Institutions. Financial Institutions select outsourcees who already possess the ability to carry out security measures and ultimately bear the costs of performance of this duty by outsourcees, as outsourcing costs. The aim is to achieve the results of security measures and reduce system risk to an acceptable degree as decided by top management.

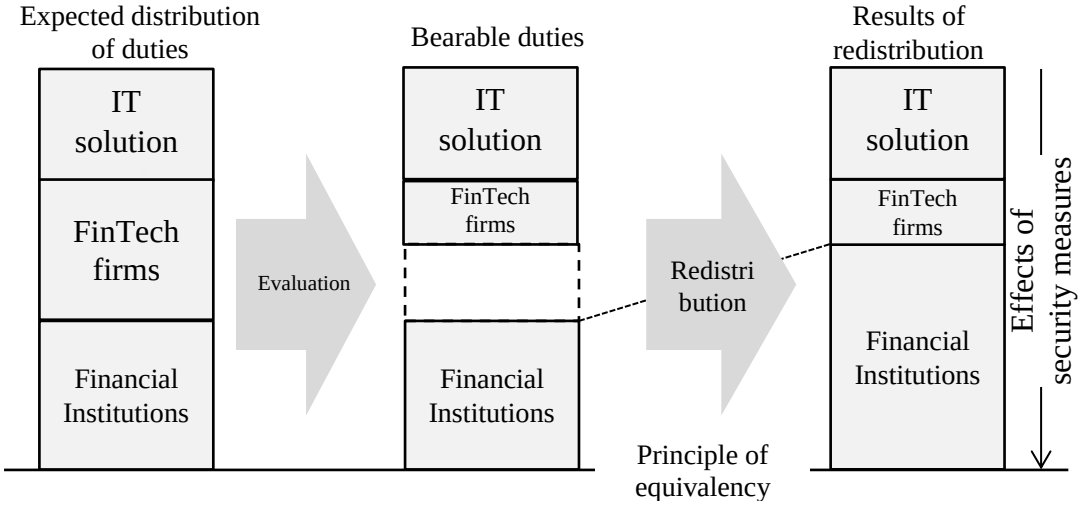
2. Allocation of duties related to security measures in FinTech operations and the principle of equivalency

In FinTech operations in which FinTech firms take part as parties related to security measures, there is a need for efforts to reduce risks to the same degree as when financial-related services are conducted by the two parties of Financial Institutions and IT solution providers. This is referred to as the “principle of equivalency.”

However, when FinTech firms also are involved, if the duties traditionally expected of IT solution providers are demanded of FinTech firms instead, then only FinTech firms capable of performing the same duties as IT solution providers would be chosen.



However, in the case of FinTech there is a need to consider the perspective of enjoying the benefits of innovation, and for this reason rules are needed on redistribution of duties.



Specifically, redistribution of duties is a measure intended to balance enjoyment of the benefits of innovation with ensuring system security (principle of equivalency) in a case in which the results of evaluation during selection show that FinTech firms lack full ability to execute security measures. In the example above, Financial Institutions would bear some of the duties of FinTech firms.

An extreme example of such redistribution would be a case in which a FinTech firm would bear no duties at all. However, since under the principle of making businesses involved in provision of financial-related services subject to such duties it would not be appropriate for such a party to implement no security measures at all, there is a minimal level of duties that FinTech firms must bear as responsible business, and these duties cannot be redistributed.

Also, redistribution of duties and the principle of equivalency are concepts that can apply both to cases in which Financial Institutions play a leading role in financial-related services (i.e., FinTech firms serve as outsourcees) and cases in which FinTech firms play a leading role (i.e., outsourcing applies mutatis mutandis to FinTech firms).

While such redistribution of duties is one option that Financial Institutions traditionally are able to employ at their discretion, by proactively describing it clearly in the Security Guidelines it is expected that relations with FinTech firms will advance and innovation will be encouraged.

Reference 6. Prospectus on establishment of the Financial Mechanization Foundation (tentative name) (excerpted)

September 1984

Purpose

Automation of financial systems has been advancing rapidly in recent years, and it is expected that in the future this will have major and complex effects on management of Financial Institutions, on relations between the financial industry and other industries, and, as a result, on credit discipline in Japan.

In particular, in light of the facts that the financial system involves funds settlement functions necessarily used in the activities of various economic sectors and development of third-generation online systems connecting Financial Institutions with non-Financial Institution third parties is advancing rapidly, it is conceivable that there will be a need to resolve quickly and steadily the various issues that may arise with regard to automation of financial systems in general, including those related to ensuring security, in order to facilitate the smooth advancement of financial automation systems.

Since such issues involve a wide range of industries, in consideration of related matters it can be considered essential to obtain the cooperation of related parties including Financial Institutions, insurers, securities companies, hardware and software makers, telecommunications carriers, central bank and regulators. That is, it would appear to be necessary both to advance various measures to ensure security through consolidation of knowledge, experience, information, and other resources based on sufficient communication among such related parties and to advance appropriate planning, proposal, development, implementation, and other activities.

In light of this point of view, in order to address the various issues related to financial automation systems in an efficient and flexible way, it would seem to be appropriate to form a privately funded independent, neutral institution with the participation of the above related parties, to effect environmental improvements to demonstrate the vitality of the private sector.

The cooperation of related parties is requested, based on their support of the purpose described above.

Activities

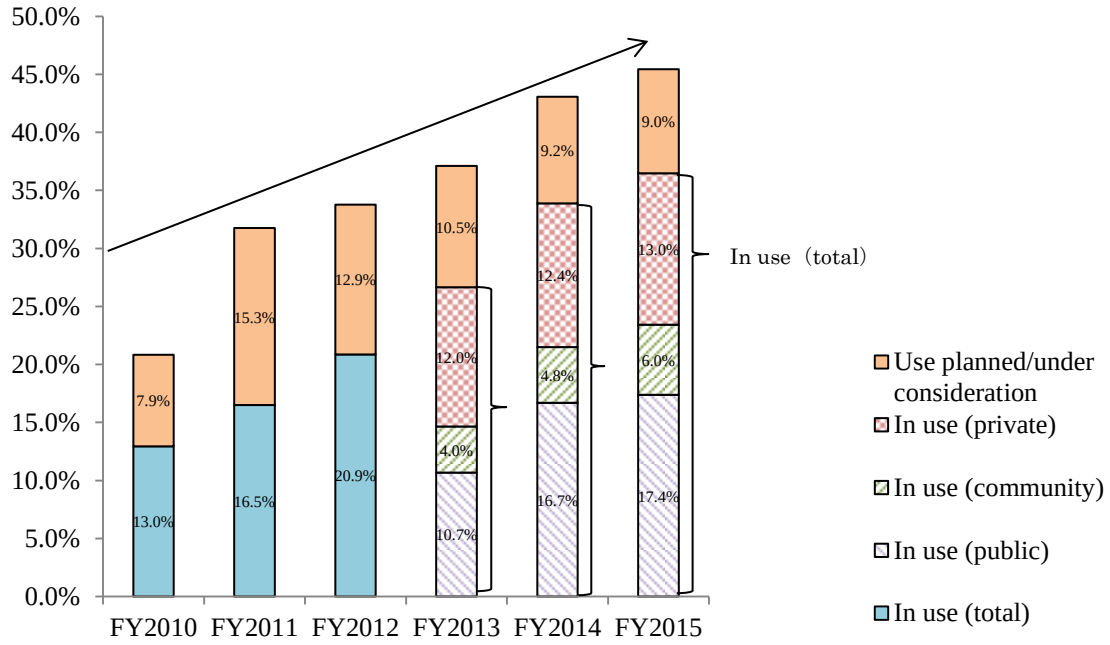
(1) Planning, investigation, and research concerning financial transactions, legal matters, investment, burdens on beneficiaries, international relations, and other matters with regard to financial automation systems
(2) Ascertaining and disclosing the state of failures and criminal activities related to financial automation systems, and promoting security measures through means including formulation of security guidelines
(3) Implementing investigation and research on joint projects related to financial automation systems, facilitation and intermediation related to financial automation systems, system audits, and training, seminars, and public-relations activities, among other activities

(Underlining added by FISC.)

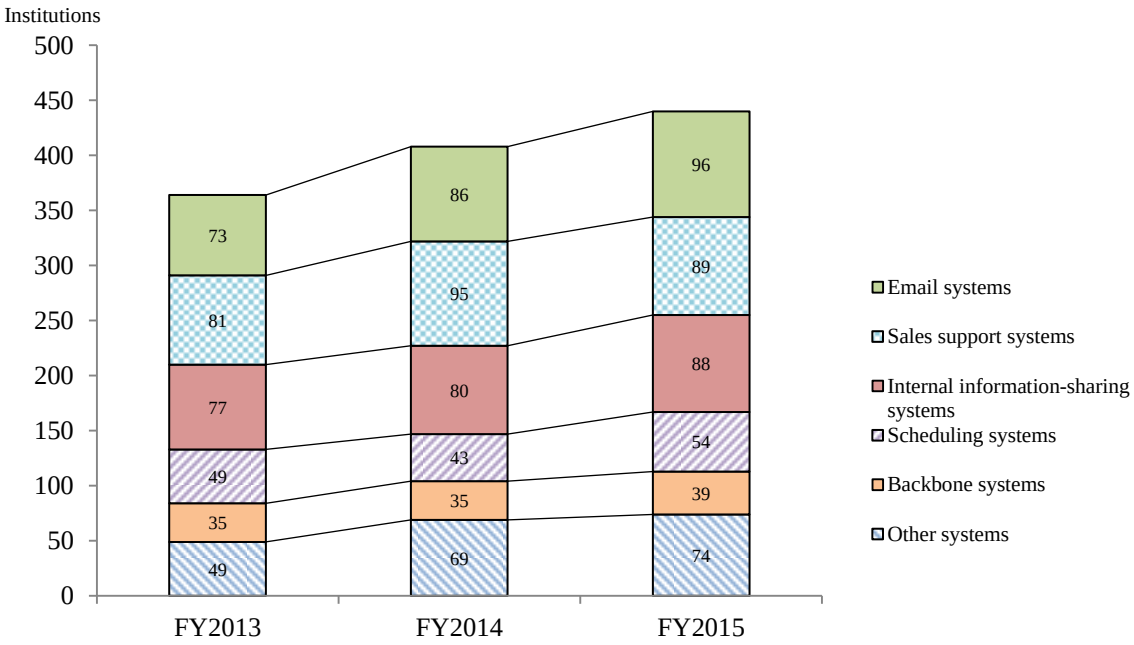
Reference 7. Cloud usage

As of FY2015, about one-half of Banking and Related Financial Institutions either currently used the Cloud or were considering doing so. These numbers are increasing from year to year, without showing a bias toward any specific systems.

Trends in Cloud use



Cloud usage environments



Source: Results of FISC survey of Financial Institutions

Reference 8. Trends among overseas regulators regarding use of cloud services

In recent years, progress has been made on formulation of guidelines on use of cloud services by Financial Institutions not only in Japan but in other developed countries as well.

In the United States, in July 2012 the Federal Financial Institutions Examination Council (FFIEC) released "IT Handbook: Outsourcing Booklet: Outsourced Cloud Computing"[77]. In addition, it appears that new studies are underway in the U.S. in light of growing use of public Cloud services.

In the United Kingdom, in July 2016 the Financial Conduct Authority (FCA) issued the "Guidance for firms outsourcing to the 'cloud' and other third-party IT services"[78].

Below, the thinking of overseas regulators concerning security measures when using cloud services is described with a focus mainly on the U.S. and the U.K., based on the above published documents along with an interview conducted by the FISC with the Office of the Comptroller of the Currency (OCC).

1. Basic thinking on risk management in cloud services

Even when Financial Institutions outsource operations to Cloud service providers, they need to implement controls similar to those in place when conducting such operations in-house and to carry out controls and risk management to ensure that risks do not increase compared to in-house operations.

> *"(Even if the institution engages in cloud computing,) outsourced relationships should be subject to the same risk management . . . that would be expected if the Financial Institution were conducting the activities in-house." (U.S.)*
> *"A firm should . . . as part of the due diligence exercise, ensure that in entering into an outsource agreement, it does not worsen the firms operational risk." (U.K.)*

2. Thinking on controls

With regard to controls, the focus is on control methods corresponding to individual management phases, such as objective evaluation when considering use, the content of contracts concluded, and monitoring during operation.

> *"Matters that are important first of all when using a public Cloud are due diligence when concluding a contract and the content of the contract itself. Furthermore, monitoring after concluding the contract also is important. For example, monitoring of the service level agreement is an effective form of monitoring, since it makes it possible to identify any problems with a Cloud service provider in advance." (U.S.)*

At the same time, the content of technical controls is entrusted to the Financial Institutions, and thus the Financial Institutions need to understand technology sufficiently and use it appropriately.

[77] http://ithandbook.ffiec.gov/media/153119/06-28-12_-_external_cloud_computing_-_public_statement.pdf
[78] https://www.fca.org.uk/publication/finalised-guidance/fg16-5.pdf

"A basic principle of supervision is that Financial Institutions choose which technologies to use. Regulators do not issue instructions on such choices. Similar degrees of internal controls and management are required no matter which technologies are used." (U.S.)
"With regard to security measures, regulators do not issue instructions concerning individual technologies, such as requiring use of encryption or firewalls. This is because technologies can change. It is enough if effective and valid security measures are implemented. For example, an encryption tool provided by a Cloud service provider might be used. In such a case, if staff of the Cloud service provider have keys to decrypt the data, then there is a risk that they could view the information they contain. At the same time, machines require maintenance, and it is understandable that the Cloud service provider's staff may need to possess such keys. Accordingly, in such a case it would be acceptable if the Financial Institution took measures to ascertain who on the staff of the Cloud service provider possesses such keys, and for what purposes. With regard to firewalls and intrusion detection systems as well, Financial Institutions need to understand their structures and test them to ensure that they operate properly." (U.S.)

3. Thinking on auditing authority

In their contracts with Cloud service providers, Financial Institutions need to make arrangements to ensure that effective controls can be implemented.

"A firm should . . . know whether its contract with the service provider is governed by the law and subject to the jurisdiction of the United Kingdom. If it is not, it should still ensure effective access to data and business premises for the firm, auditor and relevant regulator." (U.K.)

In the U.S., except in cases as stipulated in the law governing handling of personally identifying information (the Gramm-Leach-Bliley Act), there is no enforceable requirement to define auditing authority vis-a-vis Cloud service providers clearly in the contract. It can be surmised that this reflects the background factor of the fact that in the U.S., under the Bank Service Company Act, regulators can audit directly IT solution providers to which bank operations are outsourced.

"Banks should have auditing authority over Cloud IT solution providers, and this point should be stipulated in the contract. However, this is a best practice and is not enforced on banks by regulators. Legally, banks are free to determine what to stipulate in their contracts." (U.S.)
"IT solution providers to which numerous banks outsource accounting systems are subject to joint inspection by the Office of the Comptroller of the Currency (OCC), the Federal Deposit Insurance Corporation (FDIC), the Federal Reserve Board (FRB), and others, and reports on such inspection are provided to the Financial Institutions using the IT solution providers." (U.S.)

In addition, the efficacy of guarantee audit reports prepared by auditors as requested by Cloud service providers themselves is regarded highly.

"Major Cloud service providers undergo auditing by independent auditors and submit to their customers guaranteed audit reports in accordance with the standards of the American Institute of Certified Public Accountants. Since for practical purposes this is sufficient in terms including its scope, there is no need for Financial Institutions to conduct additional auditing after receiving such a report. As a practical matter it is unlikely that a major Cloud service provider with thousands of customers would be able to undergo individual auditing by each of its customers. However, it is recommended to provide in the contract for additional auditing if this report is inadequate." (U.S.)

4. Thinking on locations of data storage

There are no regulations that require domestic storage of data. Wherever data are stored, they need effectively to be accessible to Financial Institutions and regulators. For this reason, the locations of data storage need to be ascertained.

"Specific regulatory requirements for some firms . . . require effective access to data related to the outsourced activities for regulated firms, their auditors, regulators and relevant competent authorities. The term 'data' has a wide meaning. It includes but is not limited to firm, personal customer and transactional data, but also system and process data: for example Human Resource vetting procedures or system audit trails and logs. A firm should . . . ensure that data are not stored in jurisdictions that may inhibit effective access to data for UK regulators." (U.K.)
"While there is no regulatory requirement for domestic storage of data in the United States, the data must be acceptable when needed to the same extent as they would be if they were stored in the U.S." (U.S.)
"When using a public Cloud service as well, the geographical scope of data storage must be established and the bank must be able to monitor them. Regulators will inspect whether the bank monitors whether or not data are transferred to places where they should not be." (U.S.)

5. Thinking on advanced nature of technology

While Financial Institutions choose from a diverse range of Cloud services the forms best suited to their own needs, they need to understand the boundaries of their own responsibility in accordance with the form chosen and to control risks appropriately. They also need to recognize the possibility of new risks arising and to understand their content in advance and take measures as necessary. One anticipated new risk is that of the mutual effects on systems of anonymous users.

"Among public Cloud services, PaaS and IaaS services involve higher risks borne by Financial Institutions than do SaaS services. It is important that Financial Institutions understand this. Also, migration to the Cloud of systems with more of a core nature results in increased risks. However, regulators feel that the level and understanding of major IT solution providers are high, and in many cases Financial Institutions actually learn from IT solution providers." (U.S.)
"While it would be preferable for Financial Institutions' data to be stored in a fixed form, if they were stored together with that of a gaming company, for example, then the level of risk might increase accordingly. For example, there is a need for verification of whether or

not a Financial Institution would be affected by hacking of another user on the same hardware even if the Financial Institution itself were not hacked." (U.S.)
"A firm should . . . consider how data will be segregated (if using a public cloud)." (U.K.)

6. Thinking on business continuity planning

Business continuity planning needs to be discussed and documented with outsourcees in advance, and its efficacy needs to be verified periodically through drills.

"Data redundancy needs to be covered in the contract in advance. Also, when covering redundancy in the contract it is necessary to understand how it is achieved in practical terms and to test whether or not it truly functions as anticipated." (U.S.)
"A firm should have in place appropriate arrangements to ensure that it can continue to function . . . in the event of an unforeseen interruption of the outsourced services. (A firm) should: document its strategy for maintaining continuity of its operations, including recovery from an event, and its plans for . . . regularly testing the adequacy and effectiveness of this strategy." (U.K.)

7. Other matters

"Managing a cloud computing service provider may require additional controls if the servicer is unfamiliar with the financial industry and the Financial Institution's legal and regulatory requirements for safeguarding customer information and other sensitive data. Additionally, the use of such a servicer may present risks that the institution is unable or unwilling to mitigate." (U.S.)

In Japan, Cloud service providers are provided with opportunities to deepen their understanding of the financial business through means including joining FISC and participation in meetings such as those of the Council of Experts.

Reference 9. Collective consideration of the checklist used in API connection

The document *Report of Review Committee on Open APIs : Promoting Open Innovation (Interim Summary [Draft])* published by the JBA states, "To lessen the burden of responding to review on the part of firms connected with multiple banks through APIs, agencies related to information security are expected to establish API Connection Checklists (tentative name) consisting of the items that need to be confirmed and those already confirmed independently, for use when banks review the suitability of other parties connecting via API."

In response to this statement, in February 2017 the API Connection Checklist Working Group ("Checklist WG" hereinafter) was established, with FISC serving as its secretariat. Its activities include consideration of the content of controls carried out in the entry management phase—that is, the common portions of the checklist used in objective evaluation of parties connecting via APIs ("Checklist" hereinafter).

Since an open API is one method of realizing Type III in the FinTech Council, consideration of the Checklist needs to be advanced in consistency with the content of opinions offered concerning Type III in the FinTech Council. That is, there is a need for consideration conscious of the interrelations among groups studying FinTech-related security measures while reflecting the "Rules on mutatis mutandis application of outsourcing guidelines" and "minimum necessary Security Guidelines."[79]

Also, from the perspective of lessening the burden on FinTech firms, it is recommended that a socially normative Checklist be established, and for this purpose it is recommended that related parties involved in API connection—Financial Institutions, FinTech firms, and IT solution providers—take part in the process of considering the Checklist, with the aim of building consensus.

In establishing the Checklist, the above collective consideration shall be conducted, and when deliverables have been brought together as a result, such deliverables shall be handled as part of the content of opinions offered by the FinTech Council. In addition, even in a case such as when environmental changes have arisen it is expected that the above collective consideration would be conducted and the content of deliverables would be reviewed, implemented, and managed continually.

It is expected that related parties involved in API connection would use such deliverables as effective materials in accordance with the actual states of Financial Institutions, aiming both to secure overall security and to carry out innovation.

[79] The minimum necessary Security Guidelines will be established as guidelines to which businesses involved in provision of financial-related services, including those connecting via APIs, should refer. Until they are established, it is recommended to refer in consideration of related matters at least to the basic components of abilities to execute security measures (Footnote 26).

Reference 10. Topics addressed by the Council and countermeasures against them