

Report of the Council of Experts on Outsourcing in Financial Institutions

June 2016

The Center for Financial Industry Information Systems

Table of contents

Introduction	1
I. Trends in outsourcing in recent years and changes in environmental conditions of outsourcing	2
1. Trends in outsourcing in recent years.....	2
2. Changes in environmental conditions of outsourcing	3
(1) Cases of misconduct in recent years at outsourcees etc.	3
(2) Advancement of joint use.....	4
(3) Necessity of human-resources development	5
(4) Various issues related to subcontractor management (amendments to the Banking Act etc.).....	6
3. FISC initiatives through now in response to these environmental changes and this Council's recognition of issues.....	7
(1) Cases of misconduct by outsourcees and others in recent years	7
(2) Advancement of joint use.....	7
(3) Necessity of human-resources development	7
(4) Various issues related to subcontractor management (amendments to the Banking Act etc.).....	8
4. Necessity of studying IT governance	8
5. Overview of outsourcing	10
II. IT governance and IT management	12
1. IT governance necessary for security measures	13
(1) Significance of IT governance necessary for security measures	13
(2) Roles and responsibilities of top management in IT governance necessary for security measures	14
2. IT management necessary for security measures	17
(1) Roles and responsibilities of management	18
(2) Roles and responsibilities of those responsible for management planning	19
(3) Roles and responsibilities of users	19
3. Notes on staffing plans	20
4. Decision-making by top management concerning important IT-related matters	21
III. Risk-based approach	24
1. The necessity of a new form for security measures.....	25
(1) The necessity of reviewing the concepts of security measure standards.....	25
(2) Traditional thinking on security measures and related issues	26
(3) Risk-based approach	27
2. Basic principles of security measures.....	28

3.	IT governance in accordance with the basic principles	29
(1)	Significance.....	29
(2)	Rules for information systems involving serious externalities and related subjects .	30
(3)	Necessity of a simplified method	30
4.	IT governance through a simplified risk-based approach.....	30
(1)	Significance.....	30
(2)	Significance of “critical information systems”	31
(3)	Security measures and allocation of management resources for critical information systems	31
(4)	Security measures and allocation of management resources for other information systems	31
(5)	Significance of minimum necessary security guidelines.....	32
5.	Management responsibility for security measures	34
IV.	Risk Management in Outsourcing.....	35
1.	Various issues related to subcontracting.....	36
2.	Thinking on responses to various issues	36
3.	Risk management in outsourcing	39
(1)	Management processes in outsourcing.....	39
(2)	Thinking on risk-management measures in each management phase.....	42
4.	Risk management measures for subcontracting	45
(1)	Formulating requirements for selection of subcontractors and implementing advance screening.....	45
(2)	Clear description of the right to audit subcontractors	45
(3)	Responding to incidents	46
V.	Risk management at shared system centers	48
1.	The significance of shared system centers and their distinguishing features	49
(1)	The significance of shared system centers	49
(2)	Profiles of shared system centers	49
2.	Challenges involved in shared system centers	50
3.	Distinguishing features of shared system centers.....	52
4.	Ways of thinking on risk management measures specific to shared system centers	52
5.	IT governance specific to shared system centers (forms of formulating risk management measures).....	54
VI.	Thinking on future revisions to Security Guidelines etc.....	56
	List of Members and Observers of the Council of Experts on Outsourcing in Financial Institutions	57
VII.	References.....	61

Reference 1: Sample IT skills map	62
Reference 2: Breakdown of system-related expenses by purpose	63
Reference 3: Trends among overseas regulators and others regarding the risk-based approach	64
Reference 4: Thinking on externalities and sensitivity of information	67
Reference 5: FFIEC IT Examination Handbook: Management: Third-Party Management ..	69
Reference 6: History of shared system centers	71
Reference 7: Timeline of use of shared system centers	72
Reference 8: Deposits of Financial Institutions using shared system centers	73
Reference 9: Issues addressed by this Council and related measures	75

Introduction

In recent years, reliance on outsourcing of operations related to information systems has been at a very high level among Financial Institutions in Japan, and the forms of such operations have been growing more diverse, as seen in the example of the advancement of sharing of information systems through shared system centers.

At the same time, the Banking Act and other relevant laws and regulations have been amended to add subcontractors handling the operations of banks and other Financial Institutions to the subjects of demands for reports and on-site inspections by regulators, and there is a need to review the forms of subcontractor management. In addition, increasing numbers of Financial Institutions face the challenges of training and securing human resources with skills in information technology (IT) in connection with developments such as the advancement of joint use of information systems.

As described above, the conditions surrounding outsourcing of information systems have undergone massive changes in recent years. Since each of these issues is very deep rooted and few can be resolved by information systems sections alone, the first necessary step is that of thinking of companywide initiatives that include top management – that is, IT governance.

Two years ago, the Center for Financial Industry Information Systems (“FISC” hereinafter) held a meeting of the Council of Experts on the Usage of Cloud Computing by Financial Institutions to ascertain accurate information on the distinguishing features and risks of use of Cloud technology by Financial Institutions and discuss the form to take for security measures to maximize the potential of such state-of-the-art technologies while minimizing their risks. After publishing a report on the results of the Council, that report served as the basis of revisions to the Security Guidelines on Computer Systems for Banking and Related Financial Institutions (“Security Guidelines” hereinafter) to enhance risk-management measures for the Cloud, as a form of outsourcing.

The Council of Experts on Outsourcing in Financial Institutions was established in consideration of the need to address the above issues and review management measures with regard to more general outsourcing such as that of banks’ and companies’ own systems and use of shared system centers, in a form consistent with the concepts of the Cloud as a specific form of outsourcing.

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 meeting discussed the need to identify clear and practical guidelines regarding policies to contribute to increasing the efficacy of external outsourcee management through thoroughgoing study of the form of external outsourcee management at Financial Institutions in Japan from perspectives including those of IT governance and a risk-based approach. These deliberations are summarized in this report.

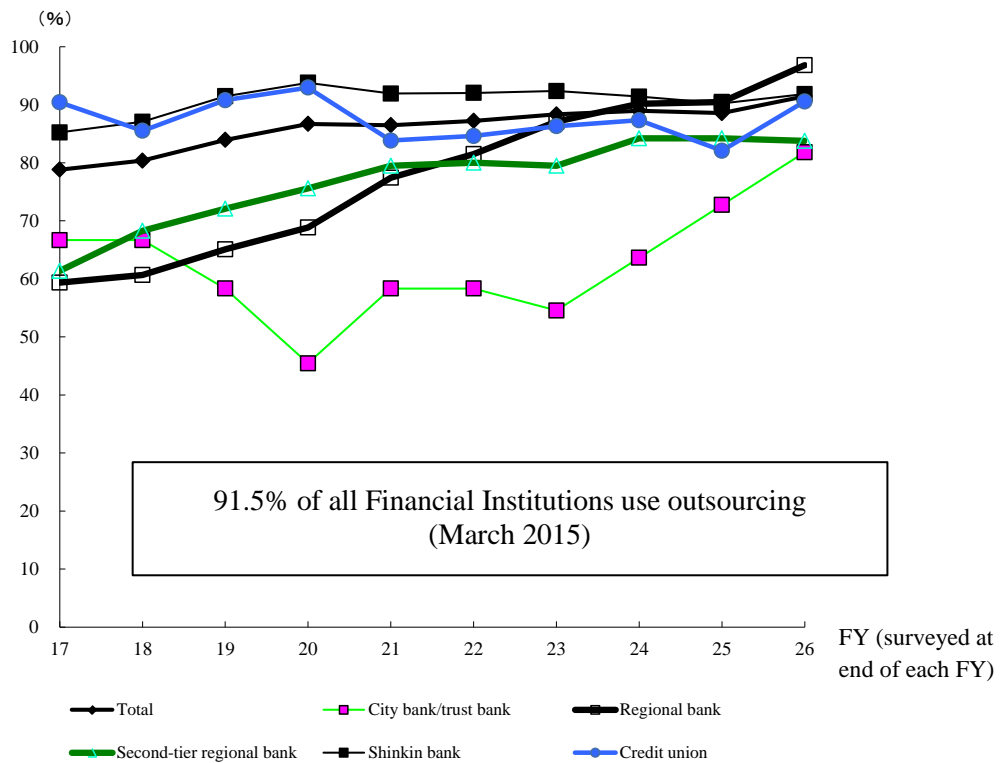
I. Trends in outsourcing in recent years and changes in environmental conditions of outsourcing

1. Trends in outsourcing in recent years

Recent years have seen marked progress in outsourcing of operations related to computer systems by Financial Institutions.

- A share of 91.5% of all Financial Institutions use outsourcing in core banking systems (as of March 2015).

(Fig. 1) Trends in outsourcing (from FISC survey)



(Fig. 2) Methods of outsourcing of backbone systems by deposit-taking Financial Institutions
(As of March 31, 2015; from a FISC survey)

System implementation (development) method	System operation method (installation location)	Financial Institutions using shared system center etc.(FISC members)
(1) Proprietary systems I. Developed in-house (proprietary specifications) II. Use of existing software packages (including partial customization)	Private data center On premises	Leading banks etc.*1 10 New form banks 5 Trust banks 6 Regional banks 5 Tier-2 regional banks 14 Credit unions 10 + Shinkin Central Bank Credit cooperatives 1 + Shinkumi Federation Ban
	Subcontractor data center Sometimes used as a backup center	Subcontractor data center
(2) Joint centers Joint use of the same system by multiple financial institutions (sometimes partially customized)		
(3) Cloud services	Subcontractor data center	—

*1 Leading banks etc. include Japan Post Bank, Shoko Chukin Bank, and Norinchukin Bank

2. Changes in environmental conditions of outsourcing

The environment for outsourcing has experienced massive changes recently.

(1) Cases of misconduct in recent years at outsourcees etc.

Risk management for outsourcing has been reviewed and FISC Security Guidelines have been revised in response to cases of misconduct by skilled management at Financial Institutions' subcontractors and sub-subcontractors. In addition, management measures and expertise are being accumulated in individual fields of outsourcing as well.

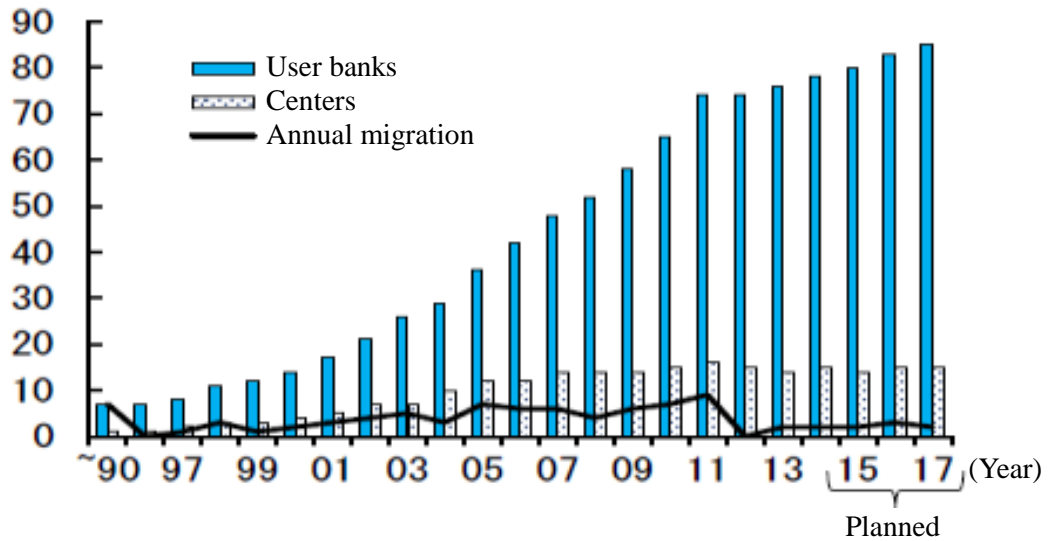
(Fig. 3) Main cases in recent years and related trends

Announced November 2012	Counterfeiting of ATM cards by an employee of a shared system center outsourcee
Announced February 2014	Counterfeiting of ATM cards by an employee of a regional bank's sub-subcontractor
March 2014	Financial Services Agency demands self-inspection by Financial Institutions

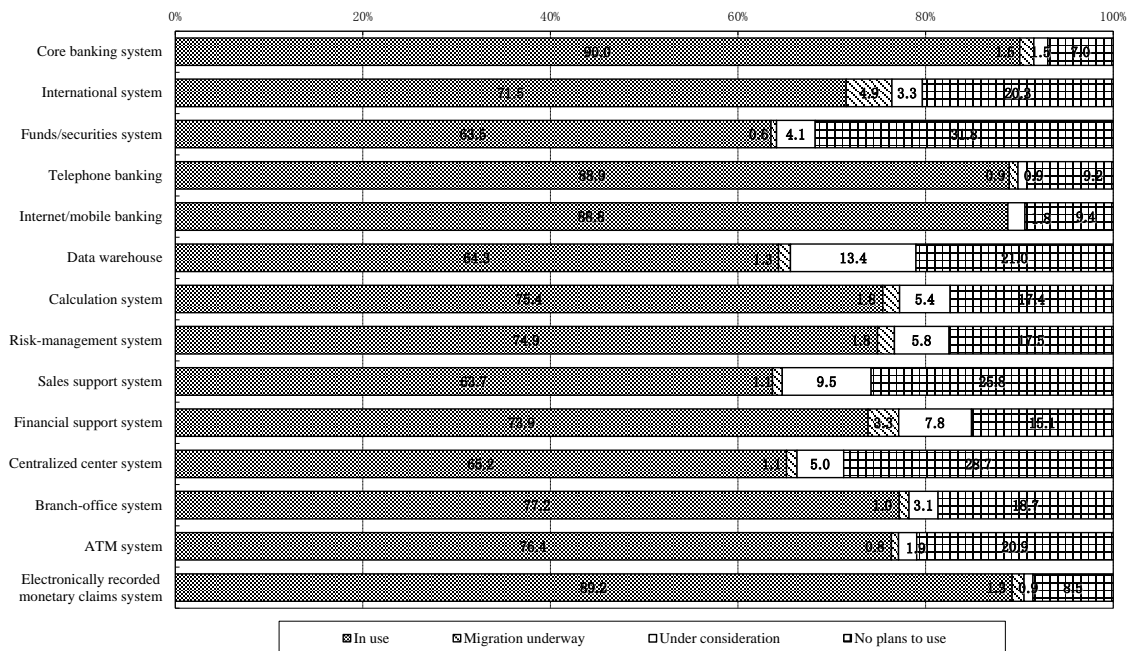
(2) Advancement of joint use

Joint use of systems is increasing across various types of business and subject operations, intended to enjoy better cost benefits than individual outsourcing and to enable use of expertise of early adopters, among other considerations.

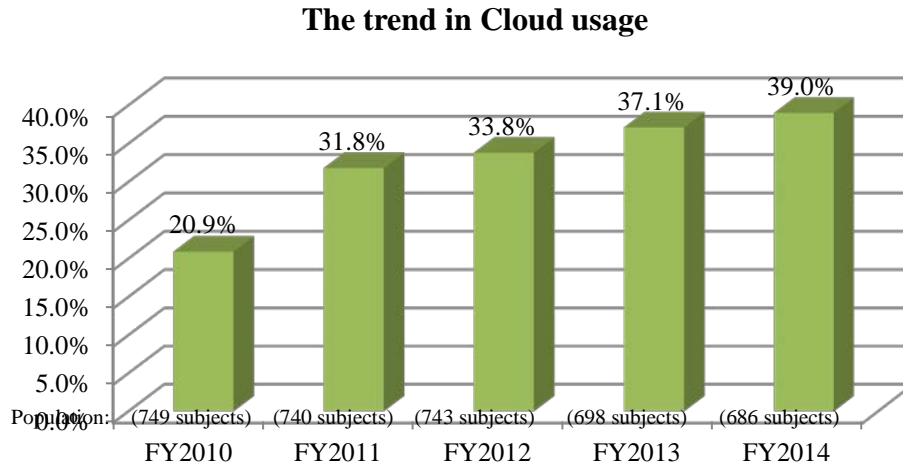
(Fig. 4) Advancement of joint use of accounting systems (regional banks, second-tier regional banks)
(From the July 2014 Financial Services Agency Financial Monitoring Report)



(Fig. 5) Shared system centers are used for numerous systems
(Deposit-taking Financial Institutions) (from 2015 FISC survey)



(Fig. 6) Use of the Cloud also is in an increasing trend
 (Deposit-taking Financial Institutions, insurance, securities, credit, etc.) (from FISC survey)



(Fig. 7) Use of the Cloud is advancing in the insurance industry
 (From the 2015 Financial Services Agency Monitoring Report)

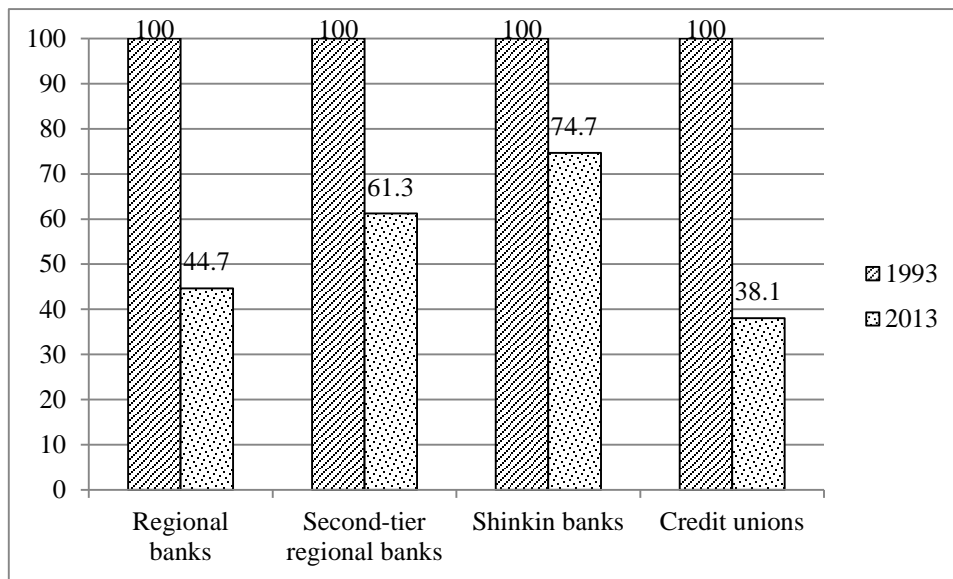
	Percentage of use	Among big four
Life insurers (42 companies)	83%	75%
Non-life insurers (33 companies)	76%	100%

(3) Necessity of human-resources development

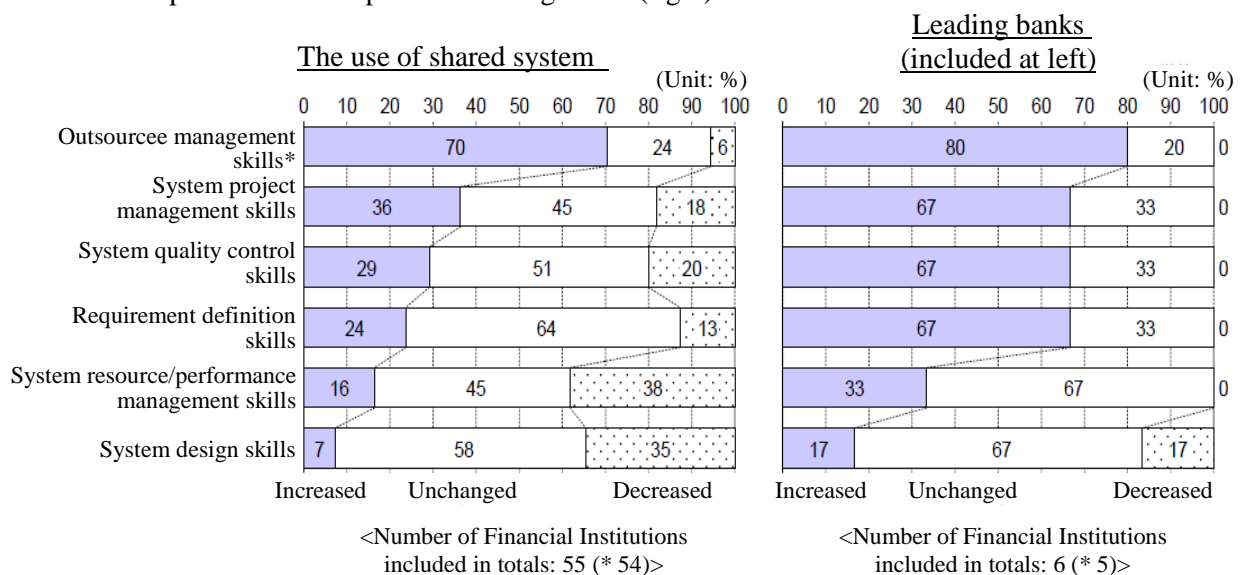
Advancing shared use of computer systems has led to the issue of decreased IT skills within companies as their IT human resources decrease.

In addition, the Policy Approaches to Strengthen Cyber Security in the Financial Sector released by the Financial Services Agency in July of last year identifies the issues of securing and training skilled personnel, calling for raising awareness and training on the knowledge needed by cyber human resources not only among engineers but also among top management responsible for decision-making and organizational direction and staff in the administrative sections that support them.

(Fig. 8) Trends in numbers of staff in IT sections; rate as of end of FY2013 vs. level of 100 at end of FY1993 (2014 FISC survey)



(Fig. 9) Changes in bank staff skills accompanying adoption of shared systems (2009 Bank of Japan report Results of Survey of 108 Regional Banks)
Decreases in skills among those participating in shared system use (left) are pronounced compared to leading banks (right).



(4) Various issues related to subcontractor management (amendments to the Banking Act etc. ¹)

While individual Financial Institutions face the need to demand management responsibility and accountability from subcontractors and those further upstream in the supply chain, in some

¹ Subcontractors in banking and other businesses (including those covering two or more levels) have been added to those from whom reports may be demanded and the subjects of on-site inspections (effective December 1, 2014).

cases the extent to which these should be demanded is not clear, leading to an increasing sense of burden.

3. FISC initiatives through now in response to these environmental changes and this Council's recognition of issues

(1) Cases of misconduct by outsourcees and others in recent years

➤ FISC initiatives

Following deliberation by the FISC Security Measures Export Committee/Study Meeting last year, in June of last year the Security Guidelines were revised and appropriate measures were implemented as interim responses for the time being with regard to areas such as strengthening control of entry to and exit from computer rooms, making access authorization for computer systems stricter, and identifying and preventing unauthorized use.

➤ Recognition of issues

- With regard to basic response measures including the risk-management approach, there is a need for separate discussions from perspectives including those of IT governance.
- The following issues have been pointed out in response to cases of misconduct involving shared-use systems.
 - The need for Financial Institutions using shared system center to develop a posture of demonstrating governance jointly
 - The need for joint auditing

There is a need to consider matters including these in discussion of outsourcing itself, while maintain consistency with Cloud risk-management measures.

(2) Advancement of joint use

➤ FISC initiatives

With regard to the Cloud, as one form of outsourcing, risk-management measures for the Cloud (i.e., clarification of IT solution provider selection procedures and ascertaining locations of data when considering use; agreement on SLA and measures to prevent vendor lock-in when concluding agreements; measures to prevent leakage of data during use of services; formulation of structures including those for independent auditing and monitoring; and simplified risk-management measures corresponding to the importance of operations) were enhanced through revisions to the Security Guidelines following the Council of Experts on the Usage of Cloud Computing by Financial Institutions.

➤ Recognition of issues

There is a need for review of the ideal form of more general management measures for outsourcing based on the opinions from the above the Council of Experts on the Cloud.

(3) Necessity of human-resources development

➤ FISC initiatives

The FISC Research Division and the Financial Services Agency are carrying out joint research on IT human-resources development, through steps that include identifying practical training plans and implementation methods and making clear the importance of incorporating IT human-resources development into medium- and long-term plans.

➤ Recognition of issues

There is a need to make clear the IT skills and scale of the workforce needed by individual

Financial Institutions in order to achieve their management objectives and business objectives and to think about how to formulate HR plans to secure these resources on a continual basis and how to realize these plans through the engagement of top management.

(4) Various issues related to subcontractor management (amendments to the Banking Act etc.)

➤ Recognition of issues

The ideal form of subcontractor management needs to be reviewed in connection with expanded inspection authority resulting from amendments to the Banking Act and other laws and regulations.

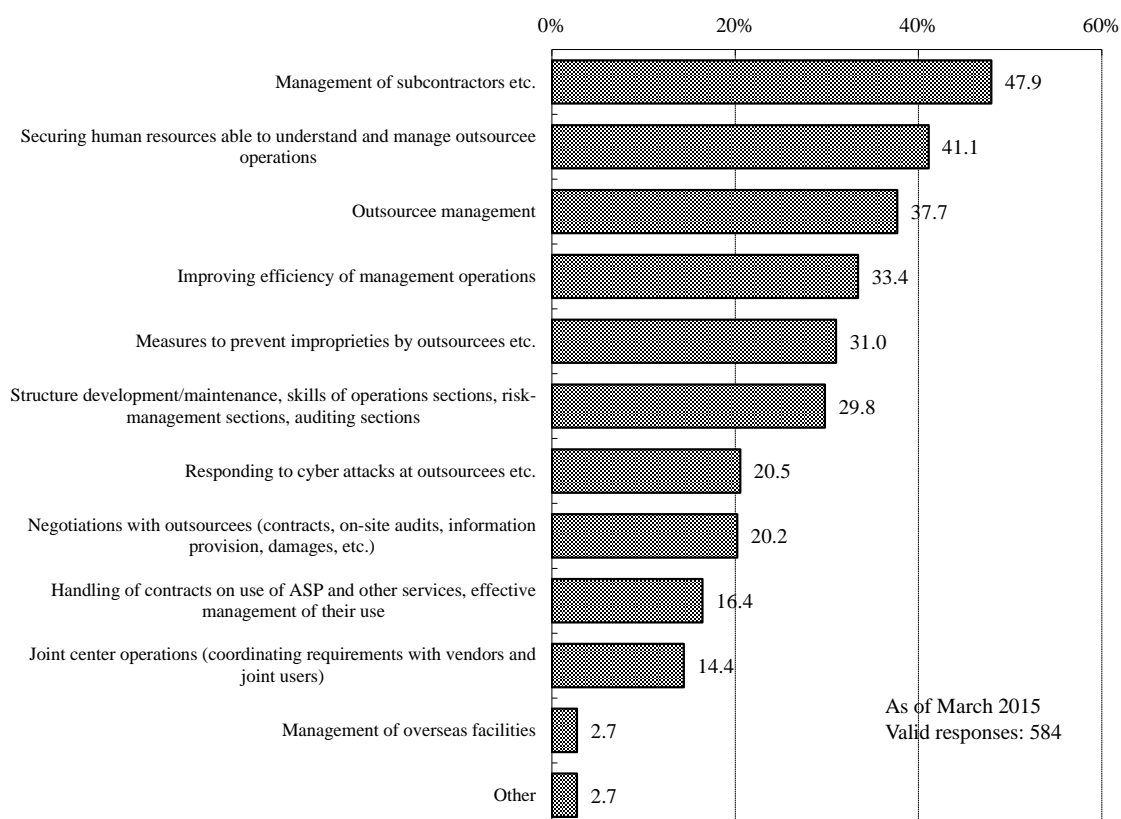
4. Necessity of studying IT governance

Each of the above matters is related to Financial Institutions as a whole, and the perspectives of IT governance – that is, appropriate involvement by top management based on assessment of each individual risk, are essential in order to address these properly.

(Fig. 10) Recognition of the issues faced by Financial Institutions in external outsourcee management

These include issues for which the engagement of top management is essential, including subcontractor management and securing human resources.

(Deposit-taking Financial Institutions, insurance, securities, credit, etc.) (From a 2015 FISC survey)



For purposes of these studies, the following definitions of IT governance are referred to.

The Financial Services Agency's definition (from the July 2015 Financial Services Agency Monitoring Report)

Management's approach to ensure timely and appropriate investment in computer systems in key areas for purposes of management strategy, efficient and stable operation of systems adopted, and proper control of these and addressing them as an organization

The IT Governance Institute's definition (also used in the Federal Financial Institutions Examination Council [FFIEC] guidelines)

IT governance is an integral part of governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives.

In addition, various domestic and international guidelines primarily consider outsourcing of computer systems to be a domain of IT management, stressing IT management together with IT governance.

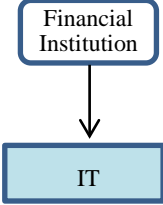
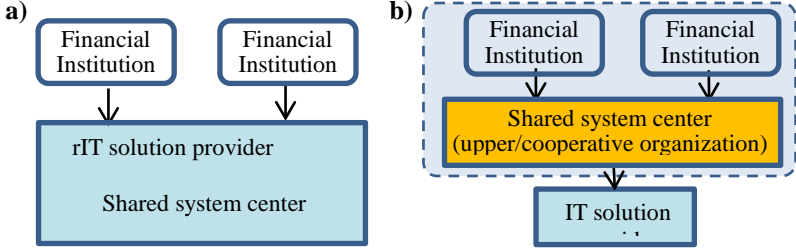
Perspectives such as these also are referred to in these studies.²

² In addition, the governance processes (assessment, instruction, and monitoring) defined in ISO38500 (IT Governance) and elsewhere also were referred to. Among ISO standards, ISO27014 (Information Security Governance) was referred to as well.

5. Overview of outsourcing

The table below summarizes the concept of outsourcing assuming subcontracting by Financial Institutions to IT solution providers or their use of IT solution providers' services.

(Fig. 11) Scope of outsourcing related to computer systems

Subject	Type A: Subcontracting (development, operation), or use of services, by individual Financial Institutions from IT solution providers	Type B: Subcontracting (development, operation), or use of services, by multiple Financial Institutions from IT solution providers (Including cases in which upper or cooperative organizations serve as liaisons with outsourcees)
Related parties	Financial Institution : IT solution provider = 1:1	Financial Institution : IT solution provider = n:1
Models		
Specific examples	<ul style="list-style-type: none"> • Development and operation of in-house systems (including outsourcing) (Including customization of packages) • Hardware/software maintenance 	<p>a) Cases in which Financial Institutions contract with IT solution providers</p> <ul style="list-style-type: none"> • Accounting shared system centers (Regional banks, Second-tier regional banks, Shinkin banks, Credit unions, etc.) • Internet-banking shared system centers (ANSER etc.) • Joint CMS³ • The Cloud • Data storage services <p>b) Cases of contracting with IT solution providers through upper or cooperative organizations</p> <ul style="list-style-type: none"> • SBK⁴ • R-one system⁵ • JASTEM⁶

Notes:

1. Handling of mutual systems and network services among Financial Institutions

Cases of use of mutual systems and network services among Financial Institutions (such as the Zengin system, integrated ATM networks, and cooperative domestic-exchange relay systems for Financial Institutions⁷) are specified under the supervision guidelines of the Financial Services Agency as being subject to risk management similar to that used for outsourcing, and these can be considered separately from outsourcing.

⇒ Types A and B above can be said to differ for the following reason: While when

³ A center established jointly by leading Financial Institutions including city banks to provide multibank firm-banking services

⁴ A business association (shared system center) under which six second-tier regional banks in the Kyushu region jointly manage a systems center

⁵ Used by 13 Labour banks and the Rokinren Bank, established by the Rokinren Bank

⁶ A system used by agricultural cooperatives and their banks across Japan, operated by the Norinchukin Bank

⁷ The ZenShinkin System (for Shinkin banks), the funds transfer system for credit unions, and the funds transfer relay system for agricultural cooperatives

connecting to other parties measures are demanded such as checking whether the system employs appropriate handling and reciprocal testing at times such as when starting or updating connections, demands do not extend to the level of ascertaining the state of operations at the other parties (FISC Security Guidelines Operations 90-1).

These networks function as backbone infrastructure, and in many cases it would be difficult and inefficient for individual Financial Institutions to select service providers and manage them individually to the exact same degree as in management of outsourcing.

Other major systems that can be considered to fit into this category include the following: SWIFT, LINC,⁸ Sompo Net,⁹ CAFIS

2. Handling of systems other than the above

Systems such as BOJ-NET, Densai.net, the Japan Securities Depository Center system, and stock exchange systems, which do not fit into the above categories, can be considered to be forms of systems that differ from types A and B and those described under Note 1 above, as systems managed as the business operations of the individual independent organizations operating them.

⁸ Life Insurance Network Center operated by the Life Insurance Association of Japan

⁹ Operated by the General Insurance Association of Japan

II. IT governance and IT management

Summary

- ◆ Top management must perform the following roles and responsibilities in IT governance necessary for security measures:
 - (1) Deciding on priorities related to security measures in medium- to long-term plans etc.
 - 1) Deciding on policies related to security measures
 - a. System strategic policies
 - b. System risk-management policies
 - c. Goals of security measures
 - d. Management resources to be invested in security measures
 - 2) Deciding on business-execution and monitoring structures related to security measures
 - (2) Deciding on matters for improvement in approaches etc. to security measures
- ◆ Management and other related parties must perform the following roles and responsibilities in IT management necessary for security measures:
 - (1) Management
 - 1) Development and maintenance of internal rules, organizational structures, etc.
 - 2) Deciding on security measures for individual information systems
 - 3) Review of internal rules, organizational structures, etc.
 - 4) Reporting to top management on information needed for security measures
 - (2) Management planning
Supporting decision-making by top management as necessary, through means including assessing priorities related to investment of management resources
 - (3) Users
Planning business models with consideration for security measures, achieving results of investment, identifying business requirements
- ◆ Top management needs to note the following points in formulating personnel plans:
 - (1) They must ascertain the state of IT human resources in specific terms including not only the numbers of personnel needed but also their quality.
 - (2) They must formulate medium- to long-term human-resources development plans reflecting the current conditions of IT human resources.
- ◆ Depending on the content of priority matters, the extent of top management making these decisions may be interpreted broadly to include not only the board of directors but also directors, executives, and others who have been delegated authority.

1. IT governance necessary for security measures

Roles and responsibilities of top management in information-system security measures

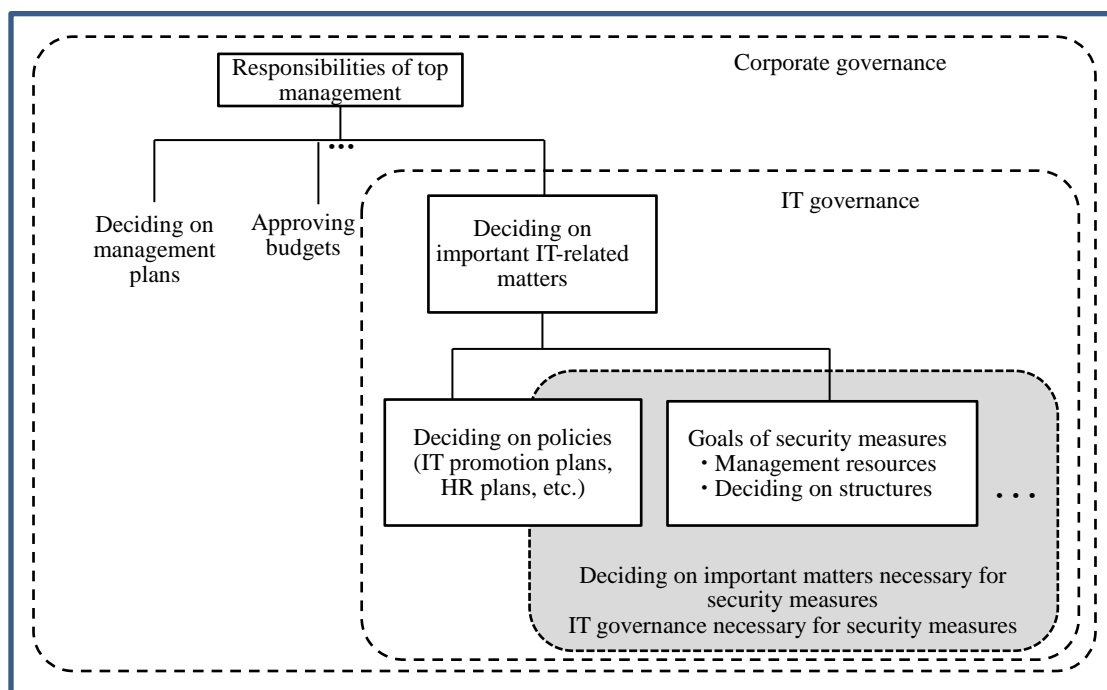
(1) Significance of IT governance necessary for security measures

Since the activities of Financial Institutions and other organizations are highly dependent on information systems, securing the security and stability of information systems is an important topic of management to such organizations. For this reason, IT governance needs to function properly so that top management¹⁰ can respond to such matters appropriately.

In general, IT governance refers to a system supporting decision-making by top management with regard to important IT-related matters within the corporate governance¹¹ system. Since they are related to the fundamentals of activities by Financial Institutions and other organizations, information-security measures and other security measures are matters that should be handled with a particularly high priority among the range of important matters related to information systems. (See Fig. 12.)

Accordingly, all members of top management of Financial Institutions and other organizations, not just the directors responsible for computer systems, bear identical levels of responsibility for ensuring the functioning of IT governance necessary for security measures.

(Fig. 12) Hierarchy of IT governance



¹⁰ Directors (including directors responsible for systems) and officers who are members of the boards of directors and similar bodies (including boards of executive officers, management conferences, risk-management committees, and other organizations making management decisions) at Financial Institutions and other organizations. For cooperative Financial Institutions, the provisions and terminology of the applicable laws or regulations apply in accordance with the type of financial institution. The FISC Security Guidelines define top management as the board of directors (executive board) etc.

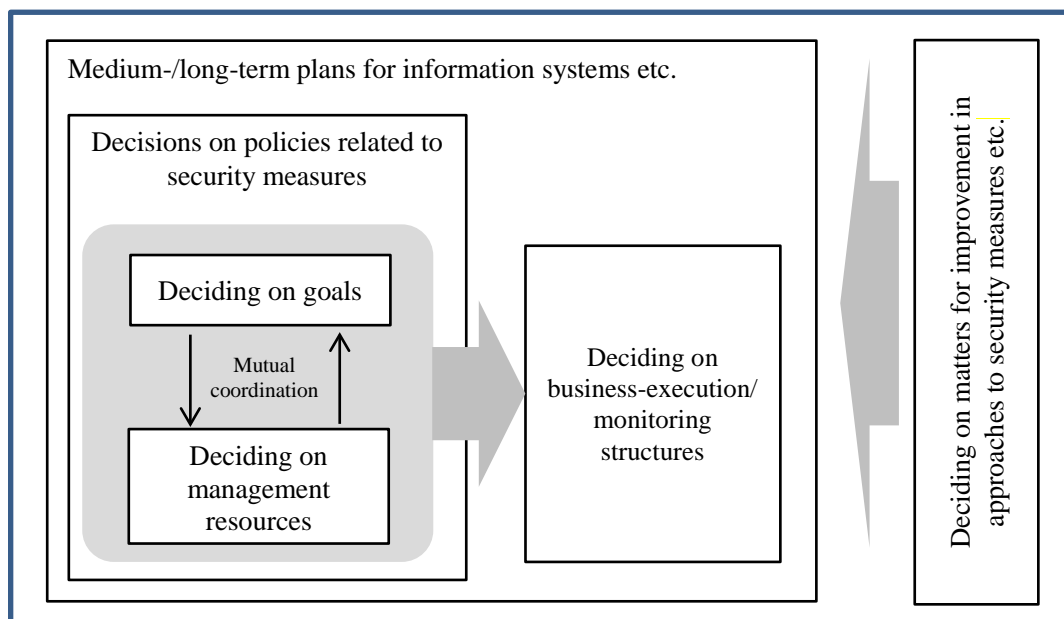
¹¹ The Draft Code of Corporate Governance (March 5, 2015) by the expert meeting on formulation of the Code of Corporate Governance in the Financial Services Agency defines this as “the structure by which a company makes decisions that are transparent, fair, speedy, and decisive reflecting the standpoints of shareholders as well as customers, employees, local communities, and others.”

(2) Roles and responsibilities of top management in IT governance necessary for security measures

Top management of Financial Institutions and other organizations, who are responsible to customers, shareholders, and other stakeholders in light of such organizations’ missions in society, need to understand fully the importance of security measures for information systems and make decisions on key related matters, to ensure the security and stability of information systems. (See Fig. 13.)

For this reason, top management needs to fulfill mainly the following roles and responsibilities in IT governance necessary for security measures.

(Fig. 13) Important matters related to security measures to be decided by top management



1) Making decisions on priority matters related to security measures in medium- and long-term plans etc.

Top management needs to make the following decisions on priority matters related to security measures in medium- and long-term plans and similar plans concerning information systems, as priority topics.

a. Deciding on policies related to security measures

The board of directors needs to make decisions on the following policies as one category of IT-related priority matters, including security measures.

i. Decisions on strategic policies for computer systems

Decisions need to be made on the following matters regarding strategic policies for information systems, based on the perspective of security measures¹² include:

- IT promotion plans
- Plans for investment in computer systems

¹² Examples include clearly indicating the goals of security measures and costs necessary to achieve those goals in policies on outsourcing (e.g., use of the Cloud, standard outsourcing, etc.), basic update plans, etc., or clearly indicating in personnel plans numbers of personnel needed in organizations involved in system risk management and countering cyber-attacks.

- HR plans intended to secure IT human resources
- ii. Decisions on system risk-management policies
 Decisions need to be made on the following matters regarding system risk-management policies, based on the perspective of security measures include:
- Development and maintenance of internal rules related to security measures, including security policies
 - Development and maintenance of the information-security management posture (including the posture for responding to cyber-attacks)
- iii. Decisions on goals to be achieved by security measures
 Top management shall make decisions on the goals of security measures to be achieved by Financial Institutions and other organizations. In deciding on goals to achieve, top management, in recognition of the fact that matters such as the extent of the impact of a deficiency or other problem could be quite large depending on the information system, shall set high goals to be achieved for information systems on which a deficiency could have severe impacts on customers, shareholders, or others while also setting suitable goals to be achieved for information systems whose impacts would be limited to within specific departments of the institution. In this way, they need to consider setting goals suited to the nature of risks. Even in these cases, it also is necessary to ensure that no major security vulnerabilities remain.
- iv. Decisions on management resources invested in security measures
 At the same time it decides on goals to be achieved by security measures, top management shall make decisions on investment of the management resources (costs, allocation policies, etc.) necessary to achieve those goals. Recognizing the fact that management resources have limits, it is important that top management consider in advance goals reflecting the management resources that the organization possesses and make decisions on allocation of resources in accordance with the nature of risks.
 In addition, in deciding on investment of resources it is necessary to pay attention to the sources of raising resources based on matters such as changes in the environmental conditions related to information security and other security measures. In particular, it must be noted that in outsourcing, one means of securing resources from outside the organization, in some cases it might be more difficult to apply internal controls due to the narrower scope and depth of information that can be ascertained directly compared to a case of securing resources internally.¹³
- b. Decisions on business-execution and monitoring structures related to security measures
 As necessary, top management must make decisions on policies for development and maintenance of business-execution structures for systems sections and other sections and monitoring structures including system audits, based on the goals to be achieved by security measures and the content of management resources invested.
 Among business-execution structures, management supervising business execution related to information systems shall develop and maintain the internal rules and organizational structures needed to implement the decisions of top management

¹³ It also must be noted that in some cases, such as when they are considered one of a number of group member companies under the umbrella of a holding company, Financial Institutions and other organizations might formulate internal plans for group member companies as well.

concerning security measures, assign IT personnel, decide on security measures for individual information systems, and verify their efficacy. Furthermore, management shall occupy a position between top management and executing sections, fulfilling the roles of properly conveying the decisions of top management to the executing sections and swiftly and accurately communicating to top management the state of information systems related to security measures. In these ways, as what could be described as the core of IT management members of management bear important roles and responsibilities, and for this reason it is recommended that top management choose as members of management officers and employees who possess sufficient knowledge and experience concerning security measures and other aspects of information systems as well as knowledge concerning all aspects of the businesses of the Financial Institutions and other organizations (including risk management and auditing).

Top management also needs to develop and maintain structures for system audits and, based on its own decisions, have system auditing sections inspect and assess the IT management (e.g., business-execution structures) necessary for security measures to confirm that it is functioning appropriately and provide advice on improvements.

2) Deciding on improvements to approaches etc. related to security measures

After verifying, through means such as reports from management and system audit reports, whether IT management is functioning properly in accordance with its own decisions on priority matters, top management must make decisions on improvements as needed and improve approaches and other matters related to security measures on a continual basis.

2. IT management necessary for security measures

— Roles and responsibilities of other parties related to security measures for information systems —

In security measures for information systems, multiple related parties perform their necessary functions as illustrated below, under the IT governance of top management. (See Fig. 14.)

IT management refers to matters such as the management by members of management of business execution related to IT by the executing sections for information systems (e.g., those responsible for systems and for system risk management), based on IT governance by top management.

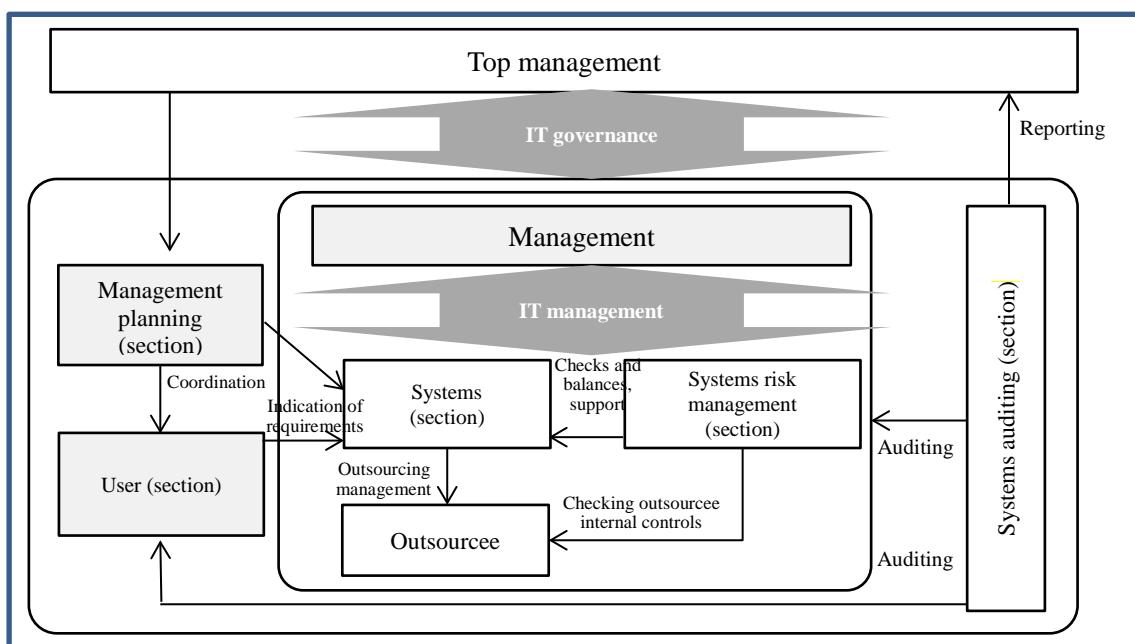
To implement the decisions of top management concerning security measures, management shall develop and maintain the necessary internal rules and organizational systems as well as making decisions on security measures for individual information systems and verifying their efficacy. Furthermore, management shall occupy a position between top management and executing sections, fulfilling the roles and responsibilities of properly conveying the decisions of top management to the executing sections and swiftly and accurately communicating to top management the state of information systems related to security measures.

The executing sections for information systems (e.g., those responsible for systems and for system risk management¹⁴) are responsible for security measures under this management structure. However, parties other than such executing sections, such as those responsible for management planning, whose tasks include assessing priorities for investment of management resources, and users whose tasks include planning business models, also play important roles in security measures.¹⁵

¹⁴ Although not shown in Fig. 14, the section handling general management of operational risk plays roles including assessment and judgment of the status of system risk based on reports received from the system risk section. In addition, the roles of the public relations section include swift disclosure of information in the event of severe system trouble or similar problems.

¹⁵ Under a model based on three lines of defense, management planning, systems, and users in the graph would be the first line of defense (administration of business lines), system risk management would be the second line of defense (as an independent function managing companywide operational risk), and system auditing would be the third line of defense (independent review). Concerning parties related to operational risk in general, see *Operational Risk – Supervisory Guidelines for the Advanced Measurement Approaches* (Basel Committee on Banking Supervision, June 2011).

(Fig. 14) Parties related to information-system security measures (ex.)



(1) Roles and responsibilities of management¹⁶

Based on IT governance by top management, members of management supervise parties such as those responsible for systems and those responsible for system risk management and are responsible themselves for the IT management necessary for security measures. They also perform the role of swiftly and accurately providing top management with the information it needs for IT governance.

- 1) Development and maintenance of internal rules, organizational structures, etc.
Together with development and maintenance of the rules, manuals, and related materials, including system risk management rules, necessary for security measures, system risk management sections shall be established and security management, system management, data management, network management, and other relevant management shall be appointed, and the necessary organizations and structures shall be developed and maintained. In addition, approaches to training and education shall be developed and maintained for the purposes of the IT human-resources development necessary for purposes such as system risk management and cyber security.
- 2) Decisions on security measures for individual information systems
Management measures for individual information systems shall be decided on based on the goals for achievement and resource investment plans decided on by top management for security measures.
- 3) Review of internal rules, organizational structures, etc.
Together with continual monitoring of the state of execution of the duties of those responsible for system risk management, the efficacy of the posture toward system risk management shall be verified and internal rules and organizational structures reviewed as

¹⁶ The description here focuses not on practical roles but on functions (roles and responsibilities) needed for security measures. In fact, roles and responsibilities of officers and employees performing management functions may be decided individually in accordance with the actual conditions of each financial institution or other organization.

- necessary.
- 4) Reporting to top management on information needed for security measures
 - a. Occurrence of incidents with severe impacts on management or markedly detrimental to the interests of customers
Examples of report content: As needed: Occurrence of severe system defects, occurrence of cyber-attacks, delays in important development projects
 - b. Status of system risk management
Examples of report content: Periodic: Status of achievement of goals of security measures, results of assessment of system risks, results of BCP drills, results of inspection of security measures
 - c. Content of improprieties or scandals at other firms
Examples of report content: As needed: Results of assessment of the Company's own security measures in reference to cases such as information leakage at other firms
 - d. Control methods related to important system risks
Examples of report content: As needed: Development and maintenance of approach to cyber security, revisions to contingency plans
 - e. Progress on individual development projects, reflecting system importance and properties
Examples of report content: Periodic: Status reports on important development projects (e.g., progress, quality, investment amounts, issues)
 - f. Results of checking the status of management by high-impact outsourcees, and problems identified
Examples of report content: Periodic: Results of assessment of existing outsourcees (e.g., technological capabilities, response capabilities, quality, internal controls)
As needed: Results of assessment related to selection of outsourcees
 - g. Results of comprehensive auditing and assessment of systems by an independent system auditor
Examples of report content: As needed: Results of auditing of system sections etc., results of auditing of important outsourcees
etc.

(2) Roles and responsibilities of those responsible for management planning

This refers to the organizations or staff involved in management strategies and tasks such as allocation of management resources. They are usually assigned to management planning sections. They provide support for decision-making by top management on system development projects including security measures, by assessing priorities related to investment of management resources as necessary, based on the results of adjustments made between sections.

(3) Roles and responsibilities of users¹⁷

This refers to the organizations or staff involved in planning of matters such as business models (for products, services, and administration) to implement management strategies, in the head-office sections responsible of Financial Institutions and other organizations. They do not include branches and other offices using systems. Users' main roles and responsibilities in security measures are outlined below.

¹⁷ At Financial Institutions and other organizations that permit end-user computing (EUC), users and systems staff are assigned to the same sections. In addition, depending on the type of business and other matters, in some cases some roles and responsibilities of users will be handled by systems staff.

- 1) **Planning business models with consideration for security measures**
 In light of their positions on the front lines in deciding the shape of information systems, users need to plan business models with consideration for security measures while working together with other parties including those responsible for systems and those responsible for system risk management, for example by ensuring that such business models do not include factors that would threaten the security and stability of information systems or including in them controls for the secure and stable operation of information systems.

- 2) **Achievement of results of investment**
 To achieve management strategies, each user shall make requests to management and others regarding system development projects needed in the operations for which it is responsible, including security measures. In doing so, users shall be accountable to management and others with regard to matters such as the usefulness of the system project and its suitability to purpose with regard to management strategies. Users remain accountable to management and others regarding the results to be achieved through the system development project in particular, including making clear projections of such results at the time of planning the system and reviewing whether the projected results have been achieved after the system goes online.

- 3) **Identification of business requirements¹⁸**
 When their requested system development project such as one involving security measures has been approved by top management, management, or others, users are responsible for identifying to those responsible for the system its business requirements, at the time system development begins. If there has been a change in business requirements during the system development process after initially providing such requirements, those responsible for the system shall be informed of the content of such changes in a timely and appropriate manner, and then those responsible for the system shall make the judgment of whether or not to accept the changes based on assessment of the impact of a change taking place during system development. Even after completion of system development, users remain responsible for the content of business requirements that they had identified.

3. Notes on staffing plans

In formulating staffing plans as a part of system strategic policies, top management must pay attention to the following matters.

- (1) Ascertaining numbers of staff, types of skills and their levels, and placement for purpose of realizing system strategies

Top management shall ascertain in specific terms the conditions of IT human resources, including not only the number of staff needed but also their quality, for maintenance and utilization of IT as the infrastructure of management of Financial Institutions and other organizations.

Personnel make up one important element of IT-related management resources, and just as with amounts of investment in information systems top management needs to ascertain their status and identify any gaps in the staffing necessary to implement system strategies.

¹⁸ At some Financial Institutions and other organizations, users not only indicate business requirements but manage the progress of system development as well.

Furthermore, they also need to ascertain in specific terms not only numbers of IT human resources but their quality (e.g., IT-related skills they possess and their levels, placement, etc.) as well. (See Materials Document 1.)

Depending on the type of Financial Institutions and other organizations, there also may be a need to consider the comprehensive possession of multiple skills by specific personnel in light of current conditions characterized by small numbers of personnel.

(2) Formulation of staff training plans in accordance with overall medium- and long-term plans

Top management shall formulate medium- and long-term human-resources development plans consistent with medium- and long-term management plans, reflecting the current state of IT human resources.

With regard to IT human resources, top management also needs to consider formulation of plans from the perspective of not just increasing numbers of personnel but human-resources development as well in cases such as when there are insufficient staff for implementation of system strategies.

In some cases the personnel subject to human-resources development as IT human resources may include personnel of Group member companies in addition to leaders, and there also is a need to give consideration to development and maintaining of an environment for such human-resources development.

In addition, in formulating plans consideration must be given to methods of assessment, treatment, and promotion of personnel as well.

4. Decision-making by top management concerning important IT-related matters

At the same time the number of choices in design of institutions has broadened in recent years, for example with the option of setting up a company with audit and supervisory committee, increasing numbers of Financial Institutions are adopting the holding-company structure as well, and the subject defined as “top management” in the Security Guidelines is likely to be interpreted broadly, to refer to more than just the board of directors.

In light of these circumstances, the form of decision-making by “top management” with regard to important IT-related matters has been organized as outlined below, reflecting a fact-finding survey.

(1) Deliberation and decision-making body on important IT-related matters

Since it is recommended that important IT-related matters reflect deliberation on subjects such as maximizing the efficiency of investment in information systems based on an overview of management resources as a whole, it is recommended that they should be decided on through deliberation by a conference or other body in which top management as a whole takes part.

In addition, although the financial groups surveyed by the Center indicate that their boards of directors were the decision-making bodies for such matters (see Fig. 15), since the majority of important IT-related matters concern business execution it is possible that they could be decided

on by bodies consisting of membership including directors, executives, and others in accordance with the actual circumstances of selection of institutions and delegation of authority,¹⁹ not just by boards of directors alone.

However, regardless of which institution is chosen, authority for decisions on fundamental matters should remain with the board of directors as a type of authority that may not be delegated, and it is conceivable that among important IT-related matters as well the board of directors should have authority for decisions on matters such as system integration policies and large-scale changes to systems.²⁰

(2) Actual state of decisions on important IT-related matters in financial holding companies and operating companies

Conceivable reasons why Financial Institutions establish holding companies may include the need for coordination among interests.²¹ The Center conducted a survey to see how decisions on important IT-related matters are made between the holding companies and operating companies in leading financial groups employing this financial holding-company structure (see Fig. 15). The survey's findings identified the following two tendencies, and it is thought that decision-making between the financial holding company and operating companies reflects the strategies and other characteristics of each group.

- Centralization of IT-related roles with the holding company
Information-systems personnel are centralized at the holding company and actual development is outsourced jointly to information systems subsidiaries, shared system centers, and others. In addition, IT-related decisions are made by an institution within the holding company, while decisions by the operating companies are minimized, limited to company-specific matters such as internal controls.
- IT-related roles performed by individual operating companies
Each subsidiary has its own information-systems personnel and conducts outsourcing individually. In addition, IT-related decisions are made by an institution within each operating company, while decisions by the holding company are minimized, limited to matters common across multiple group member companies.

¹⁹ In a company with a nominating committee, the board of directors is responsible chiefly for oversight, and in principle directors may not exercise business operations. Operating officers are responsible for business execution. In a company with an audit and supervisory board, decision-making authority on business operations may be delegated broadly from the board of directors to individual directors.

²⁰ Large-scale changes to systems refer to those that can be considered to involve degrees of risk roughly as high as those of system integration, such as redevelopment of a backbone system.

²¹ Shinsaku Iwahara's *Kinyu mochikabugaisha ni okeru group governance: Ginkoho to Kaishaho no kosaku (3)* ("Group governance in a financial holding company: Intricacies of the Banking Act and the Companies Act [3]") states, "Is it not the case that the financial holding-company structure is adopted most commonly when it is thought that the holding-company structure would be more appropriate than the direct-subsidiary structure for groupwide business administration? For example, even within megabank groups the share of businesses other than banking is increasing, leading to increasing numbers of issues that require coordination of interests with banking operations."

(Fig. 15) Study of actual state of IT governance corresponding to choice of institution

Financial group	Deliberation and decision-making on IT-related medium- and long-term plans etc.		Deliberation/ decision-making led by	Process of deliberation and decision-making between holding company and operating companies	System management structure
	Deliberating body	Decision-making body			
A	Management conference, via committee	Board of directors	Holding company	Deliberated and decided on by operating companies based on policies identified by the holding company, and then deliberated and decided on similarly by the holding company	Centralized management by holding company
B	Management conference, via committee	Board of directors	Holding company	Deliberated and decided on by operating companies after being deliberated and decided on by the holding company (Operating companies restricted to company-specific matters such as internal controls)	Centralized management by holding company
C	Management conference, via committee	Board of directors	Operating companies	Deliberated and decided on by operating companies individually (Chief duties of holding company are decisions on policies and rules and deliberation on some matters common to the entire group)	Individually operated by each operating company
D	Management conference	Board of directors	Split between holding company and operating companies by business	Joint management conferences held by holding company and operating companies (In the area of ICT, the holding company plays the leading role, with matters deliberated on simultaneously in joint management conferences. The leading party for non-ICT operations varies with the subject.)	Centralized management by holding company
E	Committee or management conference	Board of directors	Holding company	Management conferences of the holding company and operating companies held simultaneously (Operating companies play leading roles in decisions on some matters)	Centralized management by holding company
F	Committee	Board of directors	Holding company	After deliberation and decision by the holding company, operating companies deliberate and decide on the same content on another date	Centralized management by holding company
G	Management conference	Board of directors	Holding company	After deliberation and decision by operating companies following prior arrangements made between the holding company and the operating companies, the holding company deliberates and decides on matters and then issues instructions to the operating companies based on its decisions	Individually operated by each operating company

Examples of support for outside directors

- Assigning full-time staff to support outside directors
- Establishing a board of outside directors to share awareness of issues
- Having outside directors attend management conferences as observers
- Taking outside directors on site tours; etc.

III. Risk-based approach

Principles of decisions by top management and others on matters such as security measures for information systems

Summary

- ◆ The basic principles of security measures based on a risk-based approach are listed below.
 - (1) The goals to be achieved by security measures for information systems shall be decided on with sufficient content as necessary in accordance with the characteristics of the risks inherent to each information system.
 - (2) Allocation of management resources to security measures for information systems should be decided on by taking into consideration not only adjustments with new development and other efforts within the information systems budget, based on comparison with countermeasures taken after a risk has manifested itself, but also management resources as a whole, with the aim of maximizing corporate value.
 - (3) Security measures may be decided on independently only once appropriate decision-making and other activities are conducted and management is conducted properly in compliance with the above principles.
 - (4) For information systems owned by Financial Institutions and other organizations that involve serious externalities and information systems that contain sensitive information, in addition to the above considerations the goals to be achieved by security measures should be decided on by taking into consideration the externalities of such systems and the sensitive nature of the information they contain, from the relevant social and public perspectives.
- ◆ Based on the basic principles, it is recommended that Financial Institutions and other organizations aim to achieve “IT governance through a sufficiently risk-based approach.” In the process toward this goal, IT governance through a simplified risk-based approach may be employed, in which information systems are split into the two categories of “critical information systems” and “other information systems” and security measures are implemented individually for these two categories.
- ◆ Management responsibility in security measures based on the basic principles and other considerations is outlined below.
 - (1) The mission of top management is to maximize corporate value. This does not necessarily mean the pursuit of security measures aiming to eliminate all risks.
 - (2) For residual risks that remain as a result of aiming to maximize corporate value, there is a need to recognize such risks accurately and then respond to them by formulating contingency plans (“CPs” hereinafter) in accordance with their degrees and revising these in response to environmental changes.
 - (3) Top management should be considered to be fulfilling its legal responsibilities from an objective point of view only when it prepares CPs etc. for security measures and residual risks based on consideration of matters such as the Security Guidelines and other guidelines agreed upon in society (including the basic principles of security measures mentioned above) and responds as the occasion may require, based on the CPs, in the event of an incident, in addition to complying with various laws and regulations.

The Report of the Council of Experts on the Usage of Cloud Computing by Financial Institutions, issued by the Center in November 2014, recommends as the “recommended form of security measures” the “formulation of appropriate risk-management measures based on management’s own judgment, applying a risk-based approach.” These are intended to “maximize potential while keeping risks to a minimum, by ascertaining accurately the properties and risks of Cloud technologies.”

The term “risk-based approach” generally refers to the concept of putting to use the results of analysis of the properties of risks in rational decision making such as prioritizing of countermeasures. For this reason, the risk-based approach is an important concept in the pursuit of maximization of corporate value through maximizing the efficiency of decisions on allocation of management resources by top management of Financial Institutions and other organizations, not just applying to use of the Cloud only.

For this reason, in studying IT governance necessary for security measures related to outsourcing, this Council first will review the thinking behind existing security measures and then will propose some basic principles of security measures from a risk-based approach, referring to examples from abroad. Next, it will make clear matters such as IT governance in accordance with the basic principles of security measures. Furthermore, it also will propose the form that management responsibility should take in security measures.

In this way, this Council will identify clearly the form to be taken by new security measures based on a risk-based approach, together with the form that management responsibility should take. It is hoped that this will assist in balancing the sound growth of Financial Institutions and other organizations with the stability of the financial system, together with securing Japan’s competitive advantages in the financial businesses of the future.

1. The necessity of a new form for security measures

According to a survey by the Center, despite the fact that the environment in which financial institutions operate has been undergoing massive changes for more than 10 years, no major changes are apparent in the proportions of security measures, maintenance operations, and new development. For example, the proportion of new investment is low relative to that in other developed countries. (See Reference Material 2.)

While it is thought that the reasons for this are complex, the Council of Experts will examine first whether resources are allocated to security measures appropriately at present, from the perspective of the IT governance needed for security measures, starting from the underlying concepts of security measures.

(1) The necessity of reviewing the concepts of security measure standards

In considering security measures for information systems, Financial Institutions and other organizations in Japan use both the Financial Inspection Manual by the regulatory agency and the Center’s Security Guidelines, referring to the concepts of security measure standards at the beginning of the Security Guidelines concerning the forms of security measures.

Initially, the Security Guidelines was developed 30 years ago: The Center was established with the participation of related parties who possessed specialist and technical knowledge, including Financial Institutions and IT solution providers, to complement the efforts of individual Financial Institutions as their use of online technologies advanced, in light of the importance of the public nature and social responsibility of Financial Institutions while based on the principles

of self-responsibility and respect for their autonomy. It then formulated the first Security Guidelines.

Over the three decades since then, the standards in the Security Guidelines have been revised repeatedly, and today they are used widely among Financial Institutions and other organizations as common industry guidelines and the importance of security measures is well recognized. As such, they have fulfilled their initially expected role adequately.

At the same time, the roles expected of information systems in Financial Institutions and other organizations have been undergoing massive transformations with rapid progress in information technology, increasing diversity of computer configurations, and the need to secure competitive advantage for Japan's financial business in the future amid international competition, and as such the time has come to review the concepts of security measure standards, which have not undergone any massive changes in 30 years.

Under such conditions, it would be appropriate for the study of IT governance necessary for security measures in the Council of Experts on Outsourcing first to review the existing concepts of security measure standards and then to identify the form to be taken by new security measures suitable for the present time, reflecting trends in other developed countries.

(2) Traditional thinking on security measures and related issues

Looking back more than 30 years to when the Security Guidelines first were prepared, at that time Financial Institutions' information systems referred to backbone computer systems. There were almost no other information systems used in the industry, so that it was sufficient to focus thinking on backbone computer systems alone. For this reason, in their first edition 30 years ago the Security Guidelines identified as subject systems the "online systems of Financial Institutions and other organizations."

After that, due to advances in information technology the information systems used by financial institutions and other organizations no longer were limited to backbone systems alone, as other systems such as information-processing systems and section-specific systems increased in number and these came to account for a considerable proportion of the information systems as a whole. Their configurations also grew more diverse, ranging from host computers to client-server systems and cloud services.

Amid such environmental changes, although in the current eight edition the scope of the Security Guidelines still is identified as "online backbone computer systems," for "information systems other than online backbone computer systems," whose numbers are increasing and forms are diversified, it states merely that the Security Guidelines may be "adopted as appropriate" or based on "individual judgment in accordance with the importance of the services provided or information handled by the systems." As a result, the current environment is one of uncertainty in which no concept is identified for minimum security measures for other information systems, which make up a large proportion of all systems.

There are concerns that Financial Institutions and other organizations could face conditions such as the following as a result:

- In thinking about security measures for information systems other than online backbone computer systems, staff of Financial Institutions and other organizations might make choices biased toward security by thinking that it would be safer to apply uniformly to other information systems the same Security Guidelines as those established for online

backbone computer systems, instead of thinking independently about standards of application.

- Since the concepts of security measure standards do not identify the perspectives of upper limits on allocation of management resources to security measures or adjustments of allocation of management resources with new development, depending on factors such as the decision-making processes of top management of Financial Institutions and other organizations regarding allocation of management resources the choice of excessive security measures might ultimately be implemented without any changes.
- Under current conditions of uncertainty in which it could be held responsible directly for any severe system problems that could arise, top management might approve or pursue on its own excessive security measures in order to eliminate such problems as much as possible.

In these ways, the content of the concepts of security measure standards could lead to excessive security measures under current conditions, after more than 30 years have passed since their first edition.

(3) Risk-based approach

In the United States, the United Kingdom, and other developed countries abroad, the concept known generally as the “risk-based approach,” under which the results of analysis of the properties of risks are used in rational decision-making on subjects such as prioritizing countermeasures when Financial Institutions and other organizations make decisions on topics such as security measures and allocation of management resources, is a shared understanding among regulators and Financial Institutions and other organizations. (See Reference Material 3.) Its main distinguishing features are outlined below.

- It would be unreasonable to invest unlimited funds in countermeasures to prevent the manifestation of risks in pursuit of total elimination of all risks. This can be considered to be based on the idea that the closer an organization gets to a level of zero risks through investment of funds the smaller the results of additional investment and the concept of choosing the most economic course from comparison of the costs of investment in preventive measures and the costs of investment in countermeasures after the fact of manifestation of a risk. Under circumstances that management resources are not inexhaustible, it is needless to say that these ideas have rationality.
- Regulators do not necessarily codify in detail risk categorization methods and risk management measures, instead leaving these fundamentally to the discretion of Financial Institutions. This is because they employ a principles-based approach out of the belief that detailed codification might lead to overlooking of possibly better methods and impede innovation by financial institutions.
- Under such conditions, in guidelines on outsourcing and other matters regulators define operations such as important banking functions, shared services, and operations that have a strong impact on customers as priority operations and identify individual management measures for them. This can be surmised to reflect the social and public perspectives that since such operations making up part of the financial infrastructure involve both externalities and high risks it would not necessarily be appropriate to entrust all aspects of their management to Financial Institutions whose primary pursuit is that of maximal internal efficiency.

In light of the above considerations, the following section begins the discussion of the form of new security measures by explaining the basic principles of security measures as

important preconditions.

2. Basic principles of security measures

The basic principles of security measures for the information systems of Financial Institutions and other organizations, based on the risk-based approach, are described below.

- (1) The goals to be achieved by security measures for information systems shall be decided on with sufficient content as necessary in accordance with the characteristics of the risks inherent to each information system.
- (2) Allocation of management resources to security measures for information systems should be decided on by taking into consideration not only adjustments with new development and other efforts within the information systems budget, based on comparison with countermeasures taken after a risk has manifested itself, but also management resources as a whole, with the aim of maximizing corporate value.
- (3) Security measures may be decided on independently only once appropriate decision-making and other activities are conducted and management is conducted properly in compliance with the above principles.
- (4) For information systems owned by Financial Institutions and other organizations that involve serious externalities and contain sensitive information, in addition to the above considerations the goals to be achieved by security measures should be decided on by taking into consideration the externalities of such systems and the sensitive nature of the information they contain, from the relevant social and public perspectives.

(1)
The goals to be achieved by security measures should be decided on based on the results of analysis and assessment of the characteristics of the risks inherent to each information system. They also should be decided on with sufficient content as necessary while making adjustments for the state of management resources available. It is unreasonable to pursue total elimination of all risks.

(2)
Allocation of management resources to security measures is intended to cover the costs of achieving the goals of security measures; however, resources should not necessarily be allocated while giving security measures top priority. First, the costs of security measures and the costs of responding after manifestation of a risk without implementing security measures should be compared, with decisions made while also taking into consideration the option of taking risks. Next, adjustments should be made with other targets of allocation within the information systems budget, such as investment in new development. Lastly, consideration also should be given to adjusting allocation of management resources as a whole above and beyond the information systems budget. These adjustments are necessary for purposes of maximizing the efficiency of allocation of resources—that is, maximizing corporate value.

(3)
Top management, management, and others should carry out appropriate decision-making or proper management and supervision aiming to maximize corporate value while complying with principles (1) and (2) above. Security measures for information systems can be left to the discretion and independent decision-making of Financial Institutions and other organizations only if the organization as a whole is managed appropriately through these means.

(4)

Financial Institutions and other organizations constitute a part of the financial infrastructure, and in some cases they own information systems in which the manifestation of a risk could have a severe impact on customers and other Financial Institutions and other organizations, not just within the relevant organizations themselves. For this reason, the goals for achievement by security measures for such information systems involving serious externalities should be decided on taking into consideration not just internal impacts but external ones as well. However, since it is not easy for Financial Institutions and other organizations to assess external impacts on their own, there is a need for rules agreed to in society reflecting consideration for such serious externalities.

In addition, in some cases Financial Institutions and other organizations own information systems that contain sensitive information on subjects such as health and medicine. Since leakage of sensitive information could lead to wide-ranging losses through infringement of basic human rights and its handling has a social and public nature, there is a need for rules agreed to in society reflecting consideration for the sensitive nature of such information. (See Reference Material 4.)

The Center will play its necessary role in formulation of such rules agreed to in society.

The content of IT governance reflecting the above basic principles is described below.

3. IT governance in accordance with the basic principles

In order to maximize corporate value by pursuing maximal efficiency in allocation of management resources related to information systems, it is recommended that top management of Financial Institutions and other organizations fully understand risk-based approach in relevant decision-making and comply with the basic principles in security measures.

(1) Significance

This refers to top management, in deciding on policies related to security measures, categorizing information systems in accordance with their risk properties, considering allocation of management resources in pursuit of maximal efficiency, including new investment, based on the assessed results, and making comprehensive decisions on matters such as the goals to be achieved by the necessary security measures.

In consideration of allocation of management resources, under current conditions in which information systems are an important topic of management it is recommended that discussion of maximization of the efficiency of investment in information systems take into consideration all available management resources. For this reason, all members of top management, not just the directors responsible for computer systems, need to be involved in such decision-making and demonstrate appropriate IT governance. Furthermore, for this purpose it is recommended that top management involved in decision-making possess at least a minimum degree of knowledge concerning the information systems possessed by the financial institution or other organization and know about matters such as trends related information systems in general.

When top management demonstrates such IT governance in accordance with basic principles based on a risk-based approach, basically it is possible for Financial Institutions and other organizations to make choices on their own regarding matters such as the risk categories of information systems and specific content of security measures.

(2) Rules for information systems involving serious externalities and related subjects

There is a need for rules agreed to in society for information systems involving serious externalities and those containing sensitive information. As such, Security Guidelines need to be applied in the following manner.

First, information systems that involve serious externalities and those that contain sensitive information need to be assigned to high risk categories. Additionally, top management needs to apply high-level security guidelines when setting the goals to be achieved by security measures. As used here, “high-level security guidelines” refers to those standards indicated in the existing Security Guidelines with the terms “must,” “should,” “need(s) to,” “necessary,” or “recommended,” or in the imperative. In addition, allocation of the management resources needed to implement security measures needs to be conducted appropriately based on the perspective of maximizing the efficiency of resource allocation through comparison with new investment and other options.

(3) Necessity of a simplified method

Although basically it is possible for Financial Institutions and other organizations to choose on their own matters such as the risk categories of information systems and specific details of security measures if they adhere to a risk-based approach and comply with the basic principles of security measures, when doing so it would not be easy to operate such matters fully and perform accountability requirements with regard to the appropriateness of decision-making and the propriety of operations.

For example, in classification of risks, in light of the fact that system risk, as one type of operational risk, is by its nature connected to other risks, in allocation of management resources there is a need for quantitative measurement, derivation of the point at which efficiency is maximized for each of the components of the costs of necessary security measures, their results, investment in new development, and its results, and deciding on the ultimate allocation of management resources based on the results.

Accordingly, even though such a complete risk-based approach would be ideal, it is thought that not all Financial Institutions would be able to implement it.

In light of the fact that at most Financial Institutions and other organizations in Japan the traditional way of thinking on security measures is in general use, there is a need for an approach that would not result in dramatic changes to the details of implementing existing security measures while adopting a risk-based approach and new forms of security measures.

The following section describes IT governance through a simplified risk-based approach in accordance with the basic principles of security measures, as a means of achieving the desired results through a simplified method similar to a complete risk-based approach.

While this simplified method is described here for convenience’ sake, it is recommended that Financial Institutions and other organizations proceed with a more exhaustive approach aiming for a complete risk-based approach instead of sticking to this simplified approach alone.

4. IT governance through a simplified risk-based approach

(1) Significance

This refers to top management, in deciding on policies related to security measures, grouping information systems into the two main categories of critical information systems and other information systems based on their risk properties, considering allocation of management resources in pursuit of maximization of efficiency, including new investment, based on the assessed results, and making comprehensive decisions on matters such as the goals to be achieved by the necessary security measures for each category.

(2) Significance of “critical information systems”

Which systems qualify as “critical information systems” can be determined by individual Financial Institutions and other organizations in consideration of their impact on the settlement system, customers, and other factors from perspectives such as their externalities and the sensitivity of the information they contain.

First of all, critical information systems include information systems involving serious externalities and information systems containing sensitive information. In addition to these, other information systems involving similar or higher degrees of risk may be chosen independently as ones to which application of high-level security guidelines would be appropriate.²²

Today, when the business operations of Financial Institutions are highly dependent on information systems, in principle decisions on critical information systems need to be made by top management.

(3) Security measures and allocation of management resources for critical information systems

Top management needs to apply high-level security guidelines in setting goals for achievement of security measures for critical information systems. As used here, “high-level security guidelines” refers to those standards indicated in the existing Security Guidelines with the terms “must,” “should,” “need(s) to,” “necessary,” or “recommended,” or in the imperative. Allocation of the management resources needed to implement security measures needs to be conducted appropriately based on the perspective of maximizing the efficiency of resource allocation through comparison with new investment and other options.

(4) Security measures and allocation of management resources for other information systems

While goals for achievement of security measures for other information systems traditionally could be set independently, as noted above there is a concern that high-level security guidelines could be applied uniformly since they are not specified clearly. The following measures are specified in order to reduce such uncertainty regarding security measures.

First of all, in setting goals to achieve for security measures for other information systems, top management needs to apply the minimum necessary security guidelines. Other goals to achieve may be chosen independently in accordance with the actual circumstances. Next, in allocation of the management resources needed for implementation of security measures there is a need to decide on more efficient allocation of management resources taking into consideration new investment and other options.

²² Aside from the examples given here, it also is conceivable that critical information systems could be chosen from perspectives such as those of availability and integrity.

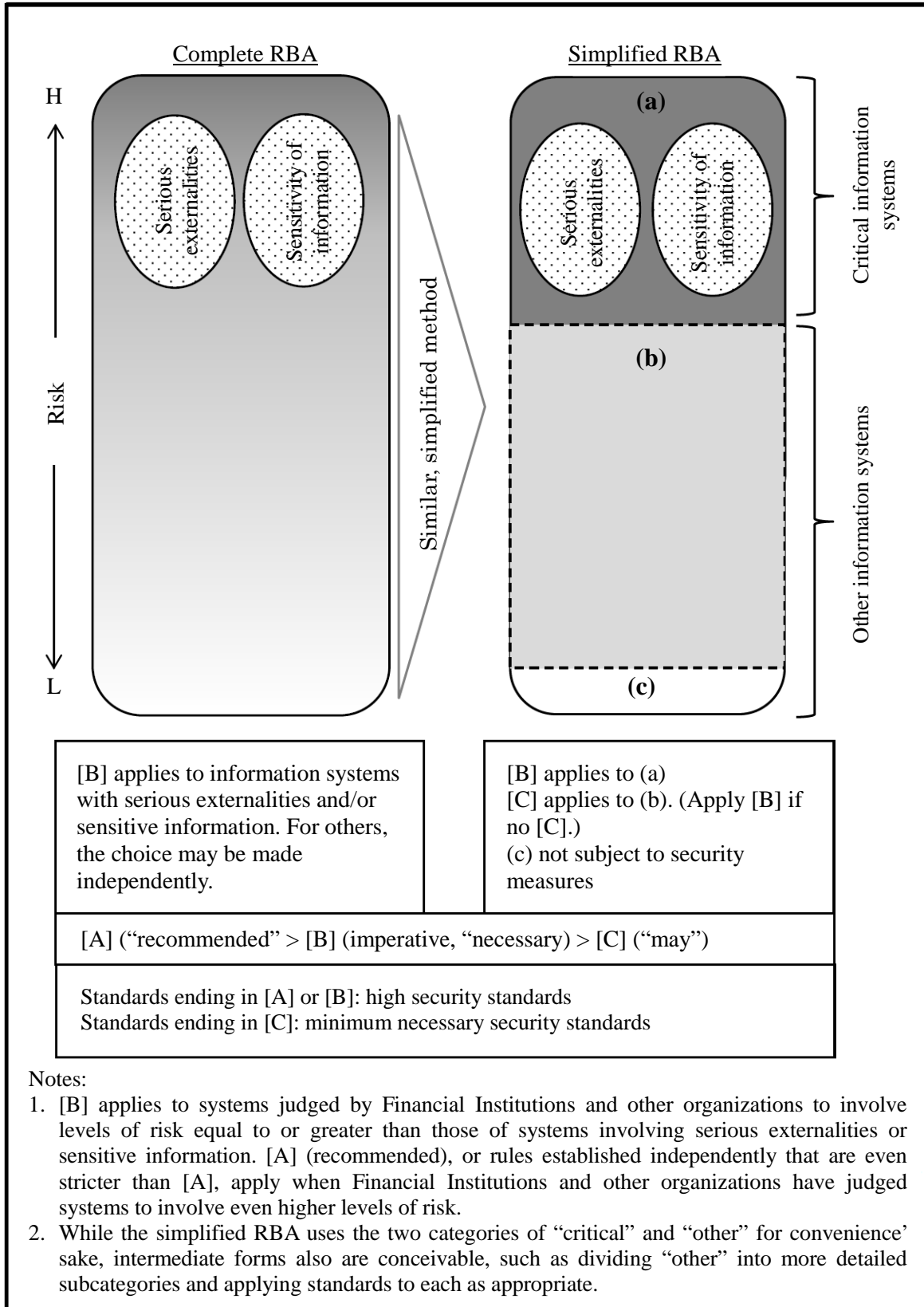
Also, since information systems that lack externalities and customer information and have only minor internal impact are very low-risk information systems, they could be considered not to be subject to application of Security Guidelines from the start. Possible information systems with only minor internal impact would be those that do not contain customer information that includes sensitive information or those that do not interface with other information systems. Such low-risk information systems for which it would be appropriate not to apply Security Guidelines may be selected independently in accordance with the actual conditions of Financial Institutions and other organizations when it would be appropriate to do so.

(5) Significance of minimum necessary security guidelines

These are similar in nature to the security measures for information systems with comparatively low risks referred to as “simplified risk management measures” in the Report of the Council of Experts on the Usage of Cloud Computing by Financial Institutions or those indicated with the term “may” in the Security Guidelines.

The existing “simplified risk management measures” now are redefined as “minimum necessary security guidelines” to be established as appropriate in future Security Guidelines. However, as noted above these should be established within the scope of the objective of reducing uncertainty regarding security measures when employing an expedient approach due to a high degree of difficulty of employing a completely risk-based approach.

(Fig. 16) Method of application of Security Guidelines in accordance with a risk-based approach (RBA)



5. Management responsibility for security measures

The form of new security measures was described above. However, there are concerns that the shared understanding among top management described above that it should not demand excessive security measures just because it could be held responsible directly for any severe system problems that could arise could prove an impediment to complying with the basic principles of security measures mentioned above.

This strong tendency toward risk avoidance could be deeply rooted in societal norms specific to Japan. While opinions are likely to vary widely concerning the appropriateness of these social norms, as noted above it is not rational for top management, whose mission is to maximize corporate value, to exhibit a strong tendency toward risk avoidance by completely refusing to tolerate risk and pursuing the total elimination of all risks.

On the other hand, in the United States, the United Kingdom, and other developed countries abroad risk preference tends in general to be higher than in Japan. For example, in the case of FinTech American and British Financial Institutions can be seen to be taking risks to enter new fields early through means including alliances and partnerships with IT startups and other nonbank players. This can be considered to reflect the fact that in the background there is a shared understanding among regulators and Financial Institutions and other organizations that it is not rational to pursue total elimination of all risks, as noted above.

Under such conditions, it is thought that in order to secure competitive advantage for Japan in financial businesses in the future both regulators and Financial Institutions and other organizations should have a shared recognition of the risk-based approach of not pursuing the total elimination of all risks. Such shared recognition also should include the understanding that when residual risks remain after taking the risk-based approach and such risks manifest themselves it would not be compatible with the concept of the risk-based approach if regulators then merely held Financial Institutions and other organizations responsible for the results of such manifestation of risks.

Based on the above concept, the form that should be taken by management responsibility for security measures is outlined below.

- (1) The mission of top management is to maximize corporate value. This does not necessarily mean the pursuit of security measures aiming to eliminate all risks.
- (2) For residual risks that remain as a result of aiming to maximize corporate value, there is a need to recognize such risks accurately and then respond to them by formulating contingency plans (“CPs” hereinafter) in accordance with their degrees and revising these in response to environmental changes.
- (3) Top management should be considered to be fulfilling its legal responsibilities from an objective point of view only when it prepares CPs etc. for security measures and residual risks based on consideration of matters such as the Security Guidelines and other guidelines agreed upon in society (including the basic principles of security measures mentioned above) and responds as the occasion may require, based on the CPs, in the event of an incident, in addition to complying with various laws and regulations.

IV. Risk Management in Outsourcing

Summary

- ◆ In light of the various issues related to subcontracting, in IT governance in outsourcing top management and others need to perform the following roles and responsibilities:
 - (1) Deciding on policies related to outsourcing of information systems (top management)
 - (2) Deciding on outsourcing of individual information systems
 - (3) Deciding on frameworks for risk management in outsourcing of individual information systems
Deciding on goals of security measures, allocation of management resources, and management structures corresponding to the outsourcing management phase
 - (4) Implementing security measures in each management phase (related parties)
 - (5) Deciding on improvements related to risk management in outsourcing

Note: Based on a risk-based approach, the decisions under (2), (3), and (5) above shall be made by top management for critical information systems but may be made by other parties for other information systems. Even for critical information systems, when the risk of the outsourced operations is low, for example as a result of breaking the operations down into their detailed components, the decision may be made by another party.

- ◆ Risk management measures for outsourcing of operations that should be added with reference to existing security guidelines for outsourcing and security guidelines for cloud services are listed below:
 - (1) Deciding on requirements for selection of subcontractors
 - (2) Conducting advance screening of subcontractors to verify the appropriateness of selection of subcontractors by outsourcees
 - (3) Clear specification by the financial institution of the right to audit subcontractors when concluding contracts with outsourcees
 - (4) Auditing on the financial institution's own responsibility when conducting audits of subcontractors
 - (5) When outsourcing critical information systems, formulating CPs with outsourcees and others during normal times, and conducting joint drills with outsourcees and others.
When a CP is implemented in an incident, monitoring the status of CP implementation by outsourcees and others.

Note: Based on a risk-based approach, for information systems other than critical information systems, verification in advance that the content of advance screening of outsourcees' subcontractors is at least of the same level as that of the financial institution or other organization may replace the step under (2) above. The right to audit under (3) need not be specified clearly in such a case. These measures may substitute for those under (2) and (3) even in the case of critical information systems if as a result of detailed subdivision of the operations the risk of subcontracted operations can be considered sufficiently low.

In outsourcing of development, similar substitute measures may be employed to those for information systems other than critical information systems.

General characteristics of outsourcing are the limited nature of the scope and depth of information that can be ascertained directly, the limited points of contact for controls, and the difficulty of applying controls. These characteristics are even more pronounced for subcontracting.²³

Amid such conditions, in recent years cases of misconduct at multiple shared system centers such as subcontractor employees counterfeiting ATM cards have served as reminders of the risks related to subcontracting. In addition, rather than being limited to shared system centers such risks are common to outsourcing as a whole, and the Banking Act and other applicable laws and regulations have been amended to call explicitly on Financial Institutions and other organizations to ensure management responsibility and accountability. This Council was formed in light of the way outsourcing thus has become an important issue to Financial Institutions and other organizations.

At the same time, this Council first examined the topics of IT governance and IT management and a risk-based approach, based on its understanding that responding to such issues involved in outsourcing is an issue faced by all Financial Institutions and the perspective of IT governance is essential to addressing this issue appropriately. In addition, through the process of the previous study by the Council of Experts on the Security Guidelines and other documents have been revised and new rules already have been developed for cloud services, as one form of outsourcing.

In proceeding with study of outsourcing as a whole, the various issues related to subcontracting and the thinking on responding to them will be made clear first, and then the ideal form of risk management in outsourcing will be reviewed based on the content that has been considered through now in the Council of Experts and elsewhere. Following that, risk management measures for subcontractor management will be proposed.

1. Various issues related to subcontracting

Subcontractor management has become recognized anew as an issue since cases of misconduct arose involving counterfeiting of cards by subcontractor staff responsible who possessed the necessary skills and authorization at multiple shared system centers of regional banks. Some Financial Institutions using joint centers have implemented their own independent countermeasures.

In addition, responses to such cases of misconduct including amendment of the Banking Act have made subcontractors subject to regulators' inspection authority not just at shared system centers but across outsourcing as a whole, so that Financial Institutions face demands for management responsibility and accountability regarding subcontracting, and clarification of responsibilities for subcontracting has become a subject of concern.

Although these cases of misconduct have been concentrated on shared system centers, since the fundamental cause stems from the distinguishing features of outsourcing such as the difficulty of applying controls to it, there is a need to consider the various issues related to subcontracting as issues common to outsourcing as a whole.

2. Thinking on responses to various issues

Today, as Financial Institutions and other organizations in Japan have aimed to maximize corporate value through means including cost savings and use of advanced technologies, amid

²³ Including subcontracting spanning two or more levels.

developments including advances in IT and growth in such organizations' lines of business, the degree of reliance on outsourcing in information systems is rising from year to year.

At their root, Financial Institutions and other organizations are companies doing business with the aim of maximizing corporate value. At the same time, however, due to their public nature including the fact that their businesses make up part of the financial infrastructure, ensuring their soundness is considered necessary by society, as seen for example in the fact that their businesses require licensing.

Accordingly, today when the information systems of Financial Institutions and other organizations are handled by outsourcees to a considerable degree and dependency on such outsourcees is increasing, demands for management responsibility and accountability are increasing with regard to securing the soundness of information systems.

At the same time, as mentioned above one characteristic of outsourcing is the difficulty of applying controls to it, and it is thought that this characteristic becomes even more pronounced in subcontracting. That is, subcontractors normally offer only indirect points of contact through outsourcees, and if the outsourced operations are subdivided and subcontracting to multiple subcontractors, then the number of such contact points increases horizontally. Furthermore, if subcontractors carry out further subcontracting themselves then the levels of the structure deepen vertically as well. Accordingly, there are concerns that as subcontracting advances the structure of controls through outsourcees grows more complex, and controls will become extremely difficult as a result.

While of course it is clear from social and public perspectives that it would be inappropriate if Financial Institutions and other organizations did not employ any controls on outsourcees and others, there also are concerns that if they were to employ complete controls to the same degree as those demanded for operations handled in house then the result could be the loss of the essential objectives of outsourcing intended to maximize corporate value, such as cost savings and use of advanced technologies. For this reason, it is important to decide on the optimal controls at the points of contact with outsourcees and subcontractors as a result of comprehensive consideration of matters such as the social and public perspectives of Financial Institutions and other organizations and the objectives of outsourcing. This is the responsibility of top management of Financial Institutions and other organizations.

On the subject of responding to various issues related to subcontracting as described above, with regard to countermeasures against cases of misconduct the Center has revised technical standards such as those on restricting access authorization as a "(tentative) response to cases of improper withdrawals" in the Security Guidelines revised last year (Revise Supplement to the Eighth Edition). However, it is conceivable that one reason behind the occurrence of such cases of misconduct is the fact that the approach to management of outsourcing, including subcontracting, in the existing Security Guidelines has not reflected adequately the distinguishing features of critical information systems at Financial Institutions and other organizations, such as their public nature and the sensitive nature of the information handed by outsourcees. In recognition of the need for thorough countermeasures in the form of identifying an ideal form of risk management in outsourcing, instead of merely revising technical standards, based on reflection on this point, the goal now is to study related matters and reflect the findings in the Security Guidelines.²⁴

²⁴ The "Summary of Revisions" in FISC's "Security Guidelines on Computer Systems for Banking and Related Financial Institutions (Revised Supplement to the Eighth Edition)" (June 2015) states concerning the "(tentative) response to cases of improper withdrawals by outsourcees," "These revisions are tentative measures. Plans call for separate consideration of revisions through means including deliberation in the Council of Experts on External Outsource Management in General

On the other hand, with regard to making clear the ideal form of responsibility for subcontracting, there is no change from the argument described under III. Risk-Based Approach: 5. Management Responsibility for Security Measures. That is, once the fundamental countermeasures in subcontracting as described above have been reflected in the Security Guidelines, Financial Institutions and other organizations will be considered to have fulfilled their responsibilities if they have decided on allocation of management resources and optimal security measures aiming to maximize corporate value based on those and are responding to residual risks appropriately.

In light of the above, the following section will study the ideal form of risk management in outsourcing with a focus on subcontracting, with the aim of setting up optimal controls, or optimal goals for security measures, for outsourcees and other parties at the points of contact with such parties—that is, in each management phase. In addition to reflecting IT governance and IT management as well as a risk-based approach, such study also needs to take into consideration the need to be understood in a way consistent with the content of measures already being developed in the Security Guidelines and other documents through the Council of Experts with regard to cloud services, a form of outsourcing.²⁵

concerning basic content such as approaches to external outsourcee management.”

²⁵ In 2014 FISC held the Council of Experts on the Usage of Cloud Computing by Financial Institutions, in June 2015 it issued the “Security Guidelines on Computer Systems for Banking and Related Financial Institutions (Revised Supplement to the Eighth Edition,” based on the results etc., each expert committee was held, and in May 2016 it issued the “Information System Audit Guidelines for Banking and Related Financial Institutions” (Revised Supplement to the Third Edition).

3. Risk management in outsourcing

In considering the form that risk management should take in outsourcing, to begin with the management process in outsourcing will be identified and its content and other matters made clear from the perspective of IT governance with regard to management responsibility and other topics. Then, thinking on risk management measures at the point of contact with outsourcing, or the management phase, will be reviewed.

(1) Management processes in outsourcing

Management processes in outsourcing, based on the content of studies through now in the Council and elsewhere, can be thought to include the following:

- ① Deciding on policies related to outsourcing of information systems
- ② Deciding on outsourcing of individual information systems
- ③ Deciding on frameworks for risk management in outsourcing of individual information systems
Deciding on the goals of security measures and the management resources and structure, including outsourcee management, necessary to achieve them based on the following management phases²⁶ :
 - a. When considering use
 - b. When concluding the contract
 - c. During development (including adoption of packages, system modifications, etc.)
 - d. During use (e.g., monitoring²⁷)
 - e. At end of use
 - f. When an incident arises
- ④ Implementing security measures in each management phase
- ⑤ Deciding on improvements related to risk management in outsourcing

- ① Deciding on policies related to outsourcing of information systems
First, make clear the thinking (e.g., purposes of use) in selection of outsourcing based on maximizing corporate value and ensuring soundness for outsourcing of information systems, as policies. Examples include the operations for which outsourcing may be used and risk management frameworks. In particular, since it is even more difficult to apply controls to subcontracting, conceivable examples of what to include in policies for such a case include the operations for which subcontracting may be used and restrictions on the levels and numbers of cases of subcontracting for each type of operation.
Since these policies should apply comprehensively to all information systems, they must be decided on by top management.

²⁶ FISC's "Report of the Council of Experts on the Usage of Cloud Computing by Financial Institutions" (November 2014) states, "It is important to formulate basic policies on use and policies related to risk management, with the engagement of top management." It also identifies five phases of such management: "when considering use," "when concluding the contract," "during operation," "upon termination of the contract," and "when an incident arises." While cloud services are focused mainly on use, since "external outsourcee management" in the current Security Guidelines covers "development" as well as "use" the new phase "during development" has been added.

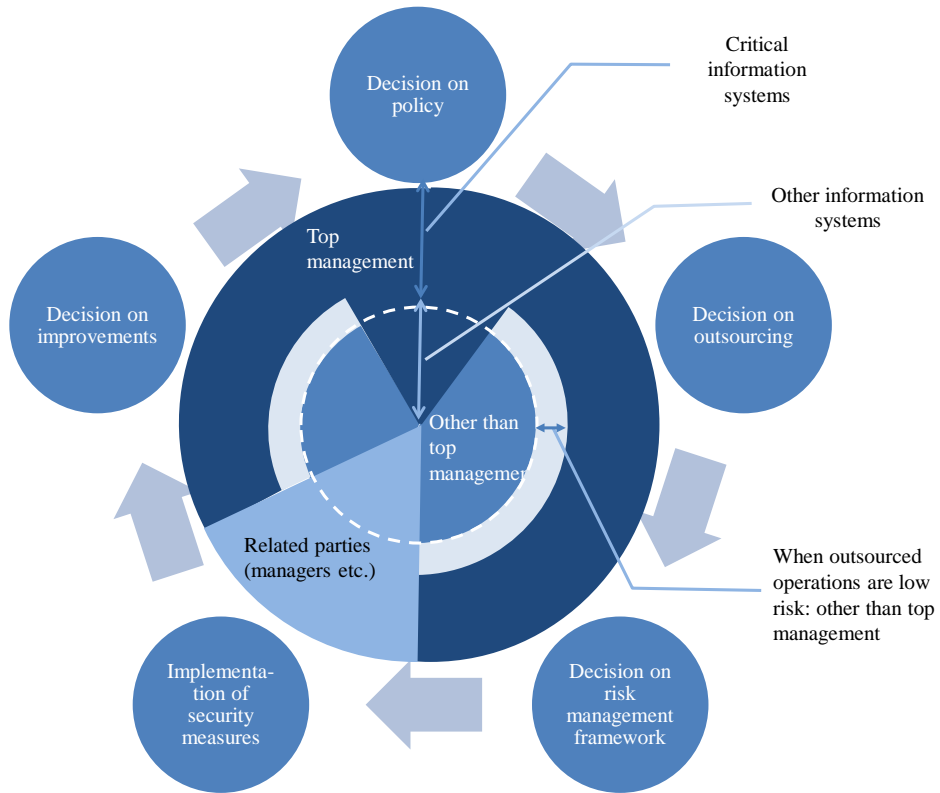
²⁷ FISC's "Information System Audit Guidelines for Banking and Related Financial Institutions" says concerning monitoring: "Monitoring is a process to confirm whether internal controls are appropriate and effective. This includes day-to-day monitoring at each level through everyday business activities, regular and irregular self-inspections by management of individual sections, and internal auditing by internal audit sections independent from the organizations audited. System audits conducted by internal audit sections are included in monitoring as independent evaluation."

- ② Deciding on outsourcing of individual information systems
 In accordance with the above policies, the purposes of outsourcing must be made clear and its appropriateness should be judged for each individual information system.
 For critical information systems, this decision must be made by top management due to the need to take into consideration comprehensively matters such as the social and public perspectives of Financial Institutions and other organizations and the purpose of outsourcing, and to the particular stress on management responsibility and accountability. For other information systems, the decision may be made by parties other than top management.
 In addition, even when outsourcing critical information systems the decision may be made by parties other than top management when the risk of the outsourced operations can be considered to be sufficiently low, for example as a result of breaking the operations down into their detailed components.²⁸
- ③ Deciding on frameworks for risk management in outsourcing of individual information systems
 Next, proceed with steps including selection of outsourcees in accordance with the above decision. Since in outsourcing it is important to decide on optimal controls at points of contact with outsourcees and others, appropriate consideration should be given to the management framework, including the goals of security measures and management resources allocated to them and structures for management of outsourcees and other measures, in accordance with each phase.
 In accordance with the basic principles of security measures, the goals of security measures should be decided on with sufficient content as necessary in accordance with the characteristics of the risks inherent to each information system and divisions on management resources allocated should be decided on by taking into consideration not only adjustments with new development and other efforts within the information systems budget, based on comparison with countermeasures taken after a risk has manifested itself, but also management resources as a whole, with the aim of maximizing corporate value.
 For reasons similar to those described under ② above, this decision must be made by top management for critical information systems. For other information systems, the decision may be made by parties other than top management.
 Also, as described under ② above even when outsourcing critical information systems this decision may be made by parties other than top management when the risk of the outsourced operations can be considered to be sufficiently low.
- ④ Implementing security measures in each management phase
 Actual security measures based on the above decisions shall be implemented in each management phase by the parties related to the security measures as shown in “IT Management Necessary for Security Measures.”
- ⑤ Deciding on improvements related to risk management in outsourcing
 As described in “IT Governance Necessary for Security Measures,” the state of implementation of security measures shall be checked and verified by related parties through means such as monitoring during operation, and continual improvements shall be made as necessary to matters such as postures toward security measures.
 For reasons similar to those described under ② above, this decision must be made by top management for critical information systems. For other information systems, the decision may be made by parties other than top management.

²⁸ The risk of the outsourced operations can be considered by quantity (e.g. outsourcing amount) in addition to the nature of outsourcing.

Also, as described under ② above even when outsourcing critical information systems this decision may be made by parties other than top management when the risk of the outsourced operations can be considered to be sufficiently low.

(Fig. 17) IT governance in the outsourcing management process



(2) Thinking on risk-management measures in each management phase

First of all, even as the structure of controls through outsourcees grows more complex, Financial Institutions and other organizations need to ascertain the state of contracting of business operations, including subcontracting. After doing so, since primary responsibility for control of subcontractors lies with the outsourcees, the main responsibility of Financial Institutions and other organizations regarding subcontracting is that of checking whether outsourcees are managing subcontractors appropriately. In addition, even during the management phase the two points of checking the appropriateness of selection of subcontractors and checking whether subcontractors' business operations are managed and supervised appropriately by outsourcees are particularly important. It also is necessary to take care to ensure that such management does not infringe on laws or regulations.²⁹

In light of this thinking, the thinking on risk-management measures in each management phase is summarized below, with a focus on subcontracting.

a. When studying use

The current Security Guidelines do not mention subcontracting under “external outsourcee management.”

On the other hand, under “use of cloud services” the Security Guidelines do include the perspective of subcontracting as one item under evaluation of Cloud businesses during study of use (Operations 108),³⁰ presenting standards that reflect consideration for subcontracting. However, since these standards include content specific to the Cloud, such as “locations of data,” with the exception of portions such as these the standards for security measures on “use of cloud services” could be referred to as standards for outsourcing as a whole in consideration of consistency with them.³¹

b. When concluding a contract

The current Security Guidelines discuss subcontracting only as one matter for consideration in connection with conclusion of contracts.³²

On the other hand, under “use of cloud services” the Security Guidelines do identify in detail “subcontractor management” as one matter recommended to be stated clearly in the contract when concluding one (Operations 109), so that, as with the case of when studying use, they can be used for reference.

Financial Institutions and other organizations need to verify, from independent perspectives as such organizations, the appropriateness of outsourcees' judgment on the requirements

²⁹ Laws that should be noted include the Act for Securing the Proper Operation of Worker Dispatching Undertakings and Improved Working Conditions for Dispatched Workers, the Employment Security Act, and the Act against Delay in Payment of Subcontract Proceeds, Etc. to Subcontractors.

³⁰ Under Operations 108, the FISC Security Guidelines on Computer Systems for Banking and Related Financial Institutions identify “state of internal controls, risk management, etc. (including subcontractor management)” as one item for use in assessment of Cloud businesses.

³¹ Since cloud services are one form of outsourcing, standards applying to outsourcing in general need to be consistent with those already established for cloud services. However, it is necessary to employ an approach of referring to cloud service standards that could be applicable to outsourcing as a whole while not using those considered specific to the Cloud as standards for outsourcing in general.

³² FISC's Security Guidelines on Computer Systems for Banking and Related Financial Institutions state in the section on outsourcing in general (Operations 88), “The following are examples of matters that should be considered when concluding contracts,” listing only “subcontracting (e.g., clarification of responsibilities related to outsourcing, necessity of prior approval by Financial Institutions and other organizations)” along with confidentiality protection and report on incident.

and procedures for selection of subcontractors. In particular, in subcontracting of operation of critical information systems this verification needs to be conducted before subcontractors begin working on the operations, since risks could materialize soon after they begin such work. From this point of view, there is a need to study individual risk management measures.

c. During development

The current Security Guidelines do cover development in standards for external outsourcee management.

On the other hand, since under “use of cloud services” the Security Guidelines focus mainly on cloud services and assume other information systems have been developed already, those standards are centered on operation and do not mention development.

To begin with it is thought that since a system is not yet live during development even if a risk were to be manifested in outsourcing of development, the extent of its impact would be limited to within the financial institution or other organization, and furthermore as long as customer information including sensitive information is not provided to outsourcees or subcontractors, systems under development are not thought to involve the risk characteristics of “critical information systems.”³³

Accordingly, in light of the risk-based approach the development standards under “external outsourcee management” in the current Security Guidelines should be revised based on this way of thinking. In addition, even outsourcing of development of “critical information systems” (including the times of not only development but also study of use, conclusion of contracts, and ending of outsourcing) may be included in the scope subject to the “minimum necessary security guidelines” established to reduce uncertainty regarding security measures.

d. During operation (monitoring etc.)

The current Security Guidelines do not mention subcontracting under either “external outsourcee management” or “use of cloud service.” For this reason, there is a need to consider new risk management measures as optimal controls for subcontractors.

When verifying whether outsourcees manage and supervise the operations management of subcontractors appropriately, Financial Institutions and other organizations also need to look at the appropriateness of checking (e.g., everyday monitoring and supervision) by outsourcees. In addition, these need to be conducted independently, from the points of view of Financial Institutions and other organizations, which are not necessarily the same as the points of view of the outsourcees.

It is conceivable that Financial Institutions and other organizations might entrust verification to third parties instead of doing it themselves. In such cases as well, it needs to be conducted from the perspectives of Financial Institutions and other organizations.

Individual risk management measures need to be considered in light of the above

³³ Another important risk related to outsourcing is that of defects being introduced by outsourcees. This is a risk that concerns information systems as a whole, not just outsourcing, and consideration of the current Security Guidelines and other documents shows that sufficient quality control is demanded.

perspectives.

e. Ending

The current Security Guidelines do not mention subcontracting under either “external outsourcee management” or “use of cloud service.”

Since at the time of ending subcontracting there are no differences in the factors involved between subcontractors and outsourcees and the same risk management measures used for outsourcees would be sufficient for subcontractors, the current Security Guidelines’ standards on “external outsourcee management” and “use of cloud services” could be referred to as standards for outsourcing as a whole.³⁴

f. Upon an incident

While the Security Guidelines require Financial Institutions and other organizations to prepare CPs in advance for responding to incidents,³⁵ they do not mention outsourcing, including subcontracting. Although the Manual on Preparation of Contingency Plans at Financial Institutions and Other Organizations (“CP Manual” hereinafter) does mention outsourcees,³⁶ it does not mention subcontracting. Also, the Security Guidelines do not mention outsourcing, including subcontracting, upon an incident under “external outsourcee management” or “use of cloud services.”

Responding to an incident, particularly one involving critical information systems, is identified in “Management Responsibility for Security Measures” under the risk-based approach as an important element in top management’s performance of its legal responsibility. For this reason, it is important to consider risk management measures related to responding to incidents in outsourcing, including subcontracting, in Security Guidelines, not just the CP Manual.

The above summary concerns critical information systems important in terms of their social and public natures. For other information systems, it can be considered sufficient to check whether outsourcees are controlling subcontractors appropriately. That is, if the controls implemented by outsourcees with regard to subcontractors function at least as appropriately as those implemented by Financial Institutions and other organizations, then it would be beneficial, from the perspective of management resources, to rely on those controls.

³⁴ Under Operations 109, the FISC Security Guidelines on Computer Systems for Banking and Related Financial Institutions recommend with regard to termination that security standards envisioning “the difficulty of coordination due to a change in policy by the Cloud operator” as one item that should be described clearly in contracts.

³⁵ Under Operations 65, the FISC Security Guidelines on Computer Systems for Banking and Related Financial Institutions state, “A contingency plan must be formulated in advance for purposes including keeping to a minimum the effect on business operations of severe damage caused by unexpected disasters, accidents, failures, etc. or damage resulting from difficulty in carrying out business operations, as well as prompt recovery.”

³⁶ FISC’s Manual for Formulating Contingency Plans at Financial Institutions and Other Organizations calls for measures including consideration of outsourcing when identifying risks, considering the posture toward communication with key outsourcees in emergencies, and including outsourcees in drills.

4. Risk management measures for subcontracting

In light of the above thinking, risk management measures for subcontracting in outsourcing of operations are proposed below.

(1) Formulating requirements for selection of subcontractors and implementing advance screening

Financial Institutions and other organizations must establish requirements for selection of subcontractors in advance in order to select appropriate subcontractors when concluding subcontracting agreements with outsourcees.

Together with factors such as specialization (e.g., qualifications held) and reliability (e.g., whether or not any problems have arisen in the past), requirements for selection need to include whether or not the subcontractor has the ability to maintain an internal risk control posture such as mutual checks and balances as needed in light of the content of the subcontracting operations. It also is conceivable that when forced, for reasons such as specialization, to subcontract to a subcontractor for which the maintenance of such a control posture would be difficult, conditions could be added such as limiting work locations to those that could be controlled by the outsourcees.

Next, when critical information systems are subcontracted, Financial Institutions and other organizations need to conduct advance screening of subcontractors assuming that outsourcees will select subcontractors, in order to verify the appropriateness of such selection in light of the above requirements for selection.

In addition, in subcontracting of information systems other than critical information systems, when outsourcees' process of screening and control of subcontractors is deemed to be at least as effective as that of the financial institution or other organization, then that organization could verify in advance the appropriateness of outsourcees' maintenance and operation of the screening and control process³⁷ and confirm the results of such verification instead of conducting advance screening of individual subcontractors.

Furthermore, even when outsourcing critical information systems, if as a result of detailed subdivision of the operations subcontracted to subcontractors the risk of such subcontracted operations can be considered sufficiently low, then the above simplified procedures may be employed in such a situation as well.

(2) Clear description of the right to audit subcontractors³⁸

When concluding subcontracting agreements with outsourcees on outsourcing of critical information systems, the agreements must state clearly that Financial Institutions and other organizations have the right to audit subcontractors, to ensure that a system is in place for checking on subcontractors.

When Financial Institutions and other organizations implement auditing of subcontractors, they need to do so under their own responsibility, in the same way as when auditing outsourcees. As

³⁷ Specific verification methods are described in FISC's Information System Audit Guidelines for Banking and Related Financial Institutions (Revised Supplement to the Third Edition), under Part 1: Chapter 3: 5. Key Points of Auditing Cloud Services, as follows:

“(2) Verification items to confirm the efficiency of subcontractor screening and management processes by Cloud operators.”

³⁸ Authority to audit needs to be specified in contract whether for subcontracting or sub-subcontracting.

used here “under their own responsibility” refers to the Financial Institutions and other organizations setting audit items in accordance with their own verification needs, reflecting the nature of risks to subcontractors, and to Financial Institutions and other organizations conducting such auditing at timing that they consider appropriate, without excessive consideration for outsourcees and others. They may conduct the auditing themselves³⁹ or entrust it to appropriate auditors.

Selection of auditors needs to conform to the requirements for selection of auditors established in FISC’s Guidelines for Auditing of Systems of Financial Institutions and Other Organizations (Third Edition, Revised and Expanded)⁴⁰.

In addition, when outsourcing information systems other than critical information systems, it is acceptable to omit from the subcontracting agreement concluded with the outsourcees a clear statement of Financial Institutions and other organizations’ right to audit subcontractors.

Furthermore, even when outsourcing critical information systems, if as a result of detailed subdivision of the operations subcontracted to subcontractors the risk of such subcontracted operations can be considered sufficiently low, then the above simplified procedures may be employed in such a situation as well.

(3) Responding to incidents

When outsourcing critical information systems (not including subcontractors for which risks can be considered sufficiently low as a result of detailed subdivision of the subcontracted to operations), CPs need to be formulated to include parties such as outsourcees and subcontractors as well. In addition, when outsourcees and others prepare their own individual CPs, their content must be consistent and mutually complementary with the CPs of the Financial Institutions and other organizations.⁴¹ Also, in normal times Financial Institutions and other organizations must implement periodic drills jointly with outsourcees and subcontractors, based on the CPs concerning those outsourcees and others.

When parties such as outsourcees and subcontractors have identified the possibility of system failures or other problems in critical information systems that could have a severe impact on the financial infrastructure as a whole, they shall report such discovery to the Financial Institutions and other organizations immediately and support the decision-making by the Financial Institutions and other organizations regarding implementation of the CP. In addition, if a decision is made to implement a CP, Financial Institutions and other organizations must notify parties such as outsourcees and subcontractors of such fact and supervise the state of CP

³⁹ When the audit method employed of asking outsourcees to provide information and verifying the appropriateness of subcontracted operations based solely on checking the content of such information is not enough, other methods include on-site audits of outsourcees or, when outsourcees have submitted the results of auditing already verified (e.g., SOC2, IT7), verifying their content and conducting on-site auditing of outsourcees centered mainly on items of concern of inadequacies in such auditing.

⁴⁰ FISC’s Information System Audit Guidelines for Banking and Related Financial Institutions (Revised Supplement to the Third Edition), under Part 1: Chapter 3: 5. Key Points of Auditing Cloud Services, as follows: “(1) Consideration of Joint Auditing Using Independent Auditing of Cloud Operators,” states with regard to selection of auditors, “As a financial institution responsible to its customers, it is necessary to select an auditor for which there would be no concerns about a possible conflict of interest with the Cloud operator. To do so, a client financial institution needs to select as an auditor an audit firm that does not carry out account auditing of the Cloud operator. Also, when selecting an audit firm employed in guaranteeing the Cloud operator’s SOC2 or IT7, there is a need to select an audit officer not employed in guaranteeing the Cloud operator’s SOC2 or IT7.”

⁴¹ As issues related to ensuring the efficiency of contingency plans (CPs) 57.1% of regional banks, 67.7% of second-tier regional banks, 44.2% of credit unions, and 60% of credit cooperatives identified “consistency between our plans and those of related parties needed for business continuity,” indicating the need for consistency between the CPs of shared system centers and those of user Financial Institutions (FISC, Results of FY2015 Survey of Financial Institutions).

implementation by outsourcees and others.

In outsourcing of development, requirements for selection of subcontractors need to be formulated. In such a case, for advance screening of subcontractors and clear description of the right to audit subcontractors, the simplified procedures above may be used for both critical information systems and information systems other than critical information systems.

(Fig. 18) New risk management measures that should be added in subcontracting

	Type of system	Formulation of requirements for selection	Advance screening	Clear description of the right to audit	Responding to incidents
Outsourcing of operation	Critical information systems	○	○	○	○
	Resulting level of risk is low	○	△1	△2	—
	Other information systems	○	△1	△2	—
Outsourcing of development	Critical information systems and other information systems	○	△1	△2	—

- Application of risk management measures required
- △1 Individual advance screening of subcontractors may be replaced with verification of outsourcees' processes of screening and control of subcontractors
- △2 Right to audit subcontractors is acceptable to omit from being stated clearly in agreements with outsourcees

V. Risk management at shared system centers

Summary

- ◆ Since a shared system center is entrusted with information systems for multiple Financial Institutions, it is not necessarily the case that it can be expected to involve smooth consensus among the Financial Institutions to the same degree as in contracting by an individual financial institution alone.
- ◆ Particularly under current conditions in which cyber-attacks are becoming more active, information can spread throughout society quickly thanks to IT advances, and settlement is being conducted 24 hours/day, 365 days/year, a delay in implementing countermeasures could lead to problems having the severe result of spreading distrust. As such, the issue of the speed of responding to an incident should be considered to be even more important than in the past.
- ◆ In responding to such issues, the roles and responsibilities of top management, such as allocation of management resources to be prepared for incidents, are extremely important.
- ◆ For this reason, it is essential first of all that top management of user Financial Institutions understand the severity of the issue of speed in responding to an incident. Based on this, top management of user Financial Institutions need to proceed swiftly with joint consideration of risk management measures to resolve such issues.
- ◆ In such study, it is recommended that user Financial Institutions alone or with outsourcees jointly formulate staffing plans to make it possible to continually assign the IT human resources needed to be ready for incidents etc.
- ◆ While risk management measures should be studied in light of factors such as the degree of joint use of systems and mutual relations between user Financial Institutions, another example of a feasible step would be the assignment to the shared system center of managers selected from user Financial Institutions.
- ◆ In auditing shared system centers, it would be beneficial to refer to the joint auditing schemes considered for cloud services.

In recent years, many Financial Institutions have increasingly been employing joint use of systems, chiefly critical information systems such as accounting systems. In fact, among Financial Institutions such as deposit-taking institutions in particular about 90% use shared system centers for their accounting systems.⁴²

Since a shared system center is entrusted jointly by multiple Financial Institutions with critical information systems such as accounting systems, as one form of outsourcing, it is a practice in which risks that could have severe impacts on financial infrastructure as a whole are concentrated on outsourcees.

Under such conditions, at multiple shared system centers cases of misconduct have arisen such as counterfeiting of ATM cards by subcontractor employees. This has led to a renewed awareness of such risks, and as the progress of use of shared system centers has led to reductions in staffing of Financial Institutions' IT sections⁴³ Financial Institutions face the danger of lacking human resources who have the skills and expertise needed for the new risk management measures that they need to implement for shared system centers. For this reason, there is a need for additional study of risk management measures suited to the unique properties of shared system centers, based on the forms that should be taken by risk management in outsourcing after clearly identifying the significance of shared system center and related issues.

1. The significance of shared system centers and their distinguishing features

(1) The significance of shared system centers

A shared system center is a form of outsourcing in which multiple specific Financial Institutions jointly subcontract activities such as operation of critical information systems to a specific outsourcee.

As used here, "joint" refers not only to cases in which user Financial Institutions have jointly concluded subcontracting agreements with outsourcees. Rather, it also includes cases in which even though user Financial Institutions have concluded subcontracting agreement with outsourcees on an individual basis the individual Financial Institutions' information systems effectively are operated together to an extent in which the impact of a system failure or other problem in an individual financial institution's system could immediately spread to other user Financial Institutions.⁴⁴

(2) Profiles of shared system centers

Use of shared system centers began as long as 45 years ago among Shinkin banks, as a measure intended to achieve goals including making investments in computer systems more efficient. Today, it is a common and important means by which Financial Institutions operate information systems. (See References 6-8.)

⁴² Among regional banks, 78.3% use shared system centers for accounting systems, while the figure is 75.0% among second-tier regional banks, 97.2% among Shinkin banks, and 97.4% among credit unions (according to a survey by FISC).

⁴³ While the number of staff needed by institutions managing accounting systems themselves averaged 53.4 persons, among those not managing accounting systems themselves it averaged 12.8 persons (FISC, Results of FY2015 Survey of Financial Institutions).

⁴⁴ In the first meeting of this Council, use of mutual systems and networks among Financial Institutions, including the Zengin System, ATM integration, and the domestic-exchange relay system among cooperative Financial Institutions, were identified as separate from the scope of outsourcing.

① Cooperative Financial Institutions

The full-fledged start of use of shared system centers took place about 30 years ago during deployment of third-generation online systems (“3G online systems” hereinafter)⁴⁵ at deposit-taking institutions and other Financial Institutions, when member Financial Institutions began joint development and joint operation with IT solution providers by Financial Institutions from the same sectors, in contrast to the individual development employed by city banks and many regional banks. Since then, use of shared system centers has continued through alliances within sectors intended for purposes such as system costs reduction and concentration of core capacity on priority operations.

Cooperative Financial Institutions set up management organizations to centralize development and operation, through investment by Financial Institutions in individual sectors. The roles of these management organizations are to support consensus-building among the Financial Institutions and to manage outsourcee IT solution providers. This structure can be considered to have continued for 45 years as a structure needed for the effective and efficient implementation of new development to enhance system functions as needed and implement security measures such as securing backup centers amid limitations on management resources.

② Regional banks

While some second-tier regional banks (known at the time as mutual banks) began joint use of systems at a relatively early stage, in general regional banks steadily began use of shared system centers since around 1998, for reasons including the needs to control system costs, to increase system staff as the domains covered by systems expanded, and to respond to technological advances.

In general, rather than establishing a management organization to handle contracting with IT solution providers as in the case of cooperative Financial Institutions, in this case individual Financial Institutions contract with IT solution providers directly⁴⁶ and organize meetings in which managers from all user Financial Institutions take part, to build consensus.

2. Challenges involved in shared system centers

Cases of misconduct have arisen at multiple shared system centers used by regional banks such as those in which subcontractor staff with the necessary skills and authority counterfeited ATM cards. At the same time, as joint use advances the numbers of staff in IT sections have decreased as a result of pursuit of efficiency, and Financial Institutions face the danger of lacking the management resources needed to fulfill management responsibility and implement risk management measures actively.

Countermeasures have been proposed for the former of these issues under “IV. Risk Management in Outsourcing” and for the latter under “II. IT Governance and IT Management: 3.

⁴⁵ A 3G online system is intended to: ① promote further streamlining of operational processing, ② develop IT infrastructure that can be expanded with flexibility to make it possible to introduce swiftly new financial instruments and services and response to expansion of business areas, ③ enhance the customer service network, ④ and enhance information functions for revenue management, risk management, and strategic business deployment, among other objectives, and at the time they required large-scale IT investment (FISC, 2016 Financial Information Systems White Paper).

⁴⁶ In selection of IT solution providers, while it may be based on the scale and IT strategies of participating Financial Institutions, in some cases institutions first choose to participate in shared system centers offered by IT solution providers with whom they are familiar and who have demonstrated good track records when the institutions operated the systems themselves. (FISC, FY 2010 Regional Financial Institutions IT Research Report, “Consideration of IT Sourcing Strategies at Regional Financial Institutions).

Notes on Staffing Plans.”

Based on the results of such previous study, additional risk management measures will be considered below after first describing the unique nature of shared system centers, as supplemental rules to secure even greater effectiveness.

3. Distinguishing features of shared system centers

While a shared system center requires procedures to achieve consensus among multiple contracts in their relationships with outsourcees, it is hard to imagine that the degree of such procedures, such as the time they take, would be the same as in the case of contracting by an individual financial institution. To begin with, it remains uncertain whether swift and smooth decision-making to the same degree as in the case of an individual financial institution would be possible at all times.⁴⁷

In particular, in the event of an incident, which involves a battle against time, there is a possibility that the severe result of spreading distrust due to delays in implementing countermeasures as a result of the above uncertainty could arise. At present, such issues of time in responding to an incident are growing increasingly severe. For example, in recent years cyber-attacks have been growing more active, and in particular the ranks of Financial Institutions targeted by such attacks are spreading to include Financial Institutions mainly using shared system centers.⁴⁸ In addition, with the spread of social media the speed at which information spreads through society has increased, so that reputation risk can grow more quickly. Furthermore, increasingly settlement is conducted 24 hours/day, 365 days/year, so that distrust could intensify instantly both day and night. This fact too probably should be considered very seriously.

Another distinguishing feature of shared system centers is the way the impact of a problem in system operation at an individual financial institution could spread immediately to multiple other user Financial Institutions.

It is conceivable that when cooperative Financial Institutions establish management organizations through joint investment they either already are responding to matters such as these through those organizations or will do so increasingly in the future. However, at other cooperative Financial Institutions and regional banks such responses might not be feasible, due to the small number of participating banks, changes in participating banks, or other reasons, so that consideration of individual risk management measures is needed.

4. Ways of thinking on risk management measures specific to shared system centers

Ways of thinking on risk management measures reflecting the above distinctive properties of shared system centers are summarized below.

⁴⁷ Some shared system centers keep numbers of users small in order to shorten the time needed to achieve such consensus. Others specify a leader bank (core bank) and use its leadership to shorten the time needed to achieve consensus. Even in such cases, it has been noted, "In decisions on development projects to realize independent functions, such as new services or functional enhancement, we need to wait for the results of consultation among the joint group, and in not a few cases it takes a long time" (FISC, FY 2010 Regional Financial Institutions IT Research Report, "Consideration of IT Sourcing Strategies at Regional Financial Institutions).

⁴⁸ The amount of damages due to the 2015 Internet banking fraudulent remittance incident reached approximately JPY3,073 million yen, even higher than the 2014 figure, and a look at the details of the victims shows that the number of victimized Financial Institutions doubled, with growth in particular among the numbers of Shinkin banks and credit unions victimized, as well as the presence of agricultural cooperatives and Labour banks among the victims (National Police Agency, Public Report, "Cyberspace Threats in 2015").

First of all, although the existing Security Guidelines do touch lightly on shared system centers under “external outsourcee management,” at the start of their discussion of external outsourcee management and in their discussion of system auditing,⁴⁹ they cannot necessarily be said to reflect the above distinctive properties of shared system centers.

While it is unlikely that differences in the degree of completeness of the decision-making procedures of user Financial Institutions could have decisive effects when information systems are managed with stability in normal times, in the event of an incident, particularly one arising in critical information systems, as noted above there is a possibility that a delay in decision-making could have severe effects.

The Financial Institutions should bear primary responsibility for responding to such incidents, deriving from the nature of the financial industry. It should not be borne by outsourcees responsible for technical aspects related to development and operation of information systems.

If critical information systems involve serious externalities, then their impact could affect the stable operation of the financial infrastructure and the economy as a whole, instead of being restricted to internal effects such as those on customers. Thus there is a need to consider such aspects fully, not just technical recovery of the system. In addition, if the system includes sensitive personal information, then its leakage could spark a run on deposits, leading to credit uncertainty and a situation that could shake the standing of Financial Institutions. As such, responding to incidents requires considerable care.

In responding to issues such as these, the initial response to an incident is vital, and thorough countermeasures need to be implemented even in normal times to ensure that these are the best possible responses.⁵⁰ For this reason, already rules are established to some degree in Security Guidelines and elsewhere. Even so, in light of the matter of time discussed above it would be hard to say that these were enough, and there is a need to take into consideration the possible occurrence of situations not foreseen in CPs and the possibility of delays in the timing of decision-making necessitated by circumstances such as unforeseen situations.

In addition, since the roles and responsibilities of top management are extremely important in allocation of management resources to areas such as maintenance of response structures for incidents or establishing key decision-making authority and processes for responding to incidents, there is a need to consider these from the perspective of IT governance. Under “Use of Cloud Services,” the Security Guidelines could mention reference standards on joint auditing during operation as a form similar to a shared system center in that it involves subcontracting by multiple parties.

With regard to other management phases, since they are only slightly related to the distinctive properties of shared system centers these are not matters that should be given additional consideration.

⁴⁹ At the start of the section on external outsourcee management, the FISC Standards and Descriptions of Security Measures for Computer Systems of Financial Institutions and Other Organizations describe the understanding that “use of ‘shared system centers,’ where multiple Financial Institutions and other organizations jointly use host computers and other systems, is becoming common.” However, with regard to security measures its only statements include “in a case such as a shared system center where operations are contracted by multiple clients, joint auditing by multiple clients may substitute for individual auditing,” and “switching to backup systems (including those installed at backup sites; including enforced switching, decisions and operation procedures for switching based on restrictions during system operation etc., and decisions on switching at shared system centers).”

⁵⁰ Conceivable examples, although these repeat initiatives already implemented, include ① developing decision-making procedures so that they can be completed in reasonable time as much as possible, ② formulating CPs that include all foreseeable situations, and ③ repeating sufficient training in normal times and not neglecting efforts to improve mastery.

5. IT governance specific to shared system centers (forms of formulating risk management measures)

First, top management of user Financial Institutions need to understand the severity of issues of time with regard to responding to incidents. Then, top management of user Financial Institutions need to proceed jointly with prompt study of risk management to resolve such issues.

In such study, it is recommended to formulate staffing plans jointly with user Financial Institutions or outsourcees so that the IT human resources needed to be prepared for incidents can be assigned on a continual basis.

While risk management measures should be studied in light of matters such as the degree of joint use of systems and mutual relations between user Financial Institutions, some examples of conceivable management measures are provided below.

Ex.: Assignment of persons responsible for responding to incidents etc.

Persons responsible for responding to incidents etc. shall be appointed and assigned to carry out operations such as instructing outsourcees in the field under the CP until decision-making is conducted by user Financial Institutions and responding to incidents not foreseen in the CP that require immediate responses.

Persons responsible for responding to incidents etc. shall be granted by user Financial Institutions the authority needed to carry out the above responses, in contracts.⁵¹

In addition, since persons responsible for responding to incidents etc. need to make judgments based on the distinguishing features of the financial industry in response to incidents, staff capable of responding to incidents and carrying out other tasks⁵² need to be chosen from user Financial Institutions.

- Roles of persons responsible for responding to incidents etc. in normal times

Since persons responsible for responding to incidents etc. need to pay attention to the state of operation of systems, for example by never overlooking even minor irregularities in normal times, to be able to respond to incidents, their roles also shall include heading the monitoring organization at the shared system center.

Persons responsible for responding to incidents etc. shall assign staff from user Financial Institutions to take part in continual monitoring activities at all times and consider organizational management based on reports from such staff, including replacement of such activities, bringing together staff from user Financial Institutions, outsourcees, and others in accordance with the circumstances.⁵³

⁵¹ As used here, “contract” refers in general to contracts needed in use of shared system centers, including not only those concluded with outsourcees but also those concluded among user Financial Institutions.

⁵² Conceivable requirements for ensuring that persons responsible for responding to incidents etc. have the aptitude needed to fulfill their roles include whether they are able to rush to the location of the shared system center or management location in the event of an incident such as a natural disaster, large-scale system failure, or cyber-attack so that operations can be carried out. In addition, since important judgments might need to be made quickly in an emergency in which, for example, it is not possible to contact user Financial Institutions, it is conceivable that they should be officers of user Financial Institutions at or above a certain rank.

⁵³ It also is conceivable that the monitoring organization may be made up largely of staff of outsourcees in light of technical considerations. At the same time, in light of the nature of monitoring as a method of management by the client of outsourcees,

- Roles of persons responsible for responding to incidents etc. when an incident arises

When an incident arises in critical information systems, persons responsible for responding to incidents etc. shall carry out operations such as carrying out the CP in the field until decision-making is conducted by user Financial Institutions and responding to incidents not foreseen in the CP that require immediate responses. Even after decision-making is conducted by user Financial Institutions, persons responsible for responding to incidents etc. shall collect information related to the properties of the financial industry in the field and provide such information to Financial Institutions in a timely and appropriate manner, as well as being responsible for providing appropriate advice in light of the situation in the field regarding measures to take in response to the situation.⁵⁴

In addition to the above, while in auditing there is a wide choice of different auditing methods available including individual auditing by Financial Institutions using the shared system center, in order to ensure the efficacy and efficiency of auditing it would be beneficial to employ as one means of auditing at the shared system center the joint auditing scheme considered for cloud services.⁵⁵

clearly it would be appropriate for the manager of the monitoring organization to be selected from the Financial Institutions.

⁵⁴ Necessary cyber security measures include having persons responsible for responding to incidents etc. handle the relevant operations when setting up a CSIRT at the shared system center to conduct not merely technical operations (such as inspection and analysis) but also financial operations (such as decision-making on dealing with Financial Institutions based on the circumstances that have arisen, dealing with customers, and explaining matters to authorities).

⁵⁵ A joint auditing scheme is proposed in FISC's System Audit Guidelines for Financial Institutions and Other Organizations (Third Edition, Expanded), under Part 1: Chapter 3: 5. Key Points of Auditing Cloud Services, identifying related processes and considerations. While it includes the Cloud-specific factor of "establishment of a joint auditing structure," considerations such as "joint auditing processes," "selection of auditors," and "auditor accountability" also would be useful for shared system centers. It is conceivable that in future revisions to the auditing guidelines integrated revisions could be made with consideration for cloud services and shared system centers, as methods of joint auditing when contracted by multiple clients.

VI. Thinking on future revisions to Security Guidelines etc.

The Security Guidelines and other guidelines for the Center will be revised in the future based on proposals from this Council. In doing so, the following points will need to be considered.

(1) The necessity of measures to mitigate dramatic changes

These revisions are expected to differ from previous ones in that they will involve thoroughgoing revisions starting from the way of thinking on application of the Security Guidelines, and their impact on Financial Institutions and other organizations referring to the Security Guidelines is expected to be quite large as well.

For this reason, in consideration of matters such as the possibility that such changes to the Security Guidelines could themselves become risk factors, it will be possible to migrate in order to the revised Security Guidelines and other guidelines at times such as when modifying systems or adopting new systems, while continuing the current handling for information systems currently operating with stability.

However, early migration will be required when problems already have arisen and there is a need to apply the higher-level risk management measures following these changes (e.g., assignment of persons responsible for responding to incidents etc. to shared system centers).

(2) Relationship to the Council of Experts on FinTech (tentative name)

The Center plans to establish a Council of Experts on FinTech (tentative name; “FinTech Council” hereinafter) during this fiscal year as a continuation of the Council of Experts on Outsourcing. Since it is conceivable that the advanced financial services using IT that are referred to collectively as FinTech might often be used in the form of outsourcing, there is a possibility that some revisions or additions to the results of the Council of Experts on Outsourcing might be necessary.

Accordingly, revisions to the Security Guidelines etc. will take place after the completion of the FinTech Council, reflecting the results of both Councils on outsourcing and FinTech.

Policies on revision of the Security Guidelines as envisioned at this time are outlined below.

(1) Addition of basic principles etc. to security measures

New forms of security measures, reflecting the risk-based approach, will be described clearly as ways of thinking on Security Guidelines.

(2) Review of subject systems and ways of thinking on application

Reflecting the basic principles and other considerations, the systems subject to the Security Guidelines and ways of thinking on their application will be revised.

(3) Reorganization of individual standards

In light of the above revisions, standards on outsourcing will be reorganized individually first. Reorganization of other standards will be considered after that.

List of Members and Observers of the Council of Experts on Outsourcing in Financial Institutions

(Honorifics omitted)

Chair	Shinsaku Iwahara	Professor, Waseda University, Graduate School of Law
Assistant Chair	Masahiro Fuchizaki	Representative Director, President & CEO, the Japan Research Institute, Ltd.
Members	Jiro Kokuryo	Vice President, Keio University; Professor, Keio University Faculty of Policy Management
	Masayuki Horie	Professor, Nihon University College of Commerce
	Hiroshi Kamiyama	Partner, Hibiya Park Law Offices
	Hiroki Kameda	Executive Officer & General Manager, Systems Div., The Bank of Tokyo-Mitsubishi UFJ, Ltd. (through fourth meeting)
	Kouji Yonei	Executive Officer/General Manager of IT & Systems Planning Department., Mizuho Financial Group, Inc. (starting with fifth meeting)
	Hisashi Sakaue	General Manager, Administration Div., The Senshu Ikeda Bank, Ltd.
	Eiko Morita	Director/Chief Operating Officer, BNP Paribas Securities (Japan), Ltd
	Masami Suzuki	General Manager, Administration Div., The Sugamo Shinkin Bank
	Hironori Sanada	General Manager In Charge of Information Systems Dept., Sumitomo Life Insurance Co.
	Kousei Asanuma	General Manager, Systems Risk Management Group, IT Div., Aioi Nissay Dowa Insurance Co., Ltd.
	Takashi Hishida	CIO Office (Executive Director), Nomura Holdings, Inc. (through first meeting)
	Motohiro Uemura	Deputy Managing Director, CIO Office (Executive Director), Nomura Holdings, Inc. (starting with second meeting)
	Naoto Watabe	Associate Partner, Financial Third Industry Consulting, IBM Japan, Ltd.
	Teruhisa Ishikawa	General Manager, OSS Solutions Center, ICT Business Div., Hitachi, Ltd.
	Toru Hayashi	Executive Manager, Planning Section, Second Financial Sector, NTT DATA Corp.
Masand Fujita	Senior Director, Financial & Social Infrastructure Sales Group, Fujitsu Ltd.	
Fujio Tanaka	General Manager, Shinkin Banking System Outsourcing Center, Financial Systems First Dept, Financial Systems Second Sector, Nihon Unisys, Ltd.	
Koutaro Narita	Lead Systems Manager, Public Business Unit, NEC Corp.	
Motohiko Nakamura	Certified Public Accountant Executive Board	

Member Information Technology (IT), The Japanese
Institute of Certified Public Accountants

Observers	Nobuo Tabe	Head of Chief Financial Inspectors /Head of Information Technology Monitoring, Inspection Coordination Division, Inspection Bureau, Financial Services Agency (through fifth meeting)
	Sayuri Katayose	Head of Chief Financial Inspectors /Head of Information Technology Monitoring, Inspection Coordination Division, Inspection Bureau, Financial Services Agency (sixth meeting)
	Takuya Okada	Director, Head of Computer System Risk and Business Continuity Group Examination Planning Div., Financial System and Bank Examination Department, Bank of Japan
	Kazuaki Omori	Director, ICT Security Office, Information Security Management Office, Promotion for Content Distribution Divisor, Information and Communications Bureau, Ministry of Internal Affairs and Communications (MIC), JAPAN
	Kazuhiro Uryu	Former Director, Office for IT Security Policy , Commerce and Information Policy Bureau

(Secretariat of the Center for Financial Industry Information Systems)

President		Tatsuo Watanabe
Executive Director		Norikazu Takahashi (sixth meeting)
Planning Div.	General Manager	Toshihiro Horiuchi (through fourth meeting)
Planning Div.	General Manager	Jutaro Kobayashi (starting with fifth meeting)
Planning Div.	Deputy General Manager	Akira Fujinaga
Research Div.	General Manager	Yasushi Nakayama
Security&Audit/Research Div.		General Manager Toshinobu Nishimura
General Affairs Div.	General Manager	Akinobu Saka (through fourth meeting)
General Affairs Div.	General Manager	Kouichiro Mizuno (starting with fifth meeting)
General Affairs Div.	Special Managing Researcher	Makoto Koriyama

◆ Secretariat staff

Akihiro Shibata, Takeya Miyahara (through fourth meeting), Fuminori Nakahodo (starting with fifth meeting), Kazuma Okamoto, Satoshi Miura (starting with fifth meeting)

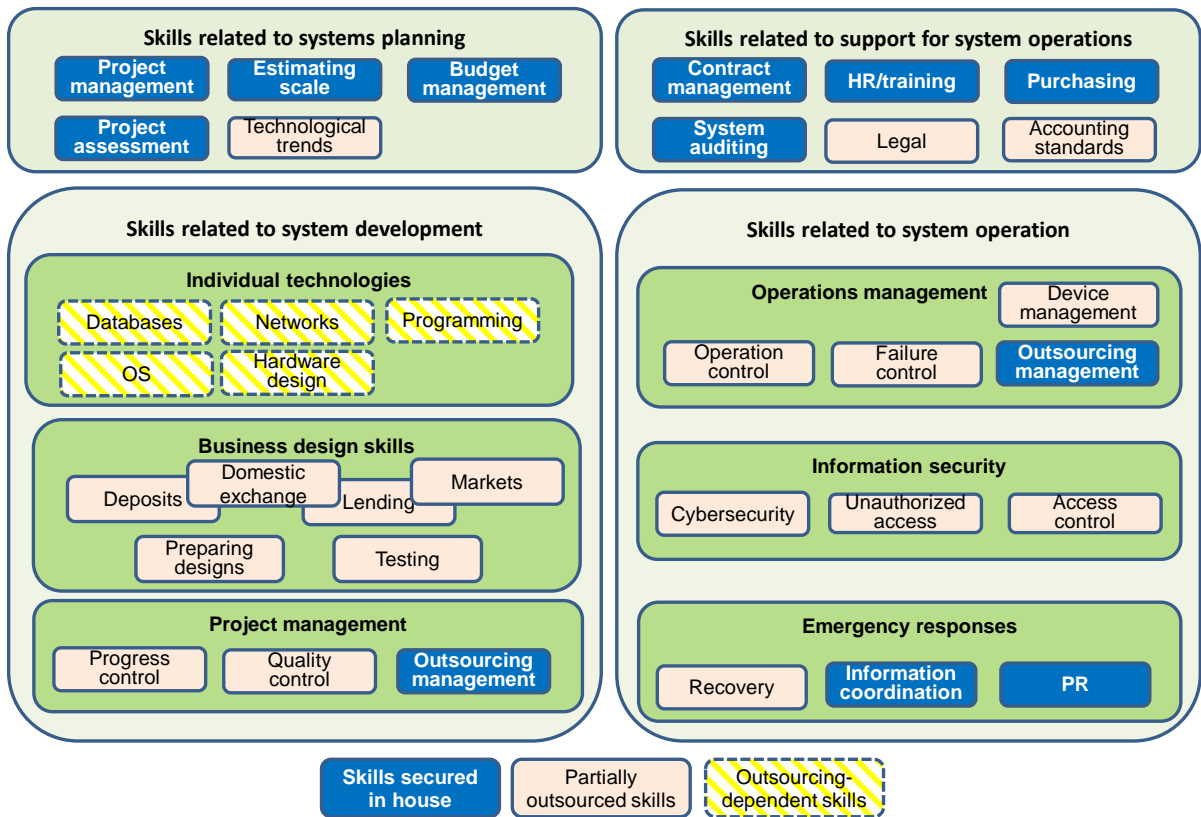
Reference: Council schedule

First meeting: October 26, 2015; second meeting: December 1, 2015; third meeting:

February 3, 2016; fourth meeting: March 23, 2016; fifth meeting: May 12, 2016; sixth meeting: June 27, 2016

VII. References

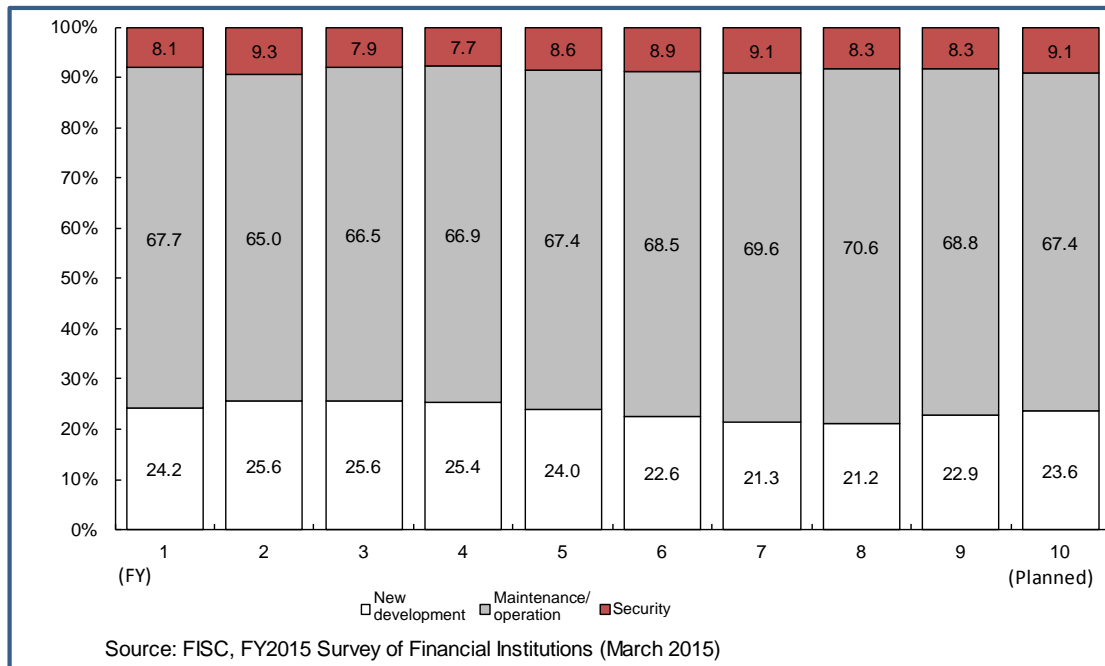
Reference 1: Sample IT skills map



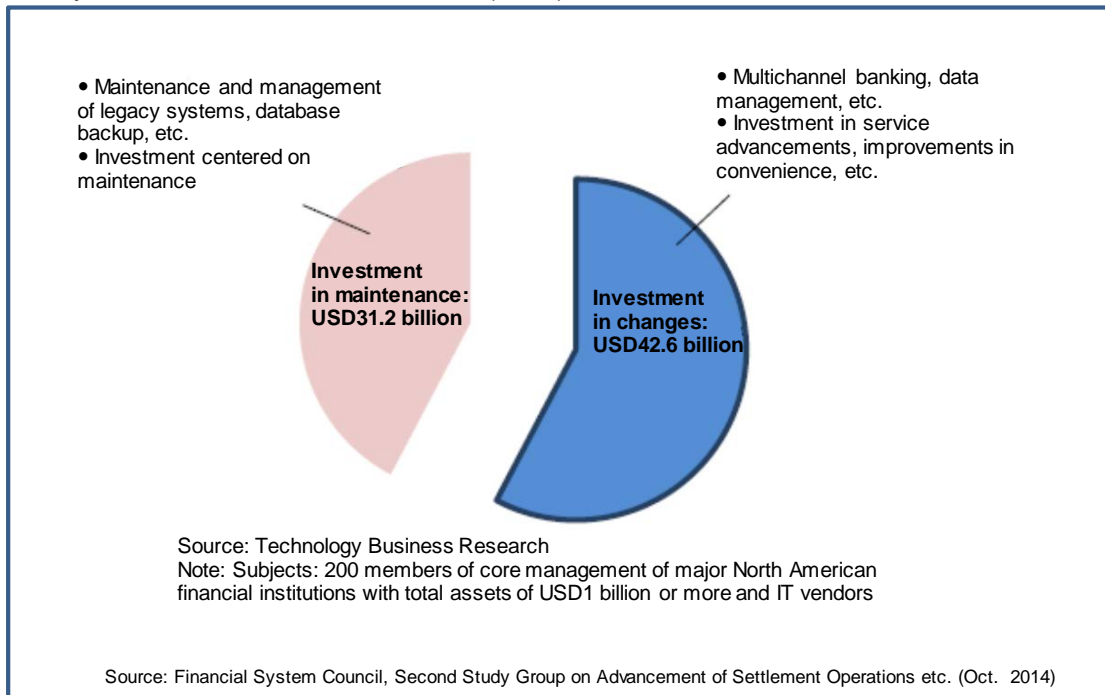
Source: Prepared by FISC

Reference 2: Breakdown of system-related expenses by purpose

Breakdown of IT expenses at Japanese banks by purpose



Priority IT investment fields of US banks (2014)



Reference 3: Trends among overseas regulators and others regarding the risk-based approach

1. Background of the risk-based approach

In Britain, after the passage of the Financial Services and Markets Act in 2000, that year the then-Financial Services Agency (FSA) announced the adoption of the “risk-based approach” as a new regulatory approach. After that, even though a new financial supervisory system was adopted in 2013 after the financial crisis spurred by the collapse of Lehman Brothers and other developments,⁵⁶ there have been no major changes in the existing concept of the “risk-based approach.”

The thinking behind the “risk-based approach” identified by regulators involves tasks such as setting priorities and distributing resources from a regulatory perspective with regard to external risk factors, based on risks for which the policy objectives of regulators are not achieved. According to the official document *Risk-based regulation in the UK* (2005), Risk Appetite is determined from the perspectives of Impact and Probability, and priority is given to responding to risks for which there is a high probability of a problem arising and the impact would be large, rather than all risks for which there is any possibility of a problem arising.

The same document describes the significance of the risk-based approach as follows: “Management resources are not unlimited. It would be infeasible to try to implement an approach that aims to eliminate all risks. This is why there is a need for a system to prioritize tasks. There is a need for optimal distribution of management resources and decision-making.”

As described above, Britain’s risk-based approach is based on thinking about how high is the likelihood of a risk being manifested and how strong of an impact it would have. Enacting this approach is left to the discretion of individual Financial Institutions. This stems from the fact that traditionally British financial regulators have adopted a principles-based approach that respects the autonomy of Financial Institutions. Basically, under this concept each financial institution is expected to decide on and implement appropriate risk-control methods, and regulators will take action if an institution has been confirmed not to be implementing appropriate and sufficient risk controls.

In the U.S., the risk-based approach is considered important, and according to the results of interviews with regulators at the end of the last fiscal year, “It is particularly important for small and medium-sized Financial Institutions to apply the risk-based approach to IT. Trying to get a perfect score in IT leads to massive costs. This approach involves thinking about the extent of measures to take by balancing costs and the damage that would result from a problem. Since small and medium-sized Financial Institutions in particular have limitations on management resources, in some cases in specific IT fields instead of trying to get a perfect score it would be better to divert those costs to other areas.” This confirmed that the risk-based approach is considered important in Financial Institutions’ IT governance.

2. Risk-management measures based on the risk-based approach

① Risk-management measures according to importance

⁵⁶ The FSA, which had been the central regulatory authority, was broken up to form the three agencies of the Financial Policy Committee (FPC), the Prudential Regulation Authority (PRA), and the Financial Conduct Authority (FCA) .

The U.S. and British regulatory systems are based on principles, and guidance and other documents do not necessarily codify matters such as methods of classifying risks and risk management measures in detail. In the interviews with U.S. regulators conducted at the end of the last fiscal year as well, the reason for not codifying such matters was stated clearly: “Codification involves the problem that even better methods might be overlooked and innovation stifled because the codified content becomes absolute.”

At the same time, it was learned that U.S. regulators require the following three points as the minimum level of measures to be taken by Financial Institutions:

- A) Compliance with the Gramm–Leach–Bliley Act (information security measures for purposes such as preventing leakage of information)
- B) Implementing a high level of security measures for high-risk transactions (such as funds transfers)
- C) Formulation of a BCP

Efforts of U.S. and British Financial Institutions include cases of determining importance through rating based on confidentiality, integrity, and availability (CIA) as well as those of determining importance based on the factors of monetary losses and external impact. Normally the system owner reports the results of this determination of importance to the risk management committee where they are subject to deliberation.

In both the U.S. and Britain, regulators require individual banks to decide on and implement management methods corresponding to the importance of transactions in accordance with each bank’s own situation.

② Definition of important operations

Even under such conditions, guidelines on overseas outsourcing both provide particular definitions of “important operations,” for example as “Operations that could have a severe impact on important banking functions or shared services or on customers,” and identify individual management measures.

In Britain, the section on outsourcing (“SYSC8”) of the handbook established by the Financial Conduct Authority (FCA) on outsourcing demands compliance with external outsourcee management measures for critical or important functions identified as those for which “a defect or failure in its performance would materially impair the continuing compliance” of the financial institution. (notification system)

In the U.S., the Office of the Comptroller of the Currency (OCC) guidelines on managing risks associated with third-party relationships require enhanced supervision by top management, through means such as requiring approval by the board of directors as a prerequisite, when outsourcing critical activities, identified as including those with significant impacts on “significant bank functions (e.g., payments, clearing, settlements, custody) or significant shared services (e.g., information technology), or other activities that . . . could have significant customer impacts.”

In Singapore, the Monetary Authority of Singapore (MAS) Technology Risk Management Guidelines, which establish principles and best practices for IT risk management, require the realization of a high degree of availability for critical systems, defining a critical system as “a system, the failure which will cause significant disruption to the operations of the (financial institution) or materially impact the (financial institution’s) service to its customers.”

3. Guidelines on IT governance

The “Management” booklet of the Information Technology Examination Handbook issued in November 2015 by the U.S. regulator the Federal Financial Institutions Examination Council (FFIEC) identifies the positioning of IT governance and IT risk management in Financial Institutions. The following three points can be identified as particular features of that booklet:

- ① Gives concrete form to the roles of the board of directors regarding IT
 - A) Reviews and approves an IT strategic plan that aligns with the overall business strategy (including an information security strategy and cybersecurity threats)
 - B) Oversees the institution’s adoption of effective IT governance processes
 - C) Oversees processes for approving outsourcees
 - D) Oversees IT performance, including projects, budgets, and priorities
 - E) Reviews the adequacy and allocation of IT resources
 - F) Approves a policy to escalate and report significant security incidents to top management, committees, government agencies, and others
 - G) Holds management accountable for the identification of, policies for, and mitigation of IT risks
 - H) Provides for effective audit coverage of IT controls

- ② Explicitly identifies roles of user sections in IT

While it explicitly identifies the roles and responsibilities of the IT committee,⁵⁷ it also prescribes that the membership of this committee include staff of user sections in addition to top management and members from IT and risk management sections. In addition, it also states with regard to the IT risk management posture that managers belonging to user sections also bear responsibility for IT-related operations,⁵⁸ making it clear that it considered coordination with user sections to be important for IT sections.

- ③ Stresses the importance of external outsourcee management (clearly defines the roles of the board of directors)

It clearly identifies external outsourcee management as one of the board of directors’ oversight responsibilities. It also calls explicitly for management of risks of outsourcees in each risk management process (risk identification, assessment, elimination, monitoring, and reporting), showing that in the U.S. external outsourcee management is considered very important and is a high priority in oversight and management.

⁵⁷ Drafting of IT strategies and supervising IT performance in response to the needs of the business side, reporting to management on matters related to IT operations, collection of appropriate information regarding IT and monitoring internal IT resources, supervising the propriety of employee training, etc.

⁵⁸ Examples include operations such as establishing IT support and processes for reporting to business line managers with regard to the needs of the business side, new product development plans, etc.

Reference 4: Thinking on externalities and sensitivity of information

Financial Institutions and other organizations that have the capability to adopt a full risk-based approach (“RBA” hereinafter) should be able, through their own ability, to ascertain accurately matters such as the amounts of economic losses that would arise from the manifestation of a risk. Thus, they should be able to handle matters such as making judgments on risk mitigation and tolerance and efficiently deciding on security measures and allocation of management resources based on these, and as such ideally there should be no need for the provision of rules on these by society.

Notwithstanding the above, the reasons why socially agreed-upon rules can be considered necessary with regard to serious externalities are described below under “Thinking on Externalities.”

In addition, even if no serious externalities are involved, there is a need for special consideration in advance regarding the handling of personal information. The reasons why socially agreed-upon rules can be considered necessary with regard to sensitive information are described below under “Thinking on Sensitivity of Information.”

■ Thinking on Externalities

- As used here, “externalities⁵⁹” refers, for example, to the possibility that a system failure or other problem in the settlement system of an individual financial institution could cause economic losses in society as a whole, including other Financial Institutions and other organizations. For example, due to the nature of settlement systems a severe failure in an individual financial institution’s system could lead to the spread of economic losses by causing distrust in other Financial Institutions and other organizations.
- As used here, “externalities” does not include the customers of individual Financial Institutions. This is because for customers it is possible to identify and respond to individual counterparties and calculate amounts of losses internally.
- On the other hand, even Financial Institutions and other organizations that have the capability to adopt a full RBA are unable to ascertain accurately matters such as amounts of losses related to information systems that involve externalities. That is, it would be difficult for individual Financial Institutions and other organizations to ascertain accurately the amounts of losses sustained by society as a whole as a result of a system failure or other problem, calculate and internalize the costs needed to prevent such failure, and reflect these properly in drafting security measures.
- While it would be possible to return part of the amount of losses sustained by society through compensation for damages after the fact, in that case too it would be difficult to identify the portion for which the relevant financial institution was responsible amid the complex chain of cause and effect if it involved distant links in the chain of settlement. (When also taking into consideration matters such as legal jurisdiction and enforcement across international borders and the hurdles of the costs of litigation, only a small portion of such losses would be likely to be returned.)
- Under such conditions, Financial Institutions and other organizations also might make decisions on security measures by leaving all or part of the societal impact of failure of their systems out of the scope of consideration for the above reasons and due to other factors such as incentives (moral hazards).
- In order to address such issues appropriately, rules such as those specified as “necessary” (i.e., those corresponding to high-level security guidelines) are needed for systems involving serious externalities with particularly high levels of risk, as rules common to Financial Institutions and other organizations.

⁵⁹ The term “externality” does not mean “outsourcing” or “third party.”

■ Thinking on sensitivity of information

- Personal information is subject to a legal and regulatory framework including the Personal Information Protection Act, and Financial Institutions and other organizations need to comply with this framework when implementing security measures for their computer systems.
- However, the personal information handled by Financial Institutions and other organizations is varied and diverse, ranging from information such as names and addresses to highly sensitive information such as records of people’s lives, including their medical histories. It would not be appropriate to handle such sensitive information without differentiating it from general personal information.
- If both these types of information were handled in the same ways, then personal information, which is present in nearly all computer systems of Financial Institutions and other organizations, would need to be subject to excessive security measures as a result of such sensitive information, and this could result in excess allocation of resources.

Reference: Guidelines on Protection of Personal Information in the Financial Sector

Article 6. Sensitive information

1. Businesses that handle personal information in the finance sector must not obtain, use, or provide to third parties information concerning political views, creed (i.e., religion, thought, or beliefs), labor-union membership, ethnicity or race, family status and legal domicile, health, medicine, or sexual lifestyle, or criminal record (“sensitive information” hereinafter), except in the following cases.
 - ① . . . (omitted)
 - ② When using biometric information corresponding to sensitive information for purposes of personal identification, with the consent of the individual concerned

- In order to avoid such circumstances, it would be appropriate to separate personal information into sensitive information whose protection should be subject to the highest level of security measures from other personal information, and to apply rules such as those specified as “necessary” (i.e., those corresponding to high-level security guidelines) for sensitive information in the same way as for systems involving serious externalities.
- Since leakage of sensitive information without the consent of the individuals concerned could lead to wide-ranging damages not limited to just economic losses but also including infringement of fundamental rights, its handling can be considered to be of a social and public nature. For this reason, it would be reasonable to handle it in the same way as systems involving serious externalities.

Naturally, Financial Institutions and other organizations may determine on their own that some of their information systems may, for various reasons, involve a degree of risk similar to or exceeding those of information systems involving serious externalities or those containing sensitive information (information systems included under (a) in the simplified RBA on p. 33 [Fig. 16]). It would be reasonable in a sense for individual Financial Institutions and other organizations to apply to such information systems rules such as those specified as “necessary” (i.e., those corresponding to high-level security guidelines), and of course it is conceivable that they might implement even higher-level measures in light of the risks involved.

Reference 5: FFIEC IT Examination Handbook: Management: Third-Party Management

Action Summary

As part of a financial institution's third-party management program, management should ensure that third-party providers effectively provide support by doing the following:

- Negotiating clear and comprehensive contracts with appropriate terms that meet the institution's requirements.
- Ensuring receipt of audited financial statements from third-party providers at least annually.
- Reviewing results of independent audits of IT controls at third-party providers.
- Monitoring the responsiveness of third-party provider's customer service, including client user group support

Financial Institutions increasingly rely on third-party providers and software IT solution providers. Larger or more complex institutions are more likely to have institution-wide third-party management programs that encompass all of these relationships. IT departments can contract with third-party providers for several services, including data processing, software development, equipment maintenance, business continuity, data storage, Internet access, and security management. In smaller or less complex institutions with less formal third-party management programs, the procurement of third-party services should be reviewed by institution staff familiar with the operational, financial, security, and compliance requirements for such relationships. The oversight of the relationship should be performed by staff with knowledge of the services provided.

The board of directors should hold senior management responsible for ensuring appropriate oversight of third-party relationships. Technology needed to support business objectives is often a critical factor in deciding to outsource. Managing such relationships is not just a technology issue; it is an enterprise-wide governance issue. An effective third-party management program should provide the framework for management to identify, measure, mitigate, monitor, and report risks associated with the use of third-party providers. Management should develop and implement enterprise-wide policies and procedures to govern the third-party management program, including establishing objectives and strategies, selecting a provider, negotiating the contract, and monitoring the outsourced relationship.

Management should evaluate the quality of service, control environment, and financial condition of the third parties providing the institution with critical IT services.⁶⁰ Third parties can include financial institution affiliates, other Financial Institutions, and third-party service providers. As appropriate, these third parties should support the responsibilities of their financial institution clients to adhere to all applicable laws, regulations, and supervisory guidance. Financial institution management should expect third-party support at a level consistent with the criticality of the services provided to the institution.

When financial institution management contracts with third-party providers for some or all IT services, it should ensure that controls over outsourced activities provide the institution with the same level of assurance as controls over those activities performed in-house. Management

⁶⁰ With regard to outsourcing of critical operations, Britain requires Financial Institutions to submit notice to regulators when planning to outsource critical operations while Singapore requires Financial Institutions to submit notice to regulators before outsourcing critical operations or making adjustments to existing outsourcing of critical operations.

should also consider additional oversight or controls over third-party providers that operate in foreign locations. Management should have mitigation strategies that address risks related to foreign-based third-party providers, if applicable. In the event that the financial institution locates any of its own operations offshore and develops third-party relationships at those locations, specific risk mitigation plans should be considered to address related foreign-based third-party risks.

Management should address exposures from third-party risks through an effective third-party management program. Some factors that management should consider or address include the following:

- Assessing whether each third-party relationship supports the institution's overall objectives and strategic plans.
- Evaluating prospective third-party providers based on the scope and importance of the services they provide.
- Tailoring the institution's third-party management program based on an initial and ongoing risk assessment of the institution's third parties and the services they provide.

The time and resources devoted to managing third-party relationships effectively depend on several factors, such as the critical nature of outsourced processes, staff knowledge, and complexity of systems.

(Emphasis in original, underlined by FISC.)

Reference 6: History of shared system centers

1. Cooperative Financial Institutions

Use of shared system centers by Shinkin banks began with the steady establishment, starting in 1971, of joint administrative centers in seven districts across Japan. In 1985, Shinkin Information Systems Center K.K.⁶¹ was established, and in 1987 the joint administrative centers migrated to 3G online systems. Following that, the district shared system centers were consolidated into two centers (east and west), and today they are operated by Shinkin Kyodo Center established in April 2013. At present, more than 90% of the Shinkin banks in Japan (244 as of March 2015) use Shinkin Kyodo Center.

Among credit unions, in 1985 Shinkumi Information Service Co., Ltd.⁶² established a national shared system center for credit unions,⁶³ and it began operating 3G online systems in 1991. It maintains the same structure today, and more than 90% of the credit unions in Japan (146 as of March 2015) use its services.

Among Labour banks, a joint administrative center for the greater Tokyo area was organized in 1971, and it began online operation in 1978. After that, a general administrative center for Labour banks was established in 1989, and in 1990 an online system used jointly by all 13 Labour banks in Japan (Unity) began operation. In 2014, the All One System began operation as the successor to that system.

Among agricultural cooperatives, Nochu Information Processing Co., Ltd.⁶⁴ was established in 1981, and today a system (JASTEM) that began operation in 1999, operated by the Norinchukin Bank,⁶⁵ is used by all agricultural cooperatives.

2. Regional banks

Use of shared system centers by some Second-tier regional banks (at the time called mutual banks) began in 1975 when SBK was established to serve eight banks located in the Kyushu region. It began offering joint online services in 1977, and since then its services have included joint use of accounting systems and joint purchase of ATMs and computer terminals for business use.

Since around 1998 regional banks have steadily begun using shared system centers aiming to keep down IT costs, increase IT staff through expanding the domains covered by computer systems, and adapt to technological advances. At present, six IT solution providers operate 13 types of shared system centers, and more than 70% of regional banks use shared system centers. Mainly, regional banks that do not compete with each other for business will use a single shared system center together, striving to cut IT costs and IT staffing requirements and enhance system functions and services through use of the expertise of early adopters, among other aims.

⁶¹ Financed with investment from each Shinkin bank (100% of total investment).

⁶² Financed with 90% investment from the Shinkumi Federation Bank and the remaining 10% from credit unions.

⁶³ Consisting of the following two organizations: the SKC Center (national shared system center for credit unions), handling accounting and information systems, and the Zenshinkumi Center, serving as a central facility mainly handling settlement operations.

⁶⁴ Financed with 90% investment from the Norin Chukin Bank and 10% from NTT Data. Renamed Nochu Information System Co., Ltd. (NIC) in 1984.

⁶⁵ Development and operation subcontracted to Nochu Information System Co., Ltd. (NIC).

Reference 7: Timeline of use of shared system centers

Business	Cooperative Financial Institutions				Regional banks ⁶⁶	
	Shinkin banks	Credit unions	Labour banks	Agricultural cooperatives	Regional banks	Second-tier regional banks
1965-1984	April 1971: Steady establishment district of joint administrative centers		Nov. 1971: Joint administrative center for the greater Tokyo area established (established for other regions later)			1975: SBK established to serve eight banks located in the Kyushu region
			May 1978: Online use of joint administrative centers begins	May 1981: Nochu Information Processing Co., Ltd. (NIC) established		Oct. 1977: Joint online services begins operation
1985-1997	Feb. 1985: Shinkin Information Systems Center Co., Ltd. established Nov. 1987: Joint administrative centers migrated to 3G online systems	May 1985: Shinkumi Information Service Co., Ltd. established; national shared system center for credit cooperatives established	Dec. 1989: General administrative center for Labour banks established			
		May 1991: 3G online systems begin operation	May 1990: New online system (Unity) begins operation			May 1997: STAR-ACE begins operation (Nagano Bank) (discontinued 2013)
1998-2007				Oct. 1999: JASTEM system begins operation	May 2011: Bank computer services begin operation (former Senshu Bank, Tottori Bank) (discontinued in 2015) March 2002: Judankai begins operation (Hachijuni Bank)	Jan. 2000: STAR-21 begins operation (Sendai Bank) (discontinued 2013) Jan. 2001: Second-tier regional bank outsourcing center begins operation (former Shokusan Bank, Fukushima Bank)
	Jan. 2003: Hokkaido Shinkin Outsourcing Center begins operation Jan. 2005: SBOC Tokyo begins operation April 2006: Shinkin joint system operation structure established Sept. 2006: Shinkin Nishi-Nippon Solutions Center begins operation			(May 2006: Deployment of JASTEM system completed)	Jan. 2003: Flight21 begins operation (Bank of Fukuoka) Jan. 2003: Banks'ware begins operation (Higo Bank) Sept. 2003: PROBANK begins operation (Toho Bank) Jan. 2004: Regional bank shared system center begins operation (Bank of Kyoto) Jan. 2007: Chance begins operation (Joyo Bank) May 2007: BankVision begins operation (Hyakugo Bank)	May 2003: BankingWeb21 begins operation (Yachiyo Bank) May 2005: Nextbase begins operation (Tokushima Bank)
2008-present	Sept. 2011: Consolidation of hardware on two east/west centers completed April 2013: Reorganized to Shinkin Kyodo Center	May 2015: 6G system begins operation	Jan. 2014: New online system (R-One System) begins operation	May 2011: Migration to next-generation JASTEM system completed (consolidation on two centers: Kanto and Kyushu)	March 2008: TSUBASA Project begins Jan. 2010: MEJAR begins operation (Bank of Yokohama) Oct. 2010: STELLA CUBE begins operation (Tokyo Tomin Bank) March 2013: BeSTAcloud begins operation (Shonai Bank)	

Source: Prepared by FISC

⁶⁶ Financial Institutions in parentheses are the first to adopt the systems. When user Financial Institutions include both regional banks and second-tier regional banks, systems are shown in the column for the first user financial institution's business type.

Reference 8: Deposits of Financial Institutions using shared system centers

The numbers of Financial Institutions using shared system centers for accounting systems as of March 2016 and their total deposits are shown below.

Business	Name of system	Number of Financial Institutions	Deposits (JPY100 million)*
Shinkin banks	Shinkin Kyodo System	244	1,002,298
	Shinkin Nishi-Nippon Solutions Center	3	35,924
	SBOC Tokyo	3	33,061
	Hokkaido Outsourcing Center	5	23,045
Credit unions (Shinkumi banks)	SKC Center (nationwide shared system center for credit associations)	145	176,201
	Maple Hiroshima	4	6,012
Labour banks	R-One System	14	178,509
Japanese Agricultural Cooperatives banks	JASTEM system	(47 members of federation of agricultural and credit cooperatives)	936,872
Regional banks, Second-tier regional banks, etc.	Regional bank shared system center	14	459,500
	Chance	7	300,017
	MEJAR	4	295,038
	BankVision	9	264,585
	Judankai	7	208,524
	Flight21	4	187,813
	Nextbase	11	142,386
	TSUBASA	1	107,333
	Banks'ware	3	95,622
	STELLA CUBE	8	80,101
	PROBANK-R2	3	76,105
BeSTAcloud	2	23,663	

(City banks, for reference)

The Bank of Tokyo-Mitsubishi UFJ,Ltd.	-	1,245,909
Sumitomo Mitsui Banking Corporation.	-	942,600
Mizuho Bank,Ltd	-	935,283
Resona Bank,Limited.	-	320,882

*1 Balances shown are current as of March 2015, not including those of Financial Institutions planning to migrate to shared system centers. Figures for regional banks, second-tier regional banks, shinkin banks, and credit unions are based on deposit figures from *Nikken Kinyu Techo*, while those for agricultural cooperatives are from the JA Bank website.

Source: Prepared by FISC

Reference 9: Issues addressed by this Council and related measures

