August 2006

Discussions on Further Advancing Operational Risk Management (2)
Summary of Discussions of the "Study Group for the Advancement of Operational Risk Management"

I. Introduction

In June, the Study Group for the Advancement of Operational Risk Management (hereinafter referred to as the Group) published information on the five sessions held to that time.[1] The Group was inaugurated in November 2005 and comprises experienced practitioners of operational risk management. The Center for Advanced Financial Technology of the Bank of Japan's Financial Systems and Bank Examination Department serves as the Group's Secretariat (see Appendix for members' list). Since its establishment, the Group has identified points at issue with respect to further advancing operational risk management, and debated possible approaches for dealing with them. This paper resumes where the last published paper left off, providing a summary of the discussions from the sixth through the eighth (and final) sessions.

As in the preceding paper, this paper does not intend to draw conclusions for each of the issues discussed. It simply presents issues and discussions concerning the advancement of operational risk management. Opinions here are those of members and do not necessarily represent those of the organization each member belongs to.

II. Discussions at the Sixth Session (held on April 20, 2006)

A. Maintaining data (internal loss data) concerning operational risk

1. Potential Issues

(1) Scope of operational risk and loss assessment methods

The scopes of market and credit risk are relatively clear because they are based on transactions traditionally handled by specific risk control sections. However, the scope of operational risk is not necessarily as clear for two reasons: (1) all business lines are exposed to it, and (2) maintaining data for quantification purposes has a short history. For this reason, while some banks classify an event into operational risk, other banks classify the same event into other risk categories such as credit, market or strategic risk, rather than operational risk. Moreover, there are problems concerning methods for assessing the amount of losses when operational risk loss events occur, such as inconsistencies of loss-measuring methods due to a variety of related transactions and the lack of consensus arising from the fact that operational risk management itself has a short history.

[1] Discussions on Further Advancing Operational Risk Management (1) were disclosed externally on June 12, 2006 in Japanese and on August 16, 2006 in English (see below for the respective URLs).
Japanese: http://www.boj.or.jp/type/release/zuiji_new/fsc0606a.pdf
English: http://www.boj.or.jp/en/type/release/zuiji_new/fsc0608c.pdf

(2) Risk factors and causality

In the case of operational risk, it is difficult to narrow down the factors causing such risk to materialize, and quite often it only materializes when several causes occur simultaneously. When maintaining loss data, therefore, difficulties arise in (1) judging whether specific losses (such as indirect losses or losses damaging to third parties, mentioned below) arise from operational risk or not; and (2) handling loss events spanning multiple business lines and event types, etc.

Moreover, while indicators exist to show the probability that market risk or credit risk may arise before losses actually occur (trends in risk factors or internal ratings in market transactions, etc.), there are no known indicators that could be decisive in forecasting losses arising from operational risk in the near future. Currently, banks are discussing the collection of near-miss data[2] and methods for addressing risk quantification of BEICF (Business Environment & Internal Control Factors), such as KRI (Key Risk Indicators) and CSA (Control Self-Assessment). As yet, however, no consensus has been reached on methods for appropriately identifying heightened risk before losses actually occur (i.e., what sort of data should be used and how).

2. Participants' Views

In addition to focusing on the continuity of risk management, banks must clarify classification standards for risk categories in order to prevent suspicions of regulatory arbitrage from arising.

[2] While the definition of a near miss is not yet properly established, one possible example is an error that did not develop into a loss because it was discovered and corrected at a certain stage of a transaction. Depending on the definition of losses in such cases, the scope of events that might be classified as near misses could narrow considerably (for example, if the personnel costs for subsequent responses to certain clerical errors were recognized as losses, the scope of "mistakes that are not accompanied by losses" would become extremely narrow).

Classification standards for risk categories (examples)

(1) Credit risk	-- Under Basel II, overlapping events between credit risk and operational risk should be quantified as credit risk. However, any serious events that are treated as credit risk events for quantification purposes should also be identified as operational risk events if they assume some operational risk characteristics. -- Since the credit risk management function does not for management purposes distinguish damage to credit caused by clerical errors from damage to credit caused by general materializations of credit risk, there are cases where the operational risk control function is responsible for qualitative controls such as measures to prevent the recurrence of clerical errors pertaining to credit operations. In such cases, a possible conservative approach is to identify and quantify overlapping events not only as credit risks but also as operational risks.
(2) Market risk	-- Losses arising from market operations, etc., should be treated as operational risk if the causes of the losses are operational risk. -- There are cases where losses are only treated as arising from operational risk if the trading rules are contravened; for example, position limits are breached.
(3) Strategic risk	-- Strategic risk falls outside the purview of Pillar I of Basel II (excluded from risk quantification), but the demarcation line between strategic and operational risk is not always clear. Against this background, there are cases where losses are treated as arising from operational risk when there are flaws in strategic judgment procedures or in the information providing the basis for such judgments behind each loss case.
(4) Settlement risk	-- Among the accidents occurring in payment and settlement of business, some have been treated as traditional risk related to manual operations or settlement risk events, even when they were fundamentally credit risk events. In this connection, if loss events are not necessarily subject to credit risk management from a regulatory capital viewpoint (including trading book risk management), it is possible to consider managing them as operational risk and making them the objects of quantification.

Further, in cases where loss events are treated not as arising from other risk categories but as from operational risk, it is necessary to clarify the matters stated below.

a. Scope of loss recognition

Other than direct losses, there are cases where so-called indirect losses and reputation losses are widely recognized.

Scope of loss recognition (examples)

	Concrete details	Examples of treatment
(1) Indirect loss, opportunity loss, opportunity cost	-- System-related repair costs, customer account restoration costs, litigation-related costs, payments to external consultants and vendors, etc., personnel overtime payments, research expenses, transportation expenses, reduction or remission of commissions receivable/loan interest, opportunity costs from suspension of business.	(a) Opportunity costs are collected, limited to cases where there is a clear link to causal events. (b) Opportunity costs and reputational losses are not collected because it is difficult to identify the amounts objectively and it is not required under Basel II.
(2)Reputational losses	-- Revenue reductions due to decline in reputation.	
(3) Profits arising from operational risk events	-- Profits posted during ex post facto processing of trading errors.	-- Identified as risk events, but not used in quantification.
(4) Quick Recovery	-- Remittance error recovered on the same day that the event occurs.	(a) For remittance errors occurring in inter-bank operations, only those amounts that could not be recovered on the same day that the events occur are recognized as gross losses. However, errors occurring in customer remittances are recognized across the board as gross losses regardless of whether they are recovered on the same day that the events occur. (b) Where remittance errors occur, amounts that cannot be recovered on the same day that the events occur are recognized across the board as gross losses irrespective of whether they arise in inter-bank operations or not.

(5) So-called "timing losses"	-- Overestimations of earnings arising from accounting errors, excessive collections of commissions, etc.	-- Recognized as losses in cases where they are treated as miscellaneous losses in subsequent accounting periods and the excessive profit posted is refunded. However, they are not recognized as losses when the excessive profit posted is refunded during the current accounting period.

There are two aspects to threshold values (minimum values) in the cases where loss data are collected–threshold values from the data collection perspective, and threshold values for the data used in risk quantification. Both should be set after taking into consideration the operational risk management situation at each bank.[3] The lower the threshold setting is, the easier it is to identify and quantify risk more accurately, but data collection costs increase. In practice, there are some cases where financial institutions set higher threshold values for risk quantification purposes than for data collection purposes, and cases where they set lower threshold values for specific sections than for the threshold values common to the entire bank in order to use the collected data for internal controls.

In view of the small number of internal loss data samples and other factors, it is useful to collect so-called near-miss data on the broadest possible scale and to use them in scenario analyses, etc. irrespective of whether they are used in quantifying operational risk. In fact, there are cases where financial institutions collect near-miss data from certain operations and use them in qualitative risk management. However, it is difficult to collect comprehensive near-miss data for the whole bank.

b. Timing of losses

One particularly problematic point at issue is when to recognize the amount of compensation from lost lawsuits, etc. as losses. In this connection, many institutions recognize losses at the point when allowances are made for them in financial accounting. When large amounts of compensation are forecast, however, there are cases where they are reflected in operational risk quantification prior to financial accounting procedures by reflecting the expected compensation value in scenario analysis data.

c. Handling loss events across business lines, etc.

[3] How threshold values are set may affect risk quantification results (especially Expected Loss, EL). How to set threshold values is not a big issue for Japanese banks because many of them set relatively low threshold values, but it is an important issue internationally.

The treatment of loss events that span risk classes such as business lines or event types[4] can be discussed in the same vein as the dependencies discussed at the Third Session and thus may greatly affect quantification results.

Moreover, it may be better to aggregate loss events, among which we also find some commonality in causality or linkage in cases where they belong to the same risk classes. Judging the commonality or linkage of causality referred to here will inevitably be somewhat subjective. For this reason, it is probably necessary (1) to determine certain standards, for example, the cases that are likely to occur simultaneously with a high probability should be combined, to enumerate methods for evaluating typical cases; and (2) to record the details and grounds for individual decisions.

Concrete examples of losses spanning business lines, etc.

(1) Losses spanning multiple times, locations	-- The same earthquake damages multiple branches. -- Typhoons cross the Japanese Archipelago over a period of a week, damaging branches in various locations. -- The same criminal uses various tricks to misappropriate the deposits of multiple customers. -- Multiple faults occur in the same computer system on different business days, but when the origins are investigated, it is recognized that the causality is the same.
(2) Losses spanning event types	-- Earthquakes damage branches (damage to physical assets), and business is suspended for five days. -- Exploiting lax supervision during work to restore services, an employee embezzles cash (internal fraud) or an outside criminal commits theft (external fraud).
(3) Losses spanning business lines	-- Earthquakes damage the head office building (accommodating multiple businesses). -- A bank's overall operations are seriously delayed by a major fault in its accounting systems, generating losses for all the bank's internal business lines from damages to customers and repayments of commissions, etc.

d. Methods for assessing losses

Using the accounting amount (book value) is one way of assessing loss amounts, but with respect to damage to physical assets, there are cases where institutions ascertain the replacement cost (market value), compare it with the book value, and use the amount closer to the actual loss.

[4]Possible treatments of losses spanning risk classes include (1) regarding them as a specific risk class (with the largest loss amount, etc.), and (2) quantifying risk for each risk class without bias, then making necessary adjustments while taking into consideration the impact of dependencies when aggregating overall operational risk for the financial institution as a whole.

III. Discussions at the Seventh Session (held on May 26, 2006)

A. Maintaining data (external data) concerning operational risk

1. Potential Issues

The basic issue when using external data is whether it is appropriate to apply examples from other organizations to one's own organization. Other points at issue include the quality of external data, mapping external data (to risk classes), and information management and internal controls at data consortia.

2. Participants' Views

It is possible to use external data for benchmarking analyses, scenario analyses, and supplementing internal data when quantifying operational risk. Such usage allows banks to check whether incidents and accidents arising at other organizations may occur in their own organization, and to introduce some counter-measures.

If reliable external data exist, the need to use them as benchmarks will probably be considerable. Using the various parameters of external data is also likely to allow the use of parametric quantification methods as well as nonparametric quantification methods. For this reason, one can assume there is a definite need for public institutions and industry associations, etc. to collect data and publish statistics.

Currently, participation in data consortia is progressing slowly because of concerns about the reliability of data and the risk of information leaks. In general, use of external data is confined to gathering information through newspaper clippings and the like, and using it as reference information in drawing up scenarios.

B. Maintaining data concerning operational risk (validating internal loss data)

1. Potential Issues

Validation systems should be maintained to ensure the quality of internal loss data (comprehensiveness and accuracy), but in practice there is not yet sufficient convergence with regard to concrete validation methods.

2. Participants' Views

Possible methods for validating internal loss data include: (1) checking against accounting figures; (2) validating consistency with qualitative data (statements in clerical malpractice reports, complaint handling records, and anomalous transaction management records, etc.); and (3) comparisons and consistency checks of internal loss data among sections. Other possible measures include incorporating a validation mechanism into loss reporting systems, and the validation of these validation systems themselves using CSA and internal audits.

In general, these validations are conducted by the risk management section, supplemented by the internal auditors.

C. Internal controls concerning operational risk and their application in management

a. Managerial involvement

1. Potential Issues

There are unlikely to be any objections to the argument that management (defined in this paper as officers ranging from sectional managers up to board members) are responsible for, and need to play a leadership role in, advancing operational risk management. However, this does not mean that sufficient convergence has been reached on a de facto practical standard approach to the specific functions to be fulfilled by each management rank, or the extent to which they should understand methods to advance operational risk management.

Specifically, the points at issue are the extent to which management should understand details of advanced methodologies (risk quantification models, scenario analyses, CSA), and outputs based thereon, and the extent of managerial involvement (both of which differ according to job rank). Of course, the nature of any such involvement will probably differ according to the size of the financial institution as well as the scope and complexity of its business.

2. Participants' Views

Bearing management policies and the risk situation in mind, it is necessary for individual financial institutions to clarify the extent to which each management rank (board of directors, CEO, executive officers, sectional managers) should understand the types of advanced methodologies, and get involved in maintaining them. Requirements pertaining to understanding and involvement may differ according to individual financial institutions and management ranking.

Among the items that management should check at this time are: (1) whether the operational risk assessment framework or results of risk evaluations are consistent with management policies, business models, and the current state and outlook of internal and external environments; and (2) whether the basic policy for operational risk management, priority measures on the risk management policy, and the allocation of operational risk capital are consistent with the matters stated in (1), the bank's overall risk capital situation, or the allocation of management resources.

Items required for managerial understanding of and involvement in advancement methodologies (examples)

Quantification models	-- Quantification results -- Important matters for understanding quantification results <Examples> Elements having a major impact on quantification results, and the extent to which they cause quantification results to fluctuate. -- Major characteristics of models <Examples> Methods of using the so-called "four elements" (internal loss data, external loss data, scenario analyses, BEICFs), types of distribution, reasons for selecting types of distribution, and methods for estimating distribution.
Scenario analysis	-- Key scenario content -- Results of scenario analyses, procedures <Examples> Scenario lists (scenario summaries, items that reveal frequency and severity), and procedures (methods for drawing up scenarios, verifiers, approaches to validation).
CSA	-- Overviews of CSA results, assessment results <Examples> Risk distributions that provide an overall view of the total financial institution. -- CSA procedures <Examples> Assessment results, implementation systems (implementation procedures, implementation units), validation systems (content of validation, sections in charge of validation, etc.).

IV. Discussions at the Eighth Session (held on June 14, 2006)

A. Internal controls concerning operational risk and their application in management (continued)

b. How to establish a system that provides effective challenges to operational risk management

1. Potential Issues

Although the system and methodologies of effective challenges for advanced operational risk management do not differ from those for other risk categories, the short history of advancing operational risk management poses difficulties in the form of a dearth of common understanding and accumulated skills. In particular, there are problems with: (i) details and methods of challenging the various kinds of advancement methodologies; (ii) documentation; (iii) the functions required of middle offices;[5] and (iv) the functions required of internal audits.

2. Participants' Views

(i) Details and methods of challenging the various kinds of advancement methodologies

[5] In this paper, this refers to sections (supervisory sections) that fulfill an operational risk control function, and subsections that fulfill a role in supplementing these operational risk control functions. For details, please refer to "Discussions at the Eighth Session" below.

It is thought to be particularly necessary to challenge technical elements and elements that depend heavily on subjective judgments.

Details and methods of challenging the various kinds of advancement methodologies (examples)

	Internal challenges (Self challenges by each section)	External challenges (Challenges by other sections in the bank)	Internal audits
Quantification models	-- Use back-testing (comparisons with internal and external loss events).[6] -- Use external consultants to supplement internal challenges.		-- Validate the model's validation system. -- Validate the model itself. -- Use external auditors.
Scenario analyses, CSA	-- Internal section challenges on the process of approving scenario analysis , etc.	-- Validate the appropriateness and comprehensiveness of assessments through horizontal comparisons between sections. -- Validate using external consultants to supplement external challenges. -- Compare with internal loss events.	-- Validate assessment system. -- Validate assessment contents.
Loss data collection	-- Confirm amounts and details of loss events when collecting data.	-- Validate compliance with data collection rules (gross/net losses rule, etc.). -- Validate comprehensiveness and integrity of data through horizontal comparisons between sections. -- Confirm consistency with financial accounting figures.	-- Validate the data collection method and system. -- Validate the integrity and comprehensiveness of the data.

(ii) Documentation

Documenting the details of methods for advancing operational management requires enormous costs, particularly when completing the initial documents and constantly

[6] While there are limitations based on the amount of data, it should be possible to some extent to validate the appropriateness of extremely unrealistic hypotheses, etc., using internal and external loss data as a reference.

updating them. However, documentation has several advantages: (1) it enhances the ability to explain the state of internal controls to interested parties inside and outside the bank; (2) it allows knowledge to be shared within the bank; and (3) it enhances the proper business processes. Since the outputs from advancement methodologies (risk quantification results, etc.) tend to be more and more important to business judgments, suitable documentation becomes all the more necessary in terms of its accountability.

With regard to documentation contents, it is important that management board members understand and approve the key points at issue according to their official responsibilities, and those independent third parties such as internal auditors validate them.

Documentation should refer to matters that may not be easily observable but have a substantial impact on quantification results (such as prerequisites for quantification), or matters that depend greatly on scenario analyses and other subjective judgments.

Documentation items (examples)

<table>
<tr><th></th><th>Specific matters</th><th>Caveats</th></tr>
<tr><td>Quantification models</td><td>-- Matters that are generally deemed important where quantification models are concerned, such as confidence intervals or the Monte Carlo simulation technique.
-- The distribution type selection process
-- Details and results of validation
-- Details and results of sensitivity analyses
-- Methods for estimating parameters
-- Methods for classifying loss events into risk quantification units
-- Methods for dealing with dependencies between data in different units</td><td>-- It is important to prepare easily understandable documentation concerning the impact according to differences in prerequisites and adoption methods on quantification results.</td></tr>
<tr><td>Scenario analysis</td><td>-- Analytical procedures
-- Standards for estimating loss frequencies and severity</td><td rowspan="3">-- Where standards are difficult to describe in writing, provide sufficient examples to enable sections within the bank to deal with them in a consistent way.</td></tr>
<tr><td>CSA</td><td>-- Assessment procedures
-- Assessment standards</td></tr>
<tr><td>Data</td><td>-- Standards for recognizing and identifying losses
-- Gross loss or net loss, single loss or multiple losses, timing of recognition, methods for assessing amounts, threshold values, etc.
-- Classification standards for risk quantification units
-- Methods for dealing with dependencies (data aggregation methods, etc.)</td></tr>
</table>

(iii) Functions required of middle offices

In order to raise the level of operational risk management for the entire institution and reduce gaps in risk management among sections, it is effective to establish a section responsible for firm-wide operational risk management with the types of functions described below. In such cases, the middle office is normally made up of the sections (control sections) that control and oversee the risk in a firm-wide manner, and sections (subsections) that control specific types of operational risks.

Whether or not to establish an independent middle office section depends on circumstances at each bank, but even if such a section is not established, it is probably necessary to implement cross-functional controls by establishing a cross-divisional committee to deal with operational risk management.

Possible middle office functions are as follows.

(a) Control section

(1) The control section plans the operational risk management framework for the entire institution. To do this, it:

- develops methods for recognizing and identifying operational risk (concrete details and responsible sections of CSA, risk quantification, KRI and validation methods, etc.);
- drafts risk control policies, which specify how risks should be controlled and which sections should be responsible; and
- formulates plans pertaining to operational risk management from the overall perspective of the bank after considering managerial intentions and instructions, the state of advancement of risk management methods at other banks, changes in the risk environment affecting the industry, the situation in front-line operations, and cost effectiveness.

(2) The control section collects and analyzes information on incidents, accidents, computer system malfunctions, clerical errors arising in each section, the results of KRI, CSA and operational risk quantification, and reports to the management with special attention to risk that should be closely watched and proposals for policies to deal with it. To do this, it:

- is responsible for establishing the proper reporting infrastructure including the design of report formats and reporting systems, and also standardizing reporting levels;
- checks consistency in quality of reports or assessments of individual sections or sub-risk categories (computer system risk, clerical risk, compliance, tangible asset risk, etc.); and

— reports to senior management, preparing concise materials so that managers can easily grasp the main points and features.

(b) Subsections

(1) Subsections establish and examine the processes and procedures (P&P) pertaining to operational risk, such as in-house guidelines on operations, for all branches and sections. Examples of guidelines are as follows.

— The writing styles used for regulations pertaining to individual sections and operations should be standardized as much as possible except in cases where the use of different descriptions due to business characteristics can be rationally justified.

— Within the area governed by a single policy, the descriptions and concepts used in higher- and lower-level rules should be examined so that there are no discrepancies between them (e.g., check for consistency among individual rules pertaining to information security policies, information security standards, and information security management).

(2) Subsections request reports from each front-line section and/or carry out on-site inspections, and provide evaluations and guidance according to the operational risk management situation at each section based on the above outcomes.

— From the perspective of a risk management expert, assessments should be conducted to ascertain whether there are any problems in internal controls at the front line, or whether the operational risk management framework is functioning effectively, and appropriate guidance should be given on how operations may be improved.

— At the same time, materials should be collected for planning measures designed to improve risk management throughout the entire bank.

This type of middle office must (1) not be directly involved with customer sales or back-office operations (payment and settlement business, management of cash and securities, and systems development and operations); and (2) report directly to the board.

The middle office must independently implement CSA, etc., to assess the risks inherent in its own operations, and oversee the outcomes of other sections.

(iv) Functions required of internal audits

(a) Relationship between CSA and internal audits

With regard to the results of CSA and other risk assessments carried out by front-line sections, the middle office must validate assessments by front-line sections,

while the internal auditors must carry out checks from the perspective of the internal auditors' validation of the effectiveness (or accuracy) of the system framework. Moreover, CSA results may be used for assessing risk with a view to drafting internal audit plans, but in such cases internal auditors must use other information for assessing risk and not depend exclusively on CSA results.

(b) Knowledge and experience that the internal auditors should possess

The internal auditors of financial institutions may not necessarily have accumulated enough knowledge on the matters discussed so far by this group (especially technical matters related to operational risk quantification models). In view of the fact that (1) operational risk quantification is becoming an increasingly important tool for risk management, and (2) middle offices tend to be responsible for risk quantification processes and there are usually no other entities but internal audits, which can validate this process within the bank, it is quite important that banks allocate personnel with knowledge and experience of the technical side of quantification.

Against this background, one possible option is to utilize external resources for some auditing functions with a view to compensating for insufficient knowledge and experience.

- Even in this case, however, the internal auditor must continue to bear final responsibility for internal audit functions. When utilizing external resources, therefore, the financial institution must ensure that it has the capability to (1) adequately assess the expertise, knowledge and experience of the external entity when making its selection, and (2) understand and assess the output of the external entity (external audit results, etc.) and, where necessary, supplement it, as well as conduct the discussions required for that purpose with the external entity.

B. Application of advancement methodologies in management

1. Potential Issues

It is important to increase third parties' confidence in the banks' adopting advancement methodologies by demonstrating the actual use of outputs of these methodologies for business judgments (so-called "use tests").

The introduction of Basel II has led banks to advance operational risk management, and has sometimes resulted in a situation where the introduction of advancement methodologies has moved ahead while their application in management has lagged. Partially reflecting these situations, it is apparent that the parties concerned have not yet reached a common understanding of the extent to which they are expected to use advancement methodologies in management.

2. Participants' Views

Possible examples of applications of advancement methodologies in management are shown in the following table.

Operational strategies and business management	-- Secure an appropriate capital buffer
	-- Offer incentives for improving risk management (performance evaluation and its linkage with remuneration)
	-- Identify priority business promotion sectors, restructuring sectors
Daily management and risk controls	-- Identify the operational risk profile (section units)
	-- Identify the operational risk profile (subdivided business lines)
	-- Prioritize risk management
	-- Set price commissions, etc.
	-- Set risk limits
	-- Plan insurance
Report as business information	
Utilize in internal audits	

<Inquiries>
Secretariat of the Study Group on the Advancement of Operational Risk Management
(c/o Center for Advanced Financial Technology
Financial Systems and Bank Examination Department, Bank of Japan)

Mr. Tsuyoshi Oyama (03-3277-3078)
Mr. Takashi Arai (03-3277-2005)
Mr. Tsuyoshi Nagafuji (03-3277-2987)

Attachment

List of Study Group Members

Mitsubishi–UFJ Financial Group	
Corporate Risk Management Division	Kenji Fujii
Corporate Risk Management Division	Fumiaki Hibi
Corporate Risk Management Division	Shunji Hayashi
Bank of Tokyo–Mitsubishi UFJ	
Corporate Risk Management Division	Katsutoshi Edamura
Corporate Risk Management Division	Takayuki Kobayashi
Mitsubishi UFJ Trust and Banking Corporation	
Corporate Risk Management Division	Keisuke Nakagiri
Sumitomo Mitsui Banking Corporation	
Operational Risk Management Department	Toshio Mano
Operational Risk Management Department	Kazuhiro Iga
Operational Risk Management Department	Fumiteru Ueno
Risk Management Department	Ken'ichi Yamazaki
Mizuho Financial Group	
Risk Management Division	Hiroshi Kakunaka
Risk Management Division	Noboru Yamada
Risk Management Division	Koji Shiiba
Risk Management Division	Takuya Mizuno
Mizuho Corporate Bank	
Risk Management Division	Jun Matsuda
Mizuho Bank	
Risk Management Division	Kazuhiro Mizoguchi
Bank of Japan	
Center for Advanced Financial Technology	Tsuyoshi Oyama
Center for Advanced Financial Technology	Takashi Arai
Center for Advanced Financial Technology	Tsuyoshi Nagafuji
Center for Advanced Financial Technology	Nobuyasu Obata
Examination of Computer System Risk Section	Atsutoshi Mori
Center for Advanced Financial Technology	Tomonori Kimata
Center for Advanced Financial Technology	Seiya Hikuma
Observing members	
Financial Services Agency	
Planning and Coordination Bureau (Supervisory Bureau)	Shunsuke Shirakawa
Planning and Coordination Bureau	Shin'ichiro Shimizu
Supervisory Bureau	Yasuhiro Matsuda
Supervisory Bureau	Takaaki Kobayashi
Supervisory Bureau	Satoshi Morinaga