Advancing Operational Risk Management

September 2005

Bank of Japan

For any information, please contact:
Risk Assessment Section
Financial Systems and Bank Examination Department

Mr. Oyama	+81-3-3277-3078	tsuyoshi.ooyama@boj.or.jp
Mr. Arai	+81-3-3277-2005	takashi.arai@boj.or.jp

Table of Contents

I. Introduction

The operating environment for financial institutions has changed significantly in recent years. Deregulation has encouraged business diversification, financial technologies have become more sophisticated, and IT and outsourcing have become widely used. In addition, international discussions have highlighted operational risk,[1] and it will become necessary to allocate capital under the Basel II Framework,[2] which will be introduced at the end of fiscal 2006. These changes are prompting financial institutions to enhance their operational risk management.

The following chapters draw on the operational risk management issues and measures by introducing cases in which domestic and overseas financial institutions have adopted advanced approaches. Our intention is to use the topics in this paper for discussions on operational risk management and its advancement at our on-site examinations and off-site monitoring of individual financial institutions.

This paper is structured as follows. Chapter II discusses the characteristics of operational risk and the reasons why there is a need to advance operational risk management. In subsequent chapters, an overview of efforts to advance operational risk management is introduced, followed by concrete approaches such as the establishment of an operational risk management section (Chapter III), operational risk quantification (Chapter IV), and identification and assessment of operational risk other than quantification (Chapter V).[3]

II. Characteristics of Operational Risk and the Need to Advance Operational Risk Management

A. What Is Operational Risk?

There is no uniform definition of operational risk, but the definition adopted by the Basel II Framework is used in this paper: "the risk of loss resulting from inadequate

---

[1] See Appendix 1.

[2] See "International Convergence of Capital Measurement and Capital Standards: A Revised Framework" (June 2004), issued by the Basel Committee on Banking Supervision.

[3] The operational risk management framework should include conventional operation management mechanisms such as checks and balances and the multiple signatory system, as well as internal audit systems, business continuity planning, and the corporate governance system. However, this paper does not address these issues. For information on these areas, please refer to the Bank's following publications: "The Current State of Internal Audits at Japanese Financial Institutions and Directions for Improvement (Risk-Based Audits)" (June 2002, available only in Japanese) and "Business Continuity Planning at Financial Institutions" (July 2003).

or failed internal processes, people or systems, or from external events."[4] Specifically, operational risk refers collectively to risks arising from manual operations (including risk of embezzlement or misappropriation), computer systems, and compliance.

Compared with other types of risk, operational risk has the following characteristics.

1. Forms of risk materialization

Unlike other types of risk, operational risk does not merely materialize in the form of visible and direct losses (or profit declines). For example, it may cause indirect losses (or profit declines) through a deterioration in reputation. There are also cases such as computer system malfunction, where losses are inflicted on not only the parties concerned but also third parties such as customers and other financial institutions (Chart 1). When operational risk materializes, therefore, it is not always easy to identify the resulting losses, including indirect losses and losses incurred to third parties in an accurate and comprehensive manner.

Operational risk can also be divided into two types according to frequency and severity of the loss events. The former comprises small-scale problems that occur at relatively high frequency, including clerical error (errors in remitting small sums of money or payment errors at bank counters) and minor problems at computer terminals. The latter comprises problems that do not occur often but have severe consequences when they occur. Examples include major malfunctions of computer systems, natural disasters such as strong earthquakes, terrorist attacks, and cases of large-scale fraud such as those at the Bank of Credit and Commerce International (BCCI) and at the New York branch of Daiwa Bank, which were uncovered in the 1990s. Because of these characteristics, the distribution of losses arising from operational risk materialization has a fat tail, as depicted in Chart 2.

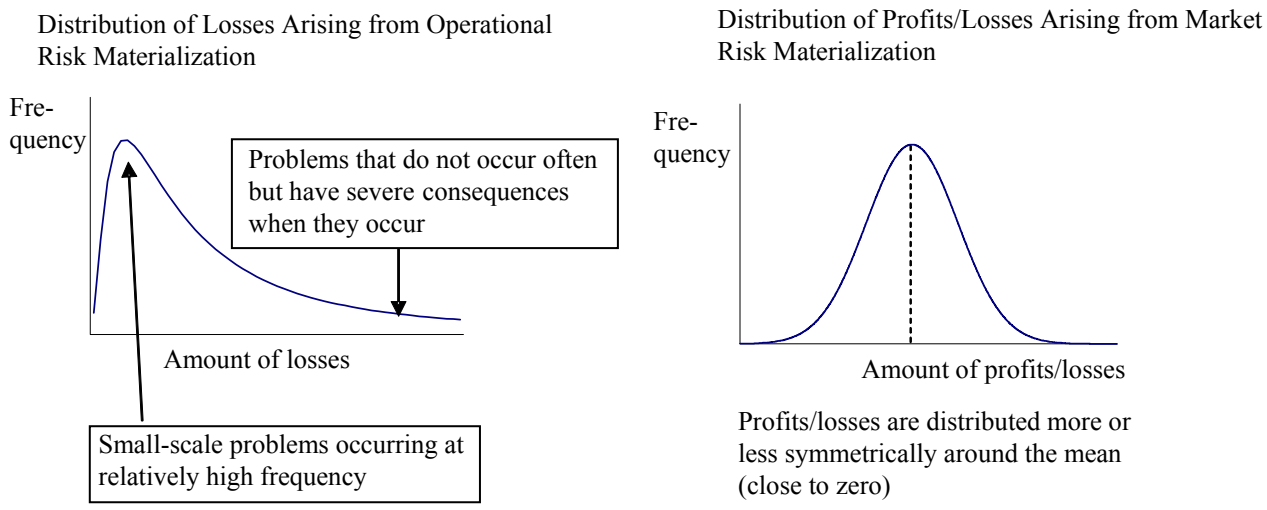
Chart 1: Examples of the Impact of Operational Risk Materialization

Direct impact on profits/losses and capital of the financial institution	- Coverage of shortfalls following cash shortages - Payments of damages/settlements/penalties following lost lawsuits, arbitrations, supervisory actions, etc. - Payments of overtime wages to employees as required to

[4] The Basel II Framework does not require capital allocations for reputational risk (the risk that an institution's reputation will deteriorate as a result of clerical error, computer system malfunction, etc.) and systemic risk (the risk that problems will affect not only the financial institution but also the entire payment system). However, this paper includes such risks in the scope of its discussion.

	repair system malfunctions, etc. - Postal charges required for mailing letters of apology to customers, etc. - Lawyers' expenses necessary to deal with problems - Reduction or exemption of commissions as a result of clerical error - Loss of earnings caused by business interruptions, delays in starting operation hours, etc.
Indirect impact on profits/losses and capital of the financial institution	- Deterioration of reputation caused by clerical error triggers a reduction in customers, leading to a fall in earnings
Impact that goes beyond the financial institution	- Cases where interruptions to the business of the financial institution arising from system malfunctions lead to a deterioration in customers' financial positions or delay in interbank payment and settlement.

Chart 2: Distribution of Losses Arising from Operational Risk



2. Causes of risk materialization

Losses can often be specified for certain risks, for example, interest rate fluctuations in the case of market risk, and changes in borrowers' creditworthiness in the case of credit risk. In the case of operational risk, however, it is normally difficult to narrow down the factors causing such risk to materialize, and quite often, it only emerges when several factors come into play simultaneously. Let us assume, for example, that customer data leak from a financial institution. In such a case, several

contributory factors can be considered, including: failure to establish proper in-house guidelines for customer information management; inadequate computer safeguards to protect customer data from improper distribution; and inadequate employee discipline. Very often, operational risk materializes when these events occur together.

In light of these characteristics, therefore, the following points should be noted when managing operational risk.

a. The need to cover a wide range of events and activities

Managing market and credit risk involves breaking down risk into exposure, for example, risk position and amount of credit, and risk factors, for example, interest rates and default probability, and keeping each of them under surveillance to monitor risk. In the case of operational risk, however, it is difficult to break down risk into the categories of exposure and risk factors, so it is necessary to control a wide range of events and activities in order to prevent materialization of operational risk.

b. The need for risk control in all sections within the institution

While the number of operations and sections exposed to market and credit risk is relatively small,[5] operational risk exists in all sections throughout the institution. Hence, all sections within the institution must improve their operational risk management levels.

c. The importance of risk management based on qualitative information

Since operational risk factors are often more difficult to identify and measure than market and credit risk factors, it is not always easy to manage them in a quantitative manner. As a result, identification of risk factors needs to rely on qualitative information even if some risk quantification methods have been introduced.

d. Reputational and systemic risk

As already mentioned, operational risk may materialize in a way that has a negative impact on bank customers' financial positions and the stable operation of the payment and settlement system. Even in such cases, financial institutions cannot always be held responsible for customers' losses, because of both explicit and implicit exemption agreements. However, the impact on the institutions' reputation can be grave. Moreover, financial institutions are required to work diligently to prevent

[5] For example, market risk is likely to exist in trading sections and credit risk can exist in marketing and lending sections at head offices and bank branches.

systemic risk from materializing as part of their mission. It is therefore vital for financial institutions to maintain the quality of their operations at a certain level, not just to avert direct losses to themselves, but also to maintain their reputation and prevent systemic risk.

B. Conventional Methods of Operational Risk Management and Recent Changes in the Operating Environment

In previous years, financial institutions dealt with operational risk by adopting various conventional measures, including drawing up in-house guidelines on operating procedures and strengthening system support (Chart 3). These measures helped ensure the soundness and improve the quality of business operations.

More recently, the operating environment for financial institutions has changed significantly as deregulation encourages business diversification, financial technologies become more sophisticated, and IT and outsourcing become widely used. Following the introduction of the Basel II Framework at the end of fiscal 2006, financial institutions will be required to allocate capital for operational risk. In addition, society in general is increasingly aware of the need for firms' management of operational risk more critically than before as a result of major disasters such as earthquakes and terrorist attacks and the uncovering of serious corporate scandals in Japan and overseas.

This background calls for efforts by financial institutions to further advance their operational risk management, for example, with the following measures. First, they must engage in more efficient management by identifying and assessing operational risk comprehensively. Second, they must establish structures that can quickly detect heightened risk and respond appropriately before the risk materializes. Third, they must create mechanisms for autonomous risk management in all sections of their operations.

Chart 3: Operational Risk Management Methods Conventionally Used by Japanese Financial Institutions

Method		Details
Multilevel checks and balances system	Reexamination and multiple signatory system	No single person completes each process alone; reexaminers and multiple signatories check it.

	Segregation of duties	Duties are segregated into different sections, e.g., the front office (e.g., trading) is separated from the middle and back offices, to prevent the front office from executing orders on its own.
	In-house inspections	Each office conducts on-site internal checks to ensure that business procedures are conducted in accordance with proper processes and procedures (P&P) and that cash balances tally with the books.
	Insistence on record-keeping	Detailed records of work are kept to allow ex post facto verification.
Standardization and streamlining of business procedures	Establishment of P&P	P&P and office ledgers that incorporate risk management procedures are prepared.
	Institution-wide guidance on business operations	Operational accuracy of branches and computer centers is raised through inspections, monitoring, and guidance by staffs at the head office.
	Strengthening systems support	Straight-through processing (STP) is adopted for business procedures in order to reduce operational errors.
Discipline and motivation	Human resource (HR) management and performance evaluations	To ensure accurate and appropriate business processing and teamwork, staffs are motivated through HR performance evaluations and a reward system.
Response to accidents and other problems	Implementation of measures to prevent recurrences	When incidents, accidents or other problems occur, relevant business procedures are reexamined, and measures to prevent recurrences are discussed and implemented.
Internal audits		Independent internal auditors check the risk situation at front offices and report the need for improvement of the business procedures to the management.

III. Overview of Efforts to Advance Operational Risk Management and the Establishment of an Operational Risk Management Section

A. Overview of Efforts to Advance Operational Risk Management

Financial institutions, particularly major banks, have been adopting various approaches to deal with the above-mentioned issues concerning operational risk management (Chart 4).

The following sections examine the key points of the implementation of these approaches, by referring to the findings obtained through the Bank's on-site examinations and off-site monitoring, and cases of major U.S. and European financial institutions.

Chart 4: Examples of Methods to Advance Operational Risk Management

Method	Main effects of introducing the method
Establishment of a section responsible for firm-wide operational risk management	Comprehensively identify and assess operational risk in the institution with the new section.
Quantification of operational risk	Comprehensively identify and assess operational risk in the institution by using the risk quantification techniques.
Other new methods for identifying and assessing operational risk	
Control self-assessment	Promote autonomous risk management at each business section.
Key risk indicators	Quickly detect heightened risk so as to enhance preventive risk management.

B. Establishment of an Operational Management Section

In order to raise the level of operational risk management for the entire institution and reduce disparities in risk management between sections, it is effective to establish a section responsible for firm-wide operational risk management with the types of functions described below.

1. Plan the operational risk management framework for the entire institution.
2. Collect and analyze information on incidents, accidents or other problems, computer system malfunctions, and clerical errors arising in each section, then report to the management.
3. Examine the adequacy and consistency of processes and procedures (P&P) pertaining to operational risk, such as the in-house guidelines on operations, of all branches and sections.
4. Request reports from each section and/or carry out on-site inspections, and evaluate and guide the operational risk management situation at each section based on the above outcomes.

It is important that the section that is responsible for firm-wide operational risk management should not be involved with customer sales or back-office operations (e.g., payment and settlement business, management of cash and securities, and systems development and operations). This is to avoid possible conflict of interest between measures for risk management and for expansion of profits, and reduction of expenses.

Many Japanese financial institutions had separately assigned risk management functions 2 to 4 above for risks related to manual operations, computer systems, and compliance[6] to sections responsible for each operation. In recent years, there has been an increase in the number of cases where, in addition to risk management functions to handle these categories of risk separately, another section has been established to coordinate them.[7] This new section plans the operational risk framework for the institution as a whole, organizes the various kinds of data reported to it by risk management functions, and reports the data to management.

IV. Quantifying Operational Risk

A. Purpose of Risk Quantification

Operational risk quantification is the task of quantitatively identifying the operational risk profile characteristics of each financial institution. It advances risk management and the business evaluation process as outlined below.

1. Identifying the operational risk profile

   Heightened risk in specific sections and businesses is detected by periodically quantifying operational risk, conducting time-series analyses, and comparing risk amounts by section and business.

2. Securing an appropriate capital buffer

   Operational risk for the entire institution is identified so that the institution can secure the necessary capital buffer for coping with any losses that may emerge as a result of risk materialization.[8]

---

[6] Generally, the above-mentioned risk management functions are handled by independent middle offices. For example, operations planning sections handle risks related to manual operations; the systems planning sections or IT management sections handle computer system risk; and compliance sections or legal sections handle compliance.

[7] In some cases, these functions are left to a firm-wide integrated risk management section, which also manages market and credit risks. In other cases, a new section has been set up to specialize in controlling operational risk management.

[8] Other possible steps include discontinuing or scaling down high-risk business, or transferring risk

3. Prioritizing risk management

   Given the limited personnel resources and budgets assigned to risk management, measures to improve risk management are considered and implemented on a prioritized basis for sections and businesses identified as posing high risks through the results of quantification.

4. Incentives for improving risk management

   The costs associated with the capital buffer allocated for operational risk as described in 2 above (capital costs) are recognized as section-specific costs in managerial accounting and built into performance evaluation schemes to provide risk management incentives.

Because of the operational risk characteristics referred to earlier, however, it is not always easy to assess all such risks quantitatively. Quantification also incurs considerable costs because it is necessary to collect loss data, develop quantitative models, and set up a framework for risk assessment. Each financial institution must therefore assess the need for quantification as well as the way to apply it after considering its cost-effectiveness according to the size of its business and risk profile.

B. Operational Risk Quantification: Technical Caveats

The most commonly used operational risk quantification method is known as the "loss distribution approach." This approach first estimates the frequency and severity distribution of losses based on scenario analysis as well as internal historical loss data, and then statistically estimates the risk amount according to the distribution (see Box 1).[9] Below are some technical caveats when using this approach.

---

outside the institution using insurance and other means.

[9] See Appendix 2.

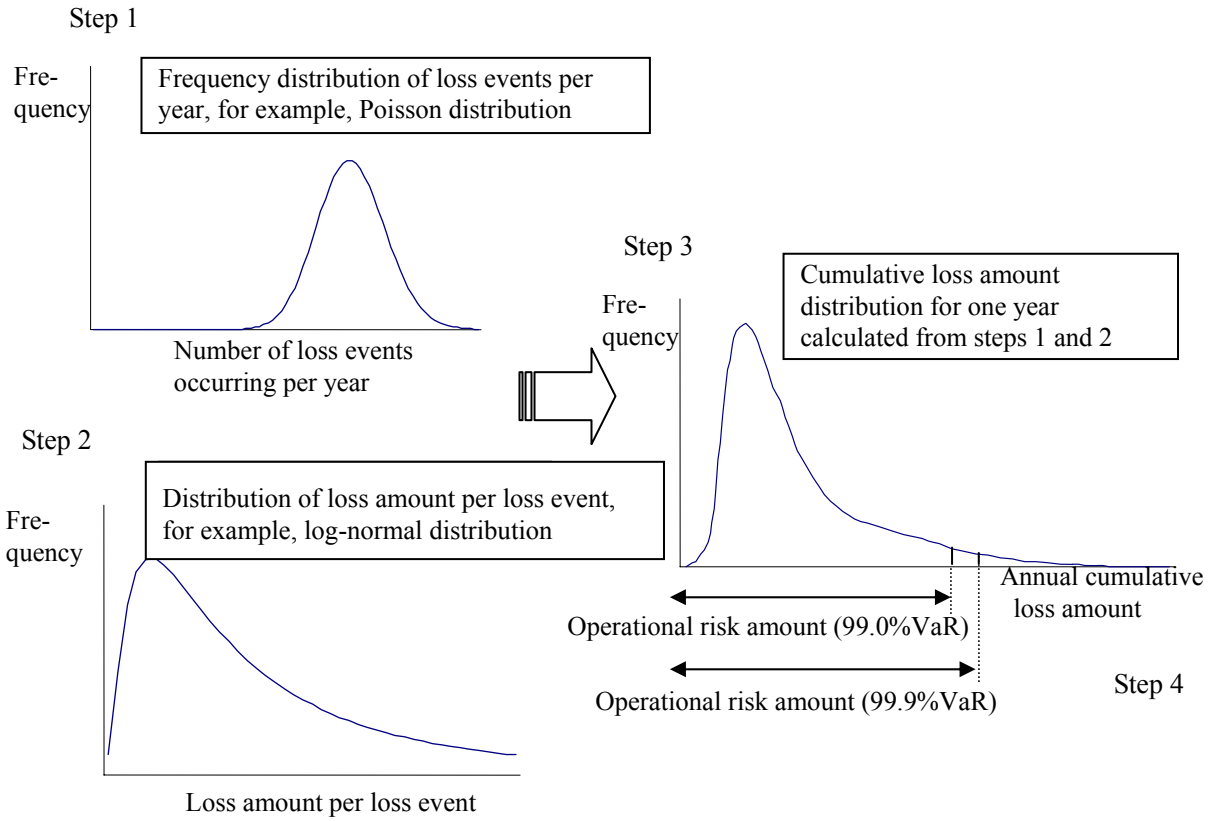
Box 1: An Example of How to Use the Loss Distribution Approach

Step 1: Using accumulated loss data, estimate the frequency distribution of the number of loss events (the number of cases where risk materializes and becomes an actual loss) occurring during a set period (e.g., one year).

Step 2: Using the loss data, estimate the frequency distribution of loss amount per loss event.

Step 3: Combine frequency distribution of the number of loss events per year and of loss amounts per loss event, and prepare the frequency distribution of the cumulative loss amount for one year by using Monte Carlo simulation.

Step 4: Based on the frequency distribution of the cumulative loss amount for one year, calculate the value at risk (VaR): the maximum potential loss statistically identified at a certain confidence level, for example, 99.0 percent, which corresponds to the operational risk amount.



1. Caveats concerning collection of loss data

To quantify operational risk, it is essential to collect and accumulate historical data (internal loss data collected by each financial institution) on operational risk-related losses such as losses incurred by operational failures, accidents, and lost lawsuits. In the data collection process, financial institutions are expected to pay due attention to the points listed in Chart 5.

Chart 5: Caveats concerning Collection of Loss Data

Process		Caveats
Collection of loss data	Sections to be covered	Cover all loss events occurring at all sections within the financial institution, major subsidiaries, affiliates, and major subcontractors.
	Types of loss events to be covered	Collect data on a wide range of loss events arising from incidents and accidents, clerical error, lawsuits, computer system malfunction, etc.
	Scope of losses	Include amounts shown under "suspense payments" and other temporary payment accounts, not just miscellaneous losses posted. Also recognize a wide range of losses, including items posted under personnel and non-personnel expenses (legal expenses and employee overtime wages that have a causal relationship with operational risk-related loss events, etc.) and reductions in profits (loss of earnings, etc.).
	Loss amounts	Collect data on both gross loss amounts and net loss amounts after subtracting recovered amounts.
	Thresh-Olds	From the viewpoint of cost-effectiveness, establish reference values (thresholds) for losses. Collect loss data that exceed said amount. It should also be possible to set different thresholds for each section and business, etc., according to the nature of the risk.
Classification of cases		Classify loss events on which data are collected according to clear criteria.
Updating of data		Update the collected loss data with appropriate timing according to ex post facto development of loss events (changes in loss amount estimates or actual figures).

2. Some caveats on quantification models

a. Identifying cases of losses with low frequency but high severity

There are two categories of operational risk-related losses—those with relatively high frequency but low severity and those with low frequency but high severity (tail loss events). The latter in particular can cause considerable impairment of capital of the financial institution, affecting its solvency. In quantifying operational risk, therefore, appropriate identification of this kind of tail loss event is essential. Financial institutions with sophisticated risk management pay attention to the above-mentioned caveats in their selection of the risk quantification models (see Box 2).

Box 2: Key Points in Selection of Risk Quantification Models

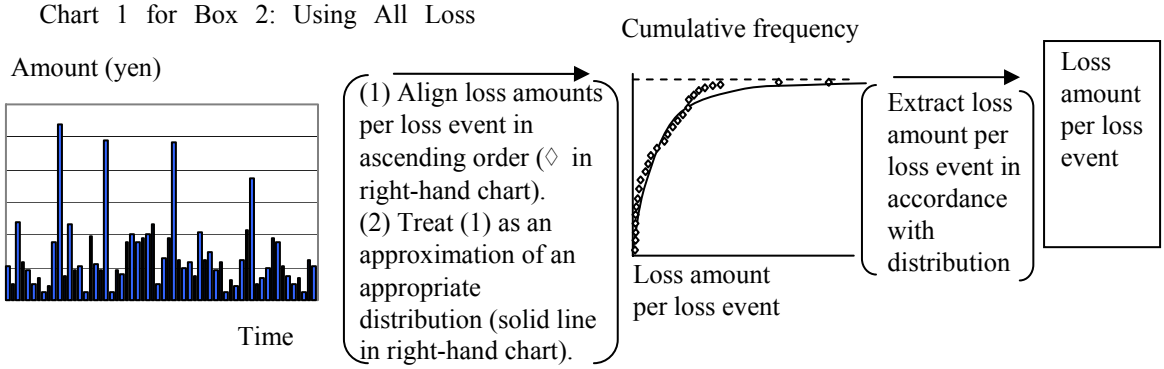
The loss distribution approach uses simulations of the number of loss events during a set period[1] and the loss amount per loss event.

With regard to the loss amount per loss event, two types of simulation methods are often used: (1) parametric method, which uses simulations of numerical data assuming a specific statistical distribution; and (2) non-parametric method, which uses simulations of actual data without assuming a specific distribution. Both types have offered the following characteristics in terms of capturing tail loss events.

1. Parametric Method

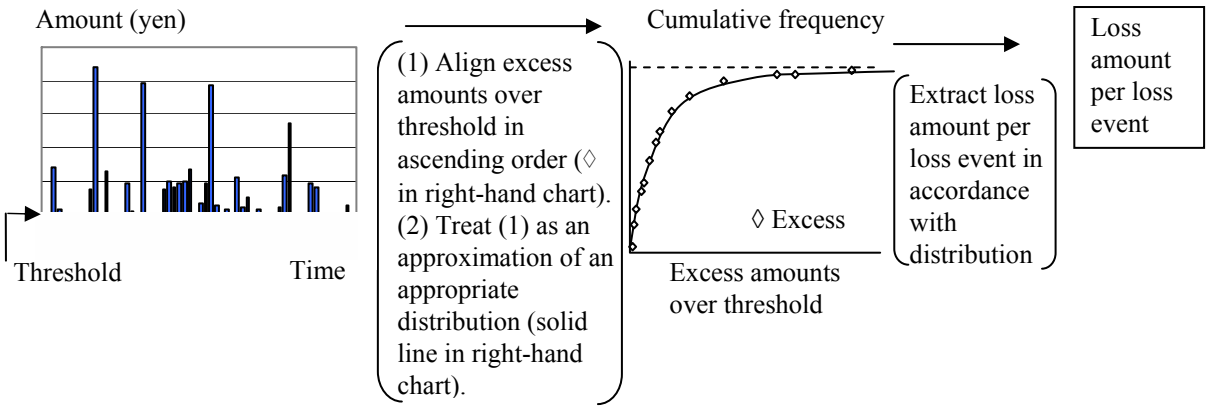
This type of method assumes specific types of distributions for loss amount per loss event and uses numerical data in accordance with said distribution in Monte Carlo simulation. When using a parametric method, the financial institution must select the type of distribution—log-normal distribution, gamma distribution, Weibull distribution, and so on—that not only best suits its own loss data but also can cope with the fat-tail characteristics of operational risk, that is, covers cases with low frequency but high severity, in order to capture tail loss events in an appropriate manner (Chart 1 for Box 2). Focusing on tail loss events, there is also an approach in which institutions select the best-matching types of distribution only for tail loss data instead of for all loss data (Chart 2 for Box 2).

Chart 1 for Box 2: Using All Loss



[1.] This paper does not discuss simulations of the number of loss events during a set period because a specific distribution—the Poisson distribution—is generally used.

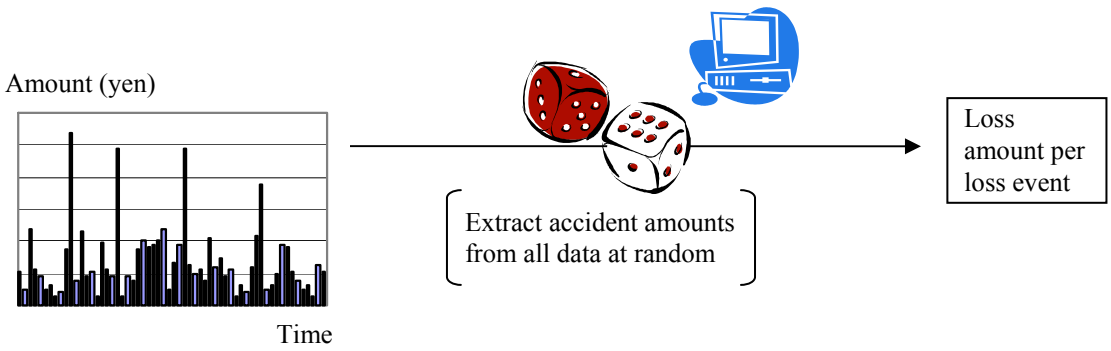
Chart 2 for Box 2: Using Data for Large Losses Only



2. Non-Parametric Method

This type of method does not assume specific type of distribution for loss amount per loss event, but uses actual historical data as in the Monte Carlo simulation (Chart 3 for Box 2). Since the simulation is based only on actual data, this method cannot capture the loss amounts that exceed the maximum data value regardless of the number of times it is repeated. When quantifying operational risk using this method, therefore, it is necessary to include the data with appropriate measures and cases of large-scale losses that fall into the category of tail loss events.

Chart 3 for Box 2: Using Actual Historical Data



b. Setting group units for quantification

It is important to classify loss events appropriately in order to quantify and analyze risks accurately. Most of the financial institutions that have adopted sophisticated approaches have established about 5–7 group units (cells) for quantification by referring to the loss data classifications indicated by the Basel II Framework.

It should be noted, however, that the more subdivided the group units for quantification are, (1) the lower the number of data items in a single unit, and (2) the higher the total risk amount estimated[10] in cases where results of individual cell qualification are simply added up.

3. Use of external loss data and scenario data

It is also possible that financial institutions cannot collect the internal loss data necessary for risk quantification with statistical significance because they have just been established or have experienced few cases with real losses. Even those financial institutions that have collected a certain amount of internal loss data generally have insufficient loss data in the tail loss event category because it is literally extremely rare for them to have faced such events as terrorist attacks, natural disasters, or major frauds.

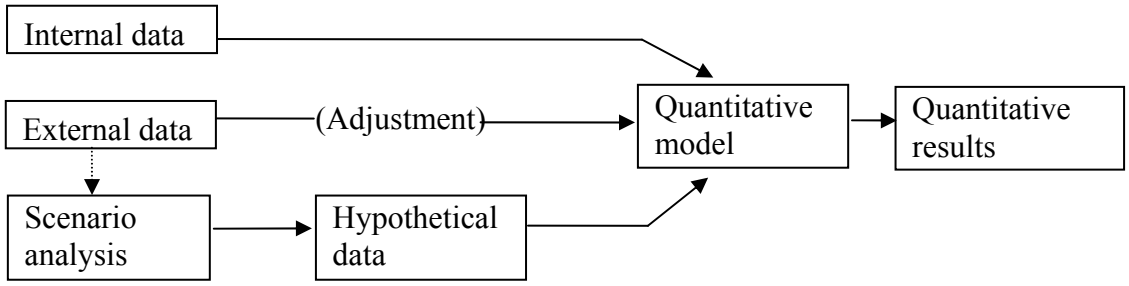
To mitigate the problem arising from such deficiencies in internal loss data, many

[10] Simply adding up the results of individual subdivided quantitative units (cells) means that when a large loss event occurs in one business, a loss event with the same impact is deemed to have occurred in another business during the same period. Except for extreme cases, such as when there are problems with internal controls and thus employee discipline has also fallen markedly, it is generally considered unlikely that loss events of this type will occur in succession within a short period of time. For this reason, making simple totals of quantitative results for individual cells can lead to an estimated risk amount on the high side.

institutions are beginning to introduce supplementary data. For example, financial institutions (1) collect loss events occurring at other institutions (external loss data),[11] or (2) create hypothetical data based on various risk scenarios leading to operational risk-related losses of the institution (scenario data). They use the hypothetical data together with internal data for risk quantification (see Box 3).

Box 3: Cases Where Hypothetical Data Based on External Data or Scenario Analysis Are Used

1. Introducing Hypothetical Data Based on External Data or Scenario Analyses into Quantitative Models



A. Introducing External Data

External data into the quantitative model. The frequency and severity of the external data are often adjusted according to the business scale, asset size, and internal control conditions at the financial institution. This is because quantification results may be distorted if external data come from organizations with a different business environment.

B. Introducing Hypothetical Data Based on Scenario Analyses

The possible occurrence (frequency) and impacts (loss amount) of earthquakes and other natural disasters, terrorist attacks, large-scale fraud, and computer system malfunctions are assumed based on hypothetical scenarios (there are also cases where external data are used in the process). These hypothetical data are then introduced into the quantitative model.

[11] There are several ways to obtain external loss data, including: (1) purchases from data vendors or bank association type organizations; (2) data exchanges with related financial institutions; and (3) accumulation of information on cases at other organizations as disclosed in news reports and other media.

Sample Scenarios

Event	Overview	Loss amount	Frequency
Earthquake	10:00 a.m.: Earthquake occurs in a city. The head office building and ten branches suffer severe damage (structural damage rate: head office XX%, branch A XX%, and branch B XX%).	Cost of restoring buildings to their original state, loss of earnings due to business interruption, and personnel costs due to the disaster response, totaling XX billion yen	Once every XX years
Computer system malfunction	11:00 a.m.: Online operations of accounting systems stop due to hardware malfunctions in XX disk device. Two days are required to restart operations.	Personnel costs for emergency operations, hardware repair costs, loss of earnings due to halt to online operations, cost of apology advertisement, etc., totaling XX billion yen	Once every XX years

2. Use of External Data Statistics

There are also cases where external data statistics (average, standard deviation, etc.)—not the external data themselves—are used in operational risk quantification in business areas where internal loss data are insufficient after adjusting them for business scale, asset size, or historical loss occurrence situation, etc., of the financial institution.

4. Using qualitative factors to revise the quantification results

Operational risk quantification results deriving from the use of historical loss data may not always reflect the current business environment or internal control situation at the financial institution. For this reason, the risk quantification results are often adjusted on the basis of qualitative factors pertaining to operational risk, in addition to adding hypothetical data based on external data or scenario analysis to the data for quantification.

The qualitative factors used for this purpose include the following.[12]

a. Results of internal audits.

b. Results of self-assessments on risk control (hereafter control self-assessments) and trends in key risk indicators (see Chapter V).

c. Recent changes in business, institution, and management strategy.

5. Verification of risk quantification processes

In risk quantification processes such as building quantitative models, collecting loss data, and making scenarios for scenario analysis, the following should be considered important: clarifying the details of the process and handling procedures in written form; gaining full understanding and approval from the management on the main points of these processes; and verification by independent third parties such as internal auditors.

C. Operational Risk Quantification: Other Caveats

Even among major financial institutions, operational risk quantification is still in the development phase, and methodologies are not as well established as in the quantification of other risk categories. For this reason, financial institutions should increase their awareness of the limits of operational risk quantification, particularly when carried out to identify the absolute level of operational risk as a primary objective. In terms of cost-effectiveness, there might be cases where attempting conservative calculations of risk amounts can provide more adequate solutions rather than refining

[12] These adjustments are primarily made when operational risk is quantified by segment. Examples include increasing risk amounts for sections where the results of internal audits are unfavorable; and increasing risk amounts for sections whose business plans call for business expansion using additional human resources. As a result, the overall operational risk may change.

the quantification model.[13]

On the other hand, in the case where the primary objective of quantifying operational risk is to identify the capital amount allocated for business sections and thereby motivate them to reduce their risk, it is necessary to further refine risk quantification conducted in each risk management unit (such as section or business).[14]

In particular, the risk quantification logic must be adequate in cases where costs for allocated capital are recognized and used for the performance evaluation of each section. This is because the success of this incentive system depends critically on whether fairness is ensured for all sections in quantifying operational risk. Unlike the case of identifying the absolute level of operational risk amount of the institution, possible risk factors must be taken into consideration, and it is not possible to obtain the understanding of each section by simply estimating risk amount conservatively.

In such cases, it is important to ensure that risk quantification for each section does not diverge from a real-world situation,[15] and to design mechanisms that do not hinder the identification of risk events. Some measures must be taken to prevent the risk managers in each section from concealing or under reporting information that may affect the results of operational risk quantification in order to avoid any adverse impact on performance evaluations for the section.

V. Approaches to Identifying and Assessing Operational Risk Other than Quantification

This chapter introduces two other methods of quantification for identifying operational risk—control self-assessments and key risk indicators. As mentioned

---

[13] Databases on incidents, accidents, clerical error and other cases of operational risk-related losses are necessary to analyze trends and then to identify the operational risk profile of the institution It is therefore desirable to build such databases regardless of institutions' intentions to introduce risk quantification techniques.

[14] Methods for calculating risk amounts according to the characteristics of risk for each section include the allocation method, in which risk amounts measured as a whole for the entire financial institution are allocated to individual businesses, according to certain rules; and the stand-alone method, in which actual risk amounts are measured for each business or section.

[15] For example, when problems with customers result in lawsuits, there is often a time lag between the causal event (such as inadequate explanations when selling a product to a customer) and the emergence of the actual loss (such as payment of damages following the loss of a lawsuit). In such cases, if an amount equivalent to the damages is used as loss data when the lawsuit is lost even though counter measures against this event have already been adopted, this can lead to an awkward situation for this section, in which it faces unreasonable penalties in the form of a very high risk amount because of the time lag.

earlier, they can be used when revising the results of operational risk quantifications but are also useful in improving the autonomous risk management of each section, quickly detecting heightened risk, and strengthening preemptive risk management.

A. Control Self-Assessments

Control self-assessments are the framework according to which the individual section or businesses within a financial institution evaluate[16] inherent risk and internal control conditions on their own, and these results are coordinated and shared within the entire organization (see Box 4). In addition to identifying the distribution of risk within the institution, this aims to encourage each section to engage in autonomous risk management.[17]

The following points should be considered when adopting the control self-assessments.

1. Ensuring the fairness and effectiveness of assessments

The self-assessment items include those that can be evaluated on the basis of objective criteria, such as transaction volumes, and items that must rely on the subjective judgments of evaluators, such as managers' expertise. With regard to the latter, financial institutions should remove ambiguity of evaluation criteria and thereby eliminate possible inconsistencies in self-assessments between sections in order to ensure the fairness and effectiveness of assessments. For this purpose, for example, institutions can employ measures such as a training course for staffs to engender a common understanding of evaluation criteria, secondary assessments by the section responsible for firm-wide operational risk management, and use of internal audits to check the appropriateness of the assessments.

---

[16] The scope of the risk that is actually subject to assessment depends on the financial institution. Some institutions include credit and market risk as assessment targets.

[17] Many of the financial institutions which adopt self-assessments on risk control submit reports on major results of the assessment to management, which uses them to identify overall risk within the institution. There are also many cases where individual sections (businesses) are required to draw up action plans to reduce risk on the basis of the assessment, and the progress in fulfilling these plans is verified by operational risk management sections or internal auditors.

Box 4: An Example of Control Self-Assessments

1. Individual sections or businesses assess the risk profile on their own and assign scores.

Inherent risk		Score
	Transaction volume	X
	Asset size	X
	Complexity of product	X
	Legal risk	X
	---	---
Weighted average (out of 10)		X

Size of risk for each business (a)

Risk management system		Score
	Result of preceding audit	Y
	Managers' expertise	Y
	Maintenance status of computer systems	Y
	---	Y
	---	---
Weighted average(out of 10)		Y

Level of risk management (b)

Total score (residual risk) (out of 10)
Z

a – b = c

2. Sum up the results of self-assessment for all sections and businesses and identify the risk within the financial institution in an integrated framework. In order to ensure that assessments are consistent, the section responsible for firm-wide operational risk management or internal auditors verify the self-assessment results for each section or business.

Section or business	Business risk (scores)	Risk management system (scores)	Residual risk (scores)	Risk level
Sales Division, Head Office	X	Y	Z	Me-dium
Financial Product Development Division	X	Y	Z	High
Trading Division	X	Y	Z	Me-dium
---	---	---	---	---
Branch 1	X	Y	Z	Me-dium
Branch 2	X	Y	Z	High
Branch 3	X	Y	Z	Low
---	---	---	---	---

2. Adopting a realistic, cost-effectiveness approach

Self-assessment with too many evaluation items costs a huge amount in human resources in sections as well as in the section responsible for operational risk management. Thus, financial institutions should take a realistic approach by considering cost-effectiveness when designing the size and details of evaluation items.

3. Drawing up audit plans based on the results of self-assessments

At some financial institutions, internal auditors draw up audit plans based on the results of control self-assessments. Financial institutions should note, however, that (1) it is difficult to completely remove the bias in the primary assessments conducted by front-line sections even if the operational risk management sections carry out secondary assessments; and (2) there is a possibility that the control self-assessment framework itself suffers from a deficiency. Therefore, it is desirable to also make use of independently collected information (such as information obtained as a result of previous audits or from off-site monitoring) when drafting internal audit plans instead of relying solely on control self-assessments.

B. Key Risk Indicators

Operational risk management based on key risk indicators is a mechanism for selecting multiple indicators that contribute to early detection of heightened risk, ongoing monitoring of their movements, and preemptive reactions as necessary (see Box 5).

The indicators include (1) those showing a deterioration in the quality of the operational process, such as the number of clerical errors and computer system malfunctions, even though they are not necessarily accompanied by actual losses; and (2) those showing the size of potential operational risk such as clerical work volumes and the number of steps in developing computer system programs.[18]

The selection of indicators and reference values for triggering the corrective

[18] At many Japanese banks, reports on the number of clerical errors and computer system troubles have been submitted to management. Recently, there has been an increase in the number of cases where the range of items subject to reporting has been expanded and the operational risk management sections have collected the data and submitted consolidated reports to management. However, it is still rare to find cases where financial institutions set trigger points on the indicators and prompt management to take concrete corrective actions in accordance with a change in the indicators.

actions must reflect the actual profile of operations and operational risk-related loss events. It is also desirable to review them as necessary.

Box 5: An Example of the Use of Key Risk Indicators

1. Select multiple indicators that can contribute to early detection of heightened risk according to the actual state of operations at each section.

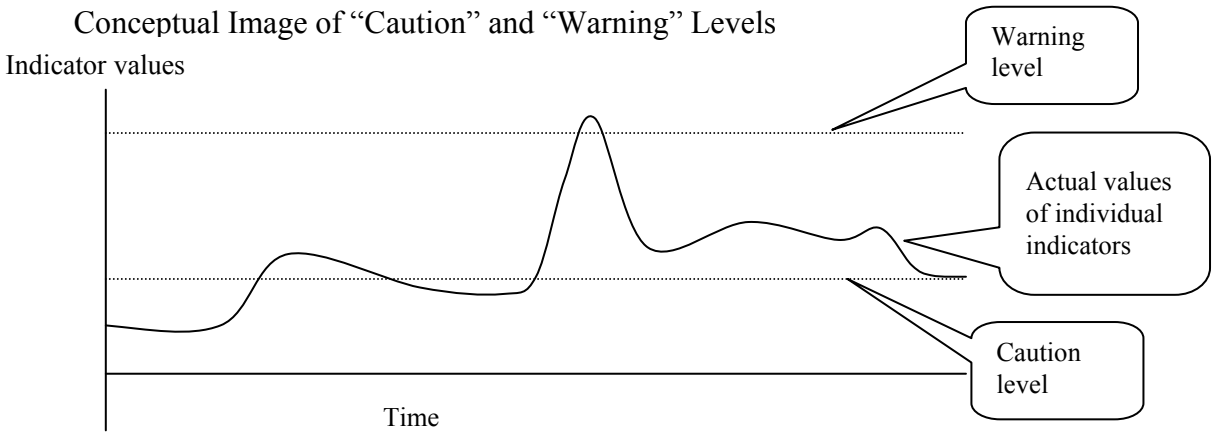
Examples of key risk indicators are as follows.

Operations:	Business volumes, customers' waiting times, number of clerical errors, number of complaints received, etc.
Computer systems:	Number of malfunctions, number of steps in developing programs, utilization ratio of system devices such as CPUs, storage, network traffic, etc.

2. Monitor movements in individual indicators (report consolidated results to management).

3. In cases where individual indicators surpass preset reference values (i.e., hit the "caution" and "warning" levels), monitoring is strengthened according to the degree to which it is exceeded (where the volumes exceed the caution level), or the business operations and risk management systems are reviewed (where the volumes exceed the warning level).

Conceptual Image of "Caution" and "Warning" Levels



The indicators subject to reporting differ according to the financial institution's business and risk profiles. The numbers of incidents, accidents, serious clerical errors, customer problems, and serious computer system malfunctions are generally subject to reporting.

VI. Conclusion

This paper has introduced recent approaches to advancing operational risk management, but this does not mean that the new methods should replace the conventional ones. Rather, the new methods are designed to enhance the effects and efficiency of the conventional ones. In that sense, the two complement each other, and there is a need to strengthen both in order to promote further improvement of operational risk management.

Various methods introduced here have been studied and applied by major financial institutions which have adopted advanced approaches to identify and manage their operational risks. Therefore, in the case of small- and medium-sized financial institutions, it is desirable to consider the state of their own businesses and organizations when adopting these methods.

Finally, the reliability of business operations at financial institutions depends to a considerable extent on the expertise, discipline, and morale of each individual employee of these institutions. Efforts to maintain and improve this aspect remain a major issue.

Appendix 1: International Trends in Reinforcing Operational Risk Management

In 1992, the Committee of Sponsoring Organizations of the Treadway Commission issued its report on a general framework for internal corporate controls in the United States: "Internal Control—Integrated Framework" (known as The COSO Report). This report subsequently became the basis of numerous frameworks issued by private-sector organizations, governments, and international institutions on internal controls for commercial companies and financial institutions.

The major frameworks are as follows.

A. Frameworks for Companies in General

1. The Committee of Sponsoring Organizations of the Treadway Commission, "Internal Control—Integrated Framework (The COSO Report)" (1992) (United States).
2. "Internal Control—Guidance for Directors on the Combined Code (The Turnbull Guidance)" (1999) (United Kingdom).
3. "The Sarbanes-Oxley Act of 2002" (United States).
4. The Committee of Sponsoring Organizations of the Treadway Commission, "Enterprise Risk Management—Integrated Framework (COSO II ERM)" (2004) (United States).

B. Frameworks for Financial Institutions

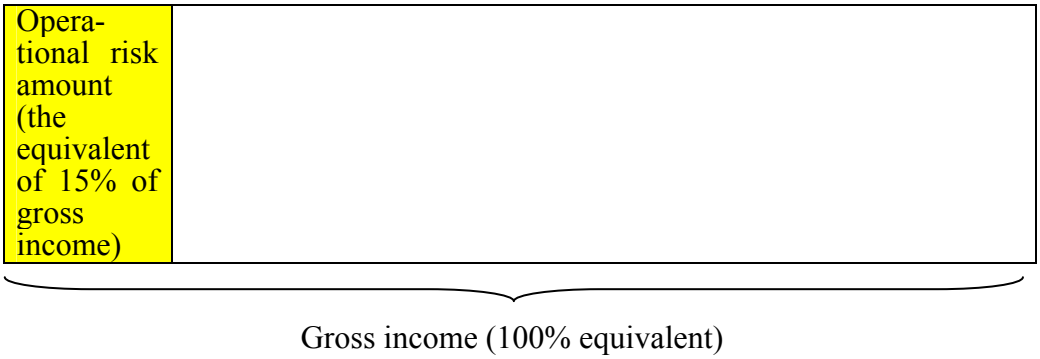
5. The Basel Committee on Banking Supervision, Bank for International Settlements, "Framework for Internal Control Systems in Banking Organizations" (1998).
6. The Basel Committee on Banking Supervision, Bank for International Settlements, "Sound Practices for the Management and Supervision of Operational Risk" (2003).

Appendix 2: Operational Risk Quantification Methods under the Basel II Framework

The Basel II Framework presents three methods for quantifying and allocating operational risk capital: the Basic Indicator Approach, the Standardized Approach, and the Advanced Measurement Approach.

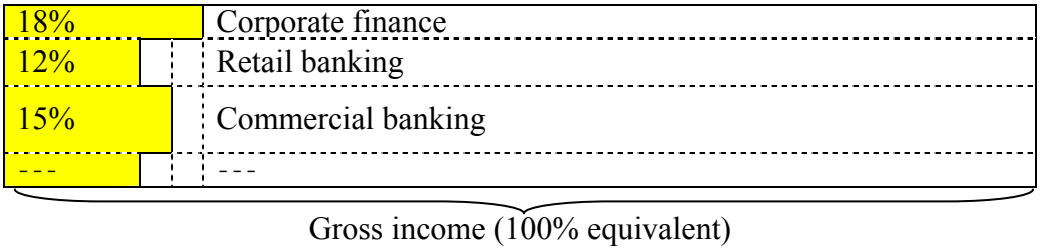
A. Basic Indicator Approach

Annual gross income[19] × 15% = amount of operational risk



B. Gross Income Allocation Approach (Standardized Approach)

Gross income by section[20] × a fixed percentage (12–18%) = amount of operational risk



C. Advanced Measurement Approach

Only minimal conditions (identification of tail loss events, etc.) to be met when adopting this approach are presented. This envisions cases where banks use the current risk quantification methods without modification.

[19] In Japan, this is expected to be "gross operating profit" used in bank accounting, to which some adjustments will be made.

[20] Specifies eight business operations: corporate finance, trading and sales, retail banking, commercial banking, payment and settlement, agency services, asset management, and retail brokerage.