Checklist for Operational Risk Management

I. Development and Establishment of Comprehensive Operational Risk Management System
by Management

[Checkpoints]

- Operational risk is the risk of loss resulting from inadequate operation processes, inadequate activities by officers and employees and inadequate systems or from external events (the type of risk included in the calculation of the capital adequacy ratio) and the risk defined by the financial institution as operational risk (the type of risk not included in the calculation of the capital adequacy ratio).
- Comprehensive Operational Risk Management refers to identification, assessment, monitoring, control and mitigation regarding operational risk in a comprehensive manner as a financial institution as a whole.
- The development and establishment of a system for comprehensive operational risk management is extremely important from the viewpoint of ensuring the soundness and appropriateness of a financial institution's business. Therefore, the institution's management is charged with and responsible for taking the initiative in developing and establishing such a system.
- When reviewing a financial institution's comprehensive operational risk management system, the inspector should examine whether the system is an appropriate one commensurate with the scale and nature of the institution's business and its risk profile as well as the levels of complexity and sophistication of the operational risk quantification (measurement) technique used by the institution (including The Basic Indicator Approach and The Standardized Approach).

It should be noted that the type and level of the operational risk quantification technique to be used by a financial institution should be determined according to the institution's strategic objectives, the diversity of its business and the level of complexity of the operational risks faced by it and therefore a complex or sophisticated operational risk quantification technique is not necessarily suited to all financial institutions.

- The inspector should determine whether the comprehensive operational risk management system is functioning effectively and whether the roles and responsibilities of the institution's management are being appropriately performed by way of reviewing, with the use of check items listed in Chapter I., whether management is appropriately implementing (1) policy development, (2)

development of internal rules and organizational frameworks and (3) development of a system for assessment and improvement activities.

- If any problem is recognized as a result of reviews conducted with the use of the check items listed in Chapter II. and later, it is necessary to exhaustively examine which of the elements listed in Chapter I. are absent or insufficient, thus causing the said problem, and review findings thereof through dialogue between the inspector and the financial institution.
- If the institution's management fails to recognize weaknesses or problems recognized by the inspector, it is also necessary to explore in particular the possibility that the Internal Control System is not functioning effectively and review findings thereof through dialogue.
- The inspector should review the status of improvements with regard to those issues pointed out on the occasion of the last inspection that are not minor and determine whether or not effective improvement measures have been developed and implemented.

1. Policy Development

(1) Roles and Responsibilities of Directors

Do directors attach importance to comprehensive operational risk management, fully recognizing that the lack of such an approach could seriously hinder attainment of strategic objectives? In particular, does the director in charge of such risk management examine the policy and specific measures for developing and establishing an adequate comprehensive operational risk management system with a full understanding of the scope, types, and nature of operational risks and the techniques of identification, assessment, monitoring and control regarding operational risks as well as the importance of comprehensive operational risk management, and with precise recognition of the current status of the comprehensive operational risk management system within the financial institution based on such understanding?

(2) Development and Dissemination of Operational Risk Management Policy

Has the Board of Directors established a policy regarding operational risk management (hereinafter referred to as the "Operational Risk Management Policy") and disseminated it throughout the institution? Is the appropriateness of the Operational Risk Management Policy being secured by way of, for example, clear statements on the following matters?

- The roles and responsibilities of the director in charge and the Board of Directors or equivalent organization to the Board of Directors with regard to comprehensive

- operational risk management
- The definition of operational risk at the financial institution
- The policy on organizational framework, such as establishment of a division concerning comprehensive operational risk management (hereinafter referred to as the "Comprehensive Operational Risk Management Division") and the authority assigned thereto
- The policy regarding identification, assessment, monitoring, control and mitigation of operational risks

(3) Revision of the Policy Development Process

Does the Board of Directors revise the policy development process in a timely manner by reviewing its effectiveness based on reports and findings on the status of comprehensive operational risk management in a regular and timely manner or on an as needed basis?

2. Development of Internal Rules and Organizational Frameworks

(1) Development and Dissemination of Internal Rules

Does the Board of Directors or equivalent organization to the Board of Directors have the Manager of the Comprehensive Operational Risk Management Division (hereinafter simply referred to as the "Manager" in this checklist) develop internal rules that clearly specify the arrangements concerning comprehensive operational risk management (hereinafter referred to as the Operational Risk Management Rules") and disseminate them throughout the institution in accordance with the Operational Risk Management Policy? Has the Board of Directors or equivalent organization to the Board of Directors approved the Operational Risk Management Rules after determining if they comply with the Operational Risk Management Policy after legal checks, etc.?

(2) Establishment of the System of Comprehensive Operational Risk Management Division

(i) Does the Board of Directors or equivalent organization to the Board of Directors have a Comprehensive Operational Risk Management Division established and have the division prepared to undertake appropriate roles in accordance with the Operational Risk Management Policy and the Operational Risk Management Rules.¹

¹ When the Comprehensive Operational Risk Management Division is not established as an independent division (e.g., when the division is consolidated with another risk management division to form a single division or when a division in charge of other business also takes charge of comprehensive operational risk management or when a Manager or Managers take charge of comprehensive operational risk management instead of a division or a department), the inspector shall review whether or not such a system is sufficiently reasonable and provides the same functions as in the case of establishing an independent division in light of the scale and nature of the institution and its risk profile.

- (ii) Has the Board of Directors allocated to the Comprehensive Operational Risk Management Division a Manager with the necessary knowledge and experience to supervise the division and enable the Manager to implement management operations by assigning him/her the necessary authority therefor?
- (iii) Has the Board of Directors or equivalent organization to the Board of Directors allocated to the Comprehensive Operational Risk Management Division an adequate number of staff members with the necessary knowledge and experience to execute the relevant operations and assigned such staff the authority necessary for implementing the business?²
- (iv) Does the Board of Directors or equivalent organization to the Board of Directors secure a check-and-balance system of the Comprehensive Operational Risk Management Division against operational divisions?

(3) Development of Comprehensive Operational Risk Management System in Operational Divisions, Sales Branches, etc.

- (i) Does the Board of Directors or equivalent organization to the Board of Directors provide a system to fully disseminate the relevant internal rules and operational procedures to operational divisions, sales branches, etc. and have them observe the rules and operational procedures? For example, does the Board of Directors or equivalent organization to the Board of Directors instruct the Manager to identify the internal rules and operational procedures to be observed by operational divisions and sales branches and to carry out specific measures for ensuring observance such as providing effective training on a regular basis?
- (ii) Does the Board of Directors or equivalent organization to the Board of Directors provide a system to ensure the effectiveness of comprehensive operational risk management in operational divisions, sales branches, etc. through the Manager or the Comprehensive Operational Risk Management Division? For example, is a person in charge of comprehensive operational risk management assigned to each operational division and sales branch for coordination with the Manager?

(4) System for Reporting to Board of Directors or equivalent organization to Board of Directors and Approval

Has the Board of Directors or equivalent organization to the Board of Directors appropriately specified matters that require reporting and those that require approval and does it have the Manager

² When a department or a post other than the Board of Directors or equivalent organization to the Board of Directors is empowered to allocate staff and assign them authority, the inspector shall review, in light of the nature of such a department or post, whether or not the structure of the Comprehensive Operational Risk Management Division is reasonable in terms of a check-and-balance system and other aspects.

report the current status to the Board of Directors or equivalent organization to the Board of Directors in a regular and timely manner or on an as needed basis or have the Manager seek the approval of the Board of Directors or equivalent organization to the Board of Directors on the relevant matters? In particular, does it ensure that the Manager reports to the Board of Directors or equivalent organization to the Board of Directors without delay any matters that would seriously affect corporate management or significantly undermine customer interests?

(5) System for Reporting to Corporate Auditor

In the case where the Board of Directors has specified matters to be directly reported to a corporate auditor, has it specified such matters appropriately and do they provide a system to have the Manager directly report such matters to the auditor?³

(6) Development of Internal Audit Guidelines and Internal Audit Plan

Does the Board of Directors or equivalent organization to the Board of Directors have the Internal Audit Division appropriately identify the matters to be audited with regard to comprehensive operational risk management, develop guidelines that specify the matters subject to internal audit and the audit procedure (hereinafter referred to as "Internal Audit Guidelines") and an internal audit plan, and approve such guidelines and plan?⁴ For example, does it have the following matters clearly specified in the Internal Audit Guidelines or the internal audit plan and provide a system to have these matters appropriately audited?

- Status of development of the comprehensive operational risk management system
- Status of observance of the Operational Risk Management Policy, the Operational Risk Management Rules, etc.
- Appropriateness of the comprehensive operational risk management processes commensurate with the scale and nature of the business, and its risk profile
- Status of improvement of matters pointed out in an internal audit or on the occasion of the last inspection

(7) Revision of the Development Process of Internal Rules and Organizational Frameworks

Does the Board of Directors or equivalent organization to the Board of Directors revise the development process of internal rules and organizational frameworks in a timely manner by reviewing its effectiveness based on reports and findings on the status of comprehensive operational risk management in a regular and timely manner or on an as needed basis?

³ It should be noted that this shall not preclude a corporate auditor from voluntarily seeking a report and shall not restrict the authority and activities of the auditor in any way.

⁴ The Board of Directors or equivalent organization to the Board of Directors only needs to have approved the basic matters with regard to an internal audit plan.

3. Assessment and Improvement Activities

1) Analysis and Assessment

(1) Analysis and Assessment of Comprehensive Operational Risk Management

Does the Board of Directors or equivalent organization to the Board of Directors appropriately determine whether there are any weaknesses or problems in the comprehensive operational risk management system and the particulars thereof, and appropriately review their causes by precisely analyzing the status of comprehensive operational risk management and assessing the effectiveness of comprehensive operational risk management, based on all information available regarding the status of comprehensive operational risk management, such as the results of audits by corporate auditors, internal audits and external audits, findings of various investigations and reports from various divisions? In addition, if necessary, does it take all possible measures to find the causes by, for example, establishing fact findings committees etc. consisting of non-interested persons?

(2) Revision of Analysis and Assessment Processes

Does the Board of Directors or equivalent organization to the Board of Directors revise the analysis and assessment processes in a timely manner by reviewing their effectiveness based on reports and findings on the status of comprehensive operational risk management in a regular and timely manner or on an as needed basis?

2) Improvement Activities

(1) Implementation of Improvements

Does the Board of Directors or equivalent organization to the Board of Directors provide a system to implement improvements in the areas of the problems and weaknesses in the comprehensive operational risk management system identified through the analysis, assessment and examination referred to in 3. 1) above in a timely and appropriate manner based on the results obtained by developing and implementing an improvement plan as required or by other appropriate methods?

(2) Progress Status of Improvement Activities

Does the Board of Directors or equivalent organization to the Board of Directors provide a system to follow up on the efforts for improvement in a timely and appropriate manner by reviewing the progress status in a regular and timely manner or on an as needed basis?

(3) Revision of the Improvement Process

Does the Board of Directors or equivalent organization to the Board of Directors revise the improvement process in a timely manner by reviewing its effectiveness based on reports and findings on the status of comprehensive operational risk management in a regular and timely manner or on an as needed basis?

II. Development and Establishment of Comprehensive Operational Risk Management System by Manager

[Checkpoints]

- This chapter lists the check items to be used when the inspector reviews the roles and responsibilities to be performed by the Manager and the Comprehensive Operational Risk Management Division.
- If any problem is recognized as a result of reviews conducted with the use of the check items listed in Chapter II., it is necessary to exhaustively examine which of the elements listed in Chapter I. are absent or insufficient, thus causing the said problem, and review findings thereof through dialogue between the inspector and the financial institution.
- If the institution's management fails to recognize problems recognized by the inspector, it is also necessary to strictly explore in particular the possibility that the systems and processes listed in Chapter I. are not functioning appropriately and review findings thereof through dialogue.
- The inspector should review the status of improvements with regard to those issues pointed out on the occasion of the last inspection that are not minor and determine whether or not effective improvement measures have been developed and implemented.

1. Roles and Responsibilities of Manager

(1) Development and Dissemination of Operational Risk Management Rules

Has the Manager, in accordance with the Operational Risk Management Policy, identified the risks, decided the methods of assessment and monitoring thereof and developed the Operational Risk Management Rules that clearly define the arrangements on risk control and mitigation, based on a full understanding of the scope, types and nature of risks and the comprehensive operational risk management technique? Have the Operational Risk Management Rules been disseminated throughout the institution upon approval by the Board of Directors or equivalent organization to the Board of Directors?

(2) Operational Risk Management Rules

Do the Operational Risk Management Rules exhaustively cover the arrangements necessary for comprehensive operational risk management and specify the arrangements appropriately in a manner befitting the scale and nature of the financial institution's business, and its risk profile? Do

the rules specify the following items, for example?

- Arrangements on the roles, responsibilities and the organizational framework of the Comprehensive Operational Risk Management Division
- Arrangements on the framework for comprehensive management by the Comprehensive
 Operational Risk Management Division of the Administrative Risk Management Division
 and the Information Technology Risk Management Division (hereinafter referred to as the
 "Operational Risk Management Divisions")
- Arrangements on the identification of risks to be subjected to comprehensive operational risk management
- Arrangements on the qualitative risk management technique for operational risks
- Arrangements on the scope of the quantification of operational risk and the technique thereof
- Arrangements on reporting of loss incidents to the Comprehensive Operational Risk Management Division
- Arrangements on the method of risk monitoring
- Arrangements on reporting to the Board of Directors or equivalent organization to the Board of Directors
- Arrangements on the procedures for allocating gross profit to the operation categories listed in Attachment 1 of "Criteria for Judging Whether A Financial Institution's Capital Is Sufficient in Light of the Assets Held, etc. under the Provision of Article 14-2 of the Banking Law" (Notification No. 19 of 2006, the Financial Services Agency)" (hereinafter referred to as the "Notification") and on the criteria for revising the procedures. This shall apply to financial institutions that use The Standardized Approach.

(3) Development of Organizational Frameworks by Manager

- (i) Does the Manager, in accordance with the Operational Risk Management Policy and the Operational Risk Management Rules, provide for measures to have the Comprehensive Operational Risk Management Division exercise a check-and-balance system in order to conduct comprehensive operational risk management system appropriately?
- (ii) Does the Manager make sure to report without delay to the Comprehensive Risk Management Division when detecting any limitations or weaknesses of the comprehensive operational risk management system that may affect comprehensive risk management?
- (iii) Does the Manager provide a system to identify risks inherent in New Products as specified in the Comprehensive Risk Management Policy, etc. in advance and report them to the Comprehensive Risk Management Division when requested to do so by the division?⁵

⁵ See "Checklist for Business Management (Governance) (for Basic Elements)," I. 3. (4).

- (iv) Does the Manager have in place an operational risk management computer system⁶ with the high reliability suited to the scale and nature of the financial institution's business, and its risk profile?
- (v) Does the Manager ensure the system of training and education to enhance the ability of employees to conduct comprehensive operational risk management in an effective manner, thus developing human resources with relevant expertise?
- (vi) Does the Manager provide a system to ensure that matters specified by the Board of Directors or equivalent organization to the Board of Directors are reported in a regular and timely manner or on an as needed basis? In particular, does the Manager provide a system to ensure that matters that would seriously affect corporate management are reported to the Board of Directors or equivalent organization to the Board of Directors without delay?

(4) Revision of Operational Risk Management Rules and Organizational Frameworks

Does the Manager conduct monitoring on an ongoing basis with regard to the status of execution of operations at the Comprehensive Operational Risk Management Division?

Does the Manager review the effectiveness of the comprehensive operational risk management system in a regular and timely manner or on an as needed basis, and, as necessary, revise the Operational Risk Management Rules and the relevant organizational frameworks or present the Board of Directors or equivalent organization to the Board of Directors with proposals for improvement?

2. Roles and Responsibilities of Comprehensive Operational Risk Management Division

1) Risk Identification and Assessment

(1) Identification of Operational Risk

(i) Does the Comprehensive Operational Risk Management Division obtain data collected by operational divisions and sales branches, etc. as necessary to identify operational risk?

- (ii) Does the Comprehensive Operational Risk Management Division, in accordance with the Operational Risk Management Policy and the Operational Risk Management Rules, broadly specify internal and external factors that may produce adverse effects on the financial institution's business based on an understanding of the possibility that operational risk may emerge in any division or department?
- (iii) Does the Comprehensive Operational Risk Management Division identify operational risk when the financial institution starts the handling of New Products, introduces a new computer

⁶ It should be noted that the computer system may be a centralized dataprocessing environment system, distribution processing system, or EUC (end user computing) type.

system and begins business at overseas offices and subsidiaries?

(2) Operational Risk Assessment

- (i) Does the Comprehensive Operational Risk Management Division appropriately assess operational risk with the use of scores (CSA, etc.) and financial and management indicators?
- (ii) Does the Comprehensive Operational Risk Management Division analyze the causes of operational risk loss incidents during the operational risk assessment process, thus fully grasping the financial institution's operational risk?

(3) Operational Risk Quantification (Measurement)

Does the Comprehensive Operational Risk Management Division quantify (measure) operational risk in a manner suited to the scale and nature of the financial institution's business, and its risk profile?

- (i) When calculating the operational risk quantity by applying weighting factors to financial indicators (gross profit, expenses, etc.) as a quantification technique, does the Comprehensive Operational Risk Management Division appropriately determine the type of indicators used and the level of weightings applied? Does the division revise the indicators used and the weightings applied in light of improvement in the level of comprehensive operational risk management, changes in internal and external environments and occurrence of significant internal losses with the use of a scoring technique?
- (ii) Does the Comprehensive Operational Risk Management Division pay attention to the check items listed in Chapter III. 2. of this checklist when using the operational risk measurement technique?

2) Monitoring

(1) Monitoring of the Operational Risk

Does the Comprehensive Operational Risk Management Division, in accordance with the Operational Risk Management Policy and the Operational Risk Management Rules, conduct monitoring with regard to the status of operational risks with an appropriate frequency in light of the financial institution's internal environment (risk profile, etc.) and external environment?

(2) Reporting to Board of Directors or equivalent organization to Board of Directors

Does the Comprehensive Operational Risk Management Division, in accordance with the Operational Risk Management Policy and the Operational Risk Management Rules, report in a regular and timely manner or on an as needed basis information necessary for the Board of Directors or equivalent organization to the Board of Directors to make an appropriate assessment

and judgment with regard to the status of the comprehensive operational risk management?

(3) Feedback to Operational Risk Management Divisions

Does the Comprehensive Operational Risk Management Division feed back the results of its assessment, analysis and review with regard to the status of operational risks to the relevant Operational Risk Management Divisions?

3) Control and Mitigation

(1) Operational Risk Control

Does the Comprehensive Operational Risk Management Division provide information necessary for the Board of Directors or equivalent organization to the Board of Directors to make decisions with regard to how to control the important operational risk assessed?

(2) Operational Risk Mitigation

Does the Comprehensive Operational Risk Management Division pay attention to the possible occurrence of new risk when implementing measures to mitigate operational risk (including insurance contracts)?

4) Review and Revision

Does the Comprehensive Operational Risk Management Division grasp changes in operational environment and risk profile as well as the limitations and weaknesses of the operational risk assessment method, and regularly review whether the method suits the scale and nature of the financial institution's business and its risk profile, and revise the method?

III. Specific Issues

[Checkpoints]

- This chapter lists the check items to be used when the inspector reviews specific issues particular to the actual status of comprehensive operational risk management.
- If any problem is recognized as a result of reviews conducted with the use of the check items listed in Chapter III., it is necessary to exhaustively examine which of the elements listed in Chapter I. and II are absent or insufficient, thus causing the said problem, and review findings thereof through dialogue between the inspector and the financial institution.
- If the institution's management fails to recognize problems recognized by the inspector, it is also necessary to strictly explore in particular the possibility that the systems and processes listed in Chapter I. are not functioning appropriately and review findings thereof through dialogue.
- The inspector should review the status of improvements with regard to those issues pointed out on the occasion of the last inspection that are not minor and determine whether or not effective improvement measures have been developed and implemented.

1. Appropriateness of Calculation of Operational Risk Equivalent Amount

1) Checkpoints for Institutions in Case of The Use of The Basic Indicator Approach and The Standardized Approach

Has the institution decided whether or not to exclude expenses that do not constitute outsourcing costs from services transaction expenses? In the case where such costs are excluded from services transaction expenses, has the institution developed criteria that specify expenses that do not constitute outsourcing costs? (Expenses that constitute outsourcing costs may be restrictively specified.)

2) Checkpoints for Institutions in Case of Use of The Standardized Approach

- (1) Has the institution calculated gross profits generated from all its business without any overlap based on the procedures for allocating gross profits to the operation categories listed in Attachment 1 of the Notification?
- (2) When an allocated value for a certain business category of Attachment 1 of the Notification (a figure obtained by multiplying the allocated profit with the weighing factor applicable according to

the business category in Attachment 1 of the Notification) is a negative number, does the institution decide whether or not to offset the negative number with a positive number for another operation category? When conducting such offsetting, does the institution ensure that objective judgment can be made?

- (3) In the case where a category in the criteria used for the calculation of the credit risk asset amount and market risk equivalent amount is similar to a category in Attachment 1 of the Notification, are the two categories compatible? When that is not the case, is the reason thereof explicitly specified?
- (4) Does the institution have objective criteria for judging whether or not a certain business is attendant to business included in any of the business categories listed in Attachment 1 of the Notification? When there is a business attendant to business included in two or more of those business categories, does the institution have criteria for allocating gross profits from such a business?
- (5) In the case where gross profits from a certain business cannot be allocated to a specific business category, does the institution specify the name of the business and the reason for the inability to allocate gross profits?
- (6) Has the institution developed its criteria for allocating gross profits to two or more of the categories listed in Attachment 1 of the Notification based on financial accounting or management accounting?

2. Check Items in Case of Employment of Operational Risk Measurement Technique

1) Establishment of Operational Risk Measurement System

- (i) Is the operational risk measurement system conceptually sound and implemented with integrity?
- (ii) Is the role of the operational risk measurement technique (model) clearly positioned under the Operational Risk Management Policy and implemented based on an understanding of the items listed below, for example? Does it determine if it is implemented with integrity to consolidated Subsidiaries as well?
 - (a) The financial institution's strategic objectives, the scale and nature of its business, and its risk profile
 - (b) The fundamental design concept of the operational risk measurement technique based on (a)
 - (c) Identification and measurement of operational risk based on (b) (scope, techniques, assumptions, etc.)
 - (d) The nature (limitations and weaknesses) of the operational risk measurement technique that derives from (c) and the validity of the technique
 - (e) Details of the method of validating (d)

(iii) In the case where capital allocation management⁷ is employed, has the capital allocation management policy been developed based on the outcomes obtained through the calculation of the operational risk measurement technique? When there are risks which are not measured with this technique, are there any reasonable grounds for excluding them from the measurement? Is the risk capital allocated with due consideration for the risks excluded from the measurement?

2) Appropriate Involvement of Directors and Corporate Auditors

(1) Understanding of Operational Risk Measurement Technique

- (i) Do directors understand that decisions concerning the operational risk measurement technique as well as the risk limits and the risk capital limits (in the case where capital allocation management is employed) have serious implications for the financial institution's corporate management and financial conditions?
- (ii) Does the director in charge of operational risk management understand the operational risk measurement technique required for the business of the financial institution and comprehend the nature (limitations and weaknesses) thereof?
- (iii) Do directors and corporate auditors seek to enhance their understanding of the operational risk measurement technique by participating in training or through other means?

(2) Approach to Comprehensive Operational Risk Management

Do directors involve themselves actively in comprehensive operational risk management based on the operational risk measurement technique?

3) Operational Risk Measurement

(1) Measurement of Operational Risk Quantity with Universal Yardstick

Does the institution grasp the operational risk quantity with the use of a uniform standard applicable to various types of operational risk? It is desirable that the uniform yardstick is used to grasp and measure all necessary operational risk elements. If there are risks that are not sufficiently grasped and measured with the uniform yardstick, does the institution ensure that all necessary elements are taken into consideration in corporate management decisions by utilizing supplementary information?

Is the measurement of the operational risk quantity conducted with a rational, objective and precise statistical technique such as a VaR method, for example?

(2) Appropriateness of Measurement Technique

In the case where the measurement technique involves calculation of the maximum loss at a

_

⁷ See Checklist for Capital Management.

certain confidence level as the operational risk quantity by processing individual operational loss incidents statistically, is attention paid to the following matters?

- Are internal loss incidents used appropriately? Are scenarios formulated based on the results of the assessment of external information and operational processes, etc. taken into consideration as loss incidents?
- Is the confidence level and holding period set by the institution appropriate?
- Is the measurement technique a rational one that appropriately covers low-frequency, large-scale loss incidents?

(3) System to Verify and Manage Operational Risk Measurement Technique, etc.

Are the validity of the operational risk measurement technique and the assumptions thereof, etc. verified during the development of the technique and thereafter on a regular basis by a person or persons with no involvement in the development and with sufficient capabilities? If any deficiency is recognized in the operational risk measurement technique or the assumptions thereof, is a corrective action taken appropriately?

Are there frameworks and internal rules in place to prevent the operational risk measurement technique and the assumptions thereof from being altered on unreasonable grounds, and is the operational risk measurement technique managed appropriately in accordance with the internal rules?

4) Records on Operational Risk Measurement Technique

Is there a system to keep records, for future reference, on the review process with regard to the selection of operational risk measurement technique and the assumptions thereof and the grounds for the selection process, in order to enable a follow-up review and utilize the records to make the measurement more sophisticated and elaborated?

5) Audit

(1) Development of Auditing Program

Has the institution developed an audit program that exhaustively covers audits of the operational risk measurement technique?

(2) Scope of Internal Audit

Is auditing conducted to check the following items?

- Consistency of the operational risk measurement technique with the strategic objectives, the scale and nature of the business, and the risk profile
- Appropriateness of employing the operational risk measurement technique in light of the nature (limitations and weaknesses) thereof

- Appropriate documentation of records on the operational risk measurement technique and timely updating thereof
- Appropriate reflection of any modification of the process of comprehensive operational risk management in the measurement technique
- Validity of the scope of measurement conducted with the operational risk measurement technique.
- Absence of any deficiency in the information system for the management

(3) Utilization of the Results of Audits

Does the Comprehensive Operational Risk Management Division appropriately revise the operational risk measurement technique based on the results of audits?

6) Operational Risk Measurement Model Developed by Outsourcing Contractor⁸

(1) Appropriateness of Operational Risk Measurement System

- (i) Does the person in charge of operational risk measurement at the financial institution have sufficient knowledge with regard to the measurement technique and understand the modeling process of operational risk measurement?
- (ii) Do the institution's Comprehensive Operational Risk Management Division and the Internal Audit Division conduct a theoretical and empirical validate of the validity of the measurement technique?

(2) Appropriateness of Operational Risk Measurement Model

- (i) Is there not any "black box" with regard to the measurement model? If there is one, has the validity of the measurement model been validated?
- (ii) Are the consistency and the accuracy of external data, internal data and scenario data secured?
- (iii) Is the measurement model selected suited to the scale and nature of the financial institution's business, and its risk profile?

(3) Management of Developer of Operational Risk Measurement Model

- (i) Is the developer consigned with the development of the operational risk measurement model capable of ensuring continuous management of the model and promoting sophistication and elaboration of the model? Does the institution regularly evaluate the developer?
- (ii) Does the developer provide sufficient user support (training, consulting and maintenance) with regard to operational risk measurement?
- (iii) Is it ensured that the developer reports to the institution on the status of its validation of the validity of the measurement model in a regular and timely manner or on an as needed basis?

⁸ When the operational risk measurement is outsourced, the verification should be conducted by using the check items listed in this paragraph.

3. Operational Risk Management Concerning Outsourced Business⁹

(1) Selection of Outsourcing Contractors

Before a business is outsourced, does the Comprehensive Operational Risk Management Division, in coordination with the Outsourcing Manager, ¹⁰ identify the operational risk inherent in the outsourced business and ensure the business is consigned to a party capable of implementing the business aptly, fairly and efficiently after recognizing possible risk management problems related to the quality of service, the reliability of service continuity, etc.? In selecting the outsourcing contractor, does the division check the following points, for example, from the viewpoint of operational risk management?

- Is the outsourcing contractor capable of providing a sufficient level of service in terms of reasonableness as a service provided by a financial institution?
- Are the financial and corporate management conditions of the outsourcing contractor sufficient to allow it to provide service and bear possible losses in accordance with the outsourcing contract?
- Is there not any problem from the viewpoint of the reputation of the employing financial institution?

(2) Terms of Outsourced Contract

Does the Comprehensive Operational Risk Management Division, in coordination with the Outsourcing Manager, provide for measures to make sure that the outsourced contract specifies the level of service to be provided by the outsourcing contractor and the sharing of responsibilities (e.g. the responsibility of the outsourcing contractor in the case where the service provided fails to meet the contract terms and the arrangement for sharing losses that may arise in relation to the outsourcing)

(3) Monitoring of Outsourcing Contractors

Does the Comprehensive Operational Risk Management Division provide for measures to regularly conduct monitoring with regard to the outsourced business in coordination with the Outsourcing Manager?

⁹ As the forms of outsourcing and the types of outsourced business are diverse, it is necessary in the verification of operational risk management concerning outsourced business to make verification in light of the details of the outsourced business and the level of importance thereof, for the outsourcing institution, etc.

¹⁰ It should be noted that this shall not prevent the Manager of the Comprehensive Operational Risk Management Division from concurrently serving as the Outsourcing Manager.

(4) Correction of Problems

Does the Comprehensive Operational Risk Management Division provide for measures to take corrective action without delay in coordination with the Outsourcing Manager when detecting any problems?

4. Administrative Risk Management System

With regard to the administrative risk management system, see Attachment 1.

5. Information Technology Risk Management System

With regard to the information technology risk management system, see Attachment 2.

6. System for Managing Other Operational Risks

With regard to a system for managing operational risks as defined by the financial institution other than administrative risks and information technology risks (hereinafter referred to as the "Other Risk Management System"), see Attachment 3.

(Attachment 1)

I. Development and Establishment of Administrative Risk Management System by Management

[Checkpoints]

- Administrative risk is the risk of a financial institution incurring a loss from the neglect by officers and employees to conduct administrative work properly, accidents caused by them and violation of Laws conducted by them in the course of the administrative work process.
- The development and establishment of a system for managing administrative risks is extremely important from the viewpoint of ensuring the soundness and appropriateness of a financial institution's business. Therefore, the institution's management is charged with and responsible for taking the initiative in developing and establishing such a system.
- The inspector should determine whether the administrative risk management system is functioning effectively and whether the roles and responsibilities of the institution's management are being appropriately performed by way of reviewing, with the use of check items listed in Chapter I., whether the management is appropriately implementing (1) policy development, (2) development of internal rules and organizational frameworks and (3) development of a system for assessment and improvement activities.
- If any problem is recognized as a result of reviews conducted with the use of the check items listed in Chapter II. and later, it is necessary to exhaustively examine which of the elements listed in Chapter I. are absent or insufficient, thus causing the said problem, and review findings thereof through dialogue between the inspector and the financial institution.
- If the institution's management fails to recognize weaknesses or problems recognized by the inspector, it is also necessary to examine in particular the possibility that the Internal Control System is not functioning effectively and review findings thereof through dialogue.
- The inspector should review the status of improvements with regard to those issues pointed out on the occasion of the last inspection that are not minor and determine whether or not effective improvement measures have been developed and implemented.

1. Policy Development

(1) Roles and Responsibilities of Directors

Do directors attach importance to administrative risk management, fully recognizing that the lack of such an approach could seriously hinder attainment of strategic objectives? In particular, does the director in charge of administrative risk management examine the policy and specific measures for developing and establishing an adequate administrative risk management system with a full understanding of the scope, types and nature of administrative risks, and the identification, assessment, monitoring and control technique as well as the importance of administrative risk management, and with precise recognition of the current status of administrative risk management within the financial institution based on such understanding?

(2) Development and Dissemination of Administrative Risk Management Policy

Has the Board of Directors established a policy regarding administrative risk management (hereinafter referred to as the "Administrative Risk Management Policy") and disseminated it throughout the institution? Is the appropriateness of the Administrative Risk Management Policy secured by way of, for example, clear statements on the following matters?

- The roles and responsibilities of the director in charge and the Board of Directors or equivalent organization to the Board of Directors with regard to administrative risk management
- The policy on organizational framework, such as establishment of a division concerning administrative risk management (hereinafter referred to as the "Administrative Risk Management Division") and the authority assigned thereto
- The policy regarding identification, assessment, monitoring, control and mitigation of administrative risks

(3) Revision of the Policy Development Process

Does the Board of Directors or equivalent organization to the Board of Directors revise the policy development process in a timely manner by reviewing its effectiveness based on reports and findings on the status of administrative risk management in a regular and timely manner or on an as needed basis?

2. Development of Internal Rules and Organizational Frameworks

(1) Development of Internal Rules

Does the Board of Directors or equivalent organization to the Board of Directors have the

Manager of the Administrative Risk Management Division (hereinafter simply referred to as the "Manager" in this checklist) develop internal rules that clearly specify the arrangements concerning administrative risk management (hereinafter referred to as the "Administrative Risk Management Rules") and disseminate them throughout the institution in accordance with the Administrative Risk Management Policy? Does the Board of Directors or equivalent organization to the Board of Directors approve the Administrative Risk Management Rules after determining if they comply with the Administrative Risk Management Policy after legal checks, etc.?

(2) Establishment of the System of Administrative Risk Management Division

- (i) Does the Board of Directors or equivalent organization to the Board of Directors have an Administrative Risk Management Division established and have the division prepared to undertake appropriate roles in accordance with the Administrative Risk Management Policy and the Administrative Risk Management Rules?¹
- (ii) Has the Board of Directors allocated to the Administrative Risk Management Division a Manager with the necessary knowledge and experience to supervise the division and enable the Manager to implement management operations by assigning him/her the necessary authority therefor?
- (iii) Has the Board of Directors or equivalent organization to the Board of Directors allocated to the Administrative Risk Management Division an adequate number of staff members with the necessary knowledge and experience to execute the relevant operations and assigned such staff the authority necessary for implementing operations?²
- (iv) Does the Board of Directors or equivalent organization to the Board of Directors secure a check-and-balance system of the Administrative Risk Management Division against operational divisions?

(3) Development of Administrative Risk Management System in Operational Divisions and Sales Branches, etc.

provides the same functions as in the case of establishing an independent division commensurate with the scale and nature of the institution and its risk profile.

¹ When the Administrative Risk Management Division is not established as an independent division (e.g., when the division is consolidated with another risk management division to form a single division or when a division in charge of other business also takes charge of administrative risk management or when a Manager or Managers take charge of administrative risk management instead of a division or a department), the inspector shall review whether or not such a system is sufficiently reasonable and

² When a department or a post other than the Board of Directors or equivalent organization to the Board of Directors is empowered to allocate staff and assign them authority, the inspector shall review, in light of the nature of such a department or post, whether or not the structure of the Administrative Risk Management Division is reasonable in terms of a check-and-balance system and other aspects.

- (i) Does the Board of Directors or equivalent organization to the Board of Directors provide a system to fully disseminate the relevant internal rules and operational procedures to operational divisions and sales branches, etc. and have such divisions and branches observe them? For example, does the Board of Directors or equivalent organization to the Board of Directors instruct the Manager to identify the internal rules and operational procedures that should be observed by operational divisions and sales branches and to carry out specific measures for ensuring observance such as providing effective training on a regular basis?
- (ii) Does the Board of Directors or equivalent organization to the Board of Directors provide a system to ensure the effectiveness of administrative risk management in operational divisions and sales branches, etc. through the Manager or the Administrative Risk Management Division?

(4) System for Reporting to Board of Directors or equivalent organization to Board of Directors and Approval

Has the Board of Directors or equivalent organization to the Board of Directors appropriately specified matters that require reporting and those that require approval and does it have the Manager report the current status to the Board of Directors or equivalent organization to the Board of Directors and the Comprehensive Operational Risk Management Division in a regular and timely manner or on an as needed basis or have the Manager seek the approval on the relevant matters? In particular, does it ensure that the Manager reports to the Board of Directors or equivalent organization to the Board of Directors and the Comprehensive Operational Risk Management Division without delay any matters that would seriously affect corporate management or significantly undermine customer interests?

(5) System for Reporting to Corporate Auditor

In the case where the Board of Directors has specified matters to be directly reported to a corporate auditor, has it specified such matters appropriately and do they provide a system to have the Manager directly report such matters to the auditor?³

(6) Development of Internal Audit Guidelines and Internal Audit Plan

Does the Board of Directors or equivalent organization to the Board of Directors have the Internal Audit Division appropriately identify the matters to be audited with regard to administrative risk management, develop guidelines that specify the matters subject to internal audit and the audit procedure (hereinafter referred to as "Internal Audit Guidelines") and an internal audit plan, and

³ It should be noted that this shall not preclude a corporate auditor from voluntarily seeking a report and shall not restrict the authority and activities of the auditor in any way.

approve such guidelines and plan?⁴ For example, does it have the following matters clearly specified in the Internal Audit Guidelines or the internal audit plan and provide a system to have these matters appropriately audited?

- Status of development of the administrative risk management system
- Status of observance of the Administrative Risk Management Policy, Administrative Risk Management Rules, etc.
- Appropriateness of the administrative risk management processes commensurate with the scale and nature of the business, and the risk profile
- Status of improvement of matters pointed out in an internal audit or on the occasion of the last inspection

(7) Revision of the Development Process of Internal Rules and Organizational Frameworks

Does the Board of Directors or equivalent organization to the Board of Directors revise the development process of internal rules and organizational frameworks in a timely manner by reviewing its effectiveness based on reports and findings on the status of administrative risk management in a regular and timely manner or on an as needed basis?

3. Assessment and Improvement Activities

1) Analysis and Assessment

(1) Analysis and Assessment of Administrative Risk Management

Does the Board of Directors or equivalent organization to the Board of Directors appropriately determine whether there are any weaknesses or problems in the administrative risk management system and the particulars thereof, and appropriately examine their causes by precisely analyzing the status of administrative risk management and assessing the effectiveness of administrative risk management, based on all information available regarding the status of administrative risk management, such as the results of audits by corporate auditors, internal audits and external audits, findings of various investigations and reports from various divisions? In addition, if necessary, does it take all possible measures to find the causes by, for example, establishing fact findings committees, etc. consisting of non-interested persons?

(2) Revision of the Analysis and Assessment Processes

Does the Board of Directors or equivalent organization to the Board of Directors revise the analysis and assessment processes in a timely manner by reviewing their effectiveness based on reports and findings on the status of administrative risk management in a regular and timely manner

⁴ The Board of Directors or equivalent organization to the Board of Directors only needs to have approved the basic matters with regard to an internal audit plan.

or on an as needed basis?

2) Improvement Activities

(1) Implementation of Improvements

Does the Board of Directors or equivalent organization to the Board of Directors provide a system to implement improvements in the areas of the problems and weaknesses in the administrative risk management system identified through the analysis, assessment and examination referred to in 3. 1) above in a timely and appropriate manner based on the results obtained by developing and implementing an improvement plan as required or by other appropriate methods?

(2) Progress Status of Improvement Activities

Does the Board of Directors or equivalent organization to the Board of Directors provide a system to follow up on the efforts for improvement in a timely and appropriate manner by reviewing the progress status in a regular and timely manner or on an as needed basis?

(3) Revision of the Improvement Process

Does the Board of Directors or equivalent organization to the Board of Directors revise the improvement process in a timely manner by reviewing effectiveness based on reports and findings on the status of administrative risk management in a regular and timely manner or on an as needed basis?

II. Development and Establishment of Administrative Risk Management System By Manager

[Checkpoints]

- This chapter lists the check items to be used when the inspector reviews the roles and responsibilities to be performed by the Manager and the Administrative Risk Management Division.
- If any problem is recognized as a result of reviews conducted with the use of the check items listed in Chapter II., it is necessary to exhaustively examine which of the elements listed in Chapter I. are absent or insufficient, thus causing the said problem, and review findings thereof through dialogue between the inspector and the financial institution.
- If the institution's management fails to recognize problems recognized by the inspector, it is also necessary to strictly explore in particular the possibility that the systems and processes listed in Chapter I. are not functioning appropriately and review findings thereof through dialogue.
- The inspector should review the status of improvements with regard to the issues pointed out on the occasion of the last inspection that are not minor and determine whether or not effective improvement measures have been developed and implemented.

1. Roles and Responsibilities of Manager

(1) Development and Dissemination of Administrative Risk Management Rules

Has the Manager, in accordance with the Administrative Risk Management Policy, identified the risks, decided the methods of assessment and monitoring thereof and developed the Administrative Risk Management Rules that clearly define the arrangements on risk control and mitigation, based on full understanding of the scope, types and nature of risks and the administrative risk management technique?

Have the Administrative Risk Management Rules been disseminated throughout the institution upon approval by the Board of Directors or equivalent organization to the Board of Directors after confirmation by the Comprehensive Operational Management Division?

(2) Administrative Risk Management Rules

Do the Administrative Risk Management Rules exhaustively cover the arrangements necessary for the Administrative Risk management and specify the arrangements appropriately in a manner befitting the scale and nature of the financial institution's business, and its risk profile? Do

the rules specify the following items, for example?

- Arrangements on the roles, responsibilities and the organizational framework of the Administrative Risk Management Division
- Arrangements on the identification of risks to be subjected to the administrative risk management
- Arrangements on the method of the administrative risk assessment
- Arrangements on the method of risk monitoring
- Arrangements on reporting to the Board of Directors or equivalent organization to the Board of Directors and the Comprehensive Operational Risk Management Division.

(3) Development of Organizational Frameworks by Manager

- (i) Does the Manager, in accordance with the Administrative Risk Management Policy and the Administrative Risk Management Rules, provide for measures to have the Administrative Risk Management Division exercise a check-and-balance system in order to conduct administrative risk management system appropriately?
- (ii) Does the Manager ensure the system of training and education to enhance the ability of employees to conduct administrative risk management in an effective manner, thus developing human resources with relevant expertise?
- (iii) Does the Manager provide a system to ensure that matters specified by the Board of Directors or equivalent organization to the Board of Directors are reported to the Board of Directors or equivalent organization to the Board of Directors and the Comprehensive Operational Risk Management Division in a regular and timely manner or on an as needed basis? In particular, does the Manager provide a system to ensure that matters that would seriously affect corporate management are reported to the Board of Directors or equivalent organization to the Board of Directors and the Comprehensive Operational Risk Management Division without delay?
- (iv) Does the Manager provide arrangements, in coordination with a person in charge of personnel management, etc., to ensure that employees (including Managers) stay away from the workplace for one full week on end at least once per year for purposes such as holidays, training or provisional internal transfer from the viewpoint of preventing inappropriate incidents? Does the Manager oversee such arrangements and ensure the implementation of the relevant measures?
- (v) Does the Manager, in coordination with a person in charge of personnel management, etc., ensure that personnel rotations are conducted appropriately so as to prevent a certain employee from engaging in the same business at the same department for a long period of time from the viewpoint of preventing inappropriate incidents? In the case where an employee must engage in the same business at the same department for a long period of time for an unavoidable reason, are there other arrangements to ensure the prevention of inappropriate incidents? Does the Manager

oversee such arrangements and ensure the implementation of the relevant measures?

- (vi) With regard to contract workers, etc., does the Manager oversee personnel management with due consideration for the following points from the viewpoint of preventing inappropriate incidents?
 - Is the scope of business that can be undertaken by contract workers, etc. clearly defined?
 - Is there a system to ensure that personnel and labor management (including the provision of training) is conducted in light of the nature of contract workers, etc. such as a lack of personnel information concerning them compared with regular employees and the fact that a check-and-balance system functions against such workers on a daily basis?

(4) Revision of Administrative Risk Management Rules and Organizational Frameworks

Does the Manager conduct monitoring on an ongoing basis with regard to the status of the execution of operations at the Administrative Risk Management Division? Does the Manager review the effectiveness of the administrative risk management system in a regular and timely manner or on an as needed basis, and, as necessary, revise the Administrative Risk Management Rules and the relevant organizational frameworks or present the Board of Directors or equivalent organization to the Board of Directors with proposals for improvement?

2. Roles and Responsibilities of Administrative Risk Management Division⁵

1) Roles and Responsibilities of Administrative Supervisory Division

(i) Does the Administrative Supervisory Division have administrative rules in place? Are the administrative rules comprehensive, appropriately specified in accordance with Laws (including but not limited to laws and regulations, etc.) and suited to the scale and nature of the financial institution's business, and its risk profile? Do the rules stipulate matters concerning administrative work not only at sales branches, etc. but also at operational divisions?

Do the administrative rules stipulate the following items clearly and exhaustively?

- Procedures for handling of cases not covered by the administrative rules and cases where there are differences of interpretation concerning the administrative rules.
- Procedures concerning exceptional cases such as handling of cash, physical certificates, and important documents
- (ii) Does the Administrative Supervisory Division, in coordination with other relevant risk management divisions, etc. provide a system to analyze the causes of problems detected as a result

⁵ It should be noted that the purpose of this inspection item is not to review whether or not divisions such as the Administrative Supervisory Division and the administrative guidance division have been established as administrative risk management divisions but to review whether or not the functions required for such divisions are being performed.

of auditing, inappropriate incidents, accidents related to operational processes, complaints and inquiries, etc. and consider measures to prevent the recurrence thereof? Does the division revise and improve the administrative rules as necessary?

- (iii) Does the Administrative Supervisory Division revise and improve the administrative rules as necessary according to changes in external environments such as legal amendments?
- (iv) Does the Administrative Supervisory Division provide for measures to consistently check the administrative risk management system at operational divisions and sales branches, etc.?
- (v) Does the Administrative Supervisory Division provide a system to prevent the Managers of operational divisions and the heads of sales branches from concealing violation of Laws?
- (vi) Has the Administrative Supervisory Division developed standards and guidelines for implementing self-inspections by operational divisions and sales branches, etc. based on the opinions of the Internal Audit Division?
- (vii) Does the Administrative Supervisory Division receive reports on the results of self-inspections by operational divisions and sales branches, etc.? Does it review the effectiveness of the self-inspections?

2) Roles and Responsibilities of Administrative Guidance Division

- (i) Does the Administrative Guidance Division provide guidance and training to ensure appropriate administrative processes at operational divisions and sales branches, etc.?
- (ii) Does the Administrative Guidance Division utilize the results of auditing by the Internal Audit Division to enhance the level of administrative work at operational divisions and sales branches, etc.?
- (iii) Does the Administrative Guidance Division promptly and accurately respond to inquiries from operational divisions and sales branches, etc.?

III. Specific Issues

[Checkpoints]

- This chapter lists the check items to be used when the inspector reviews specific issues particular to the actual status of administrative risk management.
- If any problem is recognized as a result of reviews conducted with the use of the check items listed in Chapter III., it is necessary to exhaustively examine which of the elements listed in Chapter I. and II are absent or insufficient, thus causing the said problem, and review findings thereof through dialogue between the inspector and the financial institution.
- If the institution's management fails to recognize problems recognized by the inspector, it is also necessary to strictly explore in particular the possibility that the systems and processes listed in Chapter I. are not functioning appropriately and review findings thereof through dialogue.
- The inspector should review the status of improvements with regard to the issues pointed out on the occasion of the last inspection that are not minor and determine whether or not effective improvement measures have been developed and implemented.

1. Administrative Process System at Operational Divisions and Sales Branches, etc.

1) Roles of Operational Division and Sales Branch Managers

Do the Managers of operational divisions and sales branches, etc.

- (i) maintain a constant grasp of administrative risks related to administrative processes?
- (ii) check the status of administrative processes and compliance with the administrative rules and items involving various risks?
- (iii) endeavor to prevent situations in which persons in charge of examining administrative processes and giving approval thereof fail to perform their proper functions because of excessive workloads?
- (iv) have a grasp on problems related to administrative processes at the operational divisions or sales branches of which they are in charge and make improvements?
- (v) strictly handle exceptional cases in particular?
- (vi) handle cases not covered by the administrative rules in a responsible manner in coordination with the Administrative Supervisory Division and the relevant operational divisions?

2) Strict Administrative Management

- (i) Are administrative processes conducted strictly?
- (ii) Is it ensured that examination and approval procedures are implemented strictly, rather than conducted formally or perfunctorily?
- (iii) When accidents or inappropriate incidents involving cash occur, are they immediately communicated to the Managers of the Operational Division or sales branch and also reported to the Administrative Supervisory Division and the Internal Audit Division, etc.?
- (iv) Are exceptional cases always processed upon approval from the Operational Division Managers, sales branch Managers or Managers in charge of relevant business, etc.?
- (v) When operational divisions or sales branches handle cases not covered by the administrative rules, are such cases always processed based on the instructions from the operational division or sales branch Manager in coordination with the Administrative Supervisory Division and other relevant operational divisions?

(3) Appropriateness of Self-Inspection

- (i) Are effective self-inspections conducted in a regular and timely manner or on an as needed basis by operational divisions and sales branches, etc. in accordance with the standards and guidelines for implementing such inspections in order to prevent accidents, inappropriate incidents and violation of Laws and avoid the spread of damage to customers?
- (ii) Are the results of self-inspection reported in a regular and timely manner or on an as needed basis by the relevant operational divisions and sales branches to the Administrative Supervisory Division and the Internal Audit Division?
- (iii) Are the results of self-inspection utilized to improve administrative work at operational divisions and sales branches?

2. Administrative Management System Concerning Market Transactions

1) Strict Administrative Processes

Are foreign exchange, fund, securities transactions and derivatives thereof handled strictly in accordance with the internal rules and operational procedures concerning the market transactions as follows, for example?

- (i) Does the Administrative Management Division of Market-Trading have an exhaustive grasp on all transactions (e.g. final confirmation of system input, confirmation with ticket stamping and serial numbers, etc.)
- (ii) Are transaction details input without delay?
- (iii) Are corrections of dealing ticket errors detected in the confirmation and adjustment stages

approved by the Manager of the Administrative Management Division of Market-Trading?

- (iv) Are dealing tickets marked as pending for future processing stored and recorded appropriately?
- (v) Is confirmation transmitted by someone other than the person responsible for the transaction?
- (vi) Are confirmations and dealing tickets checked against each other appropriately?
- (vii) Are dealing tickets, dealing sheets and confirmations kept and stored appropriately?
- (viii) Is documentary evidence such as transaction data held at the Office (Trading, Banking) division and the Administrative Management Division of Market-Trading subjected to checks by the Internal Audit Division and stored for a period specified by the internal rules and operational procedures, etc. (minimum of one year)?

2) Check of Transaction Details and Balance, etc.

Are transaction data from the Office (Trading, Banking) Division and the Administrative Management Division of Market-Trading cross-checked? When errors are detected, are the causes examined promptly and supplementary measures taken in accordance with the prescribed methods?

For example, in securities trading, does the institution regularly (at least once per month) check positions as shown in the dealing system of the Office (Trading, Banking) Division against the securities balances on the accounts of the Back-Office Division that have been confirmed with securities companies and the Custody Division, etc.?

3. Checklist for Field Inspection

- 1) This checklist provides examples of items to be checked when the inspector conducts field inspections on the status of administrative risk management of financial institutions, and it does not exhaustively cover all business of financial institutions.
- 2) In conducting field inspections on a financial institution, the inspector should not necessarily examine all of the items listed in this checklist if it has been confirmed that the Internal Audit Division of the institution is functioning effectively, because checks on the actual status of administrative processes are conducted by the division. On the other hand, if the Internal Audit Division is not functioning effectively, it is necessary to conduct more in-depth inspections with regard to items not listed in this checklist as well.
- 3) When the institution inspected has only recently begun to engage in new business and handle new products, checks should be conducted thereon even if those business and products are not covered by this checklist.
- 4) It should be noted that the purpose of this checklist is not pointing out minor administrative mistakes but reviewing the functioning of the risk management system.

Items	Details
1. Internal	Is attention paid to the following matters, for example, in handling of internal
Operations	operations?
	1) Management of cash and physical certificates etc.
	(1) Balance management by executive personnel
	(2) Communication of incidents involving cash
	2) Transactions treated as exceptional cases
	(1) Details of criteria for handling of exceptional cases
	(2) Causes of exceptional cases and records thereof
	(3) Approval of branch Managers or other executives and a follow-up review
	(4) Appropriateness of supplementary processing of exceptional cases
	(5) Incidents such as high frequency of exceptional cases
	3) Transactions using executive keys
	(1) Checks for base-date transactions and other unusual transactions
	(2) Selection of important transactions requiring executive keys
	4) Status of overdrafts
	(1) Determination of customers allowed overdrafts, such as customers for whom
	there is no settlement concern
	(2) Prior approval of transactions that involve financial burdens

- 5) Handling of documents and passbooks, etc.
- 6) Collection of fees, payment of costs
- 7) Handling of loss of certificates, passbooks, cards, etc. (status of setting of codes)
- 8) Management of general transfers and transfers prior to liquidation
- 9) Management of objects held in custody at branches
- 10) Management of CD cards
- 11) Handling of bills and checks, domestic exchange/transfer, foreign exchange
- 12) Items related to terrorism financing and money laundering
- (1) Customer Identity verification, compilation and storage of records on Customer Identity verification, storage of transaction records
- (2) Notification by financial institutions, etc. to the authorities with regard to suspicious transactions (Article 54, Law for Punishment of Organized Crimes, Control of Crime Proceeds and other matters)
- (3) Concealment and receipts of criminal profits (Articles 10 and 11, Law for Punishment of Organized Crimes, Control of Crime Proceeds and other matters)
- 13) Status of management and adjustment of pending cases
- 14) Personnel management of employees

2. OutsideLiaison

Is attention paid to the following matters, for example, in handling of outside liaison work?

Work

- (1) Allocations of roles and job rotation for outside liaison personnel
- (2) Complaints and inquiries from customers
- (3) Delivered funds and transfer requests made via telephone
- (4) Issuance and collection of receipts
- (5) Handling of physical certificates etc. between the outside liaison division and internal administrative divisions
- (6) Long-term custody of cash, passbooks, and ledgers, etc.
- (7) Prevention of incidents at customers using cash collection service
- (8) Outside payments

3. Deposit Business

Is attention paid to the following matters, for example, in handling of deposit business?

- 1) Provision of information to depositors
- (1) Display of major deposit interest rates at branches
- (2) Fee lists for perusal in branches
- (3) Indication of deposit products covered by deposit insurance

- (4) Provision of information regarding details of the entire product lineup
- (5) Appropriate provision of information concerning interest rates used as a basis for setting floating deposit rates and the methods of setting fixed deposit rates when there are such interest rates and methods
- 2) Cooperative deposits, "Buzumi-Ryodate" deposits
- (1) Prevention of excessive cooperative deposits, excessive "Buzumi-Ryodate" deposits, "Buzumi" deposits, and excessive "Ryodate deposits.
- (2) Measures to prevent deposit solicitation campaigns from becoming excessive
- (3) Due consideration for business plans that emphasize term-end figures
- 3) "Betsudan" deposits and provisional receipts and payments
- 4) Handling of products without principal guarantee
- 5) Illegal practices such as the provision of loans tied to deposits

4. Lending Business

Is attention paid to the following matters, for example, in handling of lending business?

- 1) Identity verification (confirmation of the intentions of the borrower, guarantor, and provider of collateral, etc.)
- 2) Appraisal and management of collateral property
- (1) Appropriateness of objective appraisals made by real estate appraisers or made with the use of standard values etc. and self appraisal by branches
- (2) Recording of data concerning collateral property and guarantee certificates, etc. on collateral ledgers, management ledgers, and the like
- (3) Provision and renewal of fire insurance
- (4) Collateral value and probability of recovering loans via collateral
- (5) Confirmation of intentions of joint guaranters (guarantee confirmation)
- 3) Loans for insurance premium payment
- 4) Management of progress with regard to loan applications
- 5) Status of handling of rejected applications
- 6) Credit management of large-lot borrowers and loss-making borrowers
- 7) Management of late repayments
- 8) Exclusive jurisdiction of branch Managers

5. SecuritiesBusiness

Is attention paid to the following matters, for example, in handling of securities business?

1) Over-the-counter bond sales

- (1) Securing of business operations pertaining to prohibited acts such as providing false indications with regard to transactions, promoting large-volume sales of specific securities held by the institution, and acts involving the use of credit provision.
- (2) Development of internal rules and operational procedures that are in accordance with laws and rules such as the Securities and Exchange Law and rules set by the Japan Securities Dealers Association and the like
- (3) Full dissemination to all employees
- 2) Investment trust sales
- (1) Appointment of internal control supervisory Managers, sales Managers, internal control Managers, etc.
- (2) Securing of business operations pertaining to prohibited acts such as solicitation of investment with positive judgment statements, discretionary account trading, loss compensation, provision of additional profits, etc., based on the principles of "self responsibility" and "suitability".
- (3) Development of internal rules and operational procedures that are in accordance with laws and rules such as the Securities and Exchange Law, the Law concerning Investment Trusts and Investment Corporations and rules set by the Japan Securities Dealers Association and the like.
- (4) Appropriate and sufficient explanation to customers of the risk of principal loss
- (5) Establishment of a space dedicated to direct sales and redemptions, etc. of investment trusts that is separated from spaces for other services (This shall apply to institutions lending spaces for investment trust sales)
- (6) Full dissemination to all employees

6. Insurance Business

Is attention paid to the following matters, for example, in handling of insurance business?

- 1) Establishment of the system of allocation of responsibilities such as the appointment of Managers in charge, etc.
- 2) Development of internal rules and operational procedures in accordance with the Insurance Business Law, etc.
- 3) Full dissemination to all employees
- 4) Securing of appropriate operations
 - (1) Full implementation of measures to prevent inappropriate practices such as taking advantage of a superior position to offer insurance products
 - (2) Provision of appropriate and sufficient explanation of risks, etc. involved

in insurance products to customers

7. Other Business

Is attention paid to the following matters, for example, in handling of other business?

- 1) Derivatives products
- (1) Qualifications and product knowledge of persons selling derivatives products
- (2) Appropriate and sufficient explanation to customers with regard to the fact that derivative products involve the risk of principal loss, etc.
- (3) Status of sending and storing of market price reports
- 2) Commodities funds
- (1) Securing of business operations pertaining to the protection of investors, including those concerning the prohibition of practices such as lending names, lending money and mediating loans, and inappropriate solicitation.
- (2) Appropriate and sufficient explanation to customers with regard to the fact that derivative products involve the risk of principal loss, etc.
- (3) Full dissemination to all employees
- 3) Mortgage securities
- (1) Securing of business operations functions pertaining to rules intended to protect purchasers, including those concerning the prohibition of lending names and inappropriate solicitation
- (2) Appropriate and sufficient explanation to customers with regard to the details of products, including explanation of whether the contract guarantees the principal
- (3) Full dissemination to all employees
- 4) Loan cash receipts and disbursements trusts
- (1) Solicitation suited to the knowledge and experience of the customer
- (2) Appropriate and sufficient explanations to customers
- (3) Full dissemination to all employees
- 5) Small-lot credit sales
- 6) Liquidation of credits from local public bodies etc.
- 7) Liquidation of general loan credits
- 8) Loan participation
- 9) Foreign exchange
- 10) Money exchange

(Attachment 2)

I. Development and Establishment of Information Technology Risk Management System by Management

[Checkpoints]

- Information technology risk is the risk that a financial institution will incur loss because of a breakdown or malfunctioning of computer systems or other computer system inadequacies, or because of improper use of computer systems.
- The development and establishment of a system for information technology risk management is extremely important from the viewpoint of ensuring the soundness and appropriateness of a financial institution's business. Therefore, the institution's management is charged with and responsible for taking the initiative in developing and establishing such a system.
- The inspector should determine whether the information technology risk management system is functioning effectively and whether the roles and responsibilities of the institution's management are being appropriately performed by way of reviewing, with the use of check items listed in Chapter I., whether the management is appropriately implementing (1) policy development, (2) development of internal rules and organizational frameworks and (3) development of a system for assessment and improvement activities.
- If any problem is recognized as a result of reviews conducted with the use of the check items listed in Chapter II. and later, it is necessary to exhaustively examine which of the elements listed in Chapter I. are absent or insufficient, thus causing the said problem, and review findings thereof through dialogue between the inspector and the financial institution.
- If any problem is detected in the information technology risk management system and it is necessary to conduct more in-depth, detailed reviews, the inspector should refer to "Safety Standards for the Computer Systems of Financial Institutions," "the accompanying explanatory materials of Safety Standards for the Computer Systems of Financial Institutions" (edited by the Center For Financial Industry Information System), etc.
- The inspector should also use this checklist to examine the risk that information held by the institution that must be protected will be altered, deleted or leaked to the outside by officers and employees of the institution or outsiders.

- If the institution's management fails to recognize weaknesses or problems recognized by the inspector, it is also necessary to explore in particular the possibility that the Internal Control System is not functioning effectively and review findings thereof through dialogue.
- The inspector should review the status of improvements with regard to the issues pointed out on the occasion of the last inspection that are not minor and determine whether or not effective improvement measures have been developed and implemented.
- The inspector should pay sufficient attention to the level of importance and nature of individual computer systems in conducting inspection of Information Technology Risk Management.
 - The level of importance of computer systems refers to the scale of effects of the systems on customer transactions and corporate management decisions.
 - The nature of computer systems refers to specific features of centralized dataprocessing environment systems, decentralized systems such as client/server computer systems configurations, End-user systems and the like, and the suitable management technique differs according to the system type.

1. Policy Development

(1) Roles and Responsibilities of Directors

Do directors attach importance to information technology risk management, fully recognizing that the lack of such an approach could seriously hinder the attainment of strategic objectives? In particular, does the director in charge of information technology risk management examine the policy and specific measures for developing and establishing an adequate information technology risk management system with a full understanding of the scope, types and nature of risks, and the techniques of risk identification, assessment, monitoring and control regarding information technology risk, as well as the importance of information technology risk management, and with precise recognition of the current status of information technology risk management within the financial institution based on such understanding?

(2) Clarification of Strategic Objectives

Does the Board of Directors, in light of information technology innovation, treat an information technology strategy as part of the strategic objectives that are in accordance with the

financial institution's corporate management policy? Does it clearly specify the following items in the information technology strategy, for example?

- Priorities concerning computer system development
- Programs to promote efficient use of information
- Computer system investment plans

(3) Development and Dissemination of Information Technology Risk Management Policy

Has the Board of Directors established a policy regarding information technology risk management (hereinafter referred to as the "Information Technology Risk Management Policy") and disseminated it throughout the institution? Is the appropriateness of the Information Technology Risk Management Policy being secured by way of, for example, including clear statements on the following matters?

- The roles and responsibilities of the director in charge and the Board of Directors or equivalent organization to the Board of Directors with regard to information technology risk management
- The policy on organizational framework, such as establishment of a division concerning information technology risk management (hereinafter referred to as the "Information Technology Risk Management Division") and the authority assigned thereto
- The policy regarding identification, assessment, monitoring, control and mitigation of information technology risks
- The security policy (basic policy concerning the proper protection of the institution's information assets that stipulates (1) information assets to be protected, (2) reasons for protection and (3) the locus of responsibility for protection, etc.)¹

(4) Revision of the Policy Development Process

Does the Board of Directors revise the policy development process in a timely manner by reviewing its effectiveness based on reports and findings on the status of information technology risk management in a regular and timely manner or on an as needed basis?

2. Development of Internal Rules and Organizational Frameworks

¹ - "Security policy" covers not only information stored in computer systems and recording media but also information printed on paper.

⁻ Refer to "Handbook for Security Policy Development in Financial Institutions" (edited by the Center For Financial Industry Information System)

(1) Development of Internal Rules

Has the Board of Directors or equivalent organization to the Board of Directors had the Manager of the Information Technology Risk Management Division (hereinafter simply referred to as the "Manager" in this checklist) develop internal rules that clearly specify the arrangements concerning information technology risk management (hereinafter referred to as the "Information Technology Risk Management Rules") and disseminated them throughout the institution in accordance with the Information Technology Risk Management Policy? Has the Board of Directors or equivalent organization to the Board of Directors approved the Information Technology Risk Management Rules after determining if they comply with the Information Technology Risk Management Policy after legal checks, etc.?

(2) Establishment of System of Information Technology Risk Management Division

- (i) Does the Board of Directors or equivalent organization to the Board of Directors have the Information Technology Risk Management Division established and have the division prepared to undertake appropriate roles in accordance with the Information Technology Risk Management Policy and the Information Technology Risk Management Rules?²
- (ii) Has the Board of Directors allocated to the Information Technology Risk Management Division a Manager with the necessary knowledge and experience to supervise the division and enabled the Manager to implement management operations by assigning him/her the necessary authority therefor?
- (iii) Has the Board of Directors or equivalent organization to the Board of Directors allocated to the Information Technology Risk Management Division an adequate number of staff members with the necessary knowledge and experience to execute the relevant operations and assigned such staff the authority necessary for implementing the operations?³
- (iv) Does the Board of Directors or equivalent organization to the Board of Directors secure a check-and-balance system of the Information Technology Risk Management Division against operational divisions?

² When the Information Technology Risk Management Division is not established as an independent division (e.g., when the division is consolidated with another risk management division to form a single division or when a division in charge of other business also takes charge of information technology risk management or when a Manager or Managers take charge of information technology risk management instead of a division or a department), the inspector shall review whether or not such a system is sufficiently reasonable and provides the same functions as in the case of establishing an independent division commensurate with the scale and nature of the institution and its risk profile.

³ When a department or a post other than the Board of Directors or equivalent organization to the Board of Directors is empowered to allocate staff and assign them authority, the inspector shall review, in light of the nature of such a department or post, whether or not the structure of the Information Technology Risk Management Division is reasonable in terms of a check-and-balance system and other aspects.

(3) Development of Information Technology Risk Management System in Operational Divisions, Sales Branches, etc.

- (i) Does the Board of Directors or equivalent organization to the Board of Directors provide a system to fully disseminate the relevant internal rules and operational procedures to operational divisions, sales branches, etc. and have such divisions and branches observe them? For example, does the Board of Directors or equivalent organization to the Board of Directors instruct the Manager to identify the internal rules and operational procedures that should be observed by operational divisions, sales branches, etc. and to carry out specific measures for ensuring observance such as providing effective training on a regular basis?
- (ii) Does the Board of Directors or equivalent organization to the Board of Directors provide a system to ensure the effectiveness of information technology risk management in operational divisions, sales branches, etc. through the Manager or the Information Technology Division?

(4) System for Reporting to Board of Directors or equivalent organization to Board of Directors and Approval

Does the Board of Directors or equivalent organization to the Board of Directors appropriately specify matters that require reporting and those that require approval and have the Manager report the current status to the Board of Directors or equivalent organization to the Board of Directors and the Comprehensive Operational Risk Management Division in a regular and timely manner or on an as needed basis or have the Manager seek the approval on the relevant matters? In particular, does it ensure that the Manager reports to the Board of Directors or equivalent organization to the Board of Directors and the Comprehensive Operational Risk Management Division without delay any matters that would seriously affect corporate management or significantly undermine customer interests?

(5) System for Reporting to Corporate Auditor

In the case where the Board of Directors has specified matters to be directly reported to a corporate auditor, has it specified such matters appropriately and do they provide a system to have the Manager directly report such matters to the auditor?⁴

(6) Development of Internal Audit Guidelines and an Internal Audit Plan

Does the Board of Directors or equivalent organization to the Board of Directors have the Internal Audit Division appropriately identify the matters to be audited with regard to information technology risk management, develop guidelines that specify the matters subject to internal audit and

⁴ It should be noted that this shall not preclude a corporate auditor from voluntarily seeking a report and shall not restrict the authority and activities of the auditor in any way.

the audit procedure (hereinafter referred to as "Internal Audit Guidelines") and an internal audit plan, and approve such guidelines and plan? ⁵For example, does it have the following matters clearly specified in the Internal Audit Guidelines or the internal audit plan and provide a system to have these matters appropriately audited?

- Status of development of the information technology risk management system
- Status of observance of the Information Technology Risk Management Policy, the Information Technology Risk Management Rules, etc.
- Appropriateness of the information technology risk management processes commensurate with the scale and nature of the business and risk profile
- Status of improvement of matters pointed out in an internal audit or on the occasion of the last inspection

(7) Revision of the Development Process of Internal Rules and Organizational Frameworks

Does the Board of Directors or equivalent organization to the Board of Directors revise the development process of internal rules and organizational frameworks in a timely manner by reviewing its effectiveness based on reports and findings on the status of information technology risk management in a regular and timely manner or on an as needed basis?

3. Assessment and Improvement Activities

1) Analysis and Assessment

(1) Analysis and Assessment of Information Technology Risk Management

Does the Board of Directors or equivalent organization to the Board of Directors appropriately determine whether there are any weaknesses or problems in the information technology risk management system and the particulars thereof, and appropriately examine their causes by precisely analyzing the status of information technology risk management and assessing the effectiveness of information technology risk management, based on all information available regarding the status of information technology risk management, such as the results of audits by corporate auditors, internal audits and external audits, findings of various investigations and reports from various divisions? In addition, if necessary, does it take all possible measures to find the causes by, for example, establishing fact findings committees etc. consisting of non-interested persons?

(2) Revision of the Analysis and Assessment Processes

⁵ The Board of Directors or equivalent organization to the Board of Directors only needs to have approved the basic matters with regard to an internal audit plan.

Does the Board of Directors or equivalent organization to the Board of Directors revise the analysis and assessment processes in a timely manner by reviewing their effectiveness based on reports and findings on the status of information technology risk management in a regular and timely manner or on an as needed basis?

2) Improvement Activities

(1) Implementation of Improvements

Does the Board of Directors or equivalent organization to the Board of Directors provide a system to implement improvements in the areas of the problems and weaknesses in the information technology risk management system identified through the analysis, assessment and examination referred to in 3. 1) above in a timely and appropriate manner based on the results obtained by developing and implementing an improvement plan as required or by other appropriate methods?

(2) Progress Status of Improvement Activities

Does the Board of Directors or equivalent organization to the Board of Directors provide a system to follow up on the efforts for improvement in a timely and appropriate manner by reviewing the progress status in a regular and timely manner or on an as needed basis?

(3) Revision of the Improvement Process

Does the Board of Directors or equivalent organization to the Board of Directors revise the improvement process in a timely manner by reviewing its effectiveness based on reports and findings on the status of information technology risk management in a regular and timely manner or on an as needed basis?

II. Development and Establishment of Information Technology Risk Management System by

Manager

[Checkpoints]

- This chapter lists the check items to be used when the inspector reviews the roles and responsibilities to be performed by the Manager and the Information Technology Risk Management Division.
- If any problem is recognized as a result of reviews conducted with the use of the check items listed in Chapter II., it is necessary to exhaustively examine which of the elements listed in Chapter I. are absent or insufficient, thus causing the said problem, and review findings thereof through dialogue between the inspector and the financial institution.
- If the institution's management fails to recognize problems recognized by the inspector, it is also necessary to strictly explore in particular the possibility that the systems and processes listed in Chapter I. are not functioning appropriately and review findings thereof through dialogue.
- The inspector should review the status of improvements with regard to the issues pointed out on the occasion of the last inspection that are not minor and determine whether or not effective improvement measures have been developed and implemented.

1. Roles and Responsibilities of Manager

(1) Development and Dissemination of Information Technology Risk Management Rules

Has the Manager, in accordance with the Information Technology Risk Management Policy, identified the risks, decided the methods of assessment and monitoring thereof and developed the Information Technology Risk Management Rules that clearly define the arrangements on risk control and mitigation, based on a full understanding of the scope, types and nature of risks and the technique of managing information technology risk? Have the Information Technology Risk Management Rules been disseminated throughout the institution upon approval from the Board of Directors or equivalent organization to the Board of Directors after confirmation by the Comprehensive Operational Risk Management Division?

(2) Information Technology Risk Management Rules

Do the Information Technology Risk Management Rules exhaustively cover the

arrangements necessary for information technology risk management and specify the arrangements appropriately in a manner befitting the scale and nature of the financial institution's business, and its risk profile. Do the rules specify the following items, for example?

- Arrangements on the roles, responsibilities and organizational framework of the Information Technology Risk Management Division
- Arrangements on the identification of risks to be subject to the information technology risk management
- Arrangements on the method of assessing information technology risks
- Arrangements on the method of monitoring information technology risks
- Arrangements on system to report to the Board of Directors or equivalent organization to the Board of Directors and the Comprehensive Operational Risk Management Division

(3) Development of Organizational Frameworks by Manager

- (i) Does the Manager, in accordance with the Information Technology Risk Management Policy and the Information Technology Risk Management Rules, provide for measures to have the Information Technology Risk Management Division exercise a check-and-balance system in order to conduct information technology risk management appropriately?
- (ii) Does the Manager ensure the system of training and education to enhance the ability of employees to conduct information technology risk management in an effective manner, thus developing human resources with relevant expertise?
- (iii) Does the Manager provide a system to ensure that matters specified by the Board of Directors or equivalent organization to the Board of Directors are reported to the Board of Directors or equivalent organization to the Board of Directors and the Comprehensive Operational Risk Management Division in a regular and timely manner or on an as needed basis? In particular, does the Manager provide a system to ensure that matters that would seriously affect corporate management are reported to the Board of Directors or equivalent organization to the Board of Directors and the Comprehensive Operational Risk Management Division without delay?
- (iv) Has the Manager assigned a security Manager responsible for overseeing appropriate management to ensure that security is maintained in accordance with the prescribed policies, standards and procedures and assigned the security Manager the authority necessary for implementing management business?
- (v) Has the Manager, with a view to securing safe and smooth operation of computer systems and the prevention of violation of Laws, specified the procedures for computer system management, assigned a computer system Manager responsible for ensuring appropriate system management and assigned the said Manager the authority necessary for implementing management operations? Has the Manager also assigned system Managers with regard to systems designed,

developed and operated by user divisions on their own, such as an end-user computing (EUC) system? It is desirable that a system Manager be assigned to all systems and operations.

- (vi) Has the Manager assigned a data Manager responsible for securing the confidentiality, completeness and usability of data and assigned the data Manager the authority necessary for implementing management operations?
- (vii) Has the Manager assigned a network Manager responsible for overseeing the status of network operation and controlling and monitoring access and assigned the network Manager the authority necessary for implementing management operations?

(4) Revision of Information Technology Risk Management Rules and Organizational Frameworks

Does the Manager conduct monitoring on an ongoing basis with regard to the status of the execution of operations at the Information Technology Risk Management Division? Does the Manager review the effectiveness of the information technology risk management system in a regular and timely manner or on an as needed basis, and, as necessary, revise the Information Technology Risk Management Rules and the relevant organizational framework or present the Board of Directors or equivalent organization to the Board of Directors with proposals for improvement?

2. Roles and Responsibilities of Information Technology Risk Management Division

1) Awareness and Assessment of Information Technology Risk

- (i) Is the Information Technology Risk Management Division aware of risks common to computer systems in general, and does it conduct assessments thereof, including an assessment of risks involved in various systems for different operational functions, such as the accounting system, information support system, external settlement system, securities system, and international system?
- (ii) Is the Information Technology Risk Management Division aware of risks concerning computer systems developed by user divisions on their own such as an EUC system, and has it assessed the risks?
- (iii) Is the Information Technology Risk Management Division aware that expansion of networks and progress in technology have led to a diversification of and increase in risks and has it made a relevant assessment?
- (iv) Is the Information Technology Risk Management Division aware of risks involved in transactions conducted over the Internet, and does it understand the scope of the risks and assessed the risks? For example, is the division aware of the risk that problems related to the absence of face-to-face contact, troubleshooting, and involvement of third parties, etc. may arise and has it

2) Monitoring of Status of Information Technology Risks

- (i) Does the Information Technology Risk Management Division conduct monitoring with regard to the status of information technology risks of the financial institution with an appropriate frequency in accordance with the Information Technology Risk Management Policy and the Information Technology Risk Management Rules, etc.?
- (ii) Does the Information Technology Risk Management Division, in accordance with the Information Technology Risk Management Policy and the Information Technology Risk Management Rules, etc., provide information necessary for the Board of Directors or equivalent organization to the Board of Directors to make appropriate assessments and decisions with regard to the status of information technology risks in a regular and timely manner or on an as needed basis?

3) Review and Revision

Does the Information Technology Risk Management Division, in accordance with the Information Technology Risk Management Policy and the Information Technology Risk Management Rules, etc., regularly review whether the information technology risk management method is suited to the scale and nature of the financial institution's business, and its risk profile, and revise the method?

III. Specific Issues

[Checkpoints]

- This chapter lists the check items to be used when the inspector reviews specific issues particular to the actual status of information technology risk management.
- If any problem is recognized as a result of reviews conducted with the use of the check items listed in Chapter III., it is necessary to exhaustively examine which of the elements listed in Chapter I. and II. are absent or insufficient, thus causing the said problem, and review findings thereof through dialogue between the inspector and the financial institution.
- If the institution's management fails to recognize problems recognized by the inspector, it is also necessary to strictly explore in particular the possibility that the systems and processes listed in Chapter I. are not functioning appropriately and review findings thereof through dialogue.
- The inspector should review the status of improvements with regard to the issues pointed out on the occasion of the last inspection that are not minor and determine whether or not effective improvement measures have been developed and implemented.

1. Information Security Management

- 1) Roles and Responsibilities of Security Manager, etc.
- (1) Roles and Responsibilities of Security Manager
- (i) Does the security Manager oversee security related to all the following areas: system planning, development, operation and maintenance?
- (ii) Does the security Manager report security problems related to serious system malfunctioning, accidents and crime, etc. to the Information Technology Risk Management Division?
- (iii) Does the security Manager ensure security with regard to the following items, for example?
 - a. Physical security
 - Measures to prevent physical intrusion and crime prevention equipment
 - Enhancement of computer operation environment
 - System for maintenance and inspection of equipment, etc.

b. Logical security

- The check-and-balance between the divisions involved in system development

and operation and within each division

- System for development management
- Measures to prevent electronic intrusion
- Program management
- Response to system problems
- Assessment and management of outside software packages at the time of introduction
- Operational security management, etc.
- (iv) Does the security Manager supervise security matters related to system, data and network management?

(2) Roles and Responsibilities of System Manager

- (i) Does the system Manager regularly inspect computer system assets and make appropriate adjustments by procuring new assets and disposing of unnecessary ones?
- (ii) Does the system Manager conduct appropriate and sufficient management with regard to all facilities and equipment installed at operational divisions, sales branches, etc. and computer centers?
- (iii) Does the system Manager conduct appropriate and sufficient management with regard to computers used outside the premises of the institution?

(3) Roles and Responsibilities of Data Manager

- (i) Does the data Manager ensure safe and smooth management of data by specifying procedures for data management and approval of data use, etc. as part of the internal rules and operational procedures and the like and fully disseminating them to relevant parties?
- (ii) Does the data Manager conduct appropriate and sufficient management to ensure protection of data and prevention of unauthorized use of data?

(4) Roles and Responsibilities of Network Manager

- (i) Does the network Manager ensure appropriate, efficient and safe network operation by specifying procedures for network management and approval of network use, etc. as part of the internal rules and operational procedures and the like and fully disseminating them to relevant parties?
- (ii) Does the network Manager have in place measures to provide a backup in the event of a network breakdown?

2) Prevention of Unauthorized Use

(i) Does the institution have in place a system to verify the authenticity of the user or the computer

terminal connected with the computer system in a manner suited to the nature of the relevant business and the connection method in order to prevent unauthorized use?

- (ii) Does the institution regularly obtain records of system operations as evidence for future audits and regularly check them in order to keep surveillance on the status of unauthorized access?
- (iii) Does the institution specify the methods of establishing and managing the rights to the use of computer terminals and access to data and files in light of the level of importance thereof?

3) Computer Viruses, etc.

Does the institution provide for a system to prevent the intrusion of computer viruses and other unauthorized programs and promptly detect such an intrusion if any and remove the intruding program?

- Infection with computer viruses
- Registry of programs that have not undergone legitimate procedures
- Intentional alteration of legitimate programs

4) Management of Transactions Conducted over Internet

- (i) Does the institution provide a system to accept complaints and consultations from customers?
- (ii) Does the institution have in place a supplementary system in case a system breakdown or malfunctioning makes appropriate processing impossible? Is the allocation of responsibilities in the event of a system breakdown specified?
- (iii) Does the institution provide countermeasures to prevent misrecognition of the service provider that may arise from Web site links, etc.?
- (iv) Does the institution disclose, on its Web site, for example, information concerning details of its financial conditions and business as well as details of the services provided through transactions conducted over the Internet?
- (v) Does the institution verify the customer identification from the viewpoint of preventing money laundering?
- (vi) Does the institution provide a system to prevent leakage of customer information and alteration etc. thereof, etc. attempted by intruding outsiders and insiders using unauthorized access?
- (vii) Does the institution, in light of the fact that transactions conducted over the Internet involve no face-to-face contact, store records on transactions with customers for a certain period of time as necessary without alteration or deletion?
- (viii) Does the institution protect customers against unauthorized use by providing the function of allowing them to check the status of their own use.
- (ix) Does the institution seek to prevent phishing in a manner befitting its business, by, for

example, providing for measures to allow users to verify the authenticity of the Web site accessed?

5) Measures to Cope with Forged or Stolen Cash Cards

- (i) Does the institution assess the security level of the ATM system, etc. according to a prescribed standard in order to prevent use of forged or stolen cash cards? Does the institution take appropriate measures after considering what to do in terms of organizational and technical aspects based on the security level assessment?
- (ii) Does the institution provide for measures to prevent unauthorized withdrawals, such as adopting an appropriate identification technology and installing information systems equipped with the function of preventing information leakage?
- (iii) Does the institution make sure to take appropriate measures when abnormal transactions are detected by establishing criteria for abnormal transactions and specifying how to respond to such transactions?

2. System Planning, Development and Operation, etc.

1) System of Mutual Check and Balance between System Development and Operation Divisions

Does the institution have system development and operation divisions established separately with separate responsibilities in order to prevent personal mistakes and malicious acts? In the case where it is difficult to establish clearly separate divisions for system development and operation due to the lack of a sufficient number of staff members, does the institution seek to introduce a check-and-balance system by rotating persons in charge of system development and operation regularly, for example? With regard to EUC and other systems for which organizational division of system development and operation is difficult, does the institution use the Internal Audit Division, etc. to exercise check and balance?

2) System of System Planning and Development

(1) Planning and Development System

- (i) Does the institution have in place internal rules and operational procedures with regard to system planning and development with a view to introducing highly reliable and efficient systems?
- (ii) Does the institution establish a cross-divisional examination organization, such as computerization committees, and conduct deliberations when engaging in system planning and

development, for example?

- (iii) Does the institution have medium and long-term development plans in place?
- (iv) Does the Board of Directors receive information concerning deliberations on effects of investment in each system as necessary according to the level of the importance of the relevant system? (The Board of Directors should always receive reports concerning deliberations on effects of investment in the system division as a whole.)
- (v) Does the institution have clear rules concerning deliberations and approval with regard to system development projects?
- (vi) Is a revision of a product system implemented upon approval?

(2) Development Management

- (i) Is the method of documentation and programming related to system development standardized?
- (ii) Is a Manager assigned for each development project, and does the Board of Directors or equivalent organization to the Board of Directors check the progress status in light of the level of importance and nature of the relevant system?

(3) Development of Internal Rules and Operational Procedures, etc.

- (i) Has the institution developed internal rules and operational procedures, etc. concerning system design, development and operation and does it revise the rules and operational procedures in a manner befitting its actual operating conditions?
- (ii) Has the institution established standard documentation rules concerning system design plans, and does it compile documents in accordance with the rules?
- (iii) Do the computer systems developed leave auditing trails (journals and other records that allow tracing of the processing history) according to the purpose of the use, etc.?
- (vi) Are manuals and documents related to development compiled in ways that can be easily understood by third parties with relevant expertise?

(4) Tests, etc.

- (i) Is appropriate and sufficient testing conducted according to testing plans?
- (ii) Is a system for testing structured in a way to prevent inadequate tests and reviews that would cause problems with long-lasting effects on customers or serious miscalculations in risk management-related documents and materials that are used for corporate management decisionmaking?
- (iii) Is general testing conducted appropriately, with involvement of user divisions, for example?
- (iv) Is acceptance made by executives and employees with sufficient knowledge?

(5) Decision on System Transition

- (i) Does the institution have a Manager assigned with clear responsibility for system transition?
- (ii) Does the institution develop system transition plans? Has it assigned clear roles and responsibilities to the system development and operation, user divisions, etc.?
- (iii) Does the institution have criteria for judgments with regard to system transition and make decisions based on them?

(6) Post-System Transition Review

- (i) Does the institution conduct a post-system transition review after a certain period from the start of operation?
- (ii) Does the institution conduct examination and assessment with regard to the fulfillment of the user requirements and the cost-effectiveness in the post-system transition review?
- (iii) Are the results of the post-system transition review reflected in future improvement plans for the relevant system?
- (iv) Are the results of the post-system transition review reported to the Managers of the system development division and user divisions, etc?
- (v) Does the institution have user divisions conduct sample checks as necessary after news products and arrangements are introduced?

(7) Human Resource Development

Does the institution provide training in ways to nurture staff adept not only in technology but also in the function skills for which system development is conducted? Does it train staff adept in derivatives, electronic payments, electronic transactions and other areas requiring high degrees of specialization, as well as in new technologies, for example?

3) System of System Operation Framework

(1) Clarification of Separation of Responsibilities

- (i) Does the institution clearly separate responsibilities for system data reception, operation, operation results verification, and data and program storage?
- (ii) Does the institution ban system operators from accessing data and programs outside of their areas of responsibility?

(2) System Operation Management

- (i) Are regular operations implemented based on work schedules, instructions, etc.?
- (ii) Are operations implemented based on approved work schedules, instructions, etc?
- (iii) Are all operations recorded, and does the Manager of the system operation division check them with the use of prescribed checklists?

- (iv) Does the institution have important operations conducted by two or more persons? Are operations automated as much as possible?
- (v) Does the institution provide arrangements to prepare report outputs and obtain and keep work histories so as to enable the Manager of the system operation division to check the results of operation processes?
- (vi) Does the institution in principle ban system developers from accessing operations? When a developer must access operations for reasons such as system problems, does the institution ensure that the Manager of the relevant operation verifies the identity of the developer and conducts follow-up inspections of the access records?

(3) Product Data Management

- (i) Has the institution specified the policy and procedures concerning the provision of product data for use in system testing?
- (ii) Is management of product data provided for use in system testing conducted appropriately, in accordance with the policy and procedures specified by the institution?

(4) System Problem Management

- (i) Does the institution provide a system to ensure that system problems are recorded and reported to the Information Technology Risk Management Division as necessary?
- (ii) Does the institution regularly analyze the details of system problems and take measures to resolve them?
- (iii) Does the institution ensure that the Information Technology Risk Management Division and other relevant divisions promptly work together to resolve major system problems that may seriously affect corporate management and report such problems to the Board of Directors?
- (iv) Does the institution provide a system to ensure that problems occurring at the outsourcing contractor consigned with system operation are reported to the institution?

4) System Audit

- (i) Does the Internal Audit Division independent from the system division regularly conduct a system audit?
- (ii) Does the Internal Audit Division have staff adept in system-related matters? Is an external audit with regard to information technology risk management conducted by accounting auditors, etc. as necessary?

3. Crime Prevention, Back-up and Prevention of Unauthorized Use

1) Crime Prevention

- (i)Does the institution have an anti-crime organization and have a Manager with clear responsibility thereof?
- (ii) Does the institution exercise appropriate and sufficient supervision over entry into and exit from work areas, handling of important keys, etc. in order to prevent acts that may threaten the safety of computer systems?

2) Computer Crimes and Accidents

Does the institution provide a system to ensure that sufficient attention is paid to the risk of computer crimes and accidents (intrusion of unauthorized programs such as viruses, destruction of CDs/ATMs and cash theft therefrom, card fraud, theft of information by outsiders, leakage of information by insiders, hardware problems, software problems, operation errors, transmission line failures, power outages, external computer failures etc.) and that follow-up checks such as inspections are conducted?

3) Disaster Mitigation

- (i) Does the institution have a disaster mitigation organization in place to mitigate damage and help continue business in the event of disaster and have a Manager assigned with clear responsibility thereof?
- (ii) When there is a disaster-mitigation organization, is it organized along the line of the institution's business and is there a Manager with clear responsibility for all business categories?
- (iii) Does the institution have measures in place to cope with fire, earthquakes, and flooding?
- (iv) Does the institution have prescribed emergency evacuation areas for important data etc.?

4) Back-up

- (i) Does the institution create back-ups to prepare for damage to and failure of important data files and programs and have a management method thereof specified?
- (ii) Does the institution take care to ensure decentralized storage and remote-location storage with regard to the back-ups created?
- (iii) Does the institution have off-site back-up systems with regard to important systems?
- (iv) Does the institution document its back-up cycle?

5) Development of Contingency Plan

- (i) Does the institution have contingency plans in place to prepare for malfunctioning of computers systems due to disaster and other events?
- (ii) Does the institution seek approval of the Board of Directors when it develops contingency plans

- or conduct important revisions of the plans? (Does it seek the approval of the Board of Directors or equivalent organization to the Board of Directors for other, less important revisions?)
- (iii) Does the institution refer to the "Handbook for Contingency Planning in Financial Institutions" (edited by the Center for Financial Industry Information System) when developing contingency plans?
- (iv) When developing contingency plans, does the institution assume emergencies arising not only from disasters but also from other factors within and outside the institution?
- (v) When developing contingency plans, does the institution analyze possible effects on the settlement systems and possible damage to customers?
- (iv) Does the institution regularly conduct practices based on contingency plans? Are such practices conducted on a company-wide basis and, as necessary, with the involvement of outsourcing contractors, etc.?

4. Name Gathering of Deposit Account

- 1) Does the institution provide a system to ensure compliance with Paragraph 4, Article 55-2 and Paragraph 1, Article 58 of the Deposit Insurance Law?
- 2) Does the institution provide a system to ensure that data concerning name gathering are appropriately maintained and registered?
- 3) Are data concerning name gathering (names written in "kana" letters for name gathering and birth dates, etc.) accurately registered? Does the institution verify the status of registration?
- 4) Does the institution take appropriate system measures in response to programming modification related to the introduction of new products and system upgrades?
- 5) Does the institution have in place a manual for procedures to be followed in the event of an incident covered by insurance before the submission of magnetic tapes, etc. to Deposit Insurance Corp.? Are similar manuals in place for procedures to be followed before data based on Item 1, Paragraph 1 and Paragraph 2 of the cabinet ordinance concerning measures specified in Paragraph 1, Article 58-3 of the Deposit Insurance Law are reflected on systems and for the process of refunding deposits for settlement without the use of the data?

5. Verification at System-Related Outsourcing Contractor

- 1) Is the outsourcing contractor aware of information technology risk with regard to the system in its entirety for which it has begun operations and does it assess the risk?
- 2) Does the outsourcing contractor regularly subject the operations to audits by way of outsourcing institutions or external audits? In the case of an external audit, does the outsourcing contractor report the results of the audit to the outsourcing institution?
- 3) Does the outsourcing contractor meet the security level required by the financial institution, etc.

and is there a prior agreement on the details thereof between the outsourcing contractor and the financial institution, etc.?

- 4) Is it ensured that user review or testing by the financial institution, etc. are conducted at the planning, design/development and testing stages?
- 5) Is it ensured that objective assessment is conducted the Quality Control Division, etc. with regard to the status of compliance with standard development rules and the status of quality control?
- 6) With regard to the status of system operation, have matters to be reported to the financial institution, etc. been specified, and does the outsourcing contractor report regularly?
- 7) Are there a prescribed system and procedures for the outsourcing contractor to report system problems?
- 8) When the outsourcing contractor undertakes business with two or more financial institutions, does it provide a system to make judgments with regard to the effects of a problem in a system for one of the institutions in regards to the business of others and take appropriate measures?

6. Risk Management System Concerning System Integration

Verification with regard to risk management related to system integration should be conducted based on "Checklist for System Integration Risk Management (Approval No. 567 dated Dec. 26, 2002).

(Attachment 3)

Development and Establishment of Other Operational Risks

[Checkpoints]

- "Other operational risks" of a financial institution are the risks defined by the institution as operational risks excluding administrative risks or information technology risks.
- The development and establishment of a system for managing operational risks other than administrative and information technology risks is extremely important from the viewpoint of ensuring the soundness and appropriateness of a financial institution's business. Therefore, the institution's management is charged with and responsible for taking the initiative in developing and establishing such a system.
- The inspector should determines whether the system for managing other operational risks is functioning effectively and the roles and responsibilities of the management are being performed appropriately by referring, as necessary, to the checklists for the administrative risk management system and the information technology risk management system, etc.

1. Roles and Awareness of Directors

Do directors attach importance to the management of operational risks as defined by the institution excluding administrative and information technology risks, fully recognizing that the lack of such an approach could seriously hinder the attainment of strategic objectives? In particular, does the director in charge of such risk management examine the policy and specific measures for developing and establishing an adequate system for managing other operational risks with a full understanding of the scope, types, and nature of other operational risks and the techniques of identifying, assessing, monitoring and controlling the said risks as well as the importance of the risk management, and with a precise recognition of the current status of the risk management within the financial institution based on such understanding?

2. Roles and Responsibilities of Major Divisions Responsible for Managing Other Operational Risks

1) Legal Risk Management Division

With regard to legal risks as defined by the financial institution, such as loss and damage arising from failure to perform duties owed to customers due to negligence and inappropriate business market practices (including fines imposed as a regulatory measure or in relation to dispute settlement, penalties for breach of contract and damages), is a division in charge of legal risk management aware of risks faced by the institution and does it appropriately conduct management thereof? For example, with regard to items listed in the "Checklist for Legal Compliance" and the "Checklist for Customer Protection Management" does the Legal Risk Management Division recognize risks that constitute legal risks as defined by the institution as such and appropriately conduct management thereof?

2) Human Risk Management Division

With regard to human risks as defined by the financial institution such as loss and damage arising from complaints/unfair treatment (issues related to pay, allowances dismissal, etc.), discriminatory practices (sexual harassment and the like), is a division in charge of human risk management aware of risks faced by it and does it conduct appropriate management thereof? As a way to ensure appropriate risk management, does the institution provide training and education so as to enhance the ability of operational divisions and sales branches, etc. to manage such risks, for example?

3) Tangible Asset Risk Management Division

With regard to tangible asset risks as defined by the financial institution such as destruction of and damage to tangible assets arising from disasters and other events, is a division in charge of tangible risk management aware of risks faced by the institution and does it conduct appropriate management thereof?

4) Reputational Risk Management Division

With regard to reputational risks as defined by the financial institution such as loss and damage arising from deterioration in the institution's reputation and circulation of unfounded rumors, is a division in charge of reputational risk management aware of risks faced by the institution and does it conduct appropriate management thereof? As a way to ensure appropriate risk management, does the division take the following measures, for example?

- Has the Reputational Risk Management Division specified how operational divisions and sales branches, etc. are to respond to circulation of unfounded rumors?
- Does the Reputational Risk Management Division regularly check whether there are unfounded rumors circulating in each media category (e.g. the Internet, speculative news reports, etc.)?

3. Appropriateness of Crisis Management System

- (i) Does a person or division in charge of crisis management conduct regular inspections and practices in normal times as part of efforts to avoid or mitigate risk in the event of an emergency?
- (ii) Do the crisis management manual and the like note the importance of initial responses such as accurate grasp of the situation, objective judgment of the situation, and information dissemination immediately after the occurrence of the emergency?
- (iii) Are the crisis management manual and the like constantly revised in light of changes in the actual status of business and risk management?
- (iv) Do the crisis management manual and the like clarify the system of assignment of responsibilities in the event of an emergency and specify a system and procedures for communication of the emergency within the institution and to other parties concerned (including the relevant authorities)?
- (v) Does the business continuity plan (BCP) provide for measures to enable early recovery from damage caused by terrorism, large-scale disasters, etc. and continuance of the minimum necessary business for the maintenance of the functions of the financial system? Does the BCP have clear provisions with regard to the following matters, for example?
 - Measures to secure the safety of customer data and the like in the event of disasters, etc.
 (storage of information printed on paper in electronic media, creation of back-ups of electronic data files and programs, etc.)
 - Measures to secure the safety of computer system centers, etc. (allocation of back-up centers, securing of staff and communication lines, etc.)
 - Avoidance of geographical concentration of back-up measures
 - A specific target period for recovery, through provisional measures such as manual operations and processing by back-up centers, of operations vital for the maintenance of the functions of the financial system, such as acceptance of individual customers' requests for cash withdrawal and remittance and processing of large-lot, large-volume settlements conducted through the interbank market and the interbank settlement system?
- (vi) Are a system and procedures for communicating and collecting information in the event of an emergency sufficient in light of the level of crisis envisioned and typical cases of emergency assumed? Does the institution make daily efforts to disseminate and collect information in a sophisticated manner?