Investigation Report

（Executive Summary)

May 20, 2011

Special Investigating Committee on System Failures

I. Outline of Investigation

1. Establishment of Third-party Committee

Over the period between the night of March 14, 2011 (unless otherwise stipulated, the year indicated herein refers to the calendar year of 2011) to the 24th of the same month, Mizuho Bank, Ltd. (hereinafter referred to as "MHBK") experienced massive information system failures (hereinafter referred to as "Failures"). During this period, the customers' economic activities were seriously affected by delays in payroll remittances and other fund transfers as well as outages of ATMs, among other problems.

MHBK decided to investigate into the causes of the Failures and develop measures to prevent the recurrence of similar events. Given the scale of the impact of the Failures on customers and society, it has determined to work to prevent the recurrence of the information system failures and recover the public trust by establishing a third-party committee comprising outside experts and specialists and having it investigate the causes of the Failures, assess the adequacy of, and make recommendations regarding the recurrence prevention measures from a neutral and impartial viewpoint. On this basis, on April 11, MHBK requested several legal professionals and systems specialists who do not have a vested interest in MHBK to become members of the committee, and established the Special Investigating Committee on System Failures (hereinafter referred to as "Committee").

The Committee is chaired by Tatsuo Kainaka (Attorney-at-law, former Justice of the Supreme Court), and has the following members: Masahito Monguchi (Attorney-at-law, former President of the Nagoya High Court), Yoriko Goto (Certified Public Accountant, Managing Partner, Financial Services Industry Group, Deloitte Touche Tohmatsu LLC), and Yasumasa Takeda (Executive Vice President, Accenture Japan Ltd.),

2. Purpose and Method of Investigation

The purpose of the investigation by the Committee is to (i) identify the causes of the information system failures and to (ii) assess the adequacy of, and make recommendations regarding MHBK's recurrence prevention measures.

With the intention to conduct a prompt and precise investigation from an independent and fair position, the Committee limited the investigation to the period up to April 11 for the substance of the matters to be investigated and the impact and scope of the Failures, and to the period up to April 30 for the actions taken after the Failures. Then, the Committee examined and analyzed MHBK's internal data gathered around the time of the Failures, the systems audit reports, the rules and regulations concerning system operations, the contracts with outsourcees and other materials, and conducted hearings of MHBK's President, Directors, Officers and employees as well as the representatives of Mizuho Financial Group, Inc., the Mizuho Group's holding company (hereinafter referred to as "MHFG"), representatives of Mizuho Information & Research Institute, Inc. (hereinafter referred to as "MHIR") and Mizuho Operation Service, Ltd. (hereinafter referred to as "MHOS"), which are MHBK's outsourcees, and other related parties, as necessary.

II. Facts Detected as a Result of the Investigation

1. Summary of the Failures

The Failures stemmed from the abnormal end of the Night Batch because of the concentration of large volume of transfers to Company A’s donation account <a> on Monday, March 14, 2011 (unless otherwise stipulated, the year indicated herein refers to the calendar year of 2011) and Company B’s donation account <b> on Tuesday, March 15 in the wake of the Great East Japan Earthquake which took place on Friday, March 11.

Although MHBK took measures to restore the underlying system to solve the above-mentioned abnormal end of the Night Batch, MHBK could not terminate the sequence of the Night Batch by the business office open time of the following day. MHBK suspended the Night Batch on both days and conducted the daily processing of the batch (hereinafter referred to as the “DJS Switching”). Thus, system operations which were normally automated were switched to manual operations, and MHBK had to handle a large volume of work manually. As a result, there was a large volume of unsent exchange transactions, as well as human errors arising out of the manual processing, leading to a substantial delay in the business office open time on the following day, and suspension of ATM services, among other events.

Even on Wednesday, March 16 and after, the number of unprocessed operations of the Night Batch increased and there were so many human errors arising out of the manual operations of the system, the extent of influence became wider and wider. For these reasons, in order to secure system recourses and conduct stagnant operations of the Night Batch, MHBK imposed ATM and Direct Channel usage restrictions. However, the Night Batch subsequently remained unprocessed due to shortage of processing time and human errors. Moreover, the Failures triggered many additional events which affected customers, such as the unavailability of certain transaction details.

2. Occurrence of the Failures

(1) Events Occurred and Restoration Measures

The Failures involved the following events: delays in processing the exchange transactions; delays of the open time of the business offices and suspension of transactions; ATM outage and usage restrictions; Direct Channel usage restrictions; and other events that affected customers.

A. Delays in Processing the Exchange Transactions

There were substantial delays in exchange processing between Tuesday, March 15 and Thursday, March 24.

(a) Abnormal End of the Night Batch and Extended Operations (Monday, March 14)

After the Great East Japan Earthquake which occurred on Friday, March 11, there was an immense volume of transfers to Company A's donation account <a>. As a result of this immense volume of transfers, the amount of processing of these transfers exceeded the Limit Value of the number of processing per account in the Night Batch, and the Night Batch abnormally ended at 22:07 on Monday, March 14. Some of the processing result data was also lost when it abnormally ended.

After the above-mentioned abnormal end of the Night Batch, MHBK took restoration measures to raise the Limit Value that caused it and rerun the Night Batch. Although the subsequent processing needed the processing result data which was lost when the above-mentioned abnormal end occurred, MHBK faced difficulty in this data restoration effort. It eventually took nearly 8 hours to finish, extending the duration of the Night Batch.

(b) Suspension of the Night Batch and Manual Operation (Monday, March 14)

As the duration of the Night Batch for Monday, March 14 was extended as explained above, MHBK suspended the Night Batch at around 7:00 on Tuesday, March 15 pursuant to the applicable procedure document to launch the Business Office Terminals on the scheduled time, and started preparing for launching the Business Office Terminals and implementing the DJS Switching.

It became impossible to utilize such automated operation as a result of the suspension of the Night Batch and implementation of the DJS Switching, and MHBK had to run the Night Batch manually. As a result, a tremendous volume of work was generated, triggering many secondary failures due to failed processing and misprocessing.

(c) Abnormal End of the Night Batch and Extended Operations (Tuesday, March 15)

As a result of Company B starting to call for donation through the use of mobile phone-based transfer service on Tuesday, March 15, an immense volume of transfers were made to the donation account <b> at and after 15:00 on Tuesday, March 15. Although the person in charge of such service within MHBK checked the data volume it could accept through the External Connection System, the number of transfers exceeded the Limit Value of the number of processing per account in the Night Batch on Tuesday, March 15, as a result of which the underlying system abnormally ended at 7:17 on Wednesday, March 16.

MHBK temporarily removed this data and reran, completing the Night Batch other than the data for the donation account <b> at 5:20 on Thursday, March 17.

At 13:30 on Thursday, March 17, MHBK erased the unnecessary data, in the course of which necessary data was also erased by erroneous processing. As a result, it took 16 hours to identify and remake such erased data, which caused a further delay in the Night Batch.

(d) Suspension of the Night Batch and Automated Operation (Tuesday, March 15)

Although MHBK tried to launch the Business Office Terminals after ending the Night Batch for Tuesday, March 15, the abnormal end of the Night Batch described in subsection (c) above occurred at 7:17 on Wednesday, March 16. As it took time to restore it, MHBK suspended the Night Batch and started to prepare for launching operation of the Branch Office Terminals and implement the necessary DJS Switching.

(e) Unsent "SHIMUKE" (Outbound Instruction) Exchange Transactions

As a result of the above-mentioned suspension of the Night Batch for Monday, March 14, the "SHIMUKE" (Outbound Instruction) exchange transactions which were scheduled to be run on Tuesday, March 15 after the end of the Night Batch were left unsent.

During that period of time, each of the branch offices conducted the "transmission of the transfer data for which processing had not been withdrawn" (release operation; hereinafter referred to as the "Release Ope") and made transfers by separate "DAKEN" (input). However, the processing which should have been completed prior to the Release Ope did not meet the Zengin deadline, and no exchange transmission through the Release Ope was made. On the other hand, only the exchanges processed by the separate "DAKEN" (input) were sent, because the transmissions by the separate "DAKEN" (input) were made independently from the Night Batch. As a result, approximately 310,000 exchange transactions which should have been sent on Tuesday, March 15 were left unsent at or around 17:00 on Tuesday, March 15.

The continuation of the extended operations of the Night Batch eventually left parts of the customer requests for exchange transaction on Wednesday, March 15 through Wednesday, March 23 unsent (approximately 1,200,000 transactions in total).

Because only parts of the exchange transactions were sent by the separate "DAKEN" (input), the sent exchange transactions might have been sent doubly had those unsent exchange transactions been sent in bulk. For this reason, MHBK needed to cancel the inputs already made.

(f) Unprocessed "HISHIMUKE" (Inbound Instruction) Exchange Transactions

As a result of the extended operations of the Night Batch, the other banks' requests for exchange transactions for the periods between Wednesday, March 16 and Friday, March 18 (a total of approximately 1,010,000) were left unprocessed.

(g) Recovery Response to the Exchange Processing Failures

As the extended operations of the Night Batch was not solved until Thursday, March 17, MHBK decided to secure its system resources by imposing restrictions on usage of ATMs, Direct Channel and other services between Friday, March 18 and Tuesday, March 22, including the three consecutive holidays, and put the greatest emphasis on solving unsent exchange transactions, and solving the extended operations of the Night Batch on and after Tuesday, March 15 which left the exchange transmissions unsent.

In order to make the manually processed Night Batch more efficient, MHBK automated its processing by improving the TARGET. MHBK started considering the technical aspects of such parallel operation on Monday (holiday), March 21, and successfully identified them. Then, MHBK decided to automatically operate its daytime online and the Night Batch in parallel on Tuesday, March 22. As a result, MHBK could finish the Time Batch for up to Monday, March 21 during the duration of the daytime online operations on Tuesday, March 22, and the Night Batch for Tuesday, March 22 after which it was switched to the normal automated operation.

As a result, the majority of the unsent "HISHIMUKE" (inbound instructions) exchange transactions were solved on or prior to Tuesday, March 22. However, on Tuesday, March 22, some of those transactions (nearly 160,000) were left unsent, and on Wednesday, March 23, parts of those transactions (nearly 1,000) were also left unsent for the same reason, which was solved on Thursday, March 24.

In order to secure the convenience of customers in connection with the restrictions on usage of ATMs, Direct Channel and other services, MHBK temporarily launched its Business Office counters between 9:00 and 17:00 on the holidays from Saturday, March 19 to Monday, March 21 (holiday), and made special payments.

B. Delay in the Business Office Open Time and Suspension of the Business Office Operations

As a result of the abnormal end of the Night Batch for Monday, March 14 and the abnormal end of the Night Batch for Tuesday, March 15 as explained above, there were the delays in the business office open time and suspension of the business office operations, as described below.

Tuesday, March 15	It became impossible to provide the lending, loan, foreign exchange and other businesses due to the effect of suspension of the Night Batch, and the transaction start time utilizing the Business Office Terminals was extended to 10.25 from 9:00, the normal open time.
Wednesday, March 16	ATM outage occurred between 8:00 and 8:33 on Wednesday, March 16, and the transaction start time utilizing the Business Office Terminals was extended to 11:12 from 9:00.
Thursday, March 17	The ATM outage occurred between 0:00 and 5:20 on Thursday, March 17, and the transaction open time utilizing the Business Office Terminals was extended to 10.46 from 9:00.

In addition, due to the repeated suspension of the Night Batch and automated operation on Monday, March 14 and after, there were certain failures in which the lending, loan, foreign exchange and other operations were suspended between Tuesday, March 15 and Tuesday, March 22, and loan modifications and full loan collection operations were suspended between Tuesday, March 15 and Friday, March 25, respectively.

C. ATM Outage and Usage Restrictions

As a result of the abnormal end of the Night Batch on Monday, March 14 as explained above, the ATM outage and usage restrictions occurred between Wednesday, March 16 and Wednesday, March 23.

D. Direct Channel Usage Restrictions

MHBK took measures to impose EB usage restrictions for Mizuho Direct, Mizuho e-Business Site and Corporate EB, among other purposes, in order to secure system resources. More specifically, the usage of Mizuho Direct was restricted between 14:30 on Wednesday, March 16 and 10:30 on Thursday, March 17, and between 14:30 on Thursday, March 17 and 12:00, Tuesday, March 22, the usage of e-Business Site and Corporate EB was restricted between 8:00 and 11:30 on Wednesday, March 16 and Thursday, March 17, and between 19:00 on Thursday, March 17 and 12:00 on Tuesday, March 22.

E. Other Events That Affected Customers

(a) Lack of Transaction Details

STEPS could not provide the Corporate EB and other related systems with some of the transaction details, and the related system lacked some of the transaction details. For Corporate EB, it became partially impossible to make inquiries about remittance/withdrawal details, and customers of this service could not identify remittances and withdrawals between Tuesday, March 15 and Tuesday, March 22.

(b) Inability to Process Funds Transfer, Return of Data with Erroneous Results, and Processing Omissions

There were the situations where MHBK became unable to create parts of the account funds transfer result data for Tuesday, March 15 and Wednesday, March 16 and data with erroneous result data was returned to its customers.

There were certain processing omissions resulting from the failure of MHBK to take steps it should primarily have taken, including verifications of the balances payable and the account holders in connection with the certain account funds transfers for Wednesday, March 16 and Thursday, March 17.

(c) Other Defects in the Transactions Associated with the Suspension of the Night Batch

The Night Batch was suspended after the manual DJS Switching at 7:17 on

Tuesday, March 15, leading to delays in the processing collection of loan repayments in the lending business, automatic renewal and withdrawals of foreign currency time deposits, automatic withdrawals of time deposits, and collection of fees and commissions as a result of the suspension of the Night Batch.

(d) Non-collection of Special Payments

As the alternative measures against the ATM usage restrictions, MHBK took measures to make special payments. However, MHBK made special payments in excess of the deposit balances. As a result, approximately 390 million yen in cash temporary payments made by MHBK at its business office counters was left uncollected as of Thursday, April 28.

(2) Subsequent Measures for the Event That Occurred

In order to minimize the inconvenience of its customers, MHBK made prompt releases of the fact that the failures occurred (Public Announcement); gave instructions as to how to respond to customers' inquiries about system failures and services provided (Responses at Business Offices and Call Centers); analyzed the side effects on customers resulting from the Failures (Analysis of External Effects), and prepared the "List of Items to Which MHBK Needs to Respond for Customers.".

A. Public Announcement

Since Tuesday, March 15 when MHBK was delayed in launching the Business Office Terminals, MHBK successively conducted public relation activities through a total of 8 press conferences in which the President & CEO and other executives were present, correspondences to the media, and announcements on its website. MHBK also timely informed the Zengin Center of the delays in connection with the Zengin System, and released correspondences and telegrams of the failures to other member banks in bulk. However, the timing of public announcement was often too late, and the contents of the releases contained expressions that could mislead customers.

B. Responses at the Business Office and Call Centers

With respect to the responses at the business offices, the Business Operation Service Promotion Division, the Business Operation Planning Division and other relevant organization issued instructions and correspondences as to the status of failures and responses associated with the implementation of the business contingency plans periodically after Tuesday, March 15. As for the call center services, MHBK assigned one devoted staff to the Personal Marketing Division so that inquiries from the call centers could be centralized, and prepared and distributed Q&A materials..

C. Analysis of External Effects

In order to fully comprehend the effects of the subject system failures on its customers, on Wednesday, March 23, MHBK organized a new operation working group (hereinafter referred to as the “Operation WG”) under the control of the System Failures Emergency Measures Task Force (hereinafter referred to as the “Failures Countermeasures TF”), and gathered information by assigning the staff members of the Operation WG to the business office counters, call centers and other organizations where they could listen to their customers.

(3) Management Involvement with the Failures

After Monday, March 14, the IT & System Division informed the executive in charge of the IT & System Group of the occurrence of failures.

At around 5:00 on Tuesday, March 15, the executive in charge of the IT & System Group directed to launch the Business Office Terminals by the business office open time, and then informed the President & CEO and Vice President of the conditions of the Failures, and their emphasis on launching the Business Office Terminals by suspending the Night Batch due to the Failures. The manager of the Business Operations Promotion Division implemented the business contingency plans at 0:00.

After that, 380,000 (later revised to 310,000) exchange transactions remained unsent. Then, at 22:00 on Tuesday, March 15, the management set up the Failures Countermeasures TF lead by the President & CEO in order to help consolidate policy development and directions and act quickly. Subsequently, the management then consolidated the efforts to draw up response policies on and give instructions as to the Failures under this framework.

3. Background to the Failures

(1) Overview of the Current System

The current systems consist chiefly of: the Core Banking System, the External Connection System (Customer), the Information Support System, and the Securities/Market System.

The Core Banking System is called STEPS, and the processing operations through STEPS are largely divided into the online operations instantly processed and the Night Batch processed in bulk. In STEPS, the daytime online operations and the Night Batch are expected to be processed alternatively, and it was not designed such that both operations would be done at the same time.

The Night Batch is managed by the automated operation system called TARGET. The DJS Switching is a process to create individual data processing features (hereinafter referred to as the "Batch Jobs") for the next day and is run after all of the Batch Jobs on the current day are completed. Such processing is regularly scheduled to be run at 4:30 or, in case of a delay of the Night Batch, 6:00. If, however, the Night Batch does not end by 6:00, there would have been no choice but to delay the online operations start time, including a delay of transaction start time in the branch offices, or to suspend the Night Batches and start online operations on schedule. If, however, MHDK elected to suspend the Night Batches and conduct the DJS Switching, it was structured such that MHDK would execute the remaining parts of the Night Batch manually and could not send exchange transactions until it terminated the Night Batch.

(2) Emergency Measures

MHBK's emergency framework is such that the President & CEO oversees business continuity management and, when an emergency situation occurs, the President & CEO establishes the "Emergency Headquarters" led by himself or the "Emergency Response PT" led by his designee to gather information, determine what response policy to adopt, and give response and other instructions.

The Basic Policies set forth that if the "emergent situations" resulting from the system failures occurs, the IT & System Division is required to make a report to the President & CEO via the executive in charge of the IT & System Group pursuant to the Reporting Standards for System Failures developed by the IT & System Division.

Furthermore, the Action Plans for Emergency Response (for each emergency situation) set forth that the executive in charge of the IT & System Group shall inform and report on any system failure that may require emergency response such as suspension of settlement/clearing functions.

(3) Implementations of the System Audit

In the audit plan for FY2010, the risk assessment of "system operation management" that is highly related to the system failures that occurred recently was rated "MH" (i.e., a field that highly requires audit and in which audit should generally be conducted), and the risk assessment of "deposit/exchange system features" was rated "R2" (i.e., a field in which audit is to be conducted within 30 months). Accordingly, internal audit was conducted pursuant to the IT Audit Procedure.

The System Risk Management Office of the IT & System Division was subject to external audits in 2005, 2006, and 2007. However, no external audit has been conducted since 2008.

On the other hand, the system audit of STEPS was supposed to be audited by MHBK, the system owner and it was not subject to system audit by the Internal Audit Division of MHIR. In addition, MHFG has conducted no audit into MHBK or MHIR prior to the Failures.

(4) System Failures Which Had Occurred after the System Integration in April 2002, and Responses

On Monday, April 1, 2002, MHBK and MHCB experienced account funds transfer processing delays and settlement and other system failures as a result of the system integration (hereinafter referred to as the "2002 Large-scale Failures"). MHBK experienced significant effects on its customers because of account funds transfer processing delays, double debits, transfer delays, and restrictions on ATM transactions. In response, MHBK developed recurrence prevention measures mainly intended for reinforcement of the management structure of the system project that had immediately caused the system failures. All of these measures had been put into practice with the completion of the system integration in December 2004.

As for the system failures which had occurred in and after 2002, the IT & System Division identified the causes for those failures, investigated into their consequences, and drew out the restoration measures in cooperation with the System Operation Division, development vendors, and operation vendors, and then implemented the restoration efforts, which were summarized in a System Failures Report after the restoration.

III. Analysis of Causes for the Failures

1. Overview of the Analysis of Causes

Examining into the causes triggering various failures based on the facts detected as a result of this investigation, the Failures are largely attributable to basic mistakes made by the personnel in charge before. However, in order to consider recurrence prevention measures, we must look at what causes such mistakes. Analyzing from this point of view, there are flaws in the system functions; Information Technology Risk management structure which could not have been prevented; emergency preparedness in restoration work; human resource development and assignment; and insufficient management and audit.

2. System Capabilities

(1) System Processing Unit in Case of Concentration of Large Volume of Transactions

Although both the processing to evaluate the transaction details of Company A's donation account <a> that caused the abnormal end of the Night Batch for that account, and the processing to allocate data to the successive Night Batch with large amount of transaction details which caused the abnormal end of the Night Batch for Company B's donation account <b> should have been conducted within the scope of the applicable Limit Value, all transaction details of those accounts were processed in bulk. As a result, MHBK exceeded the Limit Value and the Night Batch abnormally ended.

(2) System Operation Capabilities during the Extended Operations of the Night Batch

STEPS was designed such that daytime online operation and nighttime batch are in operation alternately. The Night Batch is automatically operated by TARGET. However, if the Night Batch did not end by 6:00, MHBK had to suspend the Night Batch and conduct the DJS Switching, unless it elected to extend the time to launch the Business Office Terminals. However, if MHBK conducted the DJS Switching, it had to put the remaining Night Batch into manual operation, which required much time and effort to handle. In that case, exchange data would be created and sent in bulk after the Night Batch, which would cause delay in sending exchange transactions. Nevertheless, MHBK did not discuss what measures they should take.

3. Information Technology Risk Management in an Attempt to Prevent Failures

The system failures at issue arose because the single processing conducted in the course of the Night Batch exceeded the applicable Limit Value. Such Limit Value has never been reviewed since the underlying system had started to operate, was not among the periodic inspection items. For these reasons, the persons in charge did not fully recognize even the existence of such Limit Value in the Night Batch. Thus, the periodic Information Technology Risk assessment and review of inspection items in the Information Technology Risk assessment at the time of deployment of a new product/service were insufficient.

(1) Periodic Risk Assessment of the Systems in Operation

Control items of self inspections of Information Technology Risks (hereinafter referred to as the "Information Technology Risk CSA") include checking the applicable system capacity Limit Value. The guidelines for such inspection are set forth as the

Guidelines for System Capacity Limit Management, under which it conducted inspections.

Although there were instances in which the failures relating to the Limit Value similar to the subject failures, the inspection items on the list of inspections prepared under the above-mentioned guidelines did not include the Limit Value for the transaction details in the Night Batch that related to the Failures.

In addition, a certain public body issued the survey article regarding the instances of system failures involving the financial institutions, and their countermeasures, in which similar cases of failures resulting from huge volume of transfer transactions and delays in operation of the Night Batch were introduced. However, these cases were not fully utilized, and MHBK did not reexamine the Information Technology Risk inspection items.

(2) Risk Assessment in Deploying New Product

The abnormal end of the Night Batch in connection with Company B's donation account <b> resulted from concentration of an immense volume of transfers in connection with the mobile phone-based money remittance service. MHBK, however, could not predict such an immense volume of transfers and take necessary preventive measures.

Although MHBK should have conducted tests including the Night Batch based on the expected volume of data, MHBK only tested the interfaces of Company B's system and MHBK's system and omitted a test for the volume of data because it did not need to develop a new system for this service.

The System Division would have needed to stipulate the guidelines to conduct tests of the non-functional requirements which would tend to be omitted as the requirements from the User Division (i.e., requirements for processing capacity, security and failure responses) and examine the methodology of risk assessment for new services without development of any new system.

There was no express provision regarding a contact office in such case where immense volume of transfers is anticipated as in this case, and the System Usage Division within MHBK (hereinafter referred to as the "User Division) made inquiries to the persons in charge of the External Connection System about the acceptable volume of data. It should have made inquiries to a person in charge who could judge the possible effects on the related systems, rather than the person in charge of that particular system.

4. Emergency Measures for Recovery

Pursuant to analysis of the reasons for the delayed recovery of the Failures, the following are identified. First, emergency measures were not effective. Second, possible events assumed in System Contingency Plan were not sufficient. Third, written procedures for recovery were not effective. The reason that these insufficiencies could not be detected beforehand was that checking procedures and drills could not fulfill their role of checking effectiveness.

(1) Emergency Measures

With respect to the emergency measures taken against the Failures, insufficiency in review of risk scenarios, lack of appropriate information sharing, and lack of control function are identified.

In responding to the Failures, both the systems department and the management did not conduct thorough review of the scenarios for the greatest risks assumed at each stage partially owing to lack of information, and this resulted in their making inappropriate judgment. In responding to the failures of charity account "a" on March 14th (nighttime), the systems department did not discuss internally one of the greatest risks, the risk of exchange transactions not being conducted, until the problem became apparent in the evening of the 15th. In addition, in responding to the failures of charity account "b" on March 15th (nighttime), DJS Switching was implemented as the day before even though they were facing the biggest risk event where Night Batch Processing Delays occurred and unrealized exchange transactions accumulated from the day before, which lead to a worsening of the situation.

There also was insufficiency in information sharing within MHBK and MHIR. At the point of 14th, company B gave information to users department of MHBK that a huge volume of payment by transfer was expected. However, such information was not passed from the users department to IT and systems control department, but was passed directly to MHIR. For that reason, IT and systems control department did not realize this fact until the occurrence of failure related to charity account "b" during the night of 16th. In addition, within MHIR, investigation of possible effects was conducted only with respect to the systems that the informed department was in charge, and the information was not passed to the persons in charge of the Core Banking System (STEPS).

Moreover, because of lack of control function at MHIR, MHIR had difficulties in understanding the whole situation. MHBK could not add staff members from MHBK who could control and manage the situation at an early stage, and could not fulfill its responsibility to control the whole situation. One of the causes for the delay in improvement of the difficult situation due to lack of control function was unclear chain of command between management of MHBK and MHIR in the cases of emergency.

(2) Insufficiency in Events to Be Assumed

The Failures began with abnormal termination that occurred during initial stages of processing Night Batch Processing. However, a System Contingency Plan assuming the occurrence of such an event had not been prepared. For that reason, the written procedures, "Online Response in Night Batch Processing Delays" which was prepared for assumed abnormal termination that may occur during the final stages of Night Batch Processing had to be applied.

(3) Insufficiency in Effectiveness of Written Procedures

The written procedures entitled, "Response to ABEND in the CMFAut-booking in Bulk" were utilized at the system recovery control room in responding to the Failures. However, the written procedures did not take into consideration the time expected to be taken. For that reason, implementation of work was determined pursuant to inaccurate estimate of contents of work.

Concerning branch office matters control room, we found insufficiency in consideration for Business Contingency Plans with respect to special payments and cancellation of double payment by transfer.

For special payments, the management of customers to whom such payments were made was done in the unit of each branch office. For that reason, unlawful payments from multiple branch offices to the same person occurred in the initial stage of the implementation of special payments. Although the risk of occurrence of such unlawful payments had been expected, management procedures for paid customers across multiple branch offices had not been prepared beforehand.

With respect to cancellation of doubled payment by transfer that was associated with response to unrealized exchange transactions, the procedures instructed to contact the customer after cancellation. However, because of confusions in the field, such communications to the customers were not initiated thoroughly and resulted in cases of complaints.

5. Business Management and Audit

(1) Systematic Human Resources Development and Appropriate Allocation

As the cause of the Failures, the lack of human resources who had the practical ability to analyze the effect of an event to the whole Core Banking System, or who could build a prospect for recovery of multiple failures is identified. In addition, MHBK lacked managerial personnel who could have an overview of the whole system and take leadership in response to multiple failures throughout the series of failures. Moreover, MHBK did not fully recognize the need to develop its human resources through the drills. At systems department, visualization of systems stably operated over the long term was not realized and handing over of know-how concerning such specifications was insufficient.

(2) Effectiveness of Audit

Concerning audit department, insufficiency in systems audit of STEPS, insufficiency in the audit system as a group and lack of utilization of outside audit services are identified.

A. Insufficiency in Systems Audit for STEPS

Audits are conducted by IT and systems audit room after conducting risk assessment and ranking of areas subject to the audit pursuant to "Guidelines for Assessment / Monitoring of Risk". However, "management structure for systems operation" that caused the failures discussed in this report is assessed as having the level one degree lower than that or the highest degree risks. In addition, assessment according to departments and systems rates, "deposits and exchange transaction systems" under the scope of IT systems control as having the second-degree risks. Although "deposits and exchange transaction systems" will have great effects in case of any system failures, the audit system does not treat them as requiring the highest rank of in-depth audit.

Internal audits performed for the most recent two years were focused on too much on formalities. The internal audits did not assess the points that written procedures for DJS Switching had not been reviewed for a long time and that there was problem in effectiveness of recovery processing in case of a failure in Night Batch Processing.

B. Audit System as a Group

Regarding MHIR, MHBK only has audit capacity for outside contractor pursuant to outsourcing agreement. In comparison, MHFG has the authority to conduct direct audit of its subsidiary, MHIR. However, in reality, MHFG only receives repots on results of audit by themes and by departments conducted by internal audit department of MHIR, and MHFG's audit department does not conduct a direct audit of MHIR. Moreover, audit by themes conducted by internal audit department of MHIR is not targeted at STEPS outsourced from MHBK.

As described above, systems audit for STEPS that caused the Failures and for department responsible for STEPS is conducted by MHBK's audit department only, only within the scope of audit services outsourced by MHBK, and no internal audit as a group is conducted to this day.

C. Lack of Utilization of Outside Audit Services

The Financial Institutions Inspection Manual states that, outside audit services shall be utilized as necessary with respect to audit of systems risk management structure. Also, it states that utilization of outside audit services as one of the Recurrence Prevention Measures developed pursuant to the large-scale failures in 2002.

However, cases of utilization of outside audit (assessment) services by audit department after the occurrence of the large-scale failures in 2002 were limited. There was no case of utilization where the whole systems risk management structure was assessed, apart from project audits.

IV. Proposal for Recurrence Prevention Measures

1. Assessment of Recurrence Prevention Measures

The Committee assesses MHBK's Recurrence Prevention Measures as basically adequate. This is because they openly admit that their insufficient awareness of the Information Technology Risk was one of the causes of the Failures, and considers not only measures to prevent recurrence of information system failures that are similar to the Failures but also a framework to manage Information Technology Risk in general. That said, the investigation by the Committee identified the following issues that would require further consideration:

(1) Management System for Prevention

A. Lack of Measure to Ensure Effectiveness of Evaluation of Enhancement of System Risk CSA

The Recurrence Prevention Measures indicate, for enhancement of the System Risk CSA, the need to set a maximum allowable transaction volume and review the system specifications and the controlled items with special focus on the BtoC area through cooperation among the Systems, Products and Administration Divisions. Meanwhile, it is also necessary to consider how to improve the effectiveness of the evaluations.

B. Need to Strengthen the Information Technology Risk Management Procedures upon Introduction of New Services

While the Recurrence Prevention Measures mention the need of enhancement of evaluation of the Information Technology Risk at the time of introduction of new services, the Committee believes that MHBK also needs to conduct tests that assume processing of a large volume of data to handle a large number of deposit transactions made on a particular account, even if such services do not involve any systems development.

(2) Management System for Early Recovery

As to the emergency response systems, the Recurrence Prevention Measures mention, as an improvement measure, a revision of the personnel's roles and information sharing within MHBK as well as the revision of the roles and information sharing among MHBK, MHIR and MHOS.

As for the addition of possible events for which MHBK should be prepared and the securement of the effectiveness of the procedure documents, the Recurrence Prevention Measures point out the necessity to develop a Contingency Plan and procedure documents assuming information system failures similar to the Failures and to proceed to work on a fundamental improvement after reviewing the risk scenario and clarifying the matters to be set forth in such a Contingency Plan and procedure documents.

Furthermore, the effectiveness of such Recurrence Prevention Measures is supposed to be verified through training within MHBK as well as cross-company training among MHBK, MHIR and MHOS.

While specific methods and process of the revision of each of the above-mentioned issues are yet to be considered, the Committee evaluates the above-described measures to be appropriate as a basic direction.

(3) Management of Business and Organization

A. Personnel Measures

As to the measures to enhance human resources, MHBK intends to ensure consolidation of knowledge and know-how as well as reinforcement of the management through systematic training programs to enhance the workforce. While specific plans are yet to be considered, the Committee assesses such measures to be appropriate as a basic direction.

B. Internal Audit

With respect to the internal audit department, MHBK intends to have it gain better understanding of potential risks and more diverse perspectives, and this is appropriate as a basic direction. However, improvement of the audit method in the internal audit department is critical in view of the fact, among others, that the internal audit failed to identify the problems in the effectiveness of the procedure documents. This point is as specifically indicated in the Committee's recommendations below.

2. Proposals on Recurrence Prevention Measures

(1) System Function

In the course of re-checking of Information System Contingency Plan and Business Contingency Plan, it is necessary to consider whether risks identified fully cover the potential risks. For such purpose, MHBK must re-check and re-analyze the current systems for existence of possible risks related to system design and system operational design other than those identified in relation to the system failures discussed in this report, and if any, MHBK must include them in risk scenarios of contingency plans.

(2) Management Structure for Prevention

A. Improvement of Effectiveness of Information Technology Risk CSA

MHBK performs an annual risk assessment pursuant to check lists for each system, which is called Information Technology Risk CSA. We consider that improvements in preciseness of checking procedures are also required as well as improvements in items in the check list, in order to enhance effectiveness of the risk assessment.

In order to improve items in the check lists, it is necessary to perform continuous and multidimensional risk assessment taking into consideration both internal and external environmental changes instead of merely referring to common standards referred to by financial institutions. To achieve such purpose, we advise that MHBK actively utilize viewpoint of those outside the bank, in addition to internal viewpoints of the bank such as product management, operations and systems departments.

Moreover, in order to improve preciseness of checking procedures, MHBK should not be satisfied by checks performed under the responsibilities of departments in charge of systems alone, but also needs to perform cross-checking of appropriateness of check results among multiple departments and conduct reviews with vendors and outside experts in order to realize comprehensive checking from multiple viewpoints. Moreover, Information Technology Risk Department must go beyond routine confirmation of check results and consider on-site verification.

(3) Management Structure for Early Recovery

A. Proposal on Review of Emergency Measures

The important points in review of emergency measures are realignment of the roles of each organization, clarification of the existence and scope of responsibilities of each organization, and establishment of chain of command at field-level, and, in addition to that, establishment of an integral chain of command that includes respective top management of MHBK, MHIR and MHOS.

B. Proposal on Fundamental Improvement of Information System Contingency Plan and Procedures

To realize fundamental improvement, it is important to sort out potential flaws in effectiveness in the current Information System Contingency Plan and Procedures (risk scenarios that are lacking, potential omission in written procedures, scope of required automation and other issues). We consider that review by cooperating with outsourced entities such as MHIR and utilization of outside experts are effective for resolving such flaws.

Moreover, to continue such improvement efforts rather than making it a one-time event, MHBK must review the current method of conducting periodical check of and making improvements to Information System Contingency Plan and Procedures so that such checks will go further to consider appropriateness of the contents of such plans and procedures. We advise that during such review the three companies consider together ways to realize horizontal checks of written procedures that are within the scope of MHIR and MHOS, in addition to those within the scope of MHBK.

(4) Business Management and Organizational Control

A. Human Resources Development

MHBK and MHIR shall work on systematic human resources development, conduct periodical drills on both sides, develop skills required for handling multiple failures through simulation experience, and reinforce their effort to systematically hand over know-how on the current systems which requires a long-term maintenance and stable operation within the whole group.

(a) Short-Term Measures

MHBK must promptly prepare risk scenarios in a focused way and must conduct failure response drills in order to enhance human resources development and skills. In particular, test of effectiveness of various improvement measures by drills conducted assuming the reoccurrence of the Failures is essential.

Prior to such drills, joint planning by MHBK and MHIR must be done. Such plans shall specifically include improvements on risk scenarios that must be made to supplement scenarios lacking due to the systems stability in operations over the long term. Such plans shall also include the establishment of desirable structures and roles of management and field levels in responding to failures, and points to be reviewed at drills. Moreover, drills for respective risk scenarios must be held in order to test effectiveness of the contents of the planning. Particularly, drills and testing of effectiveness must be repeated periodically for their sophistication.

After such drills have been conducted and tests on effectiveness have been made, a series of process including review of risk scenarios, determination of drills to be held periodically and on an ad hoc basis as well as establishment and documentation of failure response procedures is required.

(b) Medium to Long-Term Measures

In addition to the short-term efforts listed above, management must acknowledge the medium to long-term viewpoints and reacknowledge the importance of systems department and activate personnel exchanges between MHBK and MHIR. Moreover, by conducting systematic human resources management of not just MHBK but also the whole group, MHBK must develop human resources who are able to conduct management with understanding of the full picture of banking business and systems.

B. Audit

(a) Risk Assessment for MHBK Core Banking System (STEPS)

"Deposits and currencies systems", that are under the scope of IT systems control for the purpose of evaluation of departments and systems, are evaluated as having the second-degree of risk and are subject to audits in 30-month intervals. However, considering the importance of such systems, we advise that such audits be conducted as those for the highest degree risks in a more thorough manner, such as by checking the effectiveness of manuals and referring to similar cases of failures in the past.

After giving appropriate evaluation of effects when the risk events occur, MHBK must review the method of risk assessment by audit department prepared at the time of planning.

(b) Audit System as a Group

We found insufficiency in the audit system as a group for audit of MHIR concerning Core Banking System (STEPS). Therefore, review for enhancement of the audit system of the whole group including the clarification of the role and position of the audit department of MHFG, such as by considering direct audit by audit department of MHFG or increasing the scope of internal audit by MHIR is required.

(c) Utilization of Outside Audit Services

It is understood that MHBK will put its efforts into comprehending potential risks related to Core Banking System (STEPS) and into enhancing points of audit concerning systems such as STEPS. In order to realize this, increasing the skill of personnel in charge of audit and utilization of outside audit services need to be considered.

3. Proposals for Future

Customers' trust for MHBK's systems has been damaged by system failures discussed in this report. Computer systems of major banks are economic infrastructures. Therefore, any damage to such infrastructures has a large effect to their stakeholders including their customers. Not only MHBK but also the whole Mizuho Group must put their greatest efforts into maintenance of such infrastructures and recovery of trust. Fortunately through this investigation, we could see determination of persons concerned at MHBK to restore trust. However, once-damaged trust cannot be easily recovered. From such a viewpoint, the Committee addresses the next two points as our conclusion and proposals for the future.

The first point is continuous implementation of preventive measures.

In response to the large-scale failures in 2002, Mizuho Group established the preventive measures and it was evaluated that these measures had accomplished their initial objectives by 2004. However, Mizuho Group once again caused system failures this time. Although the system failures this time occurred in different situation from that of 2002, if Mizuho Group as an organization paid attention to stable operation of the systems learning from the failures in 2002, Mizuho Group could prevent the system failures this time. Preventive measures will not become meaningful until they are actually implemented and such measures must continuously be implemented over the long term. A long-term, continuous implementation of the preventive measures with maintained determination for recovery of trust is highly desirable.

The second point is prompt realization of system integration.

Currently, MHBK and MHCB are in a same group. However, they operate separate systems as from the time prior to consolidation. However, existence of demerits of such separate systems is clear. Therefore, also from the viewpoint of cost reduction in the long-term as well as improvement of systems, integration of systems in the whole group is desirable. "Mizuho's Transformation Program" issued in May 2010 clearly states promotion of unification of IT and systems in the group. Taking the system trouble discussed in this report as an opportunity, MHBK must carry out thorough preparation for prompt realization of unification as stated in the above program, which would lead to earlier recovery of trust of the customers.

- End -