BOJ
Reports & Research Papers

July 2008

Paper Series on Risk Management in Financial Institutions

Toward Effective Business Continuity Management: A Check list and Instructive Practices

Financial Systems and Bank Examination Department
Bank of Japan

This is an English translation of the Japanese original released in May 2008.

Financial Systems and Bank Examination Department, Bank of Japan
C.P.O. Box 30, Tokyo 103-8660, Japan

For further information about this paper, please contact:

Toru Saito (Mr.) or Haruhisa Oyama (Mr.), Financial Systems and Bank Examination Department, Tel: +81-3-3277-1230, +81-3-3277-2513

【Introduction】

- The Bank of Japan published a paper on sound practice, "Business Continuity Planning at Financial Institutions," in July 2003 in order to identify which issues need to be addressed in developing business continuity management (BCM). Based on the paper, the Bank has since been discussing BCM with financial institutions through on-site examinations and off-site monitoring. Many financial institutions in the process of developing BCM have expressed interest in knowing more specifically how to address each issue mentioned in the paper to establish effective BCM.

- Based on the framework of 2003 paper, this paper summarizes the issues to be discussed in the form of a check list, and presents instructive practices observed among the financial institutions in Japan.

- Given that the magnitude of a disaster and an expected level of recovery could differ, according to each individual financial institution's location and nature of business, there could be various approaches to BCM. In addition, instructive practices presented in this paper range from general to technical. By using this paper for reference, financial institutions could produce responses that would well suit their own circumstances and thereby steadily improve the effectiveness of their BCM.

- Financial Systems and Bank Examination Department of the Bank of Japan looks forward to enhancing its discussion with financial institutions regarding BCM in the hope of increasing the resiliency of Japan's financial and settlement systems in a disaster.

Contents

Toward Effective Business Continuity Management: Check List and Instructive Practices

1. Establishing Framework for Robust Project Management

Issues to be addressed		Observed Practices
(1) Management leadership	➢ Management is aware of the importance of business continuity and must exercise strong leadership.	・ All directors including top management are carrying out their tasks with a keen awareness of the importance of BCM. – BCM is understood to be an institution-wide project and explicitly identified as an important issue in business planning, budgeting, and risk management. ・ A director is put in charge of BCM and is exercising strong and unified leadership in all aspects from formulating basic plans to testing and training. ・ BCM is regularly (e.g., semi-annually) discussed by the board of directors and/or at other meetings.
(2) Basic policy	➢ Basic policy for business continuity is formulated and authorized.	・ Basic policy and major changes in business continuity are subject to approval from the board of directors and/or other meetings.
	➢ The following should be clarified in the basic policy: ▼ Purpose of BCM ▼ How to identify "critical operations" that have priority in business continuity	・The purposes of BCM are defined in view of the financial institution's status and nature of business, while taking the following points into consideration: 1. Preventing widespread payment and settlement disorder (alleviating the impact on the settlement system) 2. Maintaining the economic activities of residents in the disaster areas (alleviating the impact on customers) 3. Reducing managerial risks (alleviating the impact on management) ・ "Critical operations" are identified within the framework which is consistent with the above mentioned purposes.
	➢ Basic policy for BCM is reviewed in light of changes in management planning, social conditions, etc.	・ Taking into consideration changes in social conditions, basic policies for BCM are reviewed whenever business strategies are changed.
(3) Institution-wide control section	➢ Institution-wide control section and/or officer in charge of BCM being assigned.	・ The institution-wide control section and/or officer in charge are/is appointed and taking the role of formulating institution-wide project plans, coordinating departments.
	➢ The institution-wide control section and/or the officer in charge should perform the following functions based on the basic policy:	

	▼ Managing specific work items and schedule to promote BCM	・ In order to manage a institution-wide project, a roadmap and/or a yearly schedule for BCM are/is formulated. ・ In developing specific work plans, staff from the related departments meet frequently (e.g., weekly, bi-weekly) to discuss and consider specific issues of BCM (by establishing Business Continuity Committee, etc.). ・ Work items and progress are documented and managed in the form of lists to show the progress in each task at a glance.
	▼ Assigning tasks to individual departments and coordinating departments	・ The contents of plans formulated by individual departments are reviewed to eliminate redundancy and oversight. Coordination between the related departments about the mutually linked issues is conducted regularly (e.g., once a year).
	▼ Making progress reports to management	・ Progress reports are given to the board of directors and/or at other meetings regularly (e.g., semi-annually) or at important junctures in the work schedule.
	▼ Institution-wide information sharing and educational activities	・ The intra-firm electronic bulletin board has a dedicated portal for BCM. ・ BCM is taken up in employee training and/or e-learning programs.

2. Formulating Business Continuity Plan (BCP)

Issues to be addressed		Observed practices
(1) Assumptions and conditions	➢ As a precondition for BCP, the following measures are rationally carried out on the basis of importance and circumstances of each operation.	
	▼ Construct disaster scenarios that will jeopardize business continuity	・ Potential threats (causes) to the institution are identified and scenarios for serious risks are constructed based on the probability of the risks to manifest themselves and associated effects. ・ Disaster scenarios are also categorized according to estimated damage (resulting phenomena) to management resources such as staff, equipment, and workplaces.
	▼ Identify "critical operations"	・ "Critical operations" are determined, reflecting business profile and business strategy, based on the assumption that managerial resources will be substantially constrained at a time of disaster. — For example, cash payments, acceptance of funds transfer requests, processing of large-amount and/or high-volume settlements could be the candidates of "critical operations". — Given greater constraints on managerial resources available to recover operations within the recovery time objectives under certain disaster scenarios (e.g., large-scale disaster, pandemic), critical operations are prioritized and narrowed down to a few operations consistent with secured managerial resources.
	▼ Set recovery time objectives for "critical operations"	・ Recovery time objectives are set for all "critical operations," based on the maximum allowable downtime. — It is taken into consideration that recovery time objectives could differ depending on when operations are disrupted. — Recovery time objectives for critical financial settlement functions, including processing of large-amount and/or high-volume settlements through inter-bank settlement systems and/or in the money markets, are set at "within 4 hours," "within same day," etc.

	▼ Identify operational flows, departments in charge and external parties for "critical operations"	・ Operational flows are established for each "critical operation," and the related departments (including external parties) and related systems (including outsourced systems) are scrutinized without exception. ・ Detailed duties for emergencies are clearly assigned to the related departments.
	▼ Identify the volume of "critical operations"	・ The volume of "critical operations" is estimated, including that for the peak-day and peak-hour operations. — For operations to be transferred to other financial institutions, feasibility is studied and reduction in workload is estimated.
(2) Formulating BCP	➢ BCP is formulated, based on the above assumptions.	・ BCP is formulated, based on the basic policy and assumptions, and is formally adopted.
	➢ The BCPs of "important external parties" are checked and consistency with the institution's own BCP is reviewed.	・Check BCPs of "important external parties" such as payment and settlement institutions, service providers, and major counterparties, which are indispensable for recovering operations, and ensured the consistency with the institution's own BCP. The factors requiring improvement are identified and addressed in revising the existing plans.
	➢ BCP is reviewed as necessary.	・ Arrangements are made for BCP to be reviewed promptly in case the assumptions have changed, such as potential threats from new risks have heightened, new operations and systems have launched, etc. ・BCP is reviewed on a regular basis(e.g., annually), even when nothing has changed in the assumptions.
	➢ Effectiveness of BCP is checked by a third party other than the institution-wide control section.	・ Independent organizations such as internal auditors check the effectiveness of BCP, testing/training programs, testing/training results, and review of the existing plans. — Audit cover not only IT system departments but also operation departments.

3. Securing Managerial Resources

Issues to be addressed		Observed practices
(1) Overall managerial resources	➢ Managerial resources are estimated and secured properly for each of the following categories, in order to recover “critical operations” within “ recovery time objectives”:	・ Specific measures for the plan, such as manual processing, back-up systems, etc. are adopted in light of workload at the peak time and consistent with recovery time objectives. ・ BCM takes account of the availability of public infrastructure (electric power supply, water supply, transportation, telecommunications, etc.) in an emergency by conducting interviews, etc., and the BCP is formulated in a consistent manner.
	▼ Business continuity staffer	・ The number of staffers necessary to come to work for recovering “critical operations” is estimated and checked whether it is consistent with the expected number of staffers able to come to work in a disaster. — The availability of alternative access routes and means of transport is examined to cope with traffic breakdowns (e.g. by checking the number of staff able to come to work on foot, disseminate a route map of foot traffic, arranging for motorcycles, establishing dual operation systems [parallel operations at multiple locations]). – Staffers come to work in sequence consistent with the recovery time objective for each “critical operation”. ・ A plan is prepared to assemble and allocate skilled staffers appropriately for each “critical operation.” Each staffer is formally informed of his/her assignments. – The number of staffers available for each department is checked. To prepare for possible staff shortages, staffers are trained to work in different departments by cross-training programs etc. ・ Staffers who are needed to operate indispensable equipment to recover “critical operations” (particularly those in IT systems, general affairs and administration departments) , are also assigned. ・ On the assumption of assigning temp staff as business continuity staffer, employment contracts are reviewed to avoid any legal constraint (availability for overtime work, restrictions to the workplace, type of work, etc.). ・ Action guidelines for staff other than business continuity staffer are also set out (the means for returning home, standing-by at home, etc.).

	▼ Workplace	・ Work places such as back-up offices are prepared at locations that will be immune from the disaster affecting the main office. — For operations that need physical delivery to counterparties, temporary counters are secured at locations where delivery operations can take place. ・ Sufficient back-up office space is secured, based on the number of staffers and equipment needed to process “critical operations.” ・ Certain branches are designated for prioritized recovery. Facilities and equipment in these branches are deployed with priority.
	▼ Equipment, office items, supplies, etc.	・ Equipment, office items, and supplies needed for “critical operations” is stockpiled. — Equipment, including desks, chairs, telephones, fax machines, PC (terminals), power supply, etc. is stockpiled. — Concerning emergency power (including fuel for in-house power generation), equipment coolants, and other supplies (food, drinking water, necessities, medicines, etc.), the minimum volume of stockpile is prepared to cover three days of “critical operations”. ・ Explicit agreements are made with vendors to secure supply of goods and services in a time of disaster, and it is confirmed that those agreements are included in vendors’ BCPs.
(2) Off-site back-up systems	➢ Back-up system is in place at locations other than main centers, if it is difficult or impossible to recover “critical operations” by manual processing.	・ Off-site back-up systems, which are set up in back-up centers and other facilities located at a safe distance from main centers, are established for “critical operations”, except for operations that can be substituted with other systems or manual processing. — For operations planned to be substituted with manual processing etc, it is verified that alternative means has enough capacity to process the volume during peak time. ・ Under disaster scenarios, off-site back-up systems are established in locations that will not be affected simultaneously by a disaster hitting the main centers.

	➢ Off-site back-up system capacity is sufficient to process “critical operations.”	・ The capacity of off-site back-up systems is verified to perform “critical operations” during peak times, taking into account the difference in system configuration and performance between back-up systems and normal operating systems. ・ In case off-site back-up systems are shared with other firms, the above verification is done on the assumption of minimum access to back-up systems, taking into account the possibility that the systems might be used simultaneously with other firms (other users might suffer simultaneously in case of a large-scale disaster).
	➢ Time required for switch-over to off-site back-up systems is consistent with recovery time objective of “critical operations.”	・ The total time required for switch-over to off-site back-up systems is estimated for each system based on necessary steps after the disruption, such as emergency contacts, staff assembly, decision making for switch-over, switch-over operations (starting-up the system, uploading back-up data, etc.), data updating (data correction to resume operations by inputting the lost data into IT systems), etc. — Concerning data updating, the procedures are clearly documented with estimates of required time after deciding when to resume the related operations (whether to resume operations before or after updating the data of unsettled transactions). ・ In case the operation of off-site back-up systems is outsourced, the information about the above time requirements and assignment of duties is shared with outsourced providers.
(3) Back-up data and programs	➢ Back-up data and programs, which are needed to resume “critical operations,” are in place and maintained to prepare for the case of data and/or programs loss.	
	▼ Location of back-up data and/or programs	・Under given disaster scenarios, back-up data and/or programs are kept at locations that will not be simultaneously affected by a disaster hitting the main centers.
	▼ Secure measures to recover data and/or programs	・ Necessary equipment (system devices, etc.) is in place to ensure the prompt use of back-up data and/or programs for the recovery of “critical operations”.

	▼ Appropriateness concerning transmitting transaction records to a back-up system and time required for data transfer	・ The frequency of transmitting transaction records to a back-up system (which affects time needed for data updating) and the location of back-up data (which affects time needed for data transferring) are checked to be consistent with recovery time objectives. ・ In case back-up data are planned to be transferred to the recovery site at a time of disaster, the effectiveness of the means of transfer is checked against given disaster scenarios.
(4)Manual processing	➢ Scope of operations that must be covered by manual processing in a time of disaster is determined, and necessary managerial resources and operating procedures are in place	・ The following manual processings are identified to occur during the disruptions of main computer centers, and necessary countermeasures are in place. 1. Manual processing, which has to start before the completion of switch-over to off-site back-up systems due to operational time requirements 2. Manual processing in the process of system switch-over (input and collation of additional transaction records generated after transmitting to a back-up system) 3. Manual processing for operations which do not deploy off-site back-up systems

4. Establishing Decision-Making Procedures and Communication Arrangements

Issues to be addressed		Observed practices
(1)Decision-making procedures	➢ In order to activate BCP, the following points are clarified:	
	▼ Trigger points to activate BCP	・ Trigger points to activate BCP are established to ensure prompt and objective decision making in an emergency. ・ Reporting lines from related departments to crisis management office are established to provide information necessary to decide on the activation of BCP, and means of communication usable in a disaster are also prepared.
	▼ Criteria for switch-over to off-site back-up systems	・ The following factors are taken into consideration to establish criteria for the switch-over to off-site back-up systems: – Not only IT systems but also business operations need to switch over to back-up facilities – After recovery, considerable time is necessary to switch back to normal systems.
	▼ Authorized person to order the activation of BCP ▼ Authorized person to order the switch-over to off-site back-up systems	・ Decision-making persons are clearly assigned, and procedures are formulated for prompt and appropriate decision making at a time of emergency.
	➢ Following measures are taken for decision-making procedures and command structure:	
	▼ Secure location for crisis management office to function effectively under various disaster scenarios	・ The crisis management office is planned to be set at locations where the members of the crisis management team (including persons with decision-making authority) are accessible. The means of communication to contact with internal and external parties under given disaster scenarios are prepared in each crisis management office. — Several locations are secured in advance and will be used alternatively depending on the damage.
	▼ Establish rules for prompt authority delegation in case management and persons in charge at individual departments cannot be reached.	・ Explicit rules are documented for the delegation of authority, and the decision-making process is formulated for various types of disaster scenarios.

(2) Emergency communication	➢ Following measures are taken for internal and external communication in case of emergency:	
	▼ Prepare internal emergency communication measures	・ Internal emergency contact lists are prepared and are updated upon personnel rotation. — Emergency contact lists for nighttime and/or holiday and email address lists are also prepared.
	▼ Identify “important external parties” and their contact staff ▼ Identify contact staff when “important external parties” activate their BCPs.	・ Lists are prepared with respect to the relevant parties to be contacted and information to be exchanged in an emergency. — Rules for communication between overseas offices and local relevant parties are also formulated. ・ Lists are prepared with respect to “important external parties” including back-up sites and nighttime and/or holiday contacts, and are updated whenever any changes occur. — Access is ensured to the dedicated BCP website shared within the industry, and the contents of the website are referred.
	▼ Prepare several means of emergency communication	・ The following multiple emergency means of communication are prepared in case public infrastructure and communications are disrupted: — Priority telephone service, the employee safety confirmation system, satellite telephones, wireless, telephone and video conferencing systems, etc. — Functions and limitations of various means of communication are recognized.
	➢ Establish rules for public information and media when BCP is activated	・ Response rules (coverage of notification, criteria and persons for press conferences, etc.) are documented for various disaster scenarios. ・ Sample public announcements are drafted and prepared for immediate uploading on the website, etc. ・ Sample announcements for customers are drafted and prepared for immediate posting at branches and offices.

5. Compiling Manuals

Issues to be addressed		Observed practices
(1)Compilation	➢ Easily understandable manuals on operational procedures are compiled at each department.	・ Manuals describing specific procedures of each “critical operation” and IT system switch-over are compiled — Manuals describe detailed procedures about manual processing in a time of disaster, which used to be automatically processed by IT systems under normal conditions. — Manuals are checked to maintain consistency in cross-departmental operations (including operations with external parties).
	➢ Each manual is comprehensive and consistent from an institution-wide perspective.	・ Departments responsible for compiling and keeping manuals are determined so as to cover all the departments that are planned to process “critical operations” (including responsibility-sharing for cross-departmental operations). ・ Regarding cross-departmental operations, consistency of manuals between departments is ensured by being checked from an institution-wide perspective and by being prompted to revise if necessary.
(2)Ensuring effectiveness	➢ Manuals are updated at all times.	・ Manuals are kept in a manner to enable immediate access and use in case of disaster. ・ Manuals are promptly revised when changes are made in the flow of operations, organizational structure, etc.
	➢ Contents of manuals should be thoroughly familiarized by concerned staff.	・ Persons in charge of operations are thoroughly familiar with the contents of manuals, and all the related persons participate in trainings and other activities.

6. Testing/training and Reviewing

Issues to be addressed		Observed practices
(1) Testing/ training program	➢ Institution-wide control section and/or officer in charge plan effective testing/training programs, taking into account the development level of the institution's own BCP.	・ The institution-wide control section (and/or the officer in charge) develops testing/training programs for the priority issues (purpose, content, etc.) in BCM from a institution-wide perspective, based on the level of development of the institution's own BCP. —Under realistic scenarios, testing/training programs cover decision-making and communication, evacuation, relocation, back-up equipment start up, back-up center switch over, manual operation, walk-through (an exercise to check the entire operational process), etc.. — Testing/training programs are formulated from two different perspectives: to test the effectiveness of BCP and to improve business continuity staffer's level of proficiency with BCP.
	▼ Secure completeness of operations and departments that are subject to testing/training	・ Institution-wide exercises are conducted on a regular basis (e.g., once a year or more). ・ Every "critical operation" is covered by testing/training programs with different frequency depending on the importance of the operations (e.g., testing/training for the most critical operations are conducted 2 – 3 times per year).
	▼ Contents of testing/training programs vary according to the purpose of testing/training and proficiency level of BCP staff	・ In order to gradually improve the level of testing/training, the contents of testing/training programs and roles played by participants are frequently revised. — "Surprise tests" and "scenario-blind exercise" are effectively programmed and carried out depending on the type of testing/training.
(2)Conducting testing/ training	➢ Institution-wide drills are conducted on a regular basis.	・ The participants of institution-wide exercises cover a wide range of departments and sections related to business continuity (including branch offices, outsourced providers, affiliated group companies, etc). ・ Coordination between settlement system operators is also checked. — Always participate in the tests hosted by settlement system operators.
	➢ Testing/training cover all necessary procedures to recover all "critical operations".	

	▼ Check communication arrangements	・ Conducting tests of employee safety confirmation using emergency contact lists, as well as tests of reporting to the crisis management office. ・ A means of emergency communications are regularly tested (e.g., twice a year) to confirm its connection.
	▼ Set-up crisis management office and decision-making of activation of BCP	・ The members of crisis management offices are assembled to conduct decision-making exercises related to critical decisions on BCP (activations of BCP, start-up of back-up office, switch-over to back-up system). — Training exercises are also conducted for alternative staff.
	▼ Relocation to back-up offices and start up back-up equipment	・ Periodic training is conducted (e.g., twice a year) for the relocation of business continuity staffer to back-up offices and the use of communication means, terminals, documents, manuals, etc.
	▼ Switch over to off-site back-up systems	・A series of processes and operations required for switch over to off-site back-up systems (staff relocation, systems start up, uploading of back-up data, data updating, etc.) are conducted in a run-through manner with participants from user departments. ・ Actual IT systems have been used in tests as much as possible. — When the actually running systems cannot be used in tests, stand-by and testing systems are used. ・ Switch-over tests include delivery and uploading of back-up data being kept at remote sites, and confirmation of start up using back-up data. ・ Tests for data updating include identification and inputting of unsettled transaction data being damaged during transfer, and reprocessing and inputting of transaction data settled by manual operations.

(3) Analysis and report on results	➢ Results of test/training are analyzed, and feasibility of BCP and effectiveness of manuals is verified.	・ Whether recovery time objectives can be achieved for all "critical operations" are verified. — "Actual time required for recovery" is measured by taking into account that there are possible constraints on managerial resources (equipment capacity, staff, etc.) at a time of disaster. ・ After conducting tests, the findings are analyzed to specify the reasons why recovery time objectives cannot be achieved for certain operations. — The adequacy of facilities and equipment installed in back-up offices and back-up centers is also verified. ・ Manuals are verified by checking whether BCP could be conducted as planned by operational procedures described in manuals.
	➢ Test/training results and their analysis are reported to management.	・ The verification and analysis results of institution-wide exercises are reported to the board of directors and/or at other meetings whenever exercises are conducted. ・ The institution-wide control section is informed of testing/training conducted by individual departments and maintains the summaries of records and results. ・ The effectiveness of BCP is discussed by board of directors and/or at other meetings, and the measures for improvement of BCP are determined at the management level.
(4) Review of BCP	➢ Test/training results and their analysis are utilized to review BCP and manuals.	・ BCP and manuals are reviewed, based on the testing/training results and their analysis.

(Reference) Papers released by the Bank of Japan concerning business continuity planning at financial institutions:

—— All papers are posted on the Bank of Japan website (http://www.boj.or.jp/) under “Business Continuity Planning.”

- “Kinyuukikan no Kyoten-hisai wo Soutei shita Gyoumukeizoku-keikaku no Arikata [Business Continuity Plans for Site Disruption of Financial Institutions]”, March 12, 2002. (In Japanese)

- “Kinkyuuji niokeru Gyoumukeizoku Fukkyuutaisei nikansuru Ankeito-chousa Kekka nitsuite [Questionnaire Survey on Business Continuity and Contingency Plans for Emergencies]”, February 6, 2003. (In Japanese)

- “Business Continuity Planning at Financial Institutions”, July 25, 2003:

- “Kinyuukikan niokeru Gyoumukeizsoku-taisei no Koudoka nimukete [Enhancement of Business Continuity Management of Financial Institutions]”, Advanced Financial Technology Seminar, September 20, 2006. (In Japanese)

- “Questionnaire Survey on Business Continuity Management (December 2006)”, July 27, 2007

- “Kinyuukikan niokeru Shingata Influenza Taisaku no Seibi nitsuite — Naigai Kinyuukikan no Torikumi-jirei no Shokai [The Pandemic Planning at Financial Institutions – Introduction of practices both foreign and domestic Financial Institutions]”, March 17, 2008. (In Japanese)