Business Continuity Planning at Financial Institutions

July 2003

Bank of Japan

Table of Contents

Introduction

Financial institutions could face the suspension of critical operations due to natural disasters, terrorist attacks, computer problems, and other causes and hence need to secure business continuity by formulating action plans in advance to ensure quick recovery. The events of September 11 in the US demonstrated the need for such robust business continuity in many countries. This holds true for Japan which has been subject to many natural disasters, including earthquakes and typhoons, and also computer problems at financial institutions in recent years.

Most Japanese financial institutions have some form of business continuity plan in place. However, those plans still focus mainly on individual operating systems or facilities. Thus, the events of September 11 have prompted financial institutions to strengthen their business continuity so that they can cope with even larger scale disruption than previously planned for.

This paper delineates ‘sound practice’ in terms of business continuity planning at financial institutions. It should be noted at the start that individual financial institutions might be impacted differently depending on their location and nature of their business, and hence there could be various approaches to business continuity planning. It should also be noted that implementation issues are still being debated, and that practical methods are evolving. Therefore, it is desirable for financial institutions themselves to design their own management framework that addresses their own particular risk profile, and to review such framework on an ongoing basis. The Bank of Japan (the Bank) will promote discussion with financial institutions regarding business continuity planning.

Section 1 gives the Bank's basic view of business continuity planning and Section 2 details more specific and practical aspects such as how planning could be accomplished.

1 The Bank’ s View of Business Continuity Planning

1) Significance of business continuity planning

Business continuity planning at financial institutions is deemed essential for the following three reasons:

(1) Maintaining the economic activity of residents in disaster areas

Business continuity planning enables the continuation of minimum but indispensable financial services during and after disasters, thereby contributing to sustaining economic activity in a disaster area.

The suspension of financial institution operations causes critical problems during and after disasters. For example, residents in a disaster area might not be able to withdraw funds, and insufficient cash on hand would prevent them from purchasing food and other necessities. Likewise, funds could not be deposited to accounts or transferred between financial institutions, preventing residents from receiving pension and salary payments or making payments to remote areas. Thus, financial institution operations are deeply intertwined with economic activity, and financial institutions should endeavor to continue business even in a disaster situation.

(2) Preventing widespread payment and settlement disorder

Business continuity planning could prevent possible defaults at individual financial institution caused by disasters, thereby serving to restrain widespread payment and settlement disorder. Payment and settlement services are at the foundation of economic activity and form a linked chain throughout society, with funds received as a counter value for one transaction used to pay for another. Thus, the inability of financial institutions in a disaster area to effect payments could see default extending beyond the area directly affected with the potential to disrupt economic activity nationwide. Business continuity planning at financial institutions helps to mitigate such systemic risks.

(3) Reducing managerial risks

In addition to the points above, business continuity planning enables financial institutions to mitigate managerial risks.

The prolonged suspension of operations in a disaster situation makes it difficult for financial institutions to take profit opportunities, lowers their reputation among customers, and ultimately has a detrimental impact on their management. Therefore, business continuity planning is necessary in terms of mitigating these risks.

2) Key points in business continuity planning

The above three points suggest financial institutions should have adequate business continuity plans in place. The Bank has developed business continuity plans, and it is indispensable for both financial institutions and the Bank to coordinate their efforts in the interest of strengthening the resilience of the entire financial system. From discussions with financial institutions and its own experiences, the Bank has identified five critical points:

(1) Planning, testing, and reviewing

Concrete plans should be formulated so that business can continue smoothly in the event of a disruption. Attempting to do everything right from the beginning could cause the formulation process to falter. It is more effective to start with minimal plans that can respond appropriately to a suspension of key business functions such as data centers or priority locations, and then to gradually expand to cover other operations later (phased-in approach).

Plans should be regularly tested and reviewed, if necessary, to ensure that they are practical and feasible.

(2) Focusing on critical operations

Disasters result in limited access to managerial resources under severe time constraints. Business continuity planning must therefore focus on prioritized critical operations to be continued in the event of a disruption.

Financial institutions should themselves determine what constitute critical operations according to their own business profile and management strategy. Many consider the following to be of high priority: a) cash payments to customers and acceptance of funds transfer requests, and b) large amount and high volume payment processing over the payment and settlement system.

(3) Considering special circumstances under large scale disruptions

Financial institutions have many options for responding to disruptions and providing for business continuity, including switching over to back-up facilities, moving to manual processing, or entrusting operations to other institutions. Assuming the possibility of large scale disruptions such as the events of September 11, financial institutions should take into consideration the following when they study options:

i) Avoid geographical concentration of main operational offices, data centers, and back-up facilities so as to reduce risk of simultaneous damage.
ii) Be aware of the possibility that traffic suspension and other disruptions could prevent necessary staff from moving to back-up facilities.

iii) Understand that joint back-up facilities could be competed for in terms of user requests.
iv) The possibility of staff fatigue and ensuring adequate supplies because emergency conditions could continue for a prolonged period of time.
v) Diversifying communication methods because ordinary telecommunications may be suspended or severely restricted.

(4) Coordinating business continuity planning with outside parties

The operations of financial institutions are deeply intertwined. It is thus desirable that institutions coordinate with other market participants, payment and settlement system operators, and outside service providers in order to increase the effectiveness of their own business continuity planning. Such coordination ultimately strengthens the resilience of the entire financial system. It is important in this context to mutually disclose information regarding business continuity plan status and contact points in an emergency within predefined limits and with adequate information security.

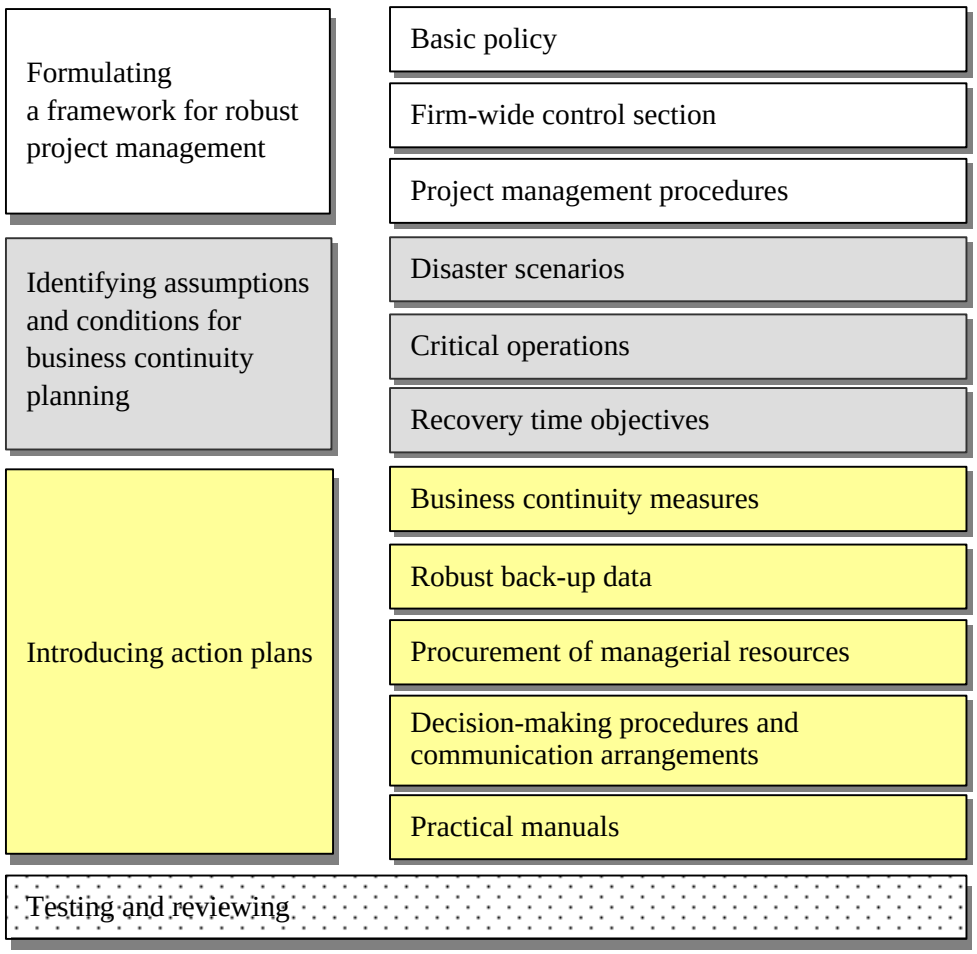
(5) Exerting strong leadership

Business continuity planning is a major project that requires the substantial investment of managerial resources and a firm-wide awareness. Management needs to exert strong leadership and to become deeply involved in the process.

2 Practical Aspects of Business Continuity Planning

The process outlined in the chart below may be followed by financial institutions in formulating business continuity planning. This section considers the practical aspects of each step.*

Chart: Process of Business Continuity Planning



* This paper focuses on aspects related to business operation. Other aspects such as announcements to the press and disseminating information to customers are also essential.

1) Formulating a framework for robust project management

(1) Basic policy

Financial institution management should develop basic policy and guidelines for business continuity planning and provide details organization-wide. These documents should clearly state the need for business continuity planning, the concepts to be used in identifying critical operations, and the executive officer in charge of initiating the plans. This formulation encourages the organization to become more aware of the need for crisis management and to implement subsequent work more efficiently.

(2) Firm-wide control section

Business continuity planning requires financial institutions to study firm-wide aspects. From this point of view, it is desirable that a firm-wide control section is designated and/or officer in charge appointed. The section is responsible for formulating specific work procedures, assigning work to individual departments, and coordinating among departments based on the policy and guidelines. In addition, the section could plan and carry out testing programs after the plans are set up, and conduct regular review thereafter.

(3) Project management procedures

Business continuity planning is an extremely difficult project that involves a large number of interested parties. This difficulty requires financial institutions to implement appropriate progress control, including reports to top management. Specifically, financial institutions must have a mechanism by which the firm-wide control section can monitor work progress and report to management so that they make decisions in a timely and flexible manner on additional resources and work priorities.

2) Identifying assumptions and conditions for business continuity planning

(1) Disaster scenarios

i) Recognition of potential threats

Following are types of disasters that could pose threats to financial institution operations: a) natural disasters such as earthquakes and typhoons, b) man-made disasters such as terrorism and computer crime, and c) technical disasters such as power outages and computer problems. Individual financial institutions need to identify potential threats, given circumstances such as the location and nature of their business.

ii) Analysis of frequency and severity

The next step is to analyze the frequency of potential threats that could emerge as well as the severity should they emerge. This analysis specifically refers to assuming the extent of the damage to offices and data centers caused by disasters, and considering how the operations of financial institutions could be suspended as a result. It is also necessary to evaluate the consequent damage stemming from such events as ATM failure, payment delays, and funding difficulties. In this analysis, financial institutions should also consider the impact on their customers and other financial institutions.

iii) Identification of material risks and damage scenarios

Having analyzed potential threats and their severity, financial institutions should identify specific scenarios with material risks. Business continuity planning should be developed based on these specific scenarios.

The following scenarios are shown as examples: a) stoppage of computer systems due to a disaster which strikes the data center, b) loss of head office functions due to a disaster which strikes the head office, and c) simultaneous suspension of operations at multiple locations due to a major earthquake.

(2) Critical operations

Disasters result in limited access to managerial resources under severe time constraints. Therefore, in the event of a disruption, financial institutions should focus on continuing prioritized critical operations.

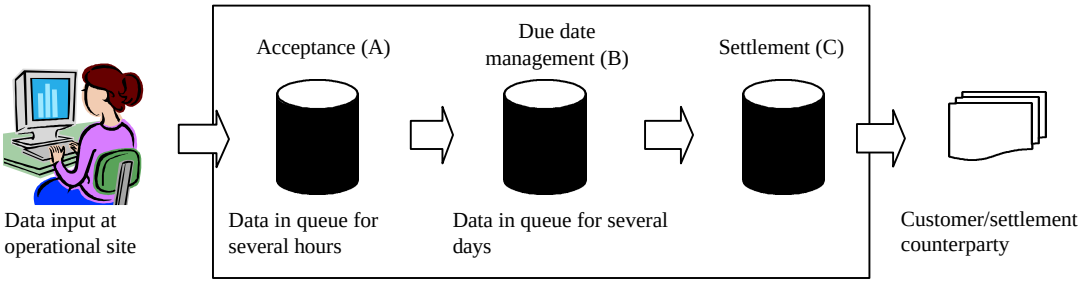
A survey conducted by the Bank Examination and Surveillance Department of the Bank indicates that many financial institutions consider the following examples as critical operations: a) cash payments to customers and acceptance of funds transfer requests, and b) large amount and high volume payment processing over the payment and settlement system.

Extra attention is needed in the handling of ‘unsettled transactions’ when prioritizing the operations above (see Box 1).

Box 1: Unsettled Transactions

'Unsettled transactions' refers to transactions that have been accepted but where processing has not been completed at a certain point in time. When computer systems fail and operation is resumed manually, it is necessary to determine whether individual transactions should be reprocessed. Otherwise, insufficient manual operations could increase the risk of double processing or failure to process.

'Unsettled transactions' easily occur when several system processes must be completed, as illustrated below. For example, an operator accepts a transaction for processing (A), manages due dates (B), and effects settlement (C). Unless the data is transferred among processes instantaneously, there is the potential for an 'unsettled transaction' to occur.



Note: This is a simplified schematic of actual processing.

(3) Recovery time objectives

Based on the necessity of operations, financial institutions set target times for the resumption of operations by provisional means such as processing at a back-up center. These targets need to include estimates of the time required to a) switch to back-up systems, b) correct data needed for on-line resumption, and c) move staff.

For reference, major financial institutions in leading countries generally plan to resume critical operations such as large amount and high volume settlements within two to four hours assuming that 'main facility functions are suspended, but transportation and other infrastructure are available and there is no human damage.'

3) Introducing action plans

(1) Business continuity measures

The next step is to study specific measures for the plan based on determined assumptions and conditions for business continuity planning. These measures should take account of the volume of clerical processing involved, the time required per transaction, and due date times for completing operations on the day of disaster. Based

on this study, financial institutions determine whether back-up facilities should be used, whether manual processing is required, or whether additional staff are needed.

(2) Robust back-up data

Regardless of the means by which operations continue, data recorded before a disaster is indispensable for quickly resuming operations. This requires a mechanism for acquiring and maintaining data back-ups. Financial institutions must identify the information required to resume critical operations, for example, raw transaction data, ledger update data, balance sheet data, and uncompleted transaction details. Then, they must acquire and maintain this back-up data in electronic or paper form.

Particularly important back-up data is generally transported by magnetic tape or transmitted by telecommunication lines to remote storage locations. In this case, however, it is critical to ensure that back-up data can be easily obtained during times of disaster. Some financial institutions maintain back-up data in back-up facilities, and others have printers specifically for data output installed in their operational centers or head office payment and settlement departments.

(3) Procurement of managerial resources

i) Managerial resources

Financial institutions determine the processing capacity required for continuity of critical operations regarding staffing, computer capacity, and telecommunication capacity. To meet this requirement, they provide adequate resources such as staff, IT equipment, and telecommunication lines.

ii) Public infrastructure availability

Operations are conducted based on the assumption that electricity, gas, water, transportation, telecommunications, and other public infrastructure can be used. Thus, business continuity planning should take account of the availability of infrastructure in an emergency.

(4) Decision-making procedures and communication arrangements

i) Decision-making procedures and command structure

Disasters impose strong time constraints on emergency decisions. Thus, financial institutions need to predetermine decision-making procedures and command and reporting lines. Currently, in many financial institutions, management has to confirm a state of emergency and then establish a ‘crisis management team’ or other disaster management organization headed by a designated executive in head office (or an alternative location if the head office must be evacuated). In most cases, their functions tend to be centralized to collect information and make decisions.

It may not be possible to contact top management or department heads in the event of large scale disruption. Thus, it is desirable that financial institutions have management systems that ensure the smooth delegation of authority in such a situation.

ii) Emergency contact lists and emergency communication means

Communication among responsible parties is essential to initiate an appropriate response to disasters. Financial institutions must have emergency contact lists and provide emergency means of communication. It is highly likely, however, that fixed line telephones, facsimiles, and mobile telephones may be suspended or subject to restrictions in the event of large scale disruption. Therefore, it is desirable to prepare several different means of communication (see Box 2). On September 11, e-mail and mobile wireless proved particularly effective.

Box 2: Emergency Means of Communication Used by Financial Institutions

1. Fixed line telephone/facsimile
2. Mobile telephone/PHS
3. E-mail (Internet mail, mobile mail)
4. Priority telephone service for use in emergencies
5. Direct hotlines
6. Wireless (mobile wireless, disaster wireless)
7. Satellite telephone
8. Telephone conferencing system
9. Video conferencing system
10. Internal broadcasting system
11. Employee safety confirmation system (uses telephone or e-mail)
12. Internal notification and automated broadcasting system to all employee homes or other registered telephone numbers (uses telephone, facsimile, and/or e-mail)
13. An emergency Web site employees can access from outside

(5) Practical manuals

Formulating practical and easily understood manuals regarding operational procedures for each department level is an effective way of ensuring the feasibility of business continuity planning. Some financial institutions store copies of manuals of other related departments for better coordination among related departments.

4) Testing and reviewing

Implementation of testing/training programs on a regular basis is essential to ensure the feasibility of business continuity planning. It is desirable to conduct testing/training programs at least annually. Testing/training indicates whether recovery time objectives can be achieved, identifies challenges, and enables financial institutions to review the adequacy of equipment that is used only in the event of a disruption.

There are various testing/training programs (see Box 3). For example, it may be difficult to conduct testing/training in which all relevant departments participate. In this situation, testing/training could be limited to specific points to be verified or a specific range of participants. It is also worth considering testing/training programs with outside parties with which the financial institution exchanges a large volume of data. As reference, the Bank holds annual testing/training sessions for BOJ-NET participants, including those with CPU connections, in order to confirm switch over to the BOJ-NET back-up center.

Box 3: Examples of Testing/Training Program

a) Communications system testing/staff movement training

Type	Description
• Decision-making and communications system	• 'Crisis management team' or other risk management organization formed, communications procedures verified and learned.
• Evacuation	• Procedures for evacuating from buildings verified and learned assuming bomb threat or fire.
• Relocation	• Procedures for moving staff from main facilities to back-up facilities verified and learned. Relocation procedures when public transportation is unavailable (walking or cycling from home) verified and learned.

b) System operation testing/business operation training

Type	Description
• Back-up equipment start up	• Start-up procedures for back-up computers and equipment not normally used verified and learned.
• Back-up center switch over	• Procedures for switching from main center to back-up center verified and learned.
• Manual operation	• Operational procedures for system failure and telephone network failure (manually written document transactions and provisional payments, etc.) verified and learned.
• Rotation	• Operational procedures including terminal input verified and learned during a full day of actual work at back-up facilities.

5) Other issues

(1) Precluding and mitigating disaster damage

Many disaster risks and damage could be prevented or mitigated through prior measures to some extent. Therefore, financial institutions need to take steps to prevent risks from materializing, in conjunction with the introduction of business continuity planning. Examples of efforts seen at financial institutions are as follows: establishing facilities at or moving them to relatively low-disaster risk locations, anti-seismic retrofitting, installation of back-up generators, enhancement of access control to restricted areas, and strengthening of firewalls to prevent hacker attacks.

(2) Location of back-up facilities

It is desirable to choose a back-up facility location that is far enough to avoid being affected by any disaster which could threaten the main facility. Otherwise, it might be subject to the same disaster. It is particularly important that back-up facilities do not share telecommunication lines or electric power supply routes with main facilities.

Likewise, it is also necessary to take account of staffing requirements when locating back-up facilities. This is particularly the case where plans call for main facility staff to move to the back-up facility. Institutions should examine the feasibility of plans in the event of a large scale disruption.

(3) Use of outside service providers

Financial institutions could provide their own back-up facilities or rely on outside service providers. Many providing their own facilities utilize not only traditional methods such as dedicated facilities, neighboring locations, and other operational centers, but also others such as having some staff work at home so that enough space can be secured for emergency staff. Financial institutions depending on outside service providers sign contracts for emergency facilities with service providers, and/or entrust operations to their affiliates or other financial institutions.

When using outside service providers, financial institutions should be aware of the need to obtain sufficient information from the service provider regarding the potential for competition with other customers. In fact, on September 11, it was reported that there was excessive demand for the facilities of outside service providers.