



# **BOJ** *Reports & Research Papers*

April 2011

Paper Series on Risk Management in Financial Institutions

## Questionnaire Survey on Business Continuity Management (November 2010)

Financial Systems and Bank Examination Department

Bank of Japan

This is an abridged English translation of the Japanese original released in February 2011.

Please contact the Financial Systems and Bank Examination Department in advance to request permission when reproducing or copying the content of this report for commercial purposes.

**[Contents]**

<b>Introduction</b>	<b>1</b>
<b>Survey coverage</b>	<b>1</b>
<b>Overview of survey findings</b>	<b>2</b>
<b>Survey findings</b>	
<b>I. Overview</b>	<b>3</b>
<b>II. Organizational status</b>	<b>6</b>
<b>III. Formulation of business continuity plan</b>	<b>7</b>
<b>IV. Securing business resources, etc.</b>	<b>12</b>
<b>V. Status of decision-making and communication systems</b>	<b>19</b>
<b>VI. Formulation of manuals</b>	<b>20</b>
<b>VII. Training and review of plans</b>	<b>21</b>
<b>VIII. Response to outbreaks of new strains of influenza and other infectious diseases</b>	<b>26</b>
<b>Toward the further enhancements of business continuity management</b>	<b>29</b>

(Address inquiries concerning this paper to)

System Risk and Business Continuity Group, Examination Planning Division, Financial Systems and Bank Examination  
Department, Bank of Japan

Noriyuki Tomioka, Takayuki Okamoto, Takehisa Kanaguchi, E-mail: csrbcm@boj.or.jp

## Introduction

This paper summarizes the findings of the "Questionnaire Survey on Business Continuity Management" (2010 survey) conducted from October to November 2010.

This survey has been conducted every other year since 2002 for financial institutions with high shares by transaction value on BOJ Net. Survey questions were formulated with reference to the basic practices of financial institutions contained in "Toward Effective Business Continuity Management: A Check List and Instructive Practices" (revised and expanded edition) published in March 2010<sup>1</sup>.

The Bank of Japan expects financial institutions to refer to the survey findings as they review their own business continuity management and to take steps to improve their effectiveness. It also hopes that the survey will add further depth to discussions of business continuity management with financial institutions and improve the robustness of Japan's financial system and payment and settlement system.

## Survey coverage

	2010 Survey		2008 Survey		2006 Survey		2004 Survey		2002 Survey	
Survey period	Oct.–Nov.2010		Oct.–Nov.2008		Dec.2006–Feb.2007		Sep.–Nov.2004		Aug.–Oct.2002	
Response rate	100%		100%		100%		100%		100%	
	Number of institutions	Share (%)	Number of institutions	Share (%)	Number of institutions	Share (%)	Number of institutions	Share (%)	Number of institutions	Share (%)
Major banks	12	14.6	12	14.3	12	14.3	14	16.3	14	20.6
Regional banks	22	26.8	17	20.2	16	19.0	16	18.6	10	14.7
Japanese securities firms	6	7.3	10	11.9	10	11.9	13	15.1	13	19.1
Foreign banks and foreign securities firms	27	32.9	29	34.5	32	38.1	26	30.2	16	23.5
Others <sup>2</sup>	15	18.3	16	19.0	14	16.7	17	19.8	15	22.1
Total	82	100.0	84	100.0	84	100.0	86	100.0	68	100.0

<sup>1</sup> Japanese original only, published by the Bank of Japan.

<sup>2</sup> "Others" includes central organizations for cooperative financial institutions, money market brokers, trust banks affiliated with securities firms, and trust banks specializing in the custodian business.

## Overview of survey findings

Overall, there has been progress from the previous survey on the preparation of business continuity management, with 90 percent responding they were "Completed and regularly reviewed". Conversely, only 30 percent responded "Effectiveness is assured" for business continuity management.

Over 90 percent have formulated business continuity plans envisioning earthquake and infectious disease (the spread of highly pathogenic new strains of influenza, etc.). Approximately three-quarters responded that plans have been formulated envisioning disasters taking place outside of business hours (nighttime or holidays, etc.) in addition to disasters during business hours. Almost all responded "In place" for the identification of "Critical operations" for priority restoration in the event of disaster and establishment of recovery target times for "Critical operations".

With respect to business resources (staff, equipment, workplaces, etc.), progress has been made in determining business continuity staffing levels, and reserve levels have improved for equipment, office supplies and other necessary resources. Most respondents utilize remote storage for data backup; for off-site backup systems, the ratio responding "Individual switchover is possible for virtually all systems" is up from the previous survey. More than 90 percent have backup offices.

Decision-making and communication systems are generally in place. More than 80 percent have contact information for "Important parties" outside the company, such as government agencies, payment systems operators, group companies and service providers.

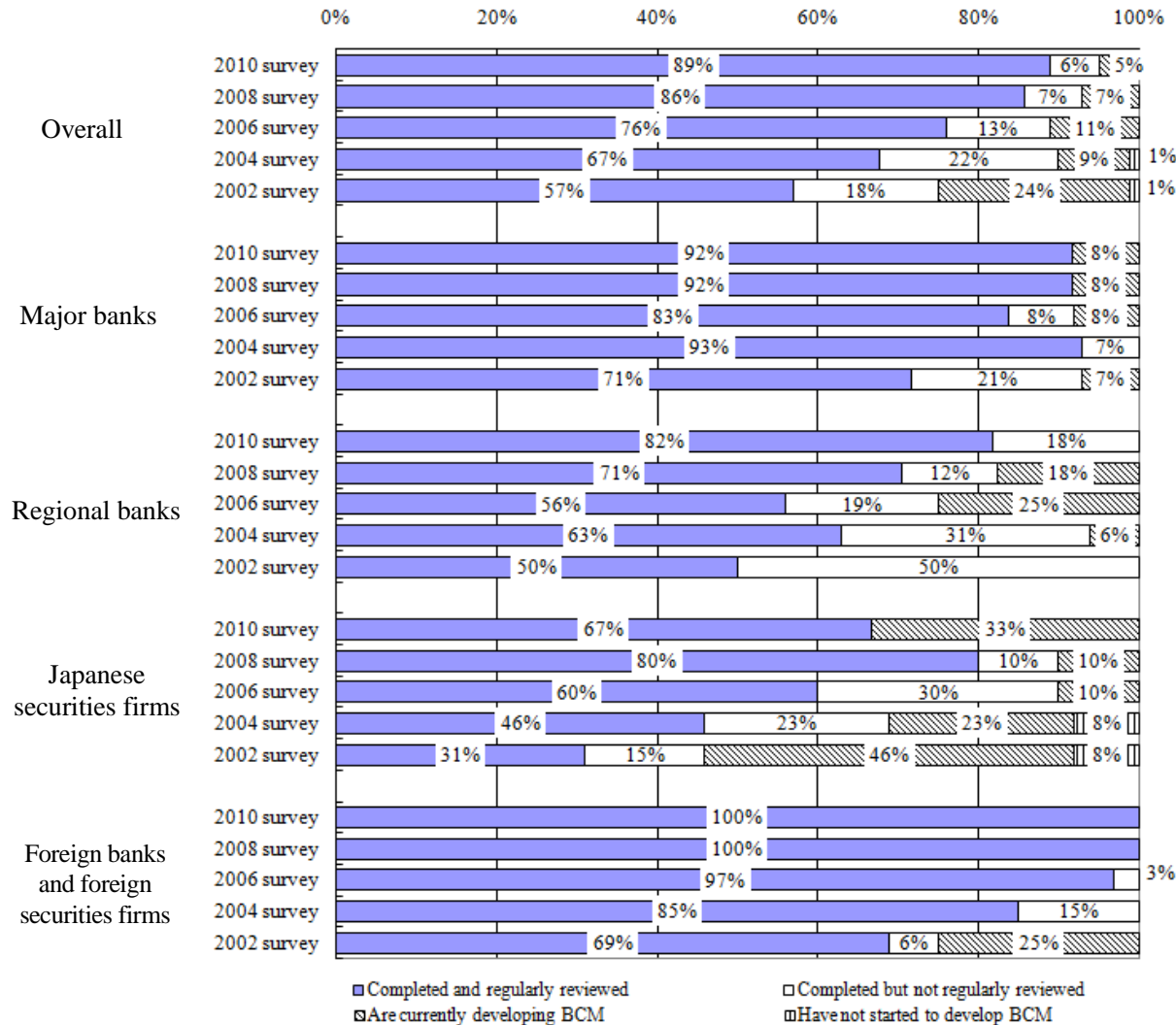
Most respondents perform regular (at least once a year) training based on formulated business continuity plans, focusing on payment and settlement operations (funds settlement and securities payment and settlement). Most review manuals, internal communication systems and procedures for critical operations in light of training results, and more than half indicated the intent to conduct street-wide training and enhance companywide training in the future.

Overall, therefore, there has been progress on business continuity management since the previous survey, but the survey also identifies issues that remain to be addressed, and we look forward to further enhancements of business continuity management and their effectiveness in the future.

# Survey findings

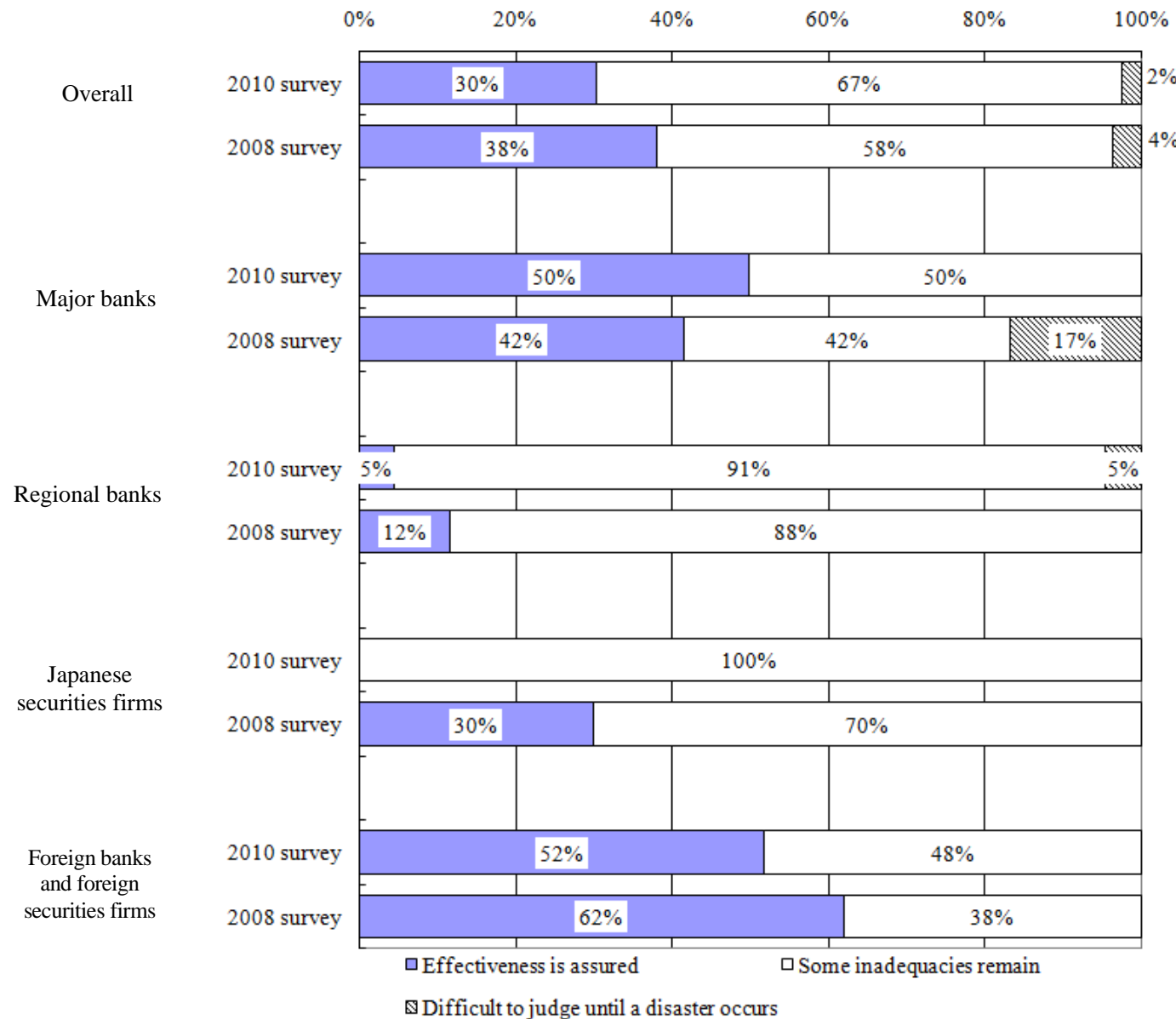
## I. Overview

### Companywide business continuity management readiness



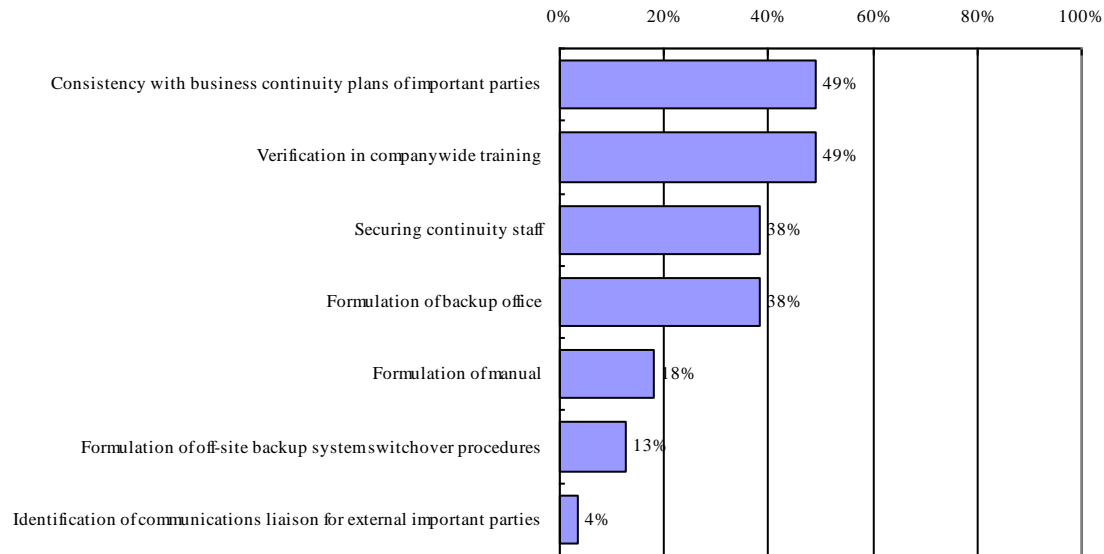
- With respect to companywide business continuity management readiness, 90 percent responded "Completed and regularly reviewed".
- By segment, more than 90 percent of major banks responded "Completed and regularly reviewed".
- More than 80 percent of regional banks responded "Completed and regularly reviewed".
  - This segment saw an increase in the ratio responding "Completed and regularly reviewed", which contributed to the overall increase.
- For Japanese securities firms, there was a decline from the previous survey in the ratio responding either "Completed and regularly reviewed" or "Completed but not regularly reviewed", and an increase in the ratio responding "Are currently developing BCM".
- All foreign banks and foreign securities firms responded "Completed and regularly reviewed".

## Effectiveness of operational continuity



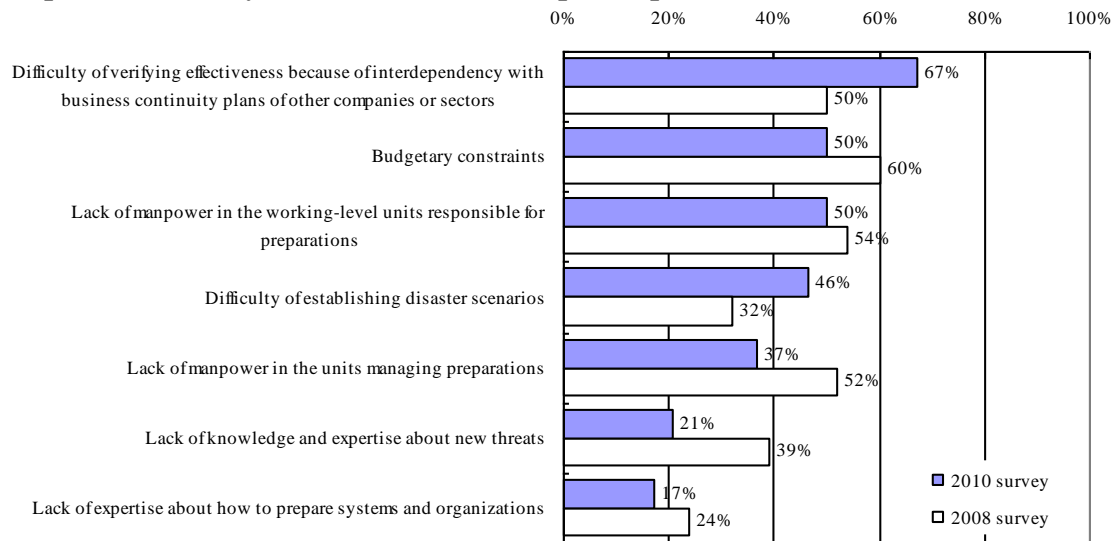
- Only 30 percent responded "Effectiveness is assured" for business continuity management.
- By segment, the ratio of major banks responding "Effectiveness is assured" increased.
- By contrast, the ratio responding "Some inadequacies remain" increased for regional banks, Japanese securities firms, foreign banks and foreign securities firms.

Specific areas of inadequacy (multiple responses)



- Approximately half of those responding "Some inadequacies remain" listed "Consistency with business continuity plans of important parties" and "Verification in companywide training" as "Specific areas of inadequacy".

Impediments to system readiness (multiple responses)

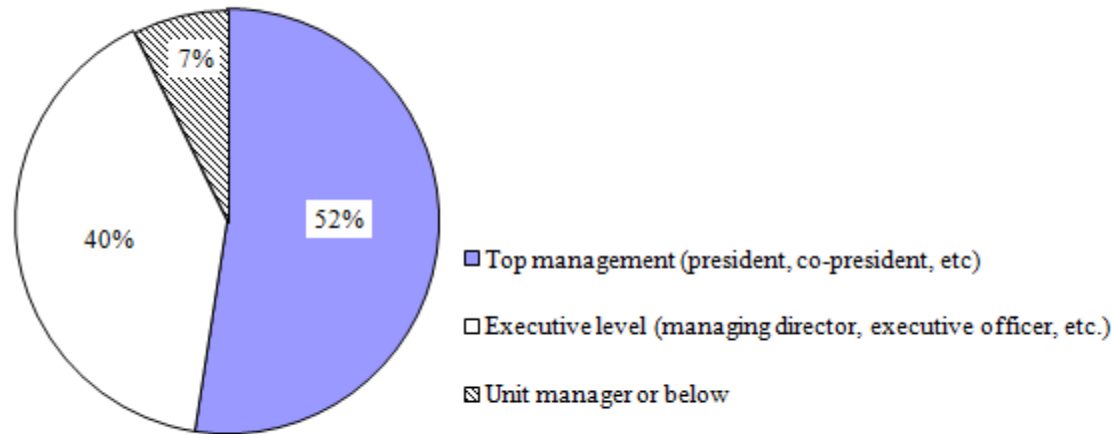


- Regarding impediments to system readiness, in the previous survey the most common answer was "Budgetary constraints", but in this survey it was "Difficulty of verifying effectiveness because of interdependency with business continuity plans of other companies or other sectors".

## II. Organizational status

### A. Leadership of management team

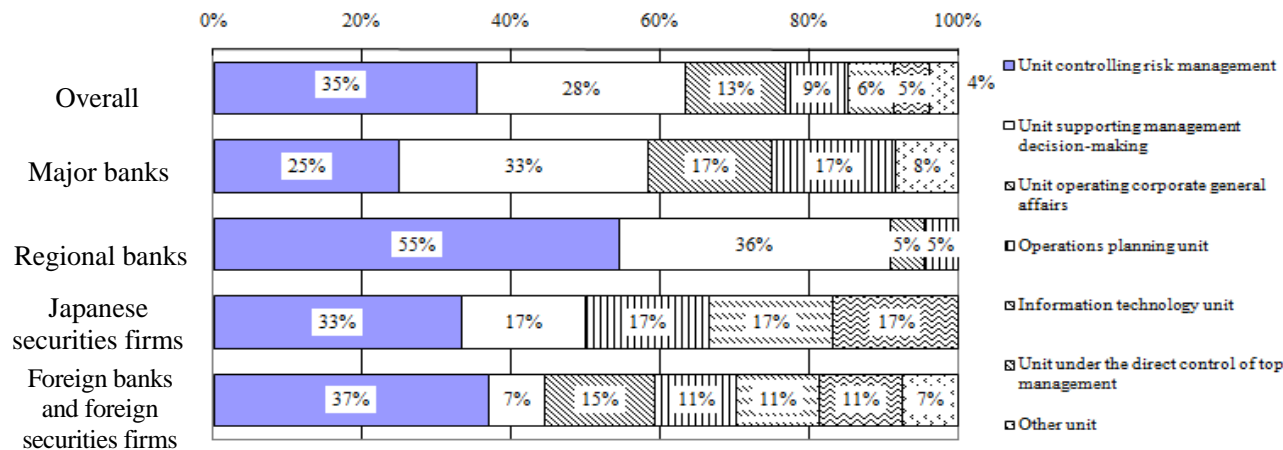
#### Level of personnel for management



- More than 90 percent responded that the level of personnel for management is at the "Executive level or higher".

### B. Establishment of supervisory unit

#### Unit with central role in preparing business continuity



- All respondents have supervisory units. Overall, ratios were relatively high for the "Unit controlling risk management" and "Unit supporting management decision-making" as supervisory units.
- The "Unit controlling risk management" is the supervisory unit at more than half of regional banks.

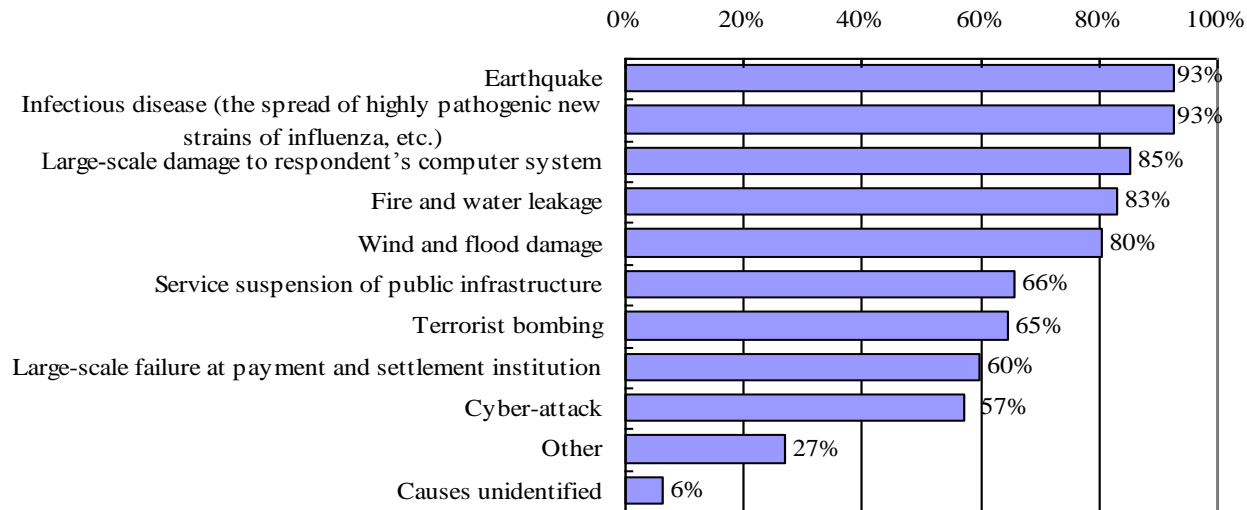


### III. Formulation of business continuity plan

#### A. Clarification of assumptions

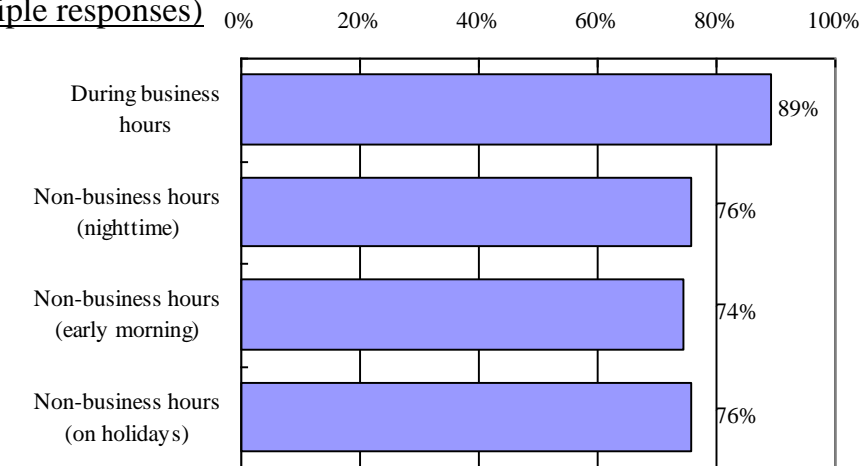
##### 1. Identification of disaster scenarios

##### Disaster scenario causes and events (multiple responses)



- For disaster scenario causes and events (potential threats to the company), more than 90 percent envisioned "Earthquake" and "Infectious disease" (the spread of highly pathogenic new strains of influenza, etc.).

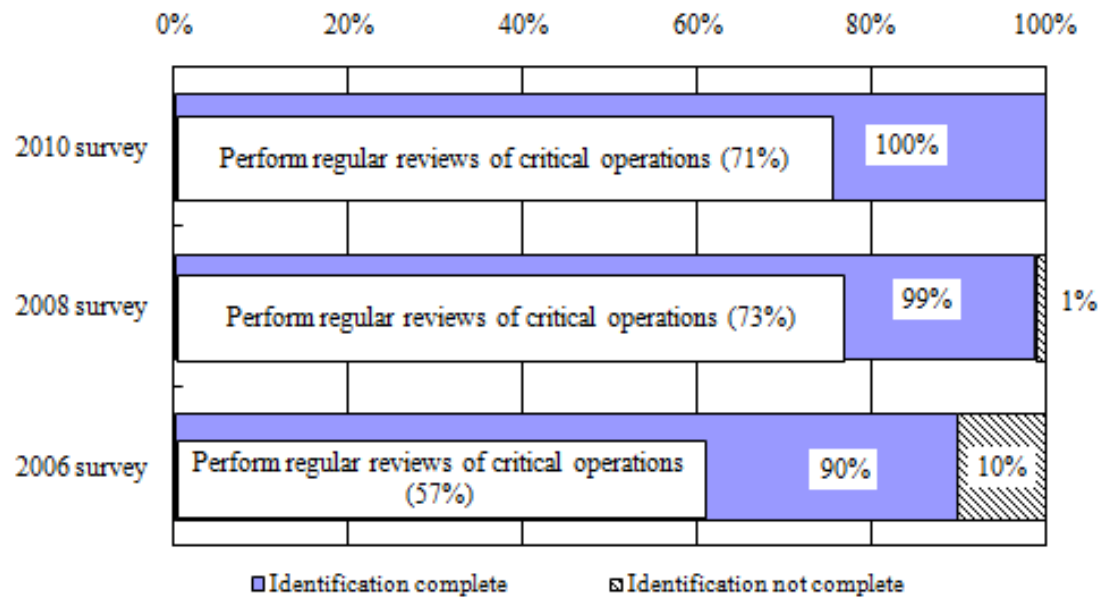
##### Timing of disaster (multiple responses)



- Approximately three-quarters envisioned disasters occurring not only during business hours but also at nighttime, on holidays and other non-business hours.

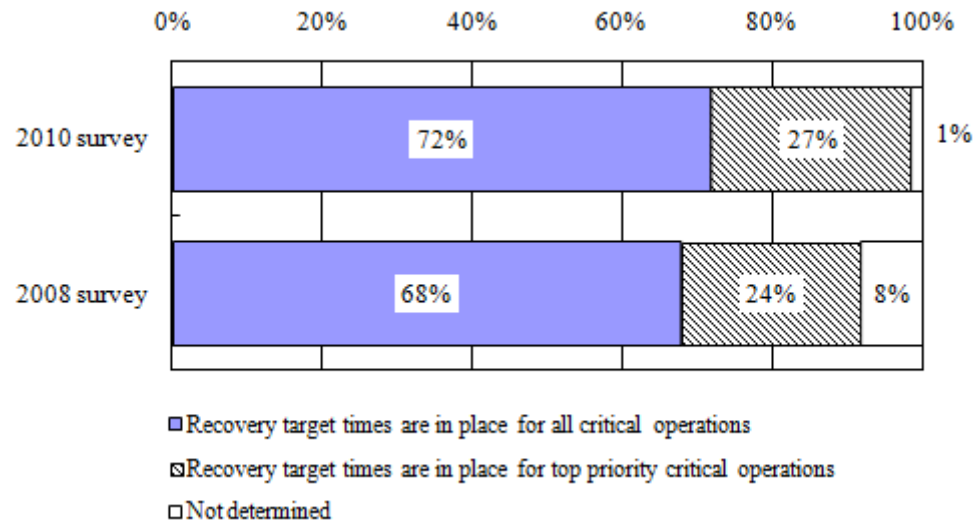
## 2. Identification of "critical operations" and establishment of recovery target times

### Identification of "critical operations"



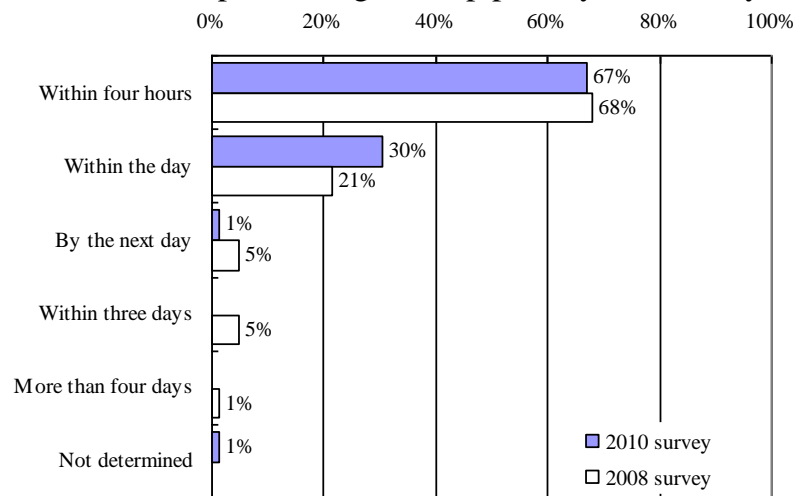
- All respondents indicated "Identification complete" for "Critical operations" given priority in disaster recovery.
- Approximately 70 percent "Perform regular reviews of critical operations."

Establishment of recovery target times for "critical operations"

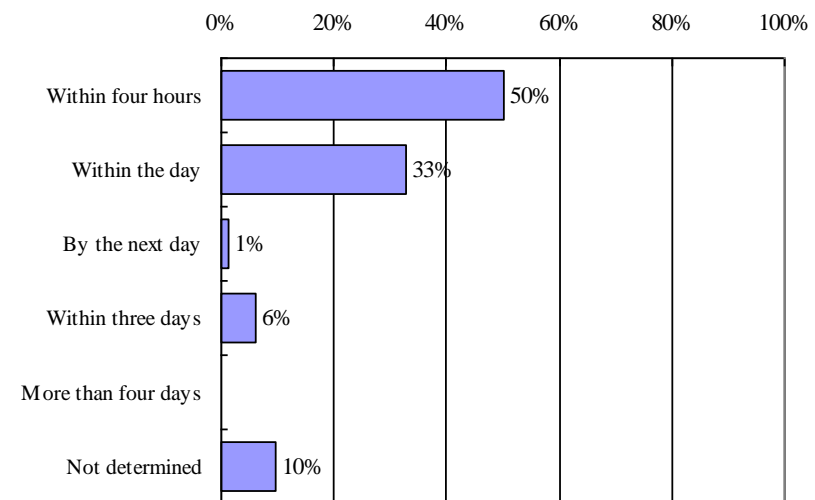


- Virtually all respondents indicated recovery target times are "In place" for "Critical operations".
- For approximately two-thirds, the recovery target time for "Critical operations given top priority in recovery" was "Within four hours". There was also an increase in the percentage responding "Within the day" from the previous survey. The percentage responding "By the next day", "Within three days", "More than four days" or "Not determined" declined from 11 percent the previous survey to 2 percent in this survey.
- Half of respondents said the recovery target time for "Critical operations for which computer systems are essential" was "Within four hours".

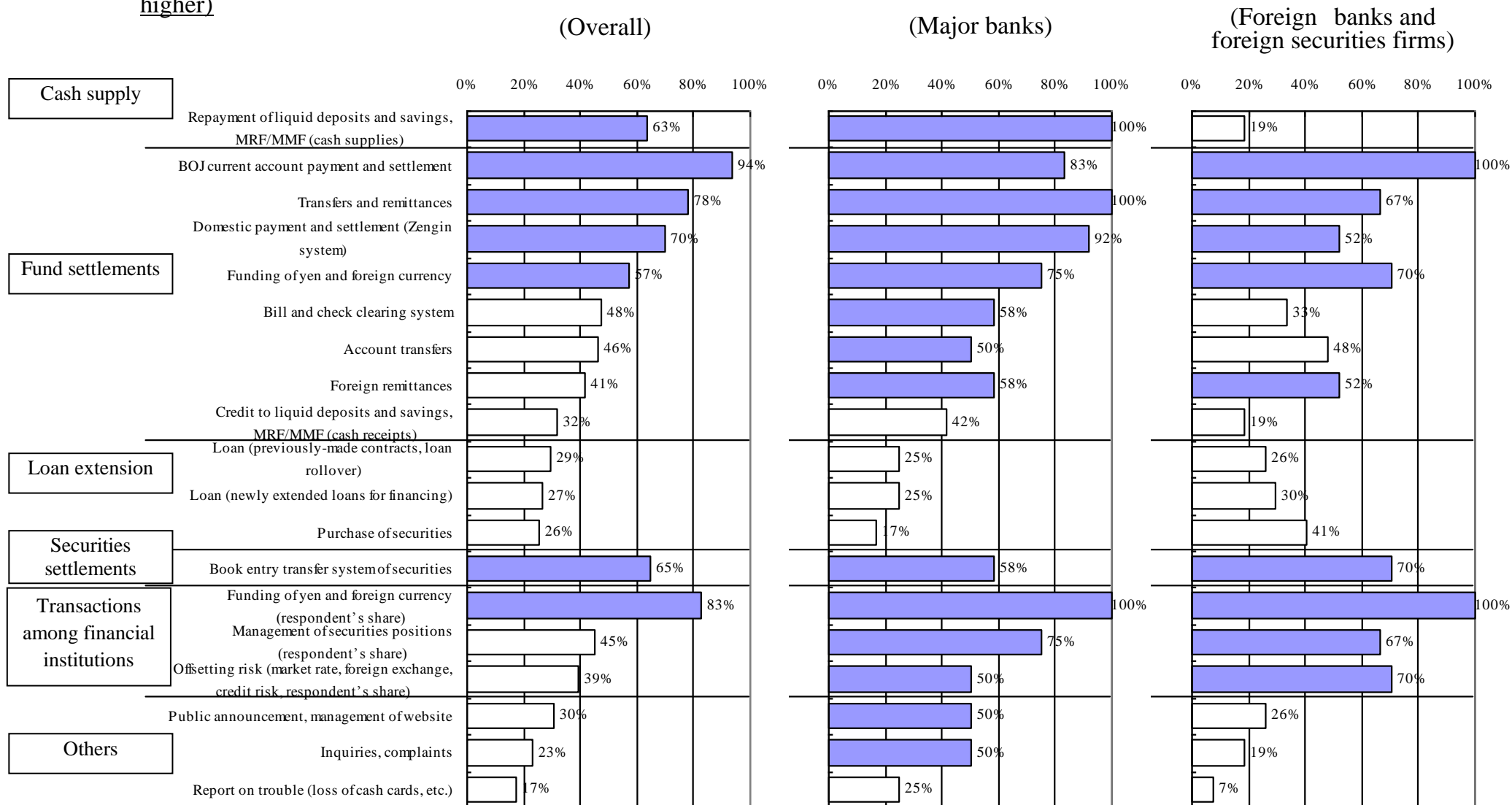
Recovery target time for "Critical operations given top priority in recovery"



Recovery target time for "Critical operations for which computer systems are essential"

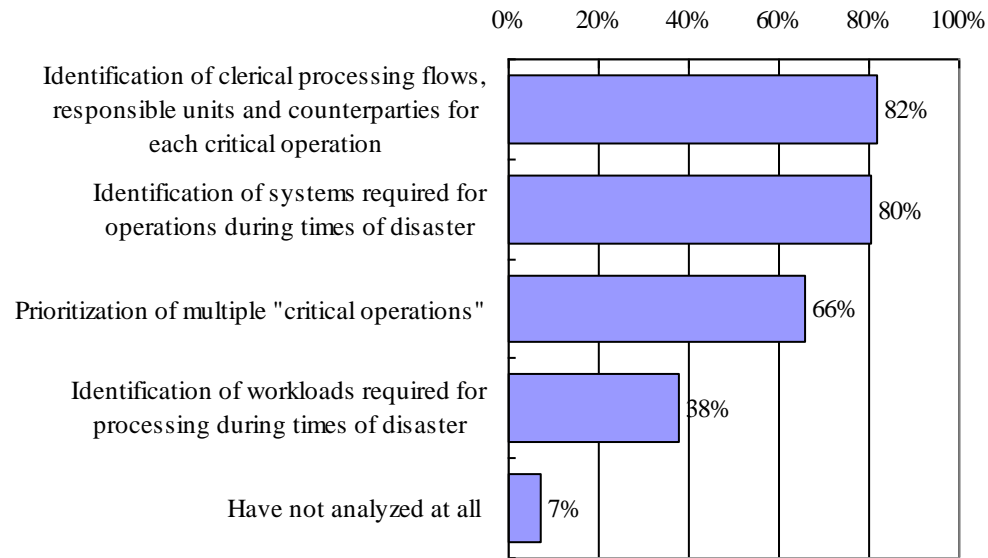


Specific "critical operations given top priority in recovery" (multiple responses) (coloring on the graph indicates 50 percent or higher)



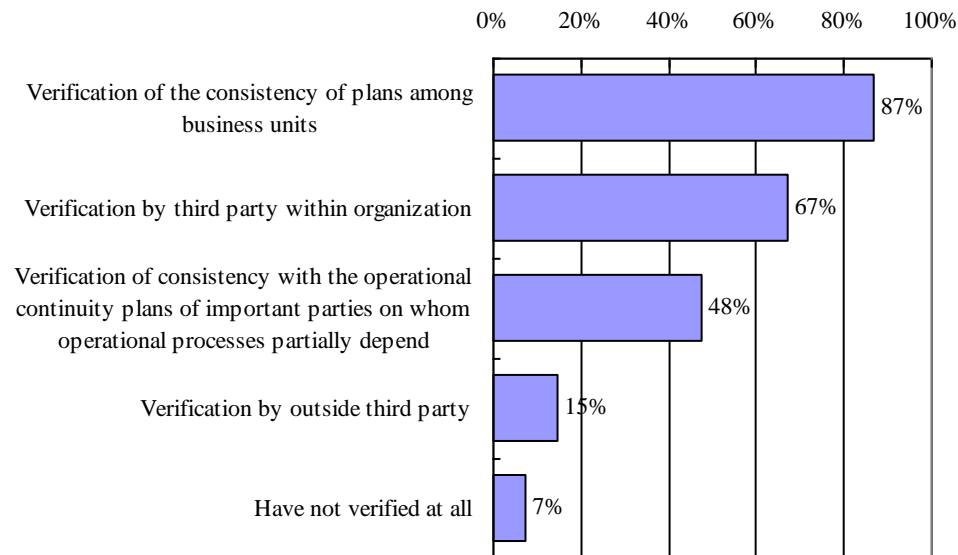
- Overall, most respondents listed "BOJ current account payment and settlement" among the "Critical operations given top priority in recovery".
- By segment, more than 90 percent of major banks listed "Cash supply", "Transfers and remittances", "Domestic payment and settlement", and "Funding of yen and foreign currency".
- All foreign banks and foreign securities firms listed "BOJ current account payment and settlement" and "Funding of yen and foreign currency".

### 3. Analysis of "Critical operations" (multiple responses)



- With respect to the analysis of "Critical operations", more than 80 percent "Identify clerical processing flows, responsible units and counterparties for each critical operation" and "Identify systems required for operations during times of disaster".
- However, only 40 percent "Identify workloads required for processing during times of disaster".

### B. Verification of content of business continuity plan (multiple responses)

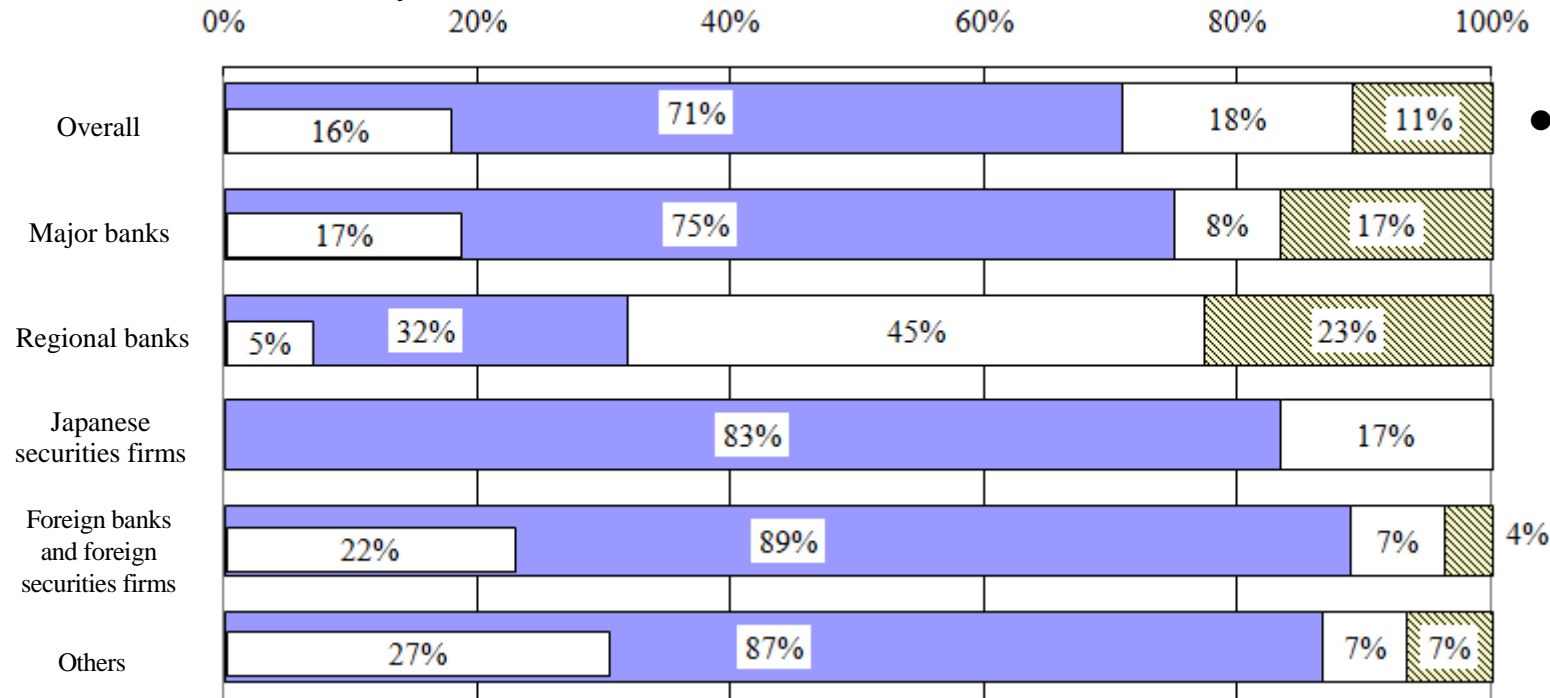


- With respect to verification of the content of business continuity plans, more than 80 percent "Verify the consistency of plans among business units".
- Roughly half "Verify consistency with the operational continuity plans of important parties on whom operational processes partially depend".

## IV. Securing business resources, etc.

### A. Securing general business resources

#### 1. Business continuity staff

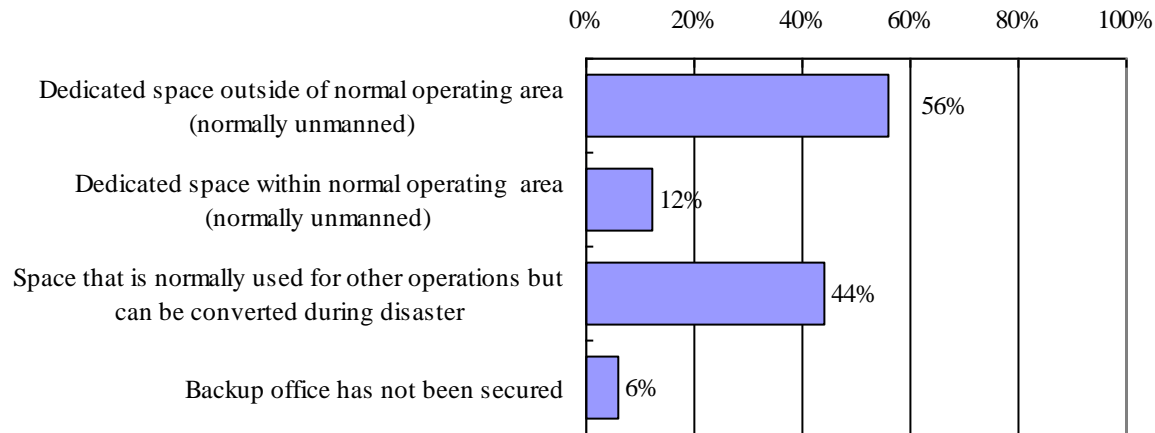


● The percentage of respondents estimating critical operations staffing numbers increased from 60 percent in the previous survey to approximately 70 percent in this survey.

- Assigned critical operations staff (percentage shown in white; percentages of respondents that have already examined the possibility of assembling such staff)
- Estimated the number of critical operations staff (staff yet to be assigned)
- Have not estimated the number of critical operations staff (estimation of such staff is a future issue)

## 2. Workplace

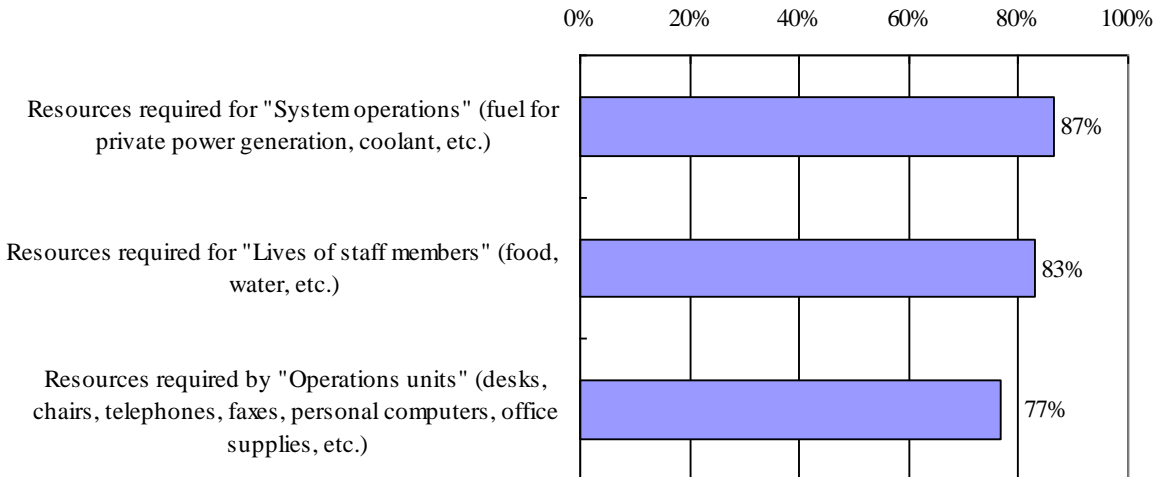
### Form of backup office<sup>3</sup> (multiple responses)



- For backup office formats, the most common were: (1) dedicated space that is normally unmanned, and (2) space that is normally used for other operations but can be converted during a disaster.

## 3. Equipment, office supplies, consumables, etc.

### Secured resources based on business continuity plan (multiple responses)

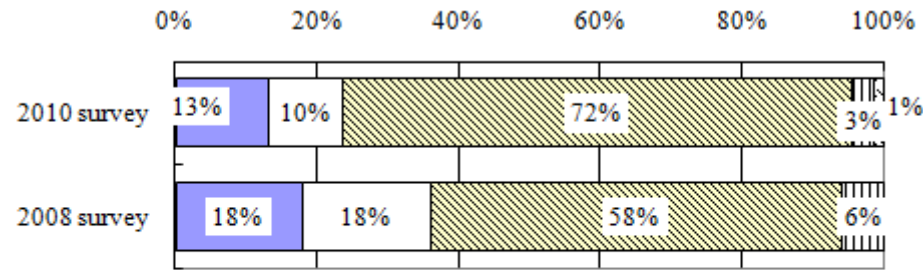


- Approximately 80 percent have secured resources for "System operations", etc.

<sup>3</sup> Operational office backup facilities.

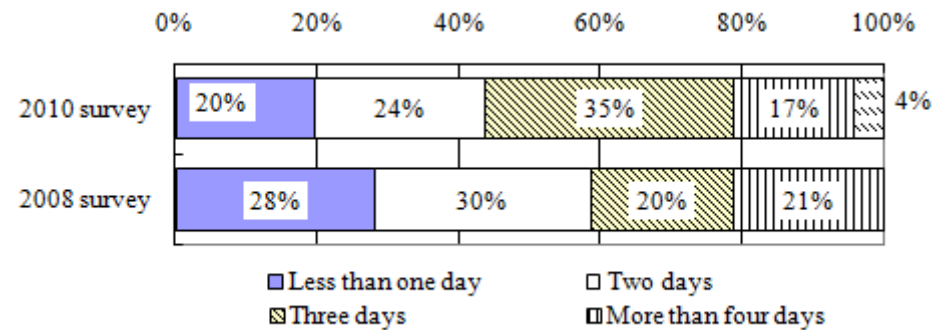
Reserve levels

(Resources required for the "Lives of staff members")



- There was an increase from the previous survey in the percentage of respondents having reserve levels of "Three days or more" of the resources required for the "Lives of staff members".

(Resources required for "System operations")

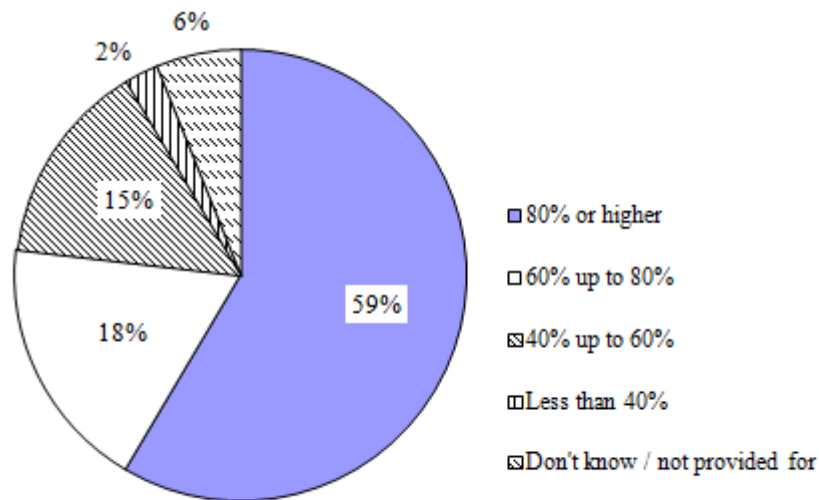


- There was also an increase from the previous survey in the percentage of respondents having "Three days or more" of the resources required for "System operations".



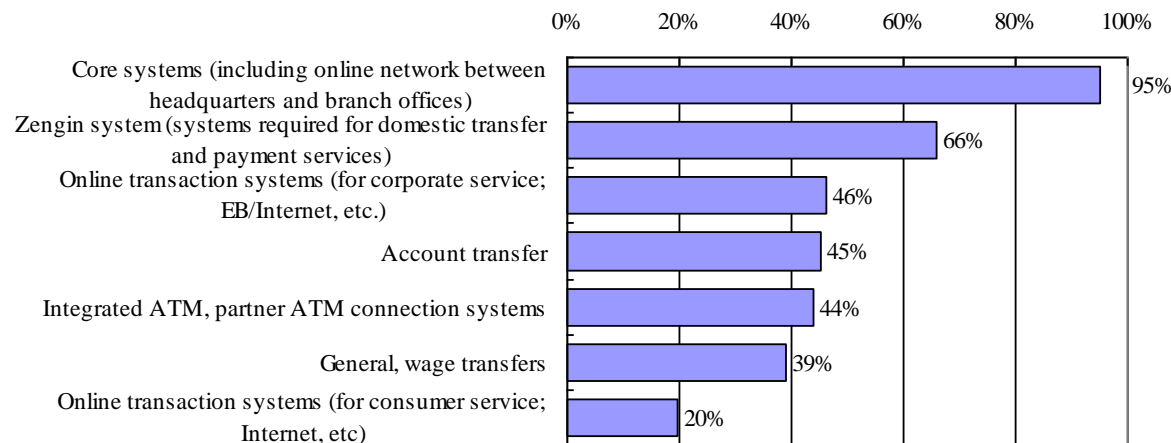
## B. Securing off-site backup system<sup>4</sup>

### "Critical operations" coverage ratio of off-site backup system



- For approximately 60 percent, the "Critical operations" coverage ratio of off-site backup systems was "80 percent or higher".

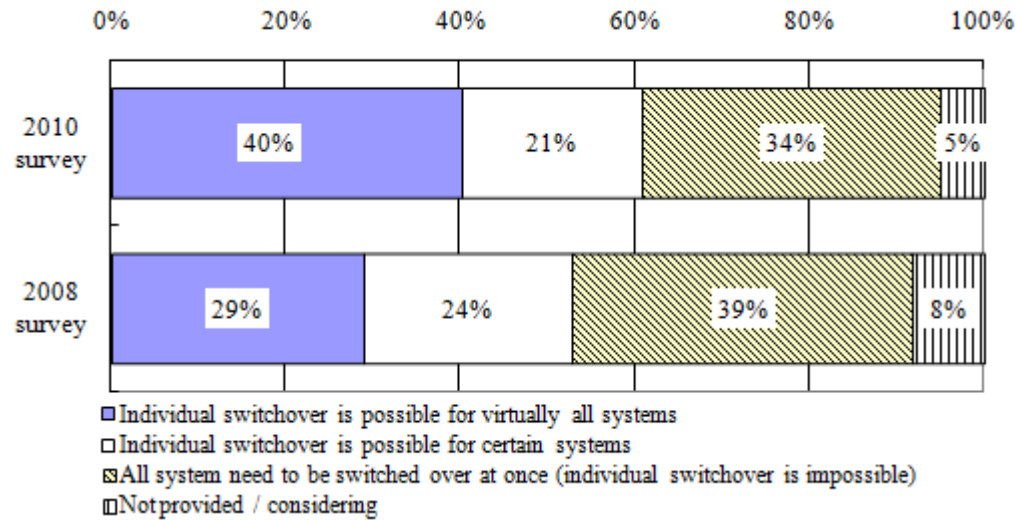
### Type of secured off-site backup systems (multiple responses)



- More than 90 percent have off-site backup systems for core systems.

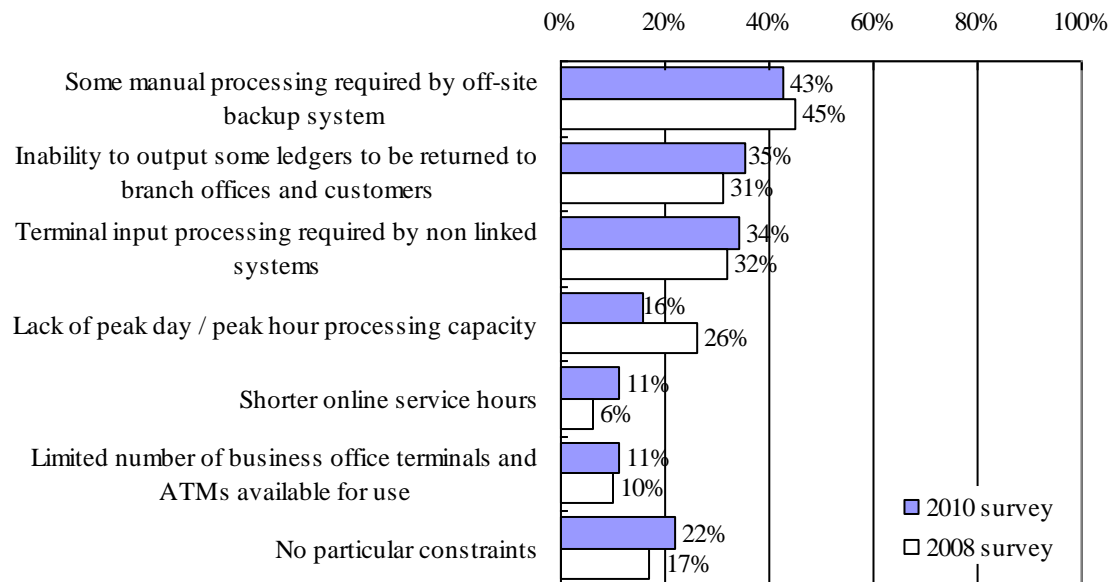
<sup>4</sup> Alternate system installed in a different location from the main computer system (i.e., "backup center," etc.).

### Off-site backup system switchover method



- For off-site backup systems, the percentage responding "Individual switchover is possible for virtually all systems" was 40 percent, an increase from the previous survey.

### Operational constraints on the use of off-site backup systems (multiple responses)

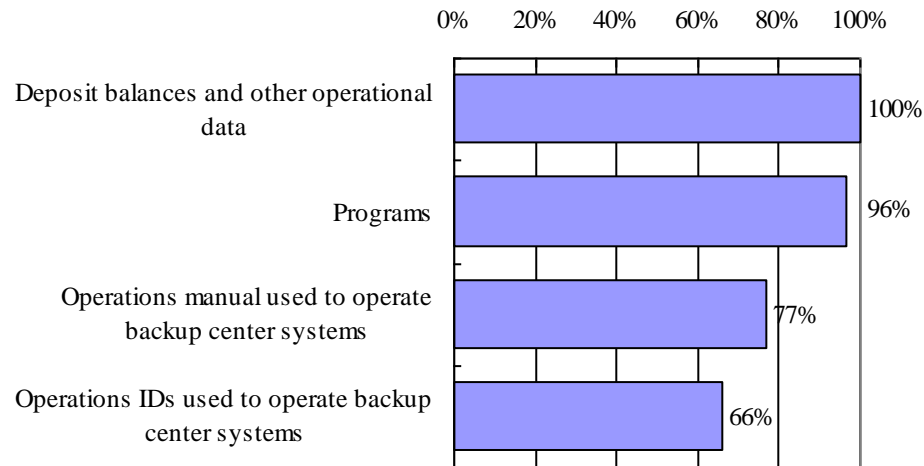


- Some of the operational constraints during the use of off-site backup systems have been alleviated since the previous survey, while others have grown more pronounced. The percentage responding "No particular constraints" increased and the percentage responding "Lack of peak day / peak hour processing capacity" decreased. Conversely, increases were seen for both "Shorter online service hours" and "Inability to output some ledgers to be returned to branch offices and customers".

## C. Securing data backup for important systems

### 1. Remote storage of data backup

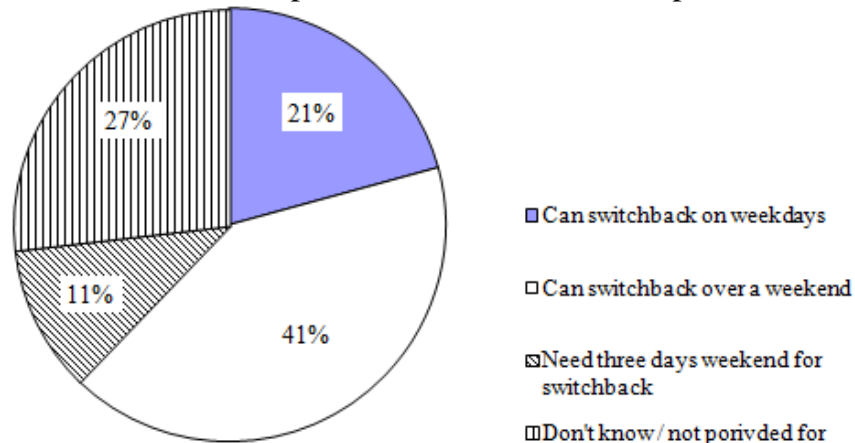
Data backup put in remote storage (multiple responses)



- All respondents provide remote storage for "Deposit balances and other operational data" and virtually all for "Programs".
- By contrast, the percentage providing remote storage for "Operations manuals and IDs used to operate backup center systems" was relatively small.

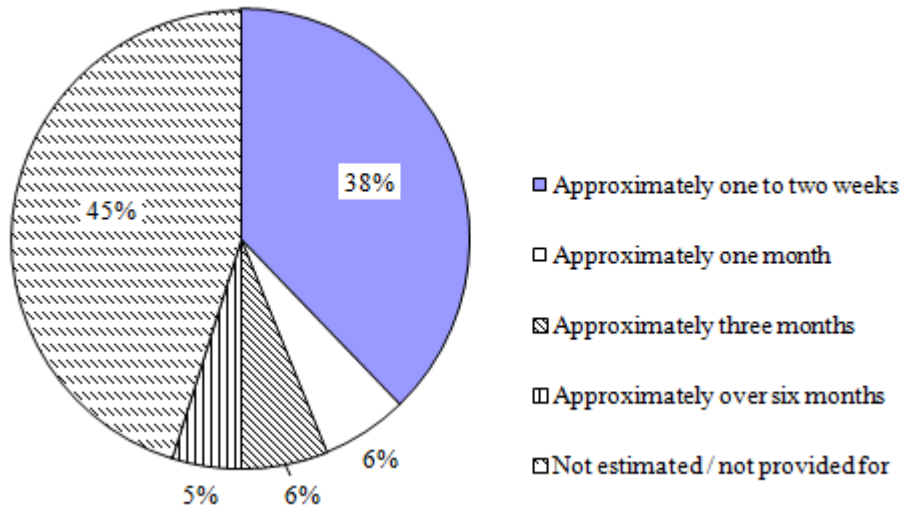
### 2. Switchback (reversion to normal computer center from off-site backup systems)

Days required for switchback (period of online service suspension, etc.)



- Approximately 40 percent responded "Can switchback over a weekend" when questioned about the days required for switchback.
- By contrast, approximately 30 percent responded "Don't know / not provided for".

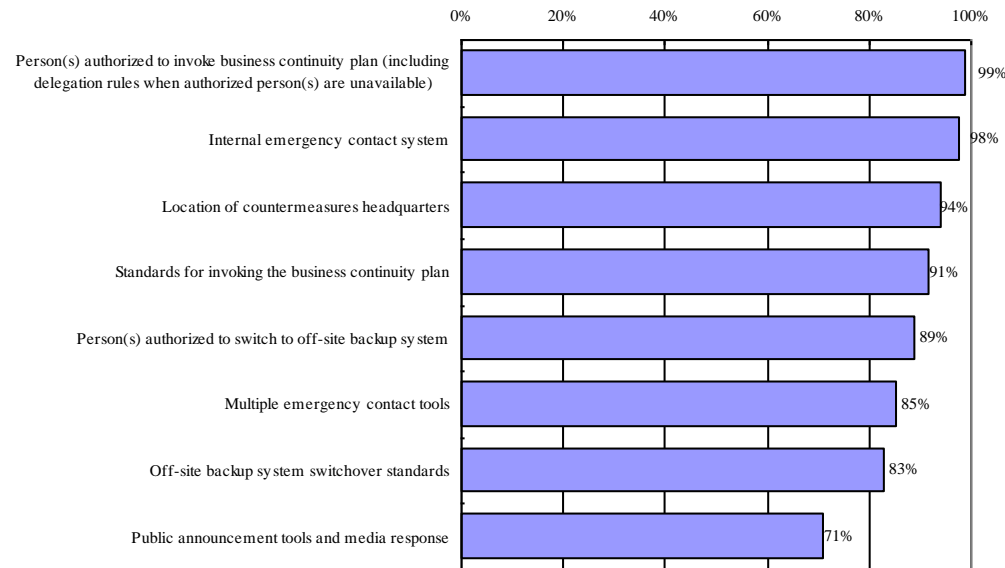
Preparatory period required for switchback



- Just under half responded "Not estimated / not provided for" for the period required to switch back (including preparatory work) after switching over to the off-site backup system.
- Most of the respondents that had made estimates would be able to switch back in "Approximately one to two weeks", though roughly 20 percent responded that more than "One month" would be required.

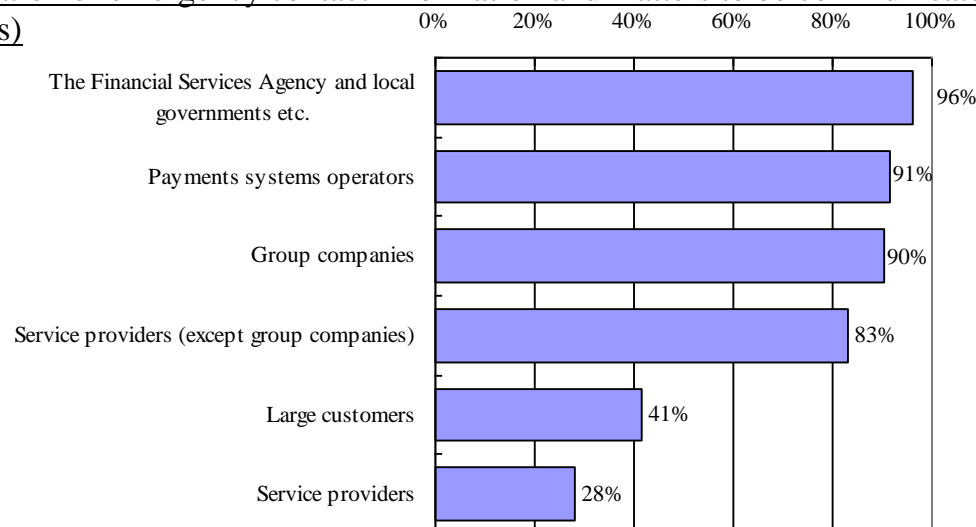
## V. Status of decision-making and communication systems

### Readiness of decision-making and communications systems when business continuity plan invoked (multiple responses)



- Most respondents said they were generally completed for the decision-making and communication systems to be used when business continuity plans are invoked.

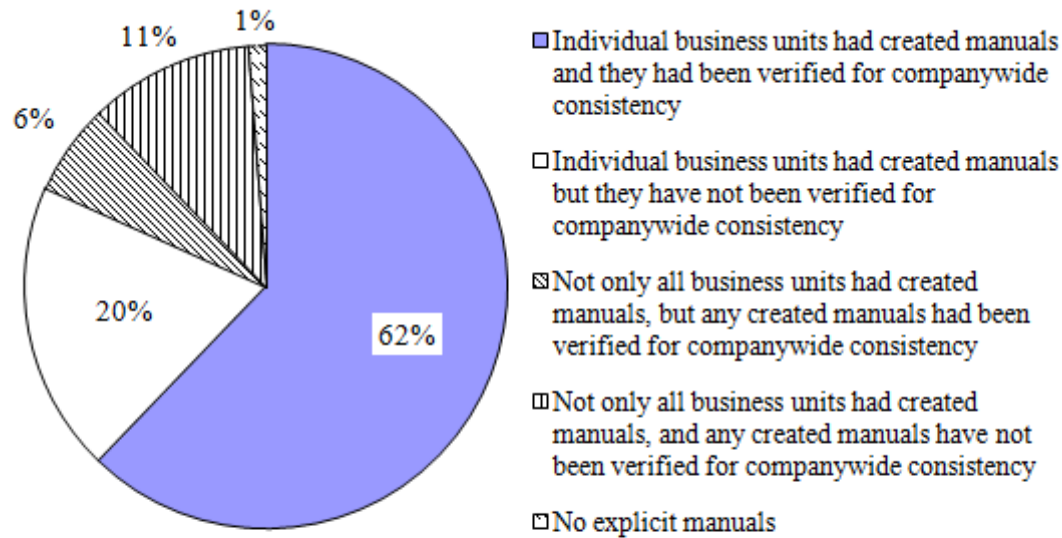
### Identification of emergency contact information and matters to be communicated to external "important parties" (multiple responses)



- More than 80 percent had contact information for "The Financial Services Agency and local governments etc.", "Payment systems operators", "Group companies" and "Service providers".

## VI. Formulation of manuals

### Status of manuals

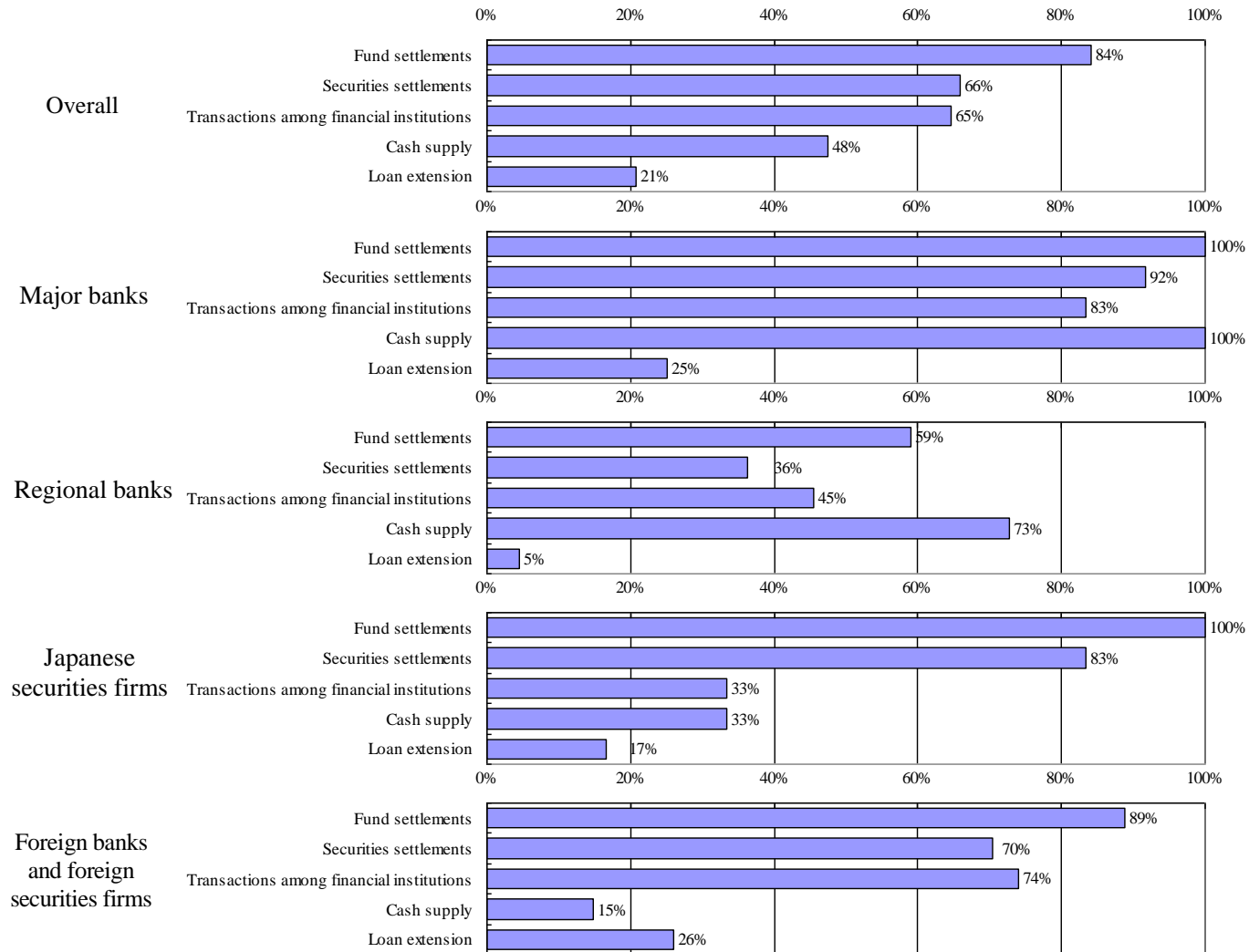


- More than 80 percent responded that "Individual business units had created manuals", and 60 percent that "Individual business units had created manuals and they had been verified for companywide consistency".

## VII. Training and review of plans

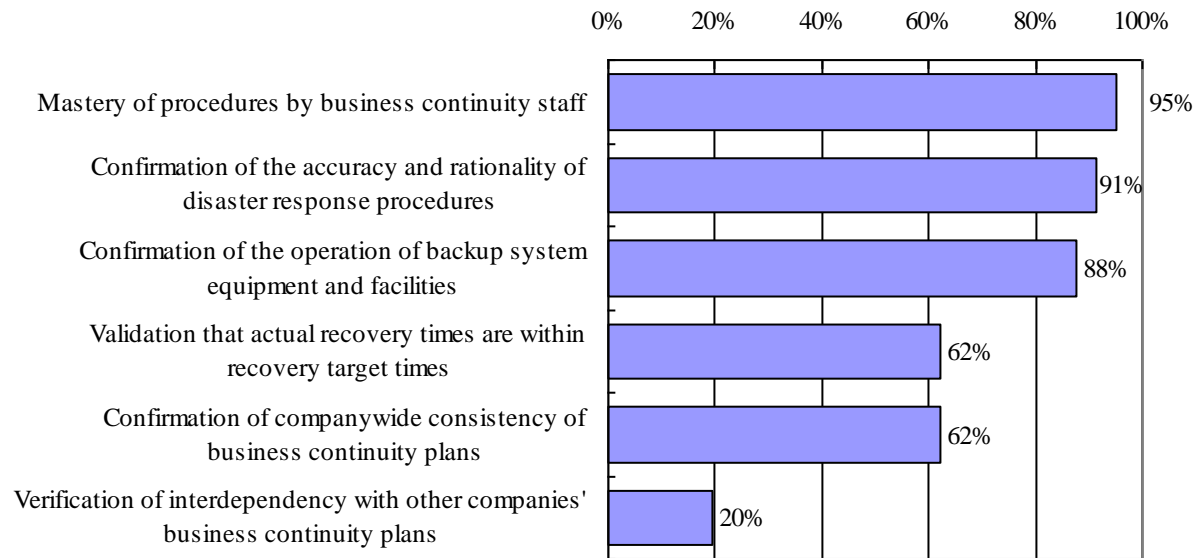
### A. Status of training

#### Operations on which regular training is given at least once per year (multiple responses)



- Overall, more than 80 percent performed "Funds settlement" training regularly, at least once per year.
- By segment, all major banks performed "Funds settlement" and "Cash supply" training.
- Roughly 60-70 percent of regional banks performed "Funds settlement" and "Cash supply" training.
- All Japanese securities firms performed "Funds settlement" training, and more than 80 percent performed "Securities settlements" training.
- Just under 90 percent of foreign banks and foreign securities firms performed "Funds settlement" training.

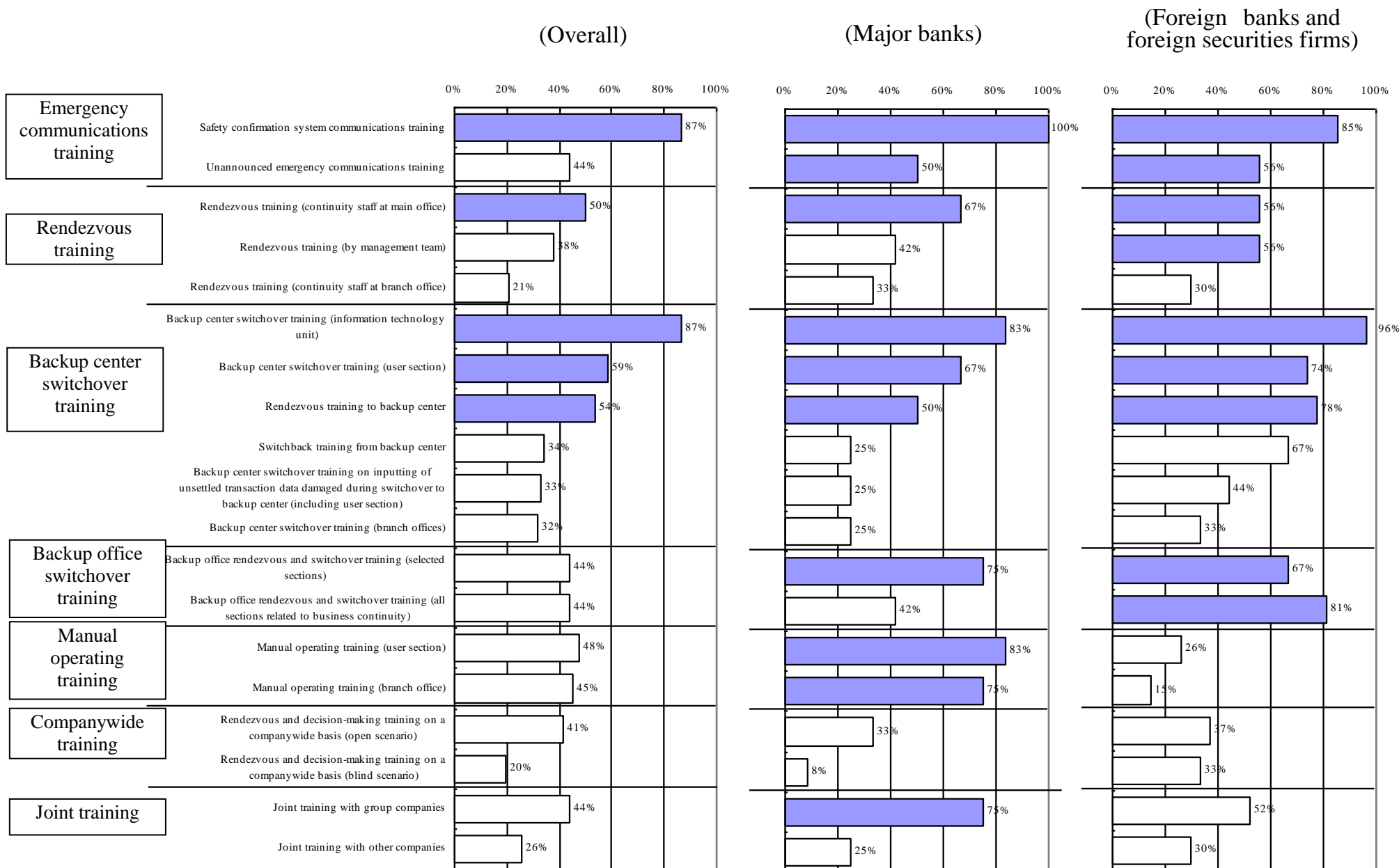
### Training objectives (multiple responses)



- Most respondents listed the objectives of training as being "Mastery of procedures by business continuity staff", "Confirmation of the accuracy and rationality of disaster response procedures" and "Confirmation of the operation of backup system equipment and facilities".
- Approximately 60 percent performed "Validation that actual recovery times are within recovery target times" and "Confirmation of companywide consistency of business continuity plans".
- However, only 20 percent performed "Verification of interdependency with other companies' business continuity plans".

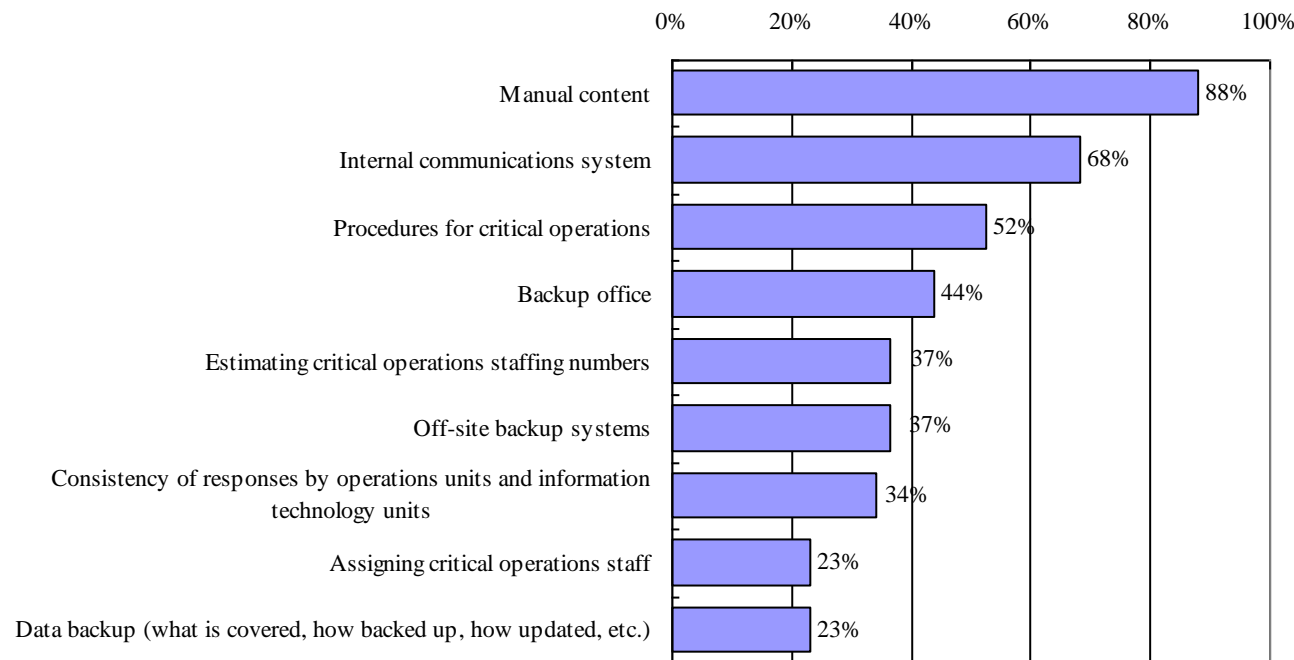


Training performed over the past 2 years (multiple responses) (colored portion of graph indicates 50 percent or higher)



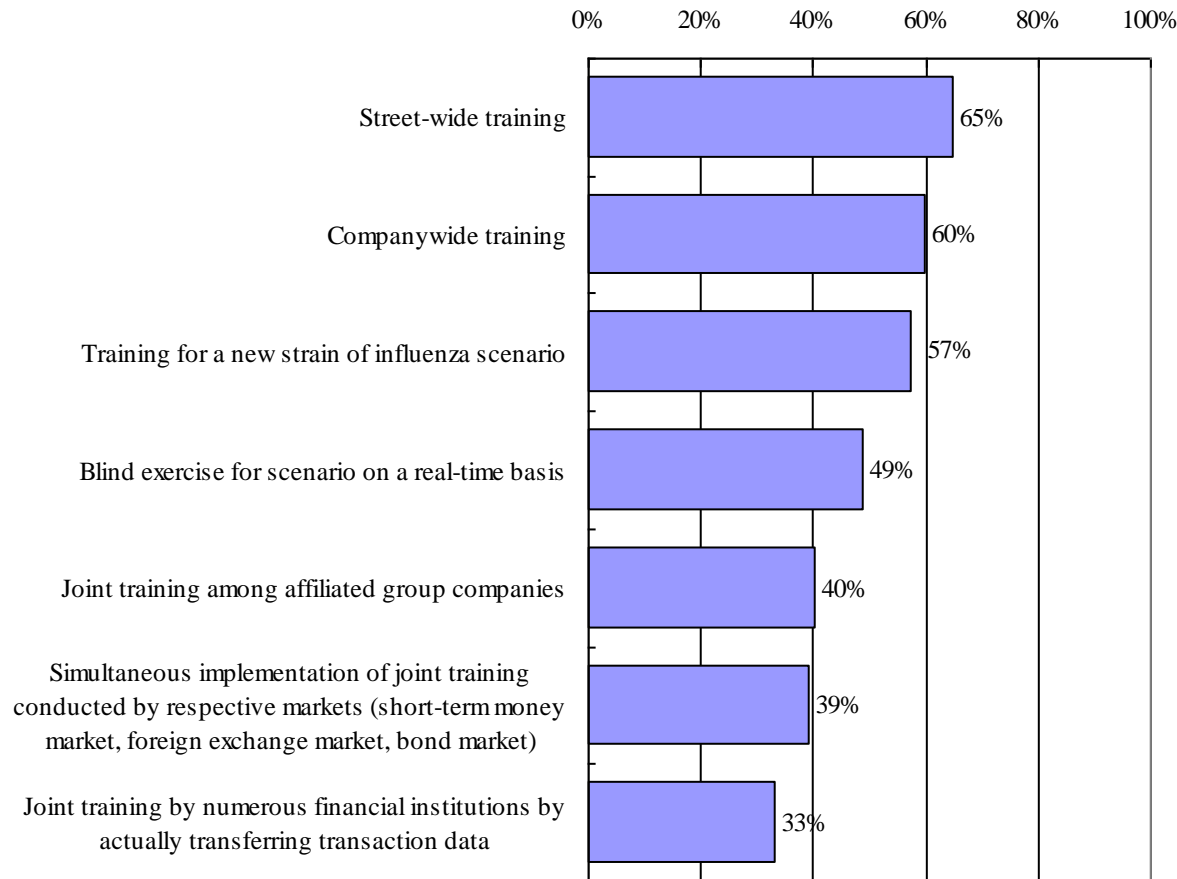
- All segments perform a wide range of training. Among the most common were "Safety confirmation system communications training" and "Backup center switchover training" by the information technology unit.
- All major banks performed "Safety confirmation system communications training." More than three-quarters performed "Backup center switchover training" by the information technology unit, "Backup office rendezvous and switchover training" by selected units, and "Manual operating training" and "Joint training with group companies" by user section and branch offices.
- Compared to other segments, a larger percentage of foreign banks and foreign securities firms performed "Unannounced emergency communications training", "Rendezvous training" by the management team, various "Backup center switchover training" and "Backup office rendezvous and switchover training" with the participation of all business continuity-related units.

**B. Analysis and reporting of training results, review of business continuity plans (multiple responses)**



- For the analysis and reporting of training results and the review of (business continuity plan), the most common responses were "Manual content", followed by "Internal communications system" and "Procedures for critical operations".

### C. Training to be enhanced in the future (multiple responses)



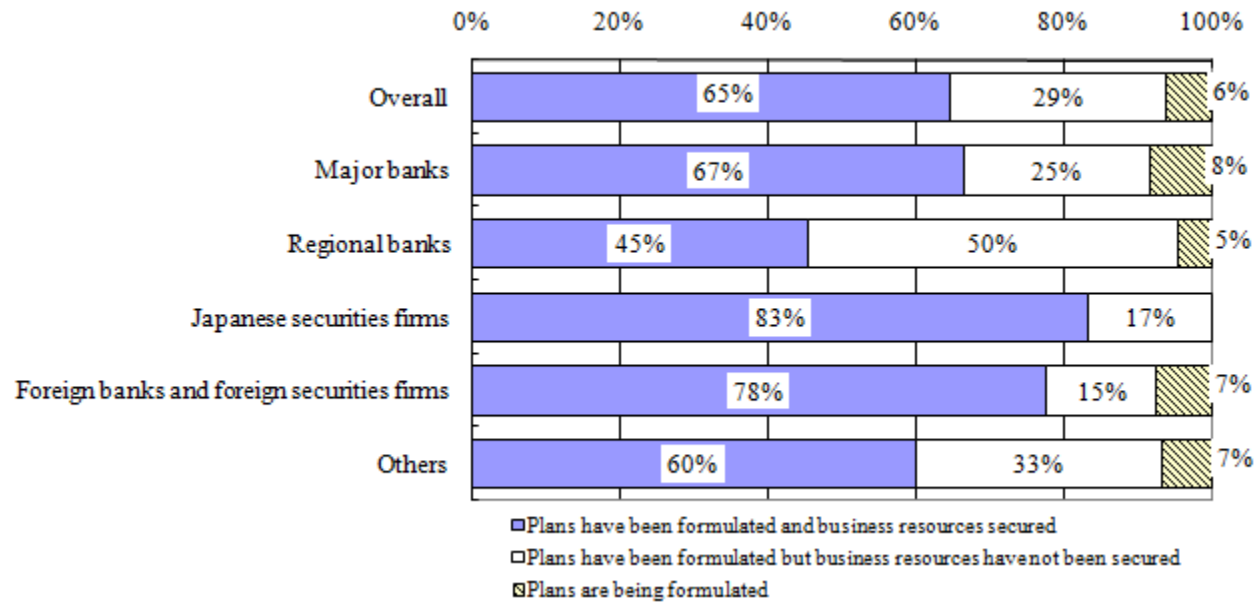
- The most common response regarding training to be enhanced in the future was "Street-wide training<sup>5</sup>", followed by "Companywide training" and "Training for a new strain of influenza scenario".

<sup>5</sup> Street-wide training differs from other forms of training in three important respects: (1) establishment of a common disaster scenario for the industry, (2) simulation of disaster response by individual companies under the common scenario, and (3) collection of results and identification of problems to facilitate desktop training that encourages enhancements to business continuity management systems at the industry level ("Outline of Street-wide Training Practices in Foreign Countries (Japanese original only)", published by the Bank of Japan, March 2010).

## VIII. Response to outbreaks of new strains of influenza<sup>6</sup> and other infectious diseases

### A. Formulation of business continuity plan

#### Formulation of business continuity plan

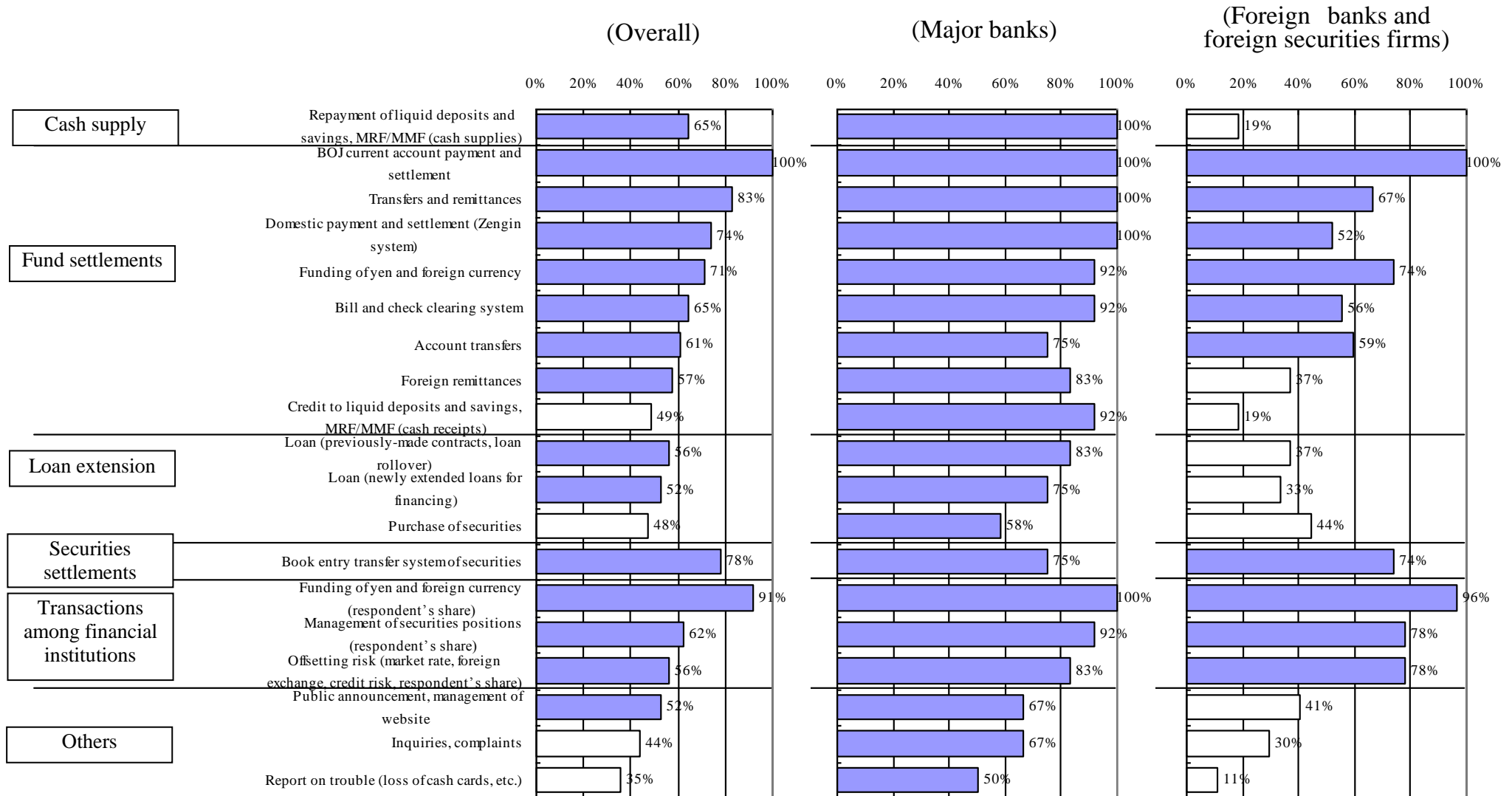


- More than 90 percent responded "Plans have been formulated" for response to outbreaks of new strains of influenza and other infectious diseases, which represents an increase from the previous survey (approximately 30 percent).

<sup>6</sup> Highly pathogenic influenza. Increases companywide absentee rate to the point that operations are impacted and it is difficult to perform all operations normally.

## B. Operational continuity for "critical operations"

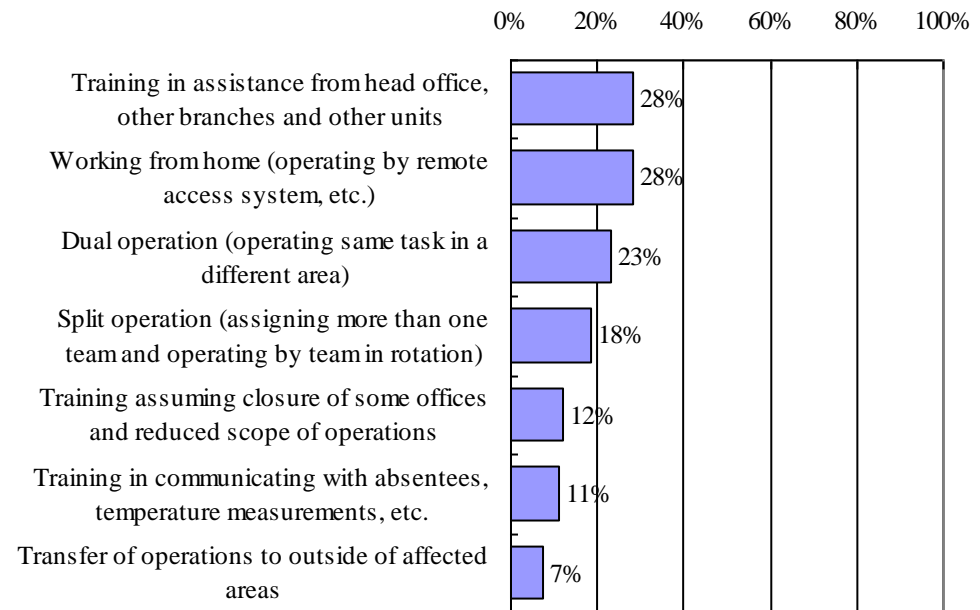
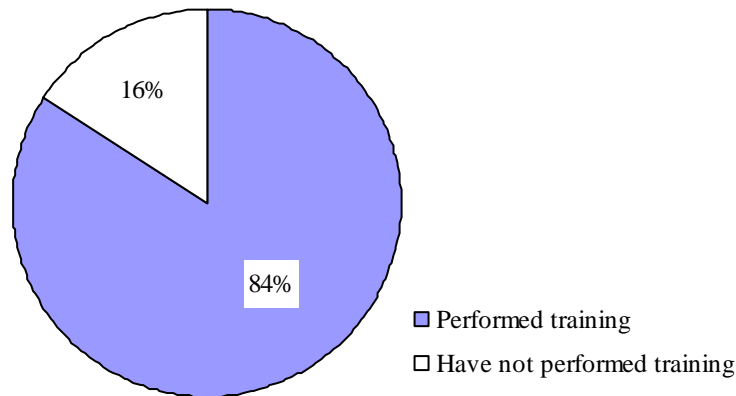
Specific content of "critical operations" envisioned for continuity during outbreaks of new strains of influenza (multiple responses) (Colored portion of graph represents 50 percent or higher)



- "Critical operations" envisioned for continuity during outbreaks of new strains of influenza are broader than the "Critical operations given top priority in recovery" envisioned earlier (p 10), in part because there is no need to assume the physical destruction of buildings and equipment, etc.
- All major banks included "Cash supply", "BOJ current account payment and settlement", "Transfers and remittances" and "Domestic payment and settlement" in "Critical operations."
- More than 90 percent of foreign banks and foreign securities firms included "BOJ current account payment and settlement" and "Funding of yen and foreign currency".

### C. Training

- Approximately 80 percent performed training for new strains of influenza. There were significant differences in the content of training.



## **Toward the further enhancements of business continuity management**

As described above, the survey confirmed that there has been progress overall on business continuity management of financial institutions since the previous survey. However, the survey also identified issues that remain to be addressed, and we look forward to further enhancements to business continuity management and their effectiveness in the future.

First, the percentage responding "Effectiveness is assured" for business continuity management declined from the previous survey (p 4). Approximately half of the respondents indicating inadequate effectiveness pointed to "Consistency with business continuity plans of important parties" and "Verification in companywide training" (p 5). We expect institutions to work with important parties to mutually verify the consistency of business continuity plans and to perform "Companywide training" and joint training with relevant parties, in order to master emergency procedures of critical operations and to test their business continuity management.

We also note that approximately 40 percent of the respondents indicating inadequate effectiveness pointed to "Securing continuity staff" and "Formulation of Backup office" (p 5). When preparing staffing and backup offices, financial institutions should take into consideration an analysis of the potential threats facing the company, the envisioned work volume for critical operations and the recovery target times, as well as taking account of cost-effectiveness, and it is necessary to calculate the staffing that can be actually gathered at the backup offices and these need to be at a location that has no physical damage when the main office is struck by a disaster.

On the systems infrastructure side, some respondents indicated that operation manuals and operation IDs required to operate off-site backup systems are not remotely stored (p 17). These needed to be remotely stored to allow smooth switchover to the off-site backup systems during times of emergency.

A substantial number responded "Not estimated / not provided for" or "Don't know / not provided for" for the preparatory periods and switchback times after having transitioned to off-site backup systems (pp. 17-18). We expect institutions to measure the preparatory periods required for switchback from backup systems by examining data transfer methods and procedures. Since there are many cases of operational constraints on the use of off-site backup systems (p 16), we expect financial institutions to be able to quickly resume the use of main computer systems.