BOJ Reports & Research Papers

Questionnaire Survey on Business Continuity Management (December 2006)

Financial Systems and Bank Examination Department

Bank of Japan

This is an English translation of the Japanese original released in March 2007.

Financial Systems and Bank Examination Department, Bank of Japan
C.P.O. Box 203, Tokyo 100-8630, Japan

For further information about this survey, please contact:
Hiroyoshi Yamazaki (Mr.) or Minoru Shiraishi (Mr.), Examination of Computer System Risk, Financial Systems and Bank Examination Department
Tel: +81-3-3664-4333

Contents

I. Introduction

■ The Bank of Japan conducted the third Questionnaire Survey on Business Continuity Management, following the previous surveys in 2002 and 2004.

■ The respondents were 84 financial institutions that have current accounts at the Bank with a large volume of transactions in payment and settlement systems.

■ The objectives of the survey were to grasp the respondents' current situation and to use the survey results as a basis for the Bank to extensively discuss business continuity issues with financial institutions.

■ Taking account of the survey results, the Bank intends to further discuss the issues with financial institutions on such occasions as on-site examinations and off-site monitoring and strengthen cooperation with them, to enhance the overall business continuity capability of the Japanese financial system.

II. Survey Respondents

	2006 Survey (Survey period: Dec. 2006-Feb. 2007) Response rate: 100%		2004 Survey (Survey period: Sep.-Nov. 2004) Response rate: 100%		2002 Survey (Survey period: Aug.-Oct. 2002) Response rate: 100%	
	Number of institutions	Share (%)	Number of institutions	Share (%)	Number of institutions	Share (%)
Major banks	12	14.3	14	16.3	14	20.6
Regional banks	16	19.0	16	18.6	10	14.7
Japanese securities firms	10	11.9	13	15.1	13	19.1
Foreign banks and foreign securities firms	32	38.1	26	30.2	16	23.5
Others[1]	14	16.7	17	19.8	15	22.1
Total	84	100.0	86	100.0	68	100.0

[1] "Others" includes central organizations for cooperative financial institutions, money market brokers, trust banks affiliated with securities firms, and trust banks specializing in custodian business.

III. Key Findings

A. Framework for Developing Business Continuity Management (BCM)

■ 76 percent of all the respondents answered that they "have established BCM," up from 67 percent in the previous survey in 2004 (see IV. A. 1.).

■ 76 percent of the respondents answered that they "have established a business continuity plan (BCP) control section, and the officer in charge is an executive." However, only 54 percent of the respondents answered that their "BCP control sections review BCPs developed by each section in charge and also review their overall consistency" (see IV. A. 3.).

B. Business Continuity Planning

1. Assumptions and Conditions for Business Continuity Planning

■ 90 percent of the respondents answered that they "have specified disaster scenarios," and 81 percent of the respondents answered that they "have made a business impact analysis of disaster scenarios" (see IV. B. 1. a.).

■ A wider range of potential threats were envisaged in disaster scenarios than in the previous surveys. As for BCPs for new types of pandemics, however, only 20 percent of the respondents answered that they "have formulated relevant BCPs and ensured necessary resources" (see IV. B. 1. b. and c).

■ As disaster scenarios for operational disruptions, 90 percent of the respondents answered that "computer systems fail, and operations are continued by a back-up system," and 75 percent of the respondents answered that "computer systems fail, and operations are continued manually." Meanwhile, only 45 percent of the respondents answered that "areas become inaccessible due to wide-area disasters or administrative measures to limit entry" (see IV. B. 1. d.).

■ 90 percent of the respondents answered that they "have identified critical operations," up from 85 percent in the previous survey. However, 33 percent of the respondents answered that they "have identified but not regularly reviewed critical operations," and only 43 percent of the respondents answered that they "have set specific recovery time objectives for all critical operations" (see IV. B. 1. e. and g.).

2. Resources Necessary for Business Continuity

■ 50 percent of the respondents answered either that they "have made estimates for staff arrangements but have not appointed critical staff" or "need to make estimates for staff arrangements" (see IV. B. 2. a.).

■ 88 percent of the respondents answered that they "have established" a back-up computer center, and 76 percent of the respondents answered that they "have established" a back-up office (see IV. B. 2. b.).

■ 38 percent of the respondents answered that "90 percent or more" of critical operations are covered by their back-up offices, and 43 percent of the respondents answered that "90 percent or more" of critical operations are covered by their back-up computer centers (see IV. B. 2. c.).

3. Recovery Time Objectives for the Most Critical Operations

■ 65 percent of the respondents answered that they set recovery time objectives of "within 4 hours" for the most critical operations (see IV. B. 3.).

4. Back-Up Arrangements for Critical Operations

■ 64 percent of the respondents answered that "processing capacity of a back-up system is equal to that of a main system" (see IV. B. 4. c.).

■ However, only 51 percent of the respondents answered that they "have estimated the time for both data mirroring and data updating and have also examined the compatibility with BCPs" in relation with starting up back-up systems (see IV. B. 4. b.).

5. Decision-making Procedures and Communication Arrangements for BCP Implementation

■ 80 percent of the respondents answered that they "have established" "management systems that ensure the smooth delegation of authority when contact with top management or division heads is not possible" and "ways to contact important external parties such as payment and settlement institutions, outside service providers, and major clients." Meanwhile, only 49 percent of the respondents answered that they "have established" "contact points and ways to contact important external parties when the parties invoke their BCPs" (see IV. B. 5.).

6. Manuals for BCP Implementation

■ Only 26 percent of the respondents answered that they "have prepared manuals for all procedures of critical operations, including follow-up data input and manual operations" (see IV. B. 6. a.).

C. Exercises and Reviews of BCPs

■ 88 percent of the respondents answered that they "conduct exercises on a regular basis." However, only 39 percent of the respondents answered that they "conduct exercises for all of critical operations" (see IV. C. 1. b. and c.).

■ 81 percent of the respondents answered that they "conduct exercises using computer systems and equipment that are to be actually used when BCPs are "invoked." The most commonly conducted exercises are "communication in emergency" and "switch-overs to a back-up computer center with only computer staff involved." Meanwhile, only 32 percent of the respondents answered that they conduct "switch-overs to a back-up computer center with branch offices involved as well," and only 23 percent answered that they conduct "input of unsettled transaction records while switching over to a back-up computer center" (see IV. C. 1. d. and f.).

■ 58 percent of the respondents answered that they "have assessed the attainability of recovery time objectives, identified challenges, reported to management, and reviewed BCPs as appropriate" (see IV. C. 2.).

■ 99 percent of the respondents answered that they "have participated in joint exercises" organized by other financial institutions, and 96 percent of the respondents affirm the need to enhance joint exercises (see IV. C. 3. a. and b.).

D. Overall Assessment

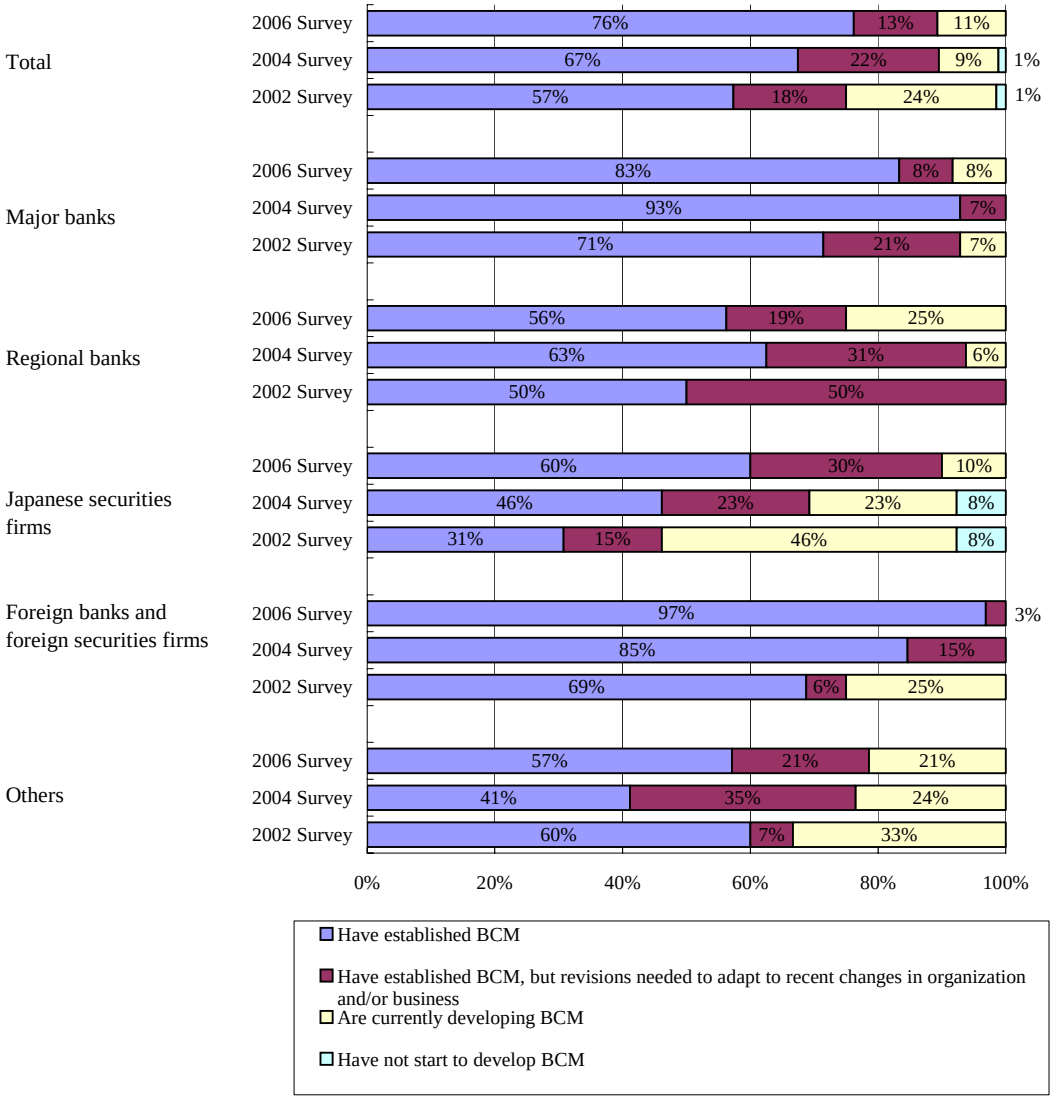
■ Only 14 percent of the respondents answered that "feasibility of business continuity has been secured," whereas 62 percent of the respondents answered that "feasibility of business continuity has been mostly secured although some uncertainties remain" (see IV. D. 1.).

■ As for critical issues to be addressed, 65 percent of the respondents answered that they should "expand or refine BCPs," and 49 percent of the respondents answered that they should "improve back-up facilities" (see IV. D. 2.).

IV. Survey Results

A. Framework for Developing Business Continuity Management (BCM)

1. Development of BCM

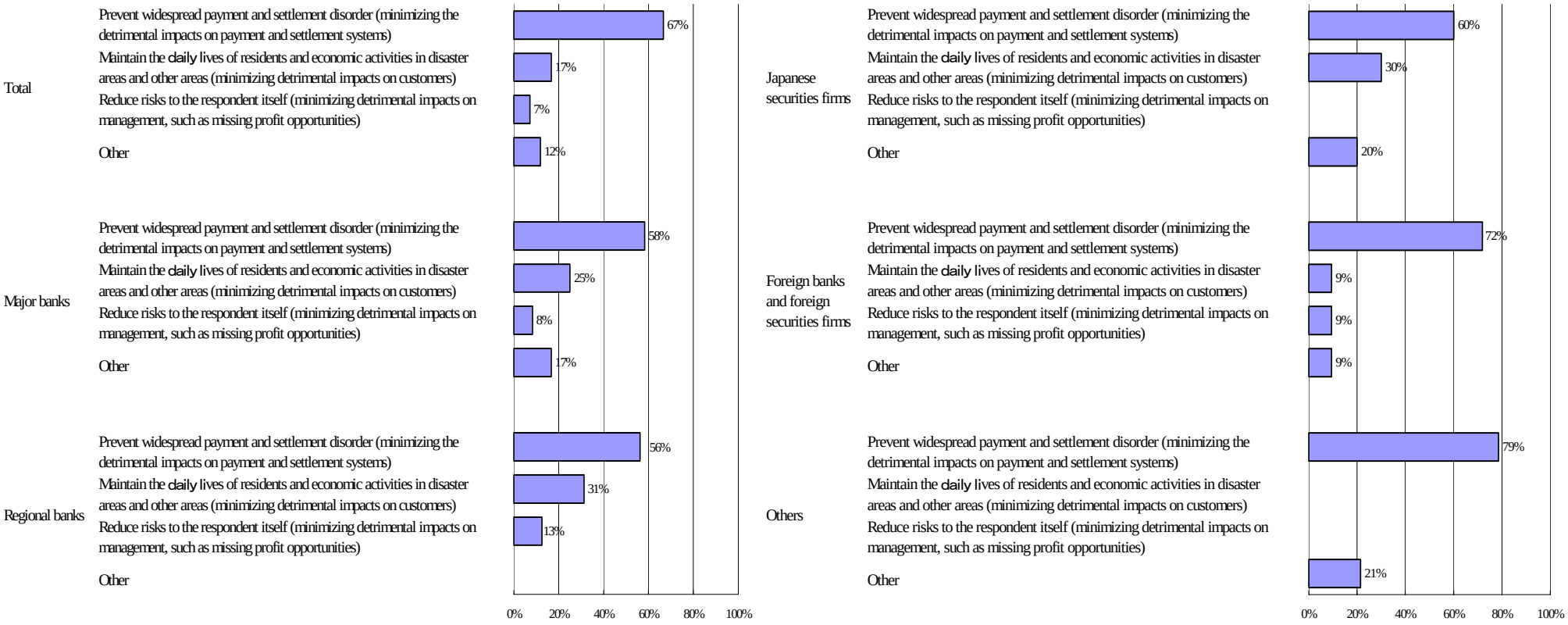


■ 76 percent of the respondents answered that they "have established BCM," up from 67 percent in the previous survey in 2004.

■ By type of financial institution, 83 percent of major banks and 97 percent of foreign banks and foreign securities firms responded that they "have established BCM." Meanwhile, only 56 percent of regional banks and 60 percent of Japanese securities firms responded likewise.

2. Objectives of Business Continuity[2]

(Percentage of the respondents that mentioned each objective as the most important one)



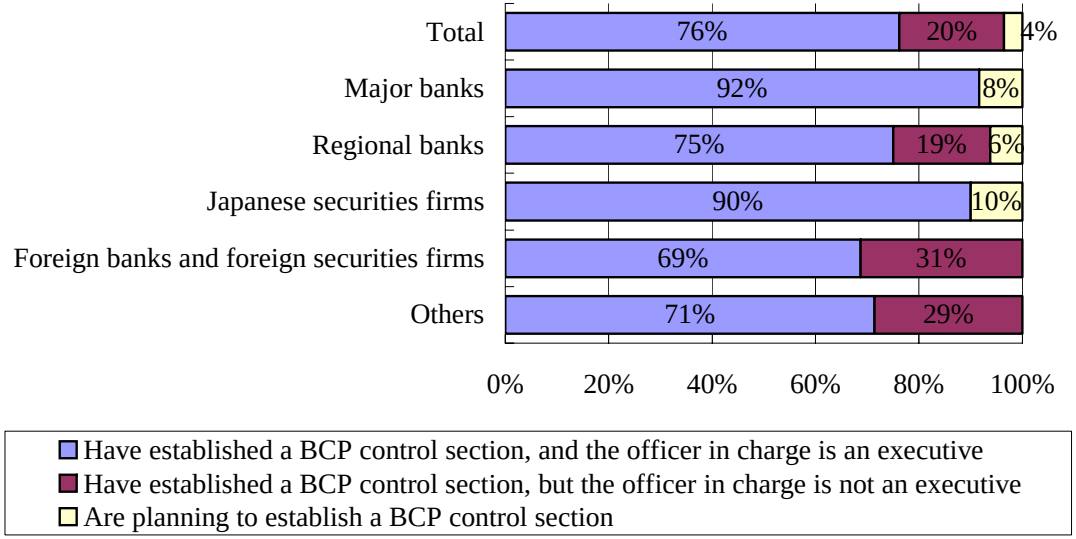
■ 67 percent of the respondents answered that they "prevent widespread payment and settlement disorder," and 17 percent of the respondents answered that they "maintain the daily lives of residents and economic activities in disaster areas and other areas" as the most important objective of business continuity.

▼ Other responses included answers such as to "ensure the safety of customers and employees," "protect customers' assets," and "take social responsibility and maintain reputation."

[2] Multiple answers were allowed.

3. Sections in Charge of Formulating and Reviewing Business Continuity Plans (BCPs)

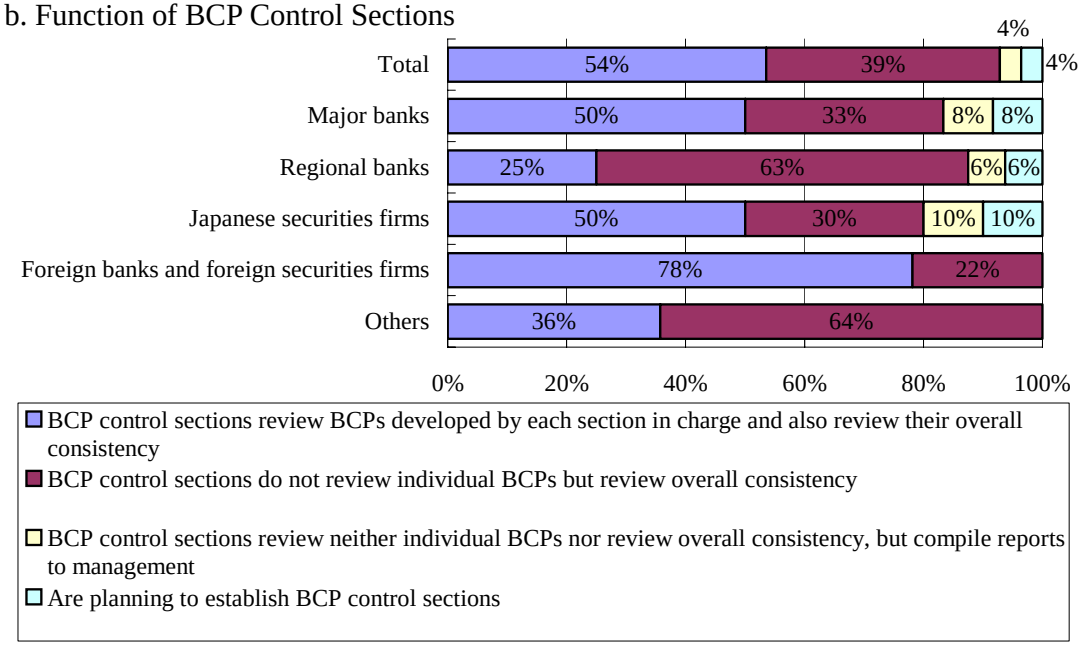
a. Establishment of BCP Control Sections



■ 76 percent of the respondents answered that they "have established a BCP control section, and the officer in charge is an executive."

■ By type of financial institution, 92 percent of major banks and 90 percent of Japanese securities firms responded that they "have established a BCP control section, and the officer in charge is an executive."

b. Function of BCP Control Sections



■ Only 54 percent of the respondents answered that their "BCP control sections review BCPs developed by each section in charge and also review their overall consistency."

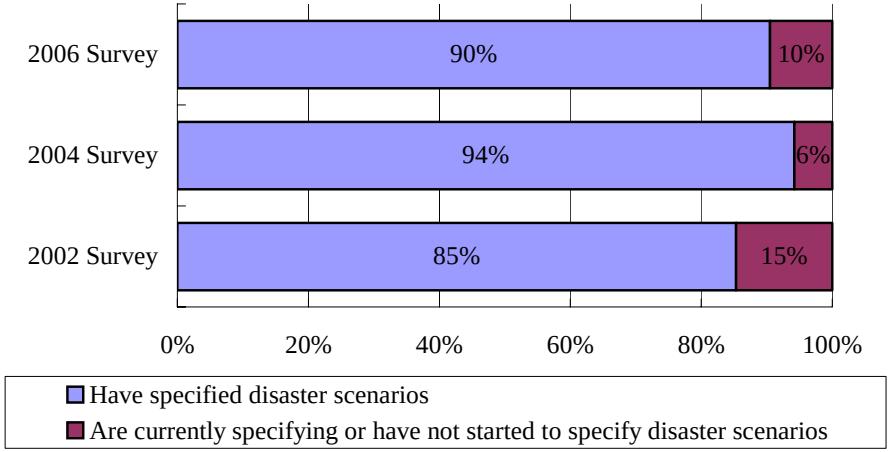
■ By type of financial institution, 78 percent of foreign banks and foreign securities firms responded that their "BCP control sections review BCPs developed by each section in charge and also review their overall consistency," while only 50 percent of major banks and 25 percent of regional banks responded likewise.

B. Business Continuity Planning

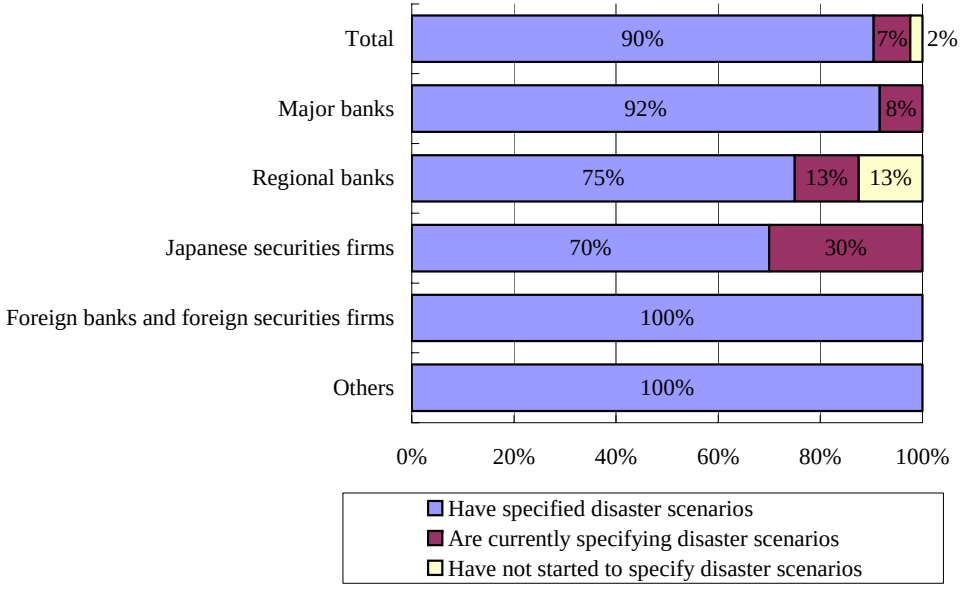
1. Assumptions and Conditions for Business Continuity Planning

a. Disaster Scenarios

(1) Specification of Disaster Scenarios



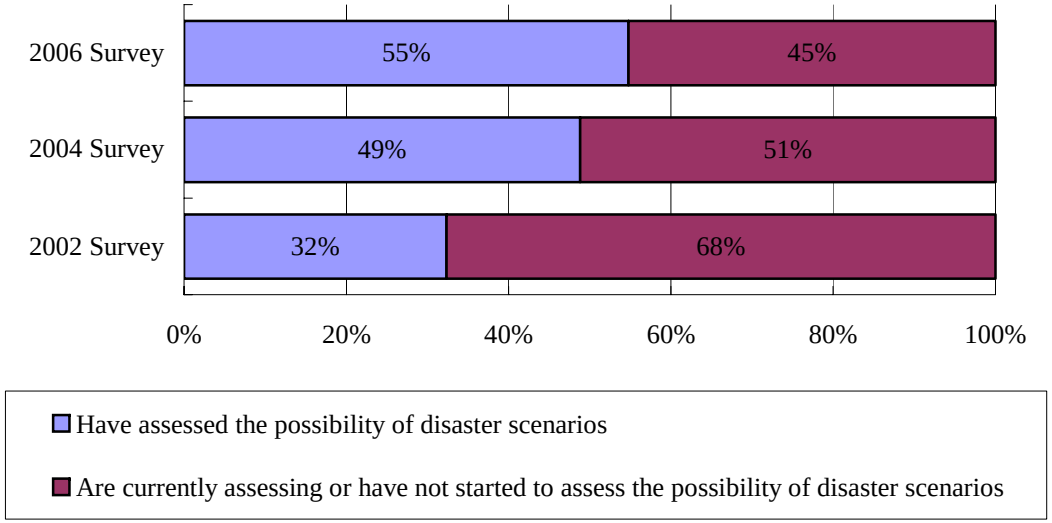
■ 90 percent of the respondents answered that they "have specified disaster scenarios."



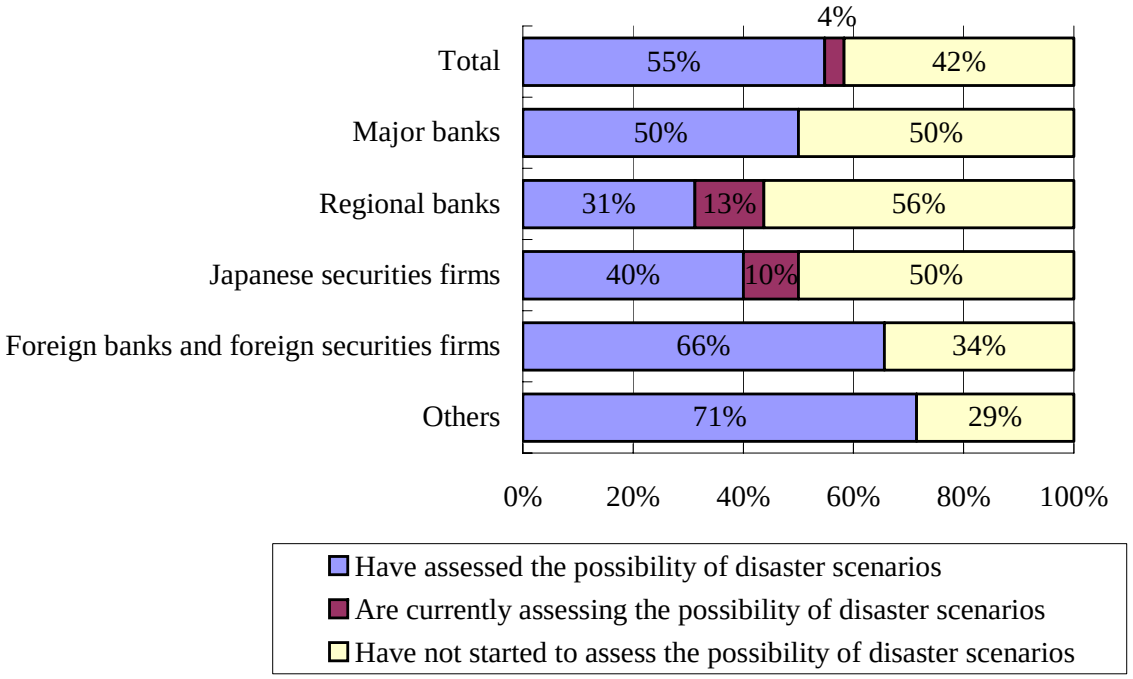
■ By type of financial institution, 92 percent of major banks and all foreign banks and foreign securities firms responded that they "have specified disaster scenarios."

■ On the other hand, only 75 percent of regional banks and 70 percent of Japanese securities firms responded likewise, while the remainder answered that they "are currently specifying disaster scenarios" or "have not started to specify disaster scenarios."

(2) Assessment of the Possibility of Disaster Scenarios

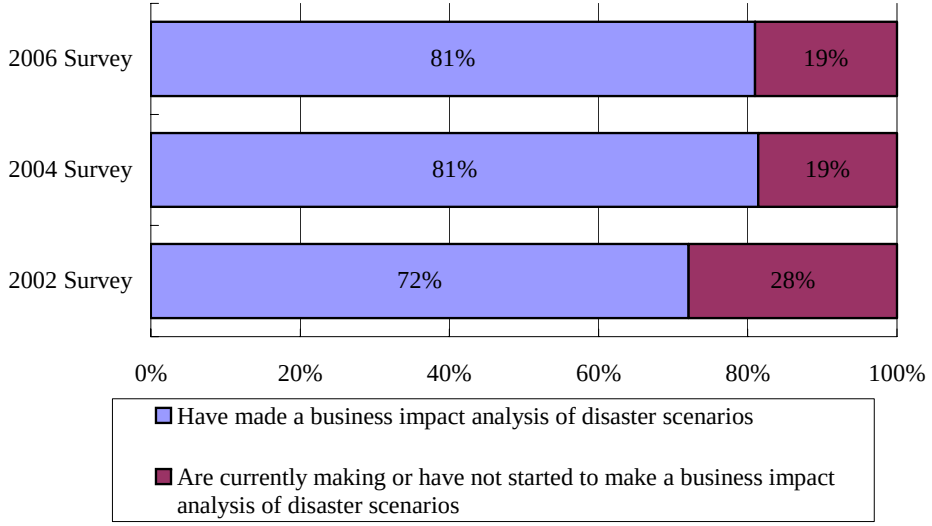


■ 55 percent of the respondents answered that they "have assessed the possibility of disaster scenarios."

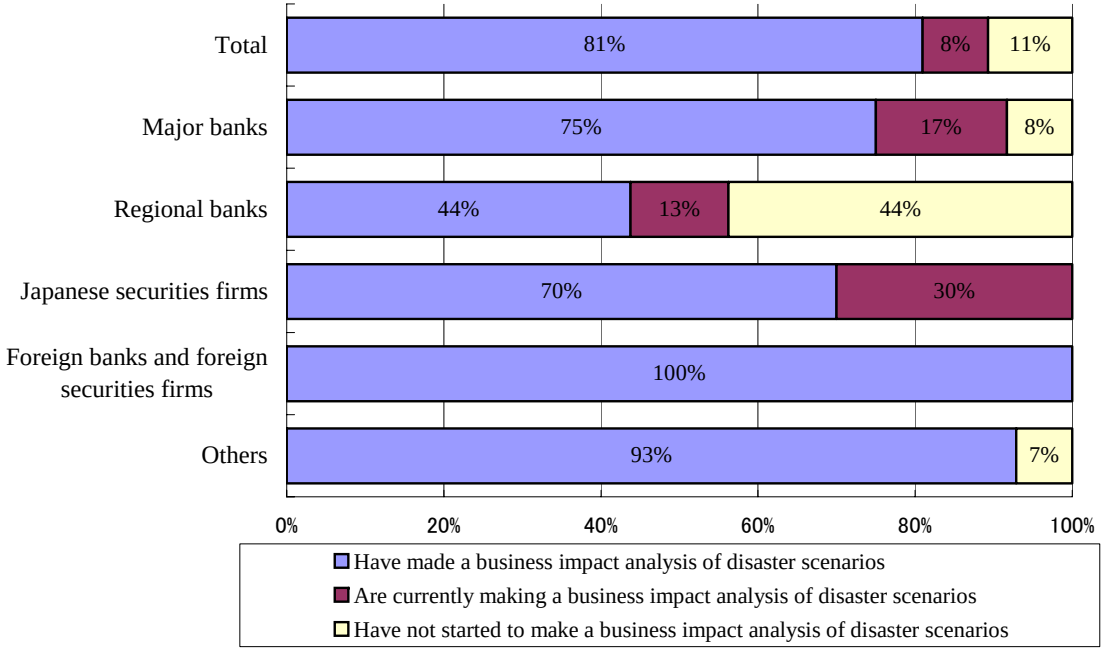


■ By type of financial institution, 50 percent of major banks, 31 percent of regional banks, and 40 percent of Japanese securities firms responded that they "have assessed the possibility of disaster scenarios."

(3) Business Impact Analysis of Disaster Scenarios

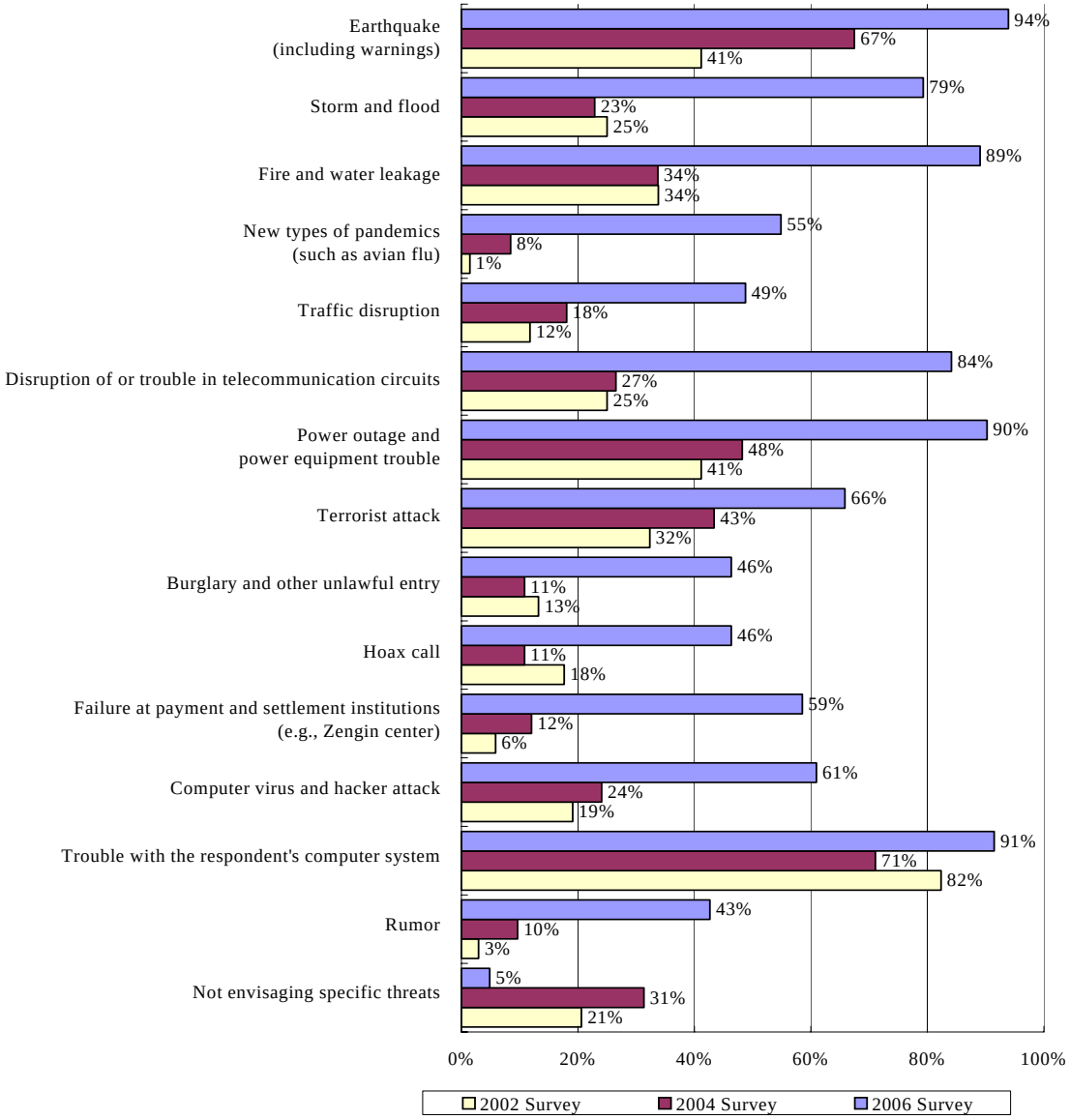


■ 81 percent of the respondents answered that they "have made a business impact analysis of disaster scenarios."



■ By type of financial institution, 75 percent of major banks and all foreign banks and securities firms responded that they "have made a business impact analysis of disaster scenarios," while only 44 percent of regional banks responded likewise.

b. Potential Threats in Disaster Scenarios[3]



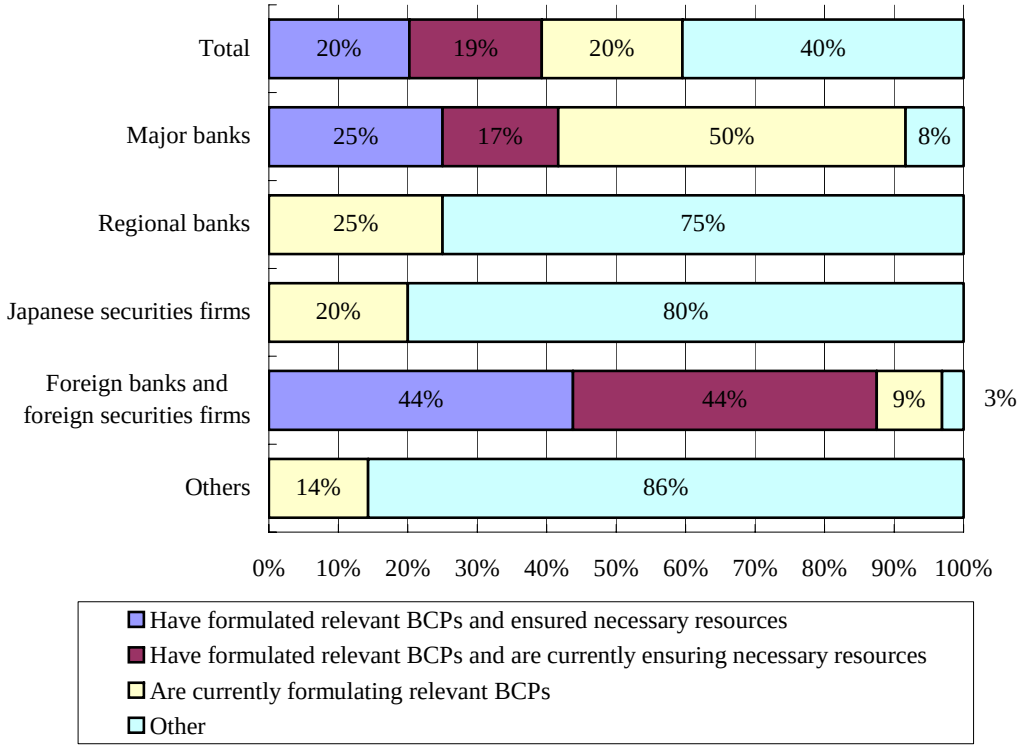
■ In the latest survey, a wider range of potential threats were envisaged in disaster scenarios than in the previous surveys.

▼ While responses concentrated on such threats as "trouble with the respondent's computer system" and "earthquake" in the previous surveys, respondents in the latest survey envisage a wider range of potential threats, including "disruption of or trouble in telecommunication circuits," "computer virus and hacker attack," and "new types of pandemics."

▼ Other responses included answers such as "nuclear power plant accident," "volcanic eruption," "financial crime," and "information leakage."

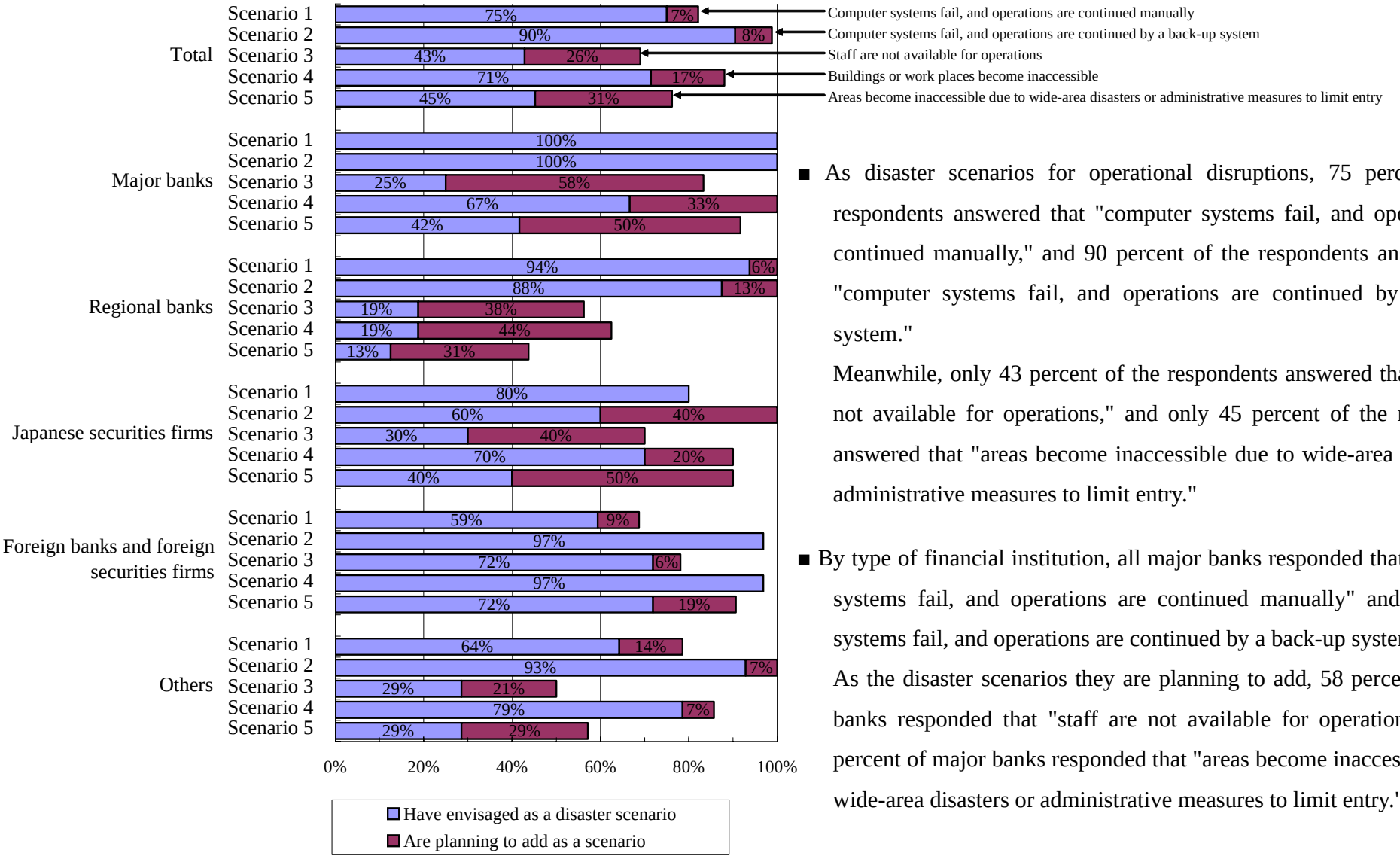
[3] Multiple answers were allowed.

c. BCPs for New Types of Pandemics (Such as Avian Flu)



■ Only 20 percent of the respondents answered that they "have formulated relevant BCPs and ensured necessary resources" for staff shortage lasting for a period of time caused by the outbreak of new types of pandemics.

d. Disaster Scenarios for Operational Disruptions



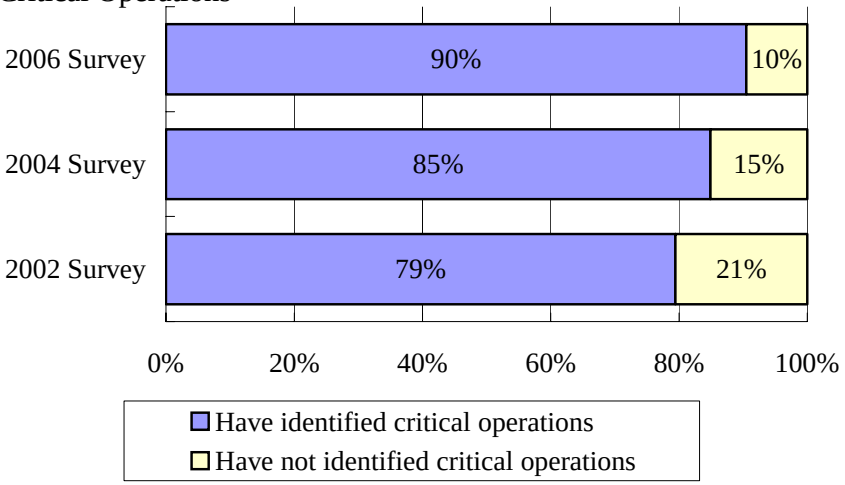
■ As disaster scenarios for operational disruptions, 75 percent of the respondents answered that "computer systems fail, and operations are continued manually," and 90 percent of the respondents answered that "computer systems fail, and operations are continued by a back-up system."

Meanwhile, only 43 percent of the respondents answered that "staff are not available for operations," and only 45 percent of the respondents answered that "areas become inaccessible due to wide-area disasters or administrative measures to limit entry."

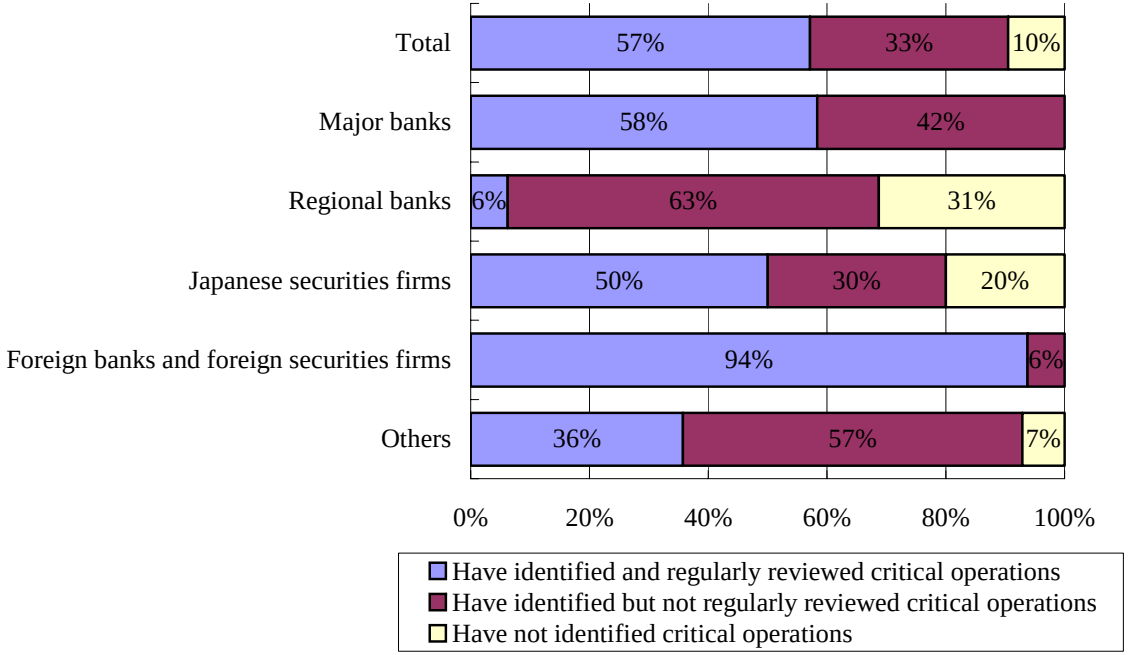
■ By type of financial institution, all major banks responded that "computer systems fail, and operations are continued manually" and "computer systems fail, and operations are continued by a back-up system."

As the disaster scenarios they are planning to add, 58 percent of major banks responded that "staff are not available for operations," and 50 percent of major banks responded that "areas become inaccessible due to wide-area disasters or administrative measures to limit entry."

e. Identification of Critical Operations



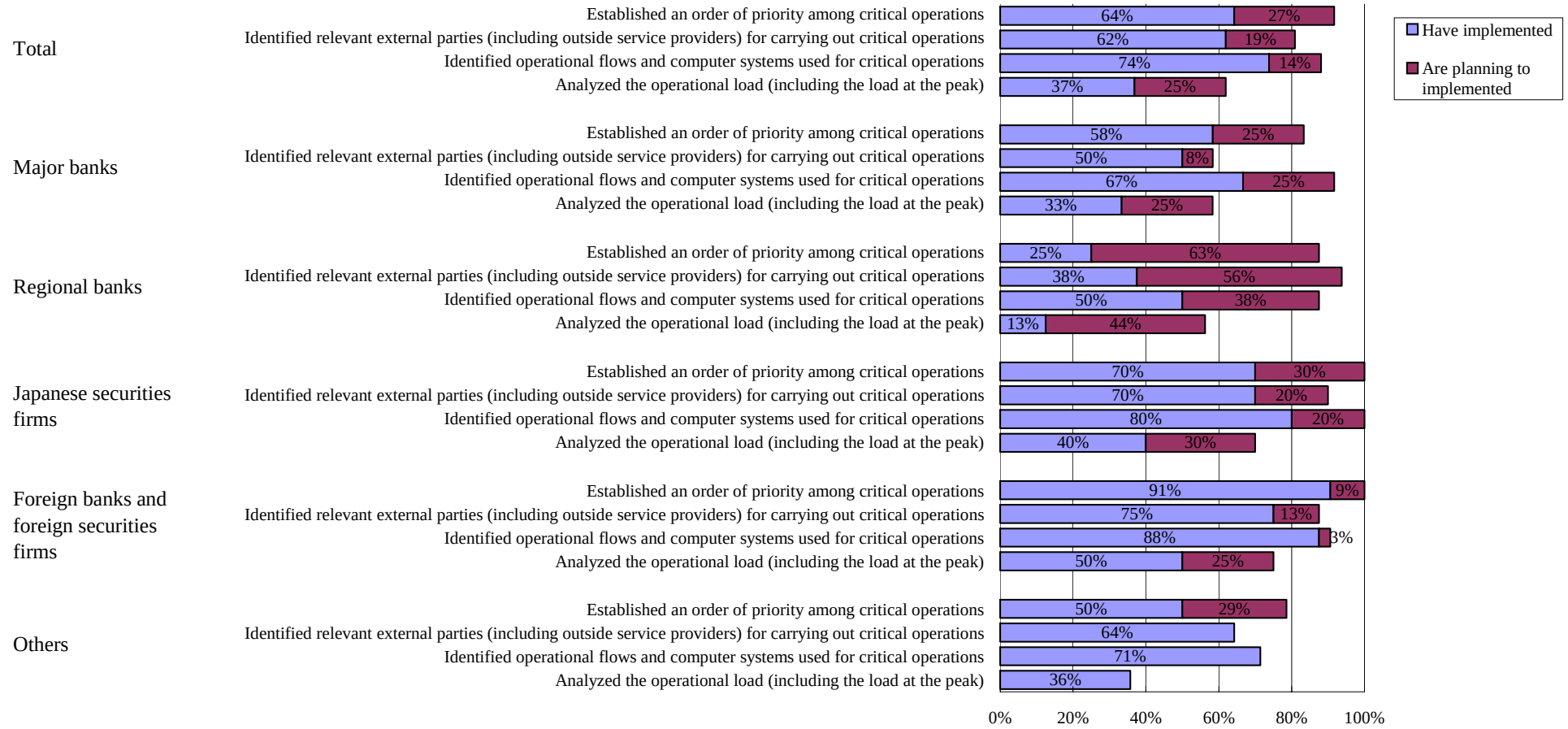
■ 90 percent of the respondents answered that they "have identified critical operations," up from 85 percent in the previous survey.



■ The breakdown of the responses to this question shows that only 57 percent of the respondents answered that they "have identified and regularly reviewed critical operations" and 33 percent of the respondents answered that they "have identified but not regularly reviewed critical operations."

■ By type of financial institution, 94 percent of foreign banks and foreign securities firms responded that they "have identified and regularly reviewed critical operations."

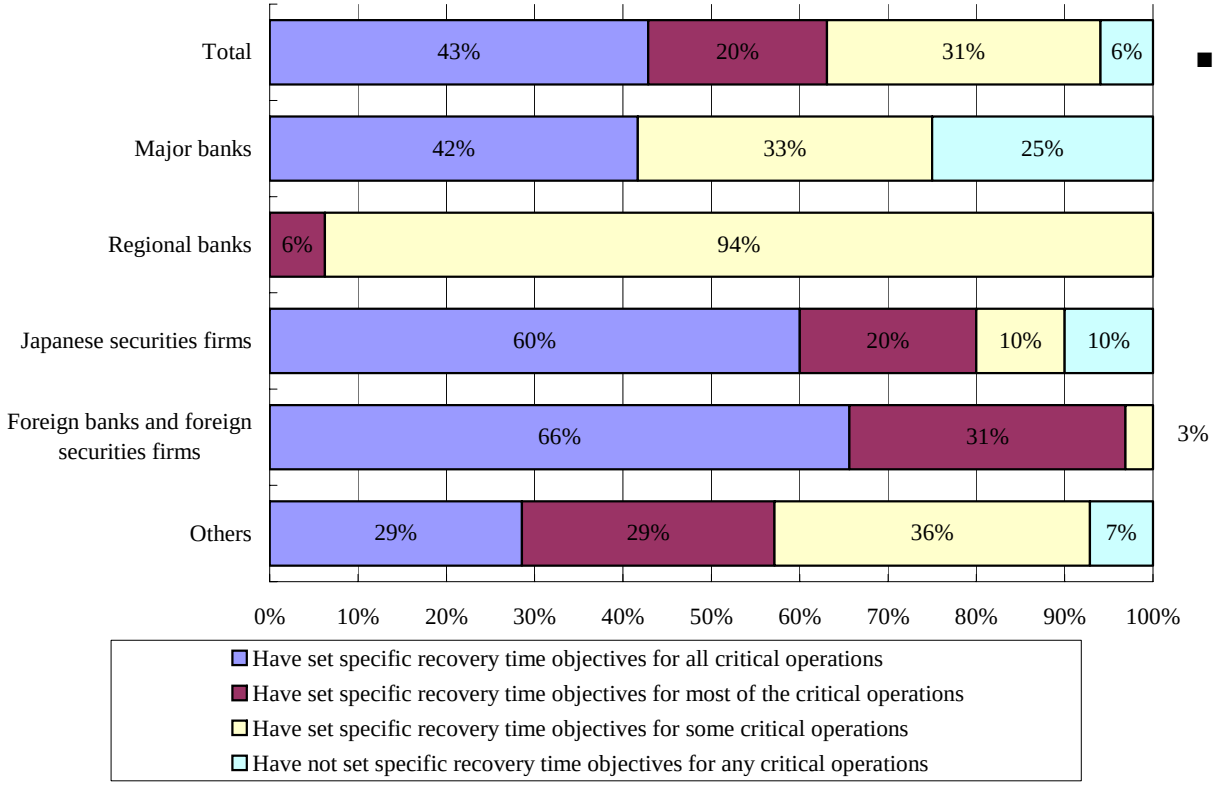
f. Approaches to Business Continuity with regard to Critical Operations



■ As for approaches to business continuity, more than 60 percent of the respondents answered that they have "established an order of priority among critical operations," "identified relevant external parties (including outside service providers) for carrying out critical operations," and "identified operational flows and computer systems used for critical operations." Meanwhile, only 37 percent of the respondents answered that they have "analyzed the operational load (including the load at the peak)."

▼ Other responses included answers such as "established an order of priority among critical operations at the head office" and "identified resources necessary for continuing critical operations."

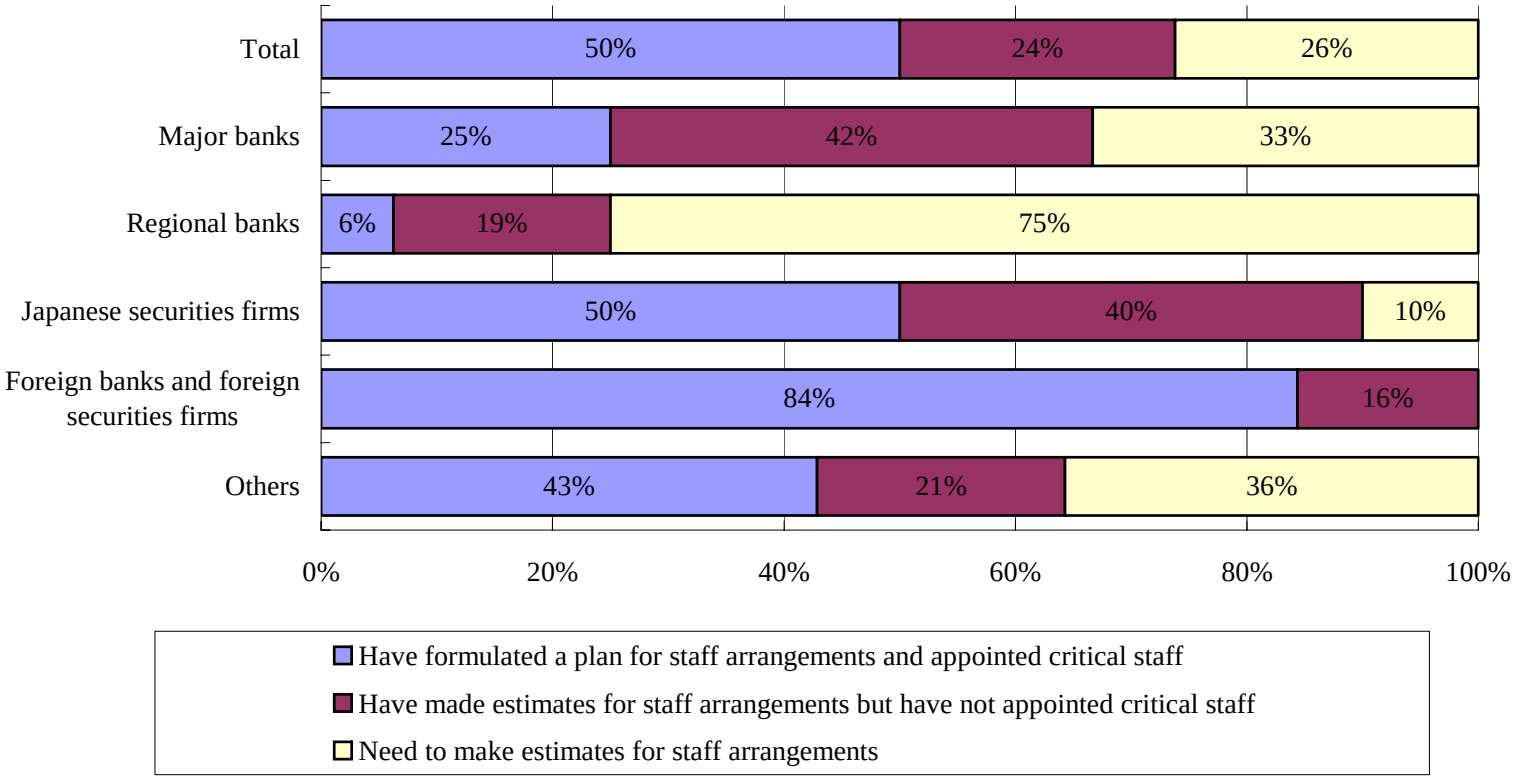
g. Recovery Time Objectives for Critical Operations



■ Only 43 percent of the respondents answered that they "have set specific recovery time objectives for all critical operations."

2. Resources Necessary for Business Continuity

a. Staff

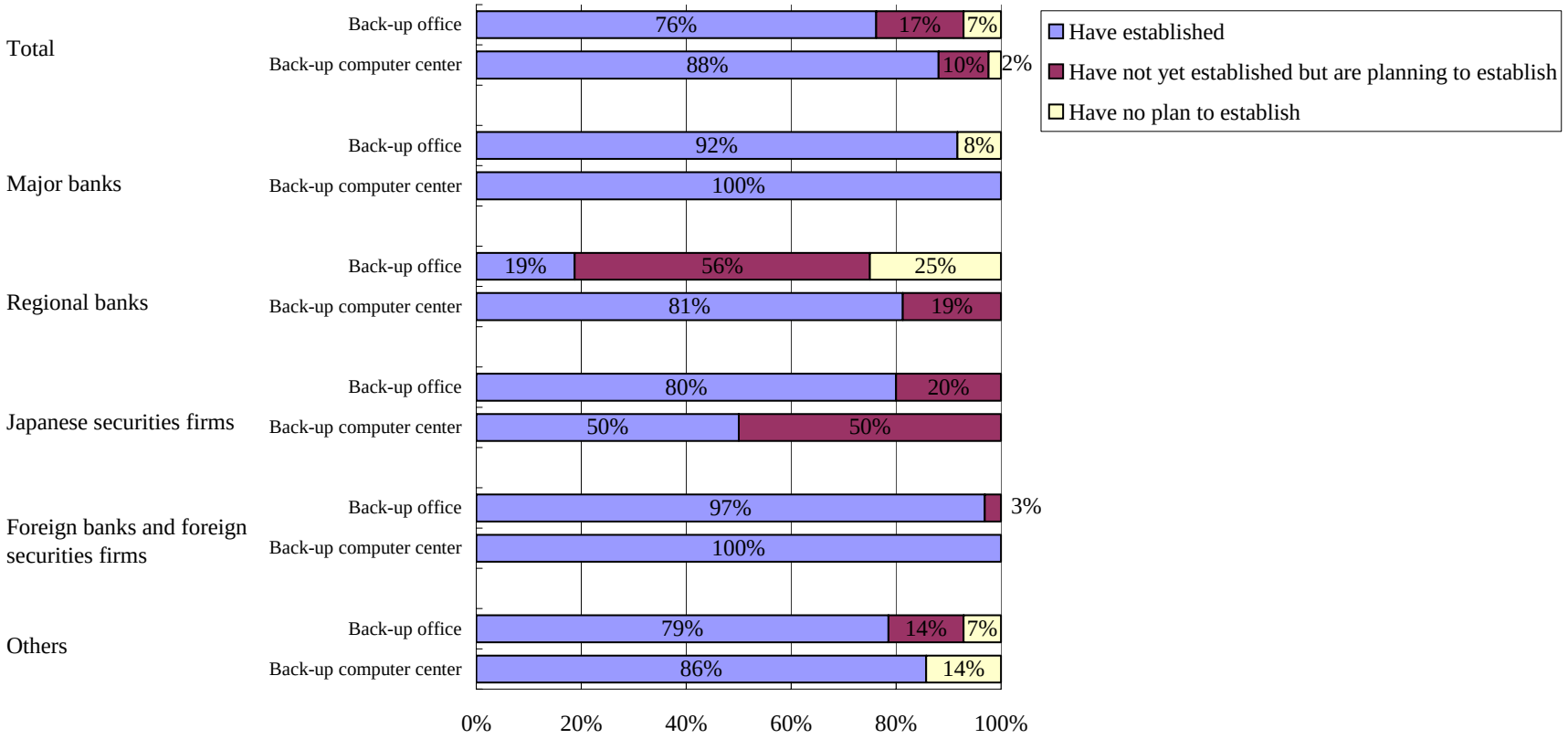


■ 50 percent of the respondents answered that they "have made estimates for staff arrangements but have not appointed critical staff" or "need to make estimates for staff arrangements."

■ By type of financial institution, 75 percent of major banks and 94 percent of regional banks responded that they "have formulated a plan for staff arrangements but have not appointed critical staff" or "need to make estimates for staff arrangements."

Meanwhile, 84 percent of foreign banks and foreign securities firms responded that they "have formulated a plan for staff arrangements and appointed critical staff."

b. Back-Up Facilities

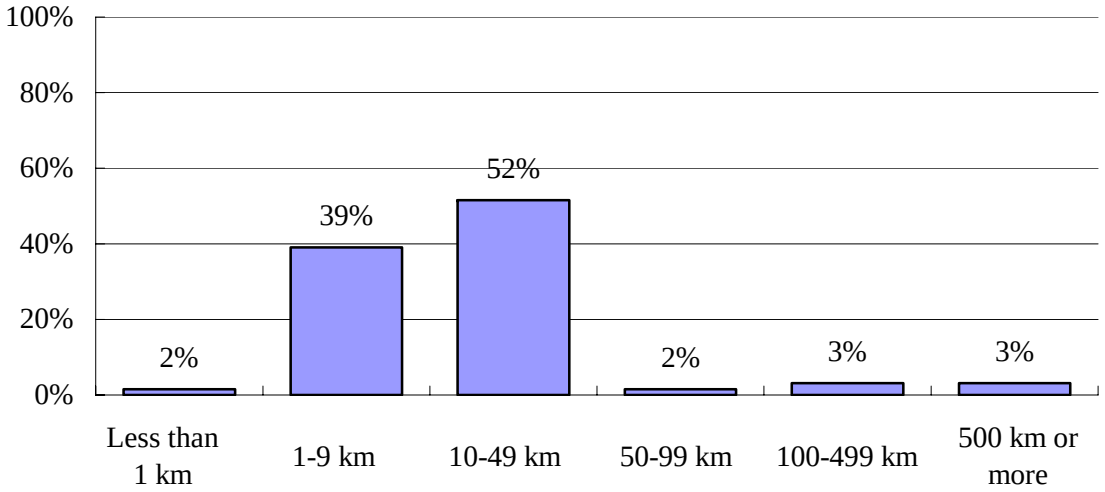


■ 76 percent of the respondents answered that they "have established" a back-up office, and 88 percent of the respondents answered that they "have established" a back-up computer center.

■ By type of financial institution, most major banks as well as foreign banks and foreign securities firms responded that they "have established" both a back-up office and a back-up computer center.

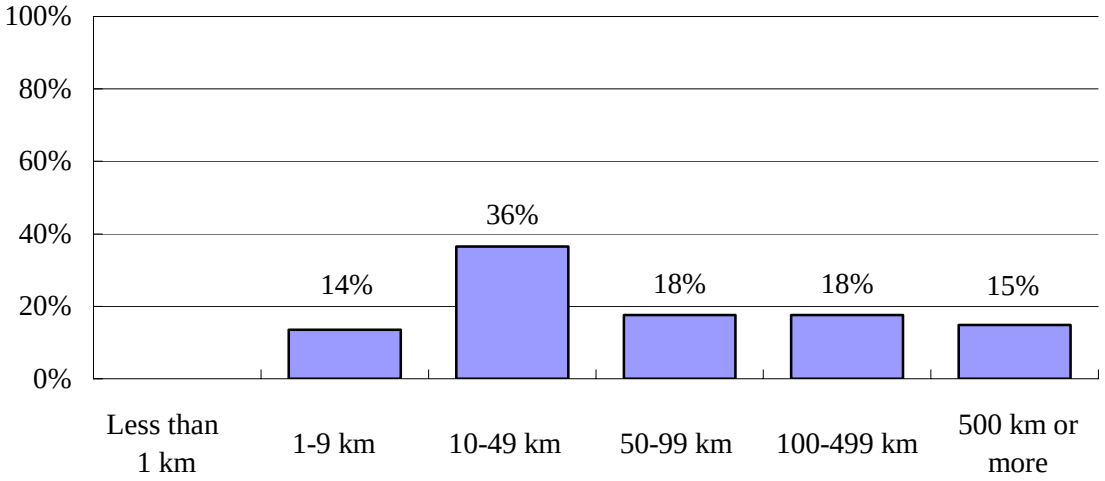
On the other hand, only 50 percent of Japanese securities firms responded that they "have established" a back-up computer center, while the other 50 percent responded that they "have not yet established but are planning to establish."

(1) Distance between Main and Back-Up Offices



■ Among respondents who answered that they "have established" a back-up office, 91 percent answered that they had established their back-up offices within a range of 1 to 49 kilometers from their main offices.

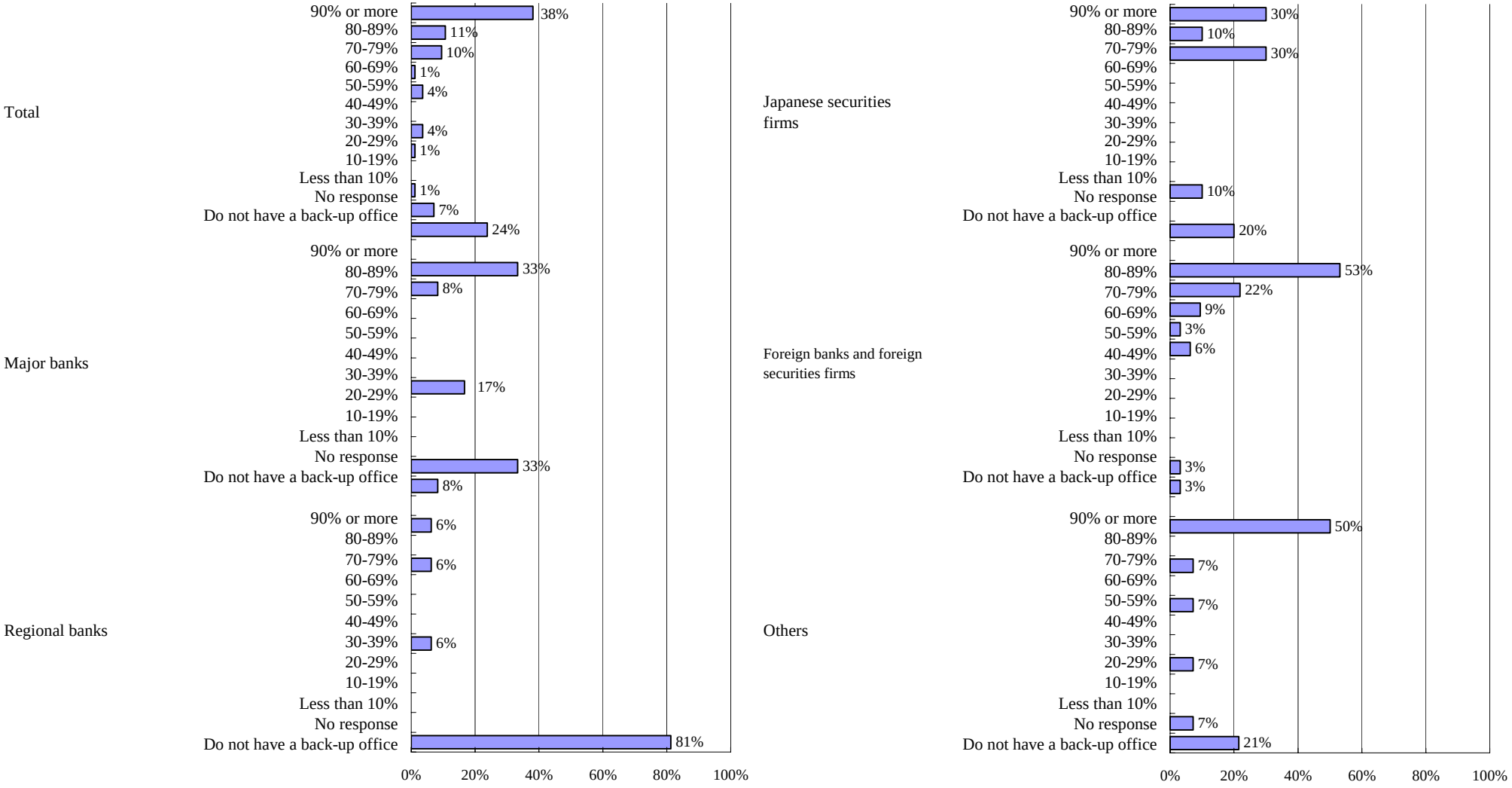
(2) Distance between Main and Back-Up Computer Centers



■ Among respondents who answered that they "have established" a back-up computer center, 36 percent answered that they had established their back-up computer centers within a range of 10 to 49 kilometers from their main offices, and this response was chosen most often.

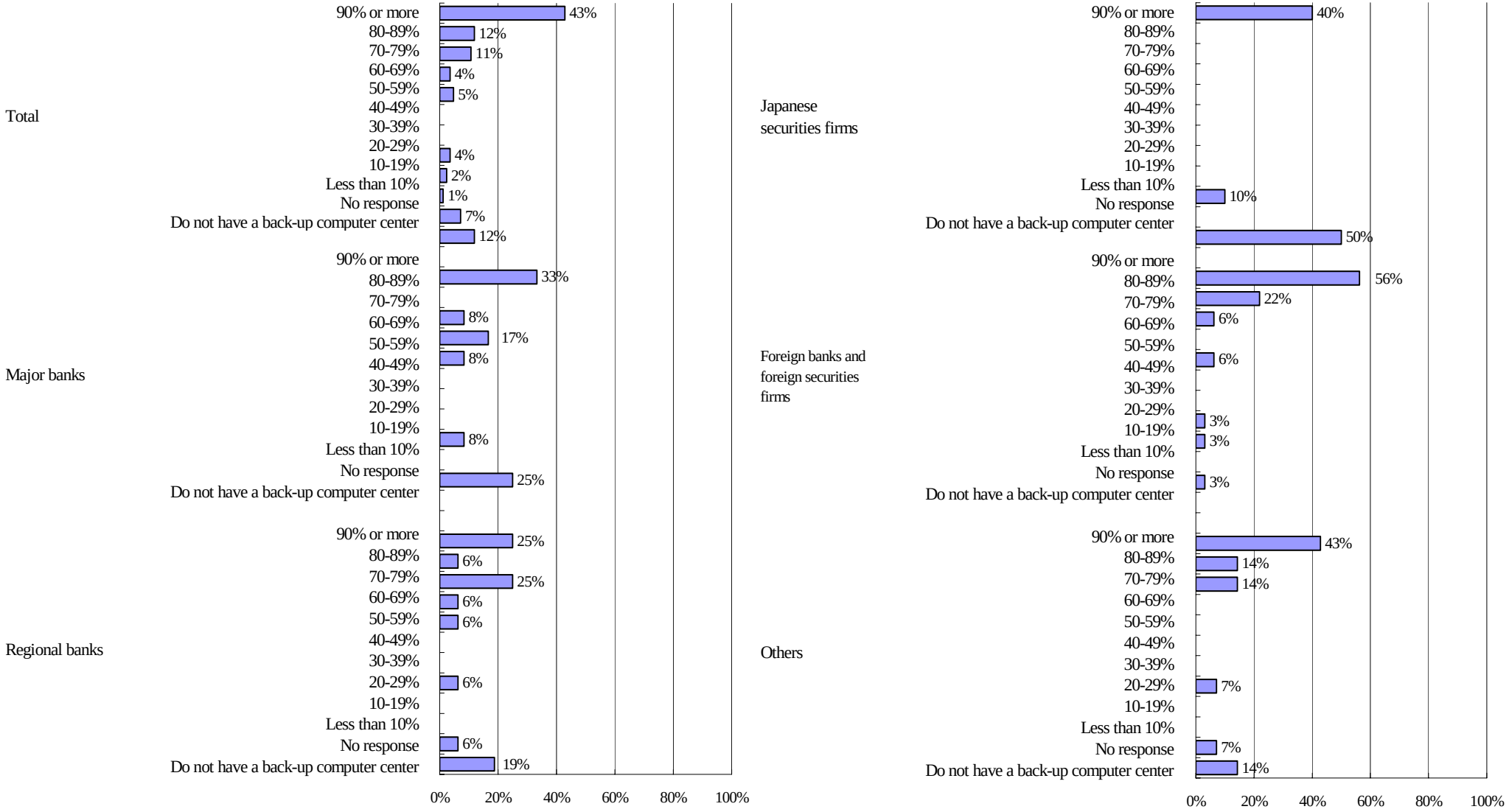
c. Critical Operations Covered by Back-Up Facilities

(1) Critical Operations Covered by Back-Up Offices



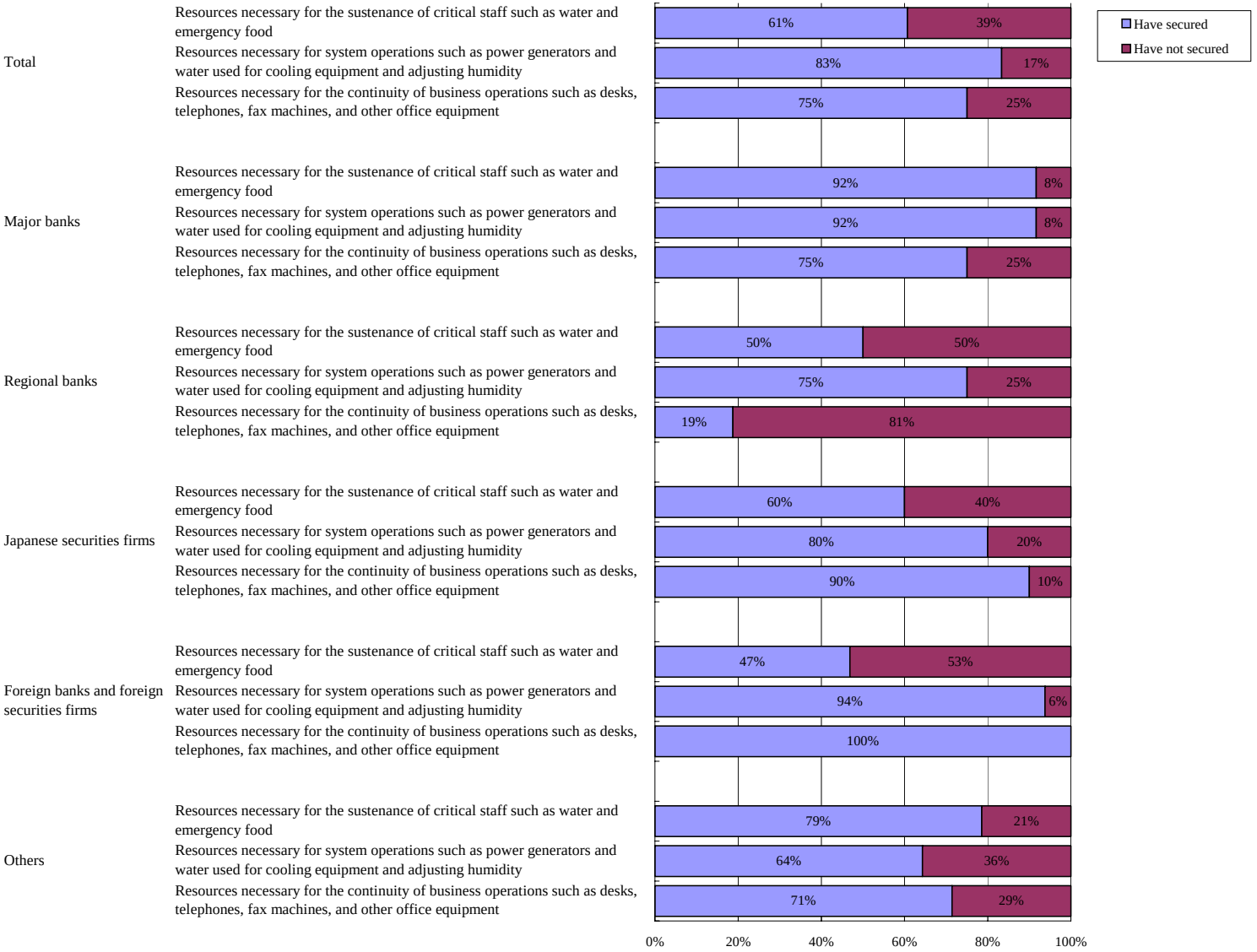
■ 38 percent of the respondents answered that "90 percent or more" of critical operations are covered by their back-up offices.

(2) Critical Operations Covered by Back-Up Computer Centers



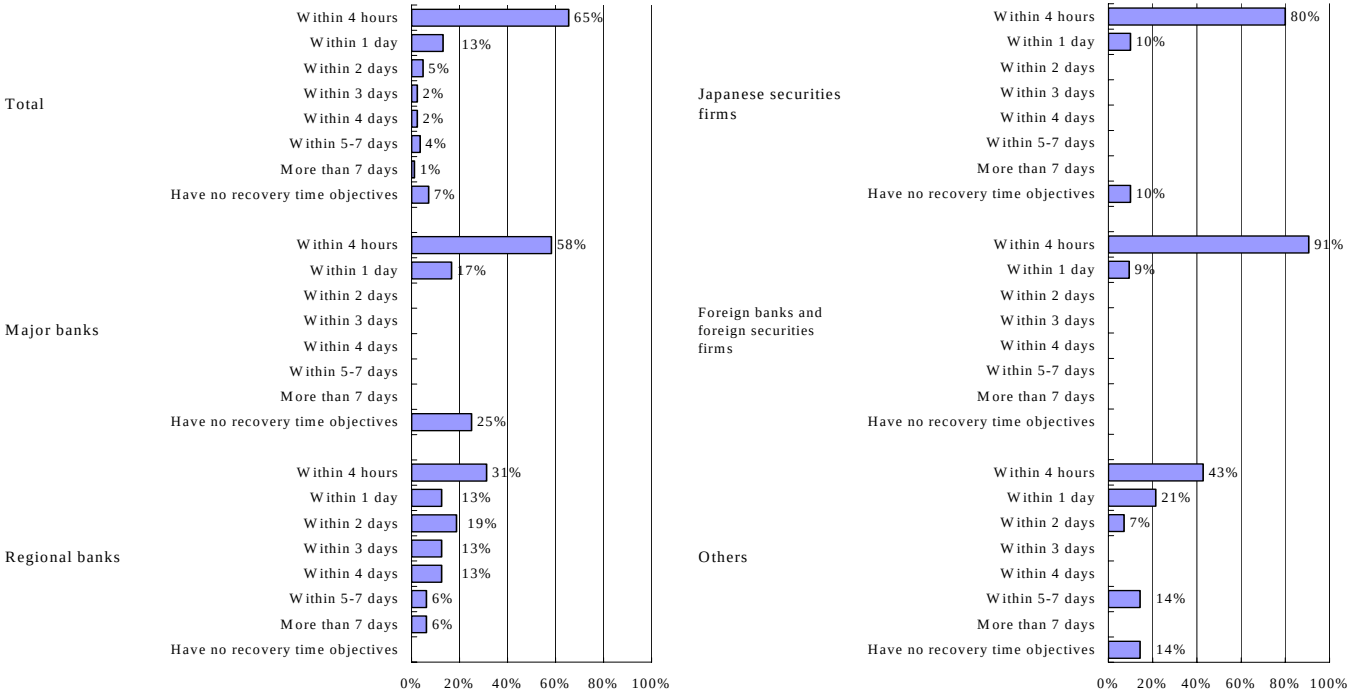
■ 43 percent of the respondents answered that "90 percent or more" of critical operations are covered by their back-up computer centers.

d. Other Back-Up Resources



■ More than 60 percent of the respondents answered that they "have secured" all three categories of back-up resources.

3. Recovery Time Objectives for the Most Critical Operations



■ 65 percent of the respondents answered that they set recovery time objectives of "within 4 hours" for the most critical operations.

■ By type of financial institution, 80 percent of Japanese securities firms and 91 percent of foreign banks and foreign securities firms responded that they set recovery time objectives of "within 4 hours."

58 percent of major banks responded that they set recovery time objectives of "within 4 hours," while 25 percent of major banks responded that they "have no recovery time objectives."

On the other hand, 31 percent of regional banks responded that they set recovery time objectives of "within 4 hours," while remaining regional banks, the responses varied from "within 1 day" to "more than 7 days."

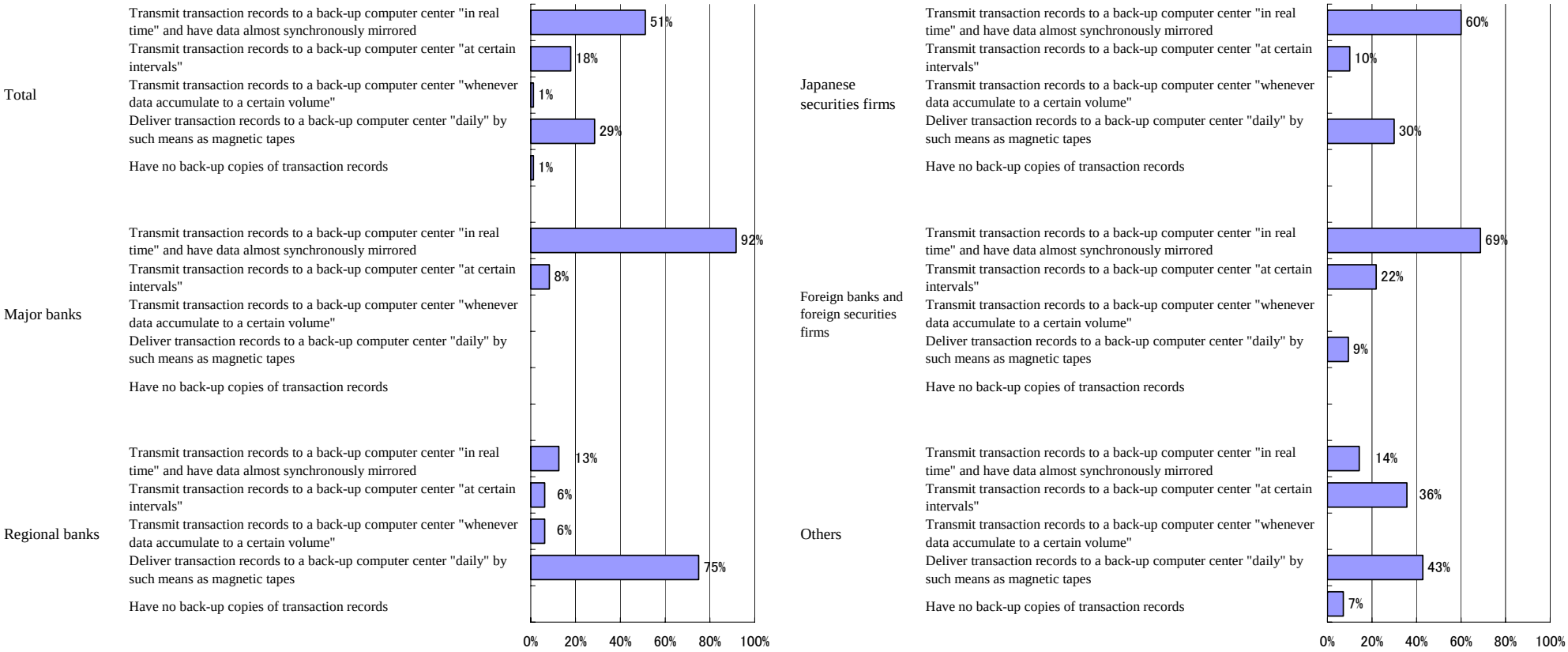
Operations cited as the most critical

Banks: Operations related to deposits, funds transfer, funds settlement, credit extension, and liquidity management

Securities firms: Operations related to securities contracts and settlement of funds and securities

4. Back-Up Arrangements for Critical Operations

a. Back-Up Methods for Transaction Records

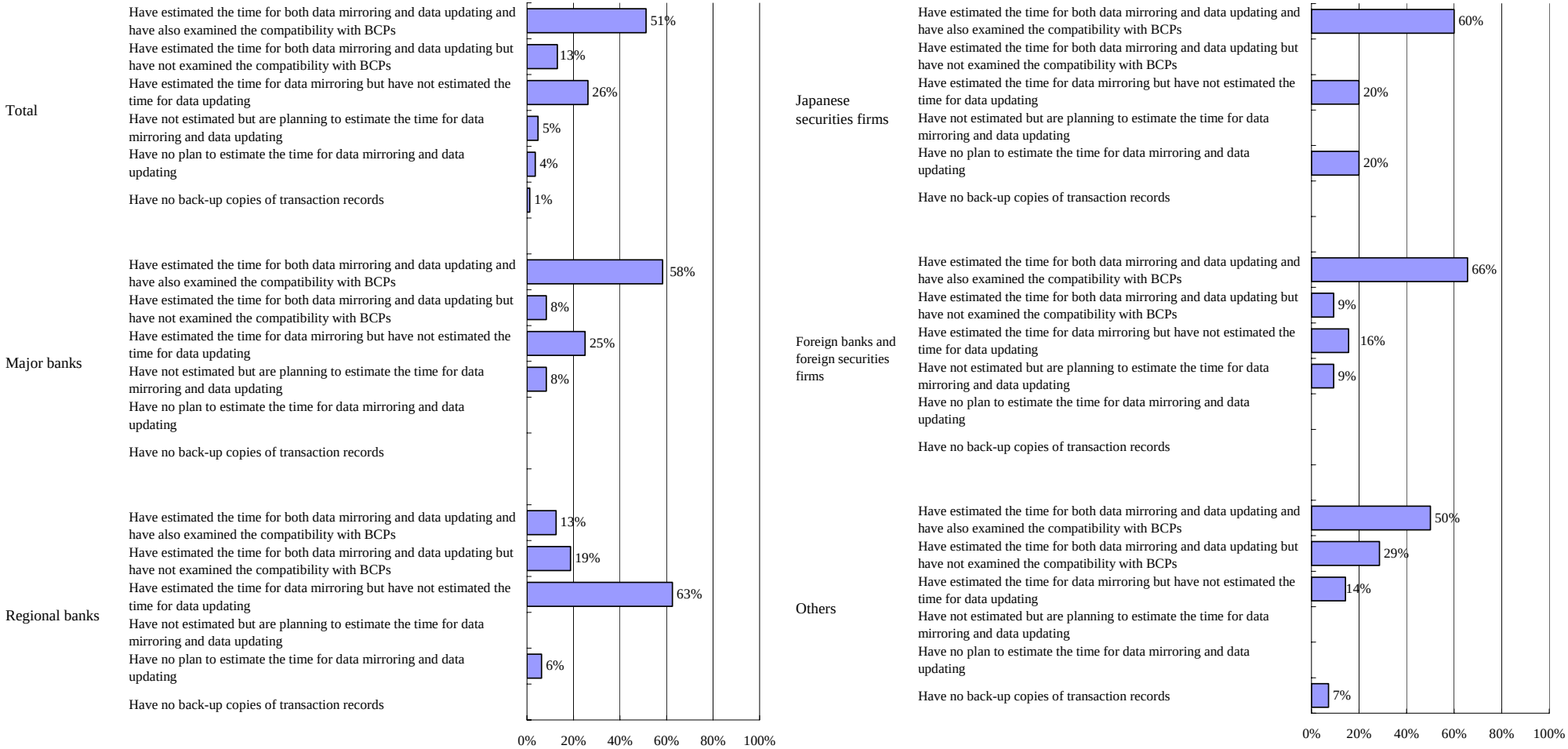


■ 51 percent of the respondents answered that they "transmit transaction records to a back-up computer center 'in real time' and have data almost synchronously mirrored."

■ By type of financial institution, 92 percent of major banks and 69 percent of foreign banks and foreign securities firms responded that they "transmit transaction records to a back-up computer center 'in real time' and have data almost synchronously mirrored."

On the other hand, 75 percent of regional banks responded that they "deliver transaction records to a back-up computer center 'daily' by such means as magnetic tapes."

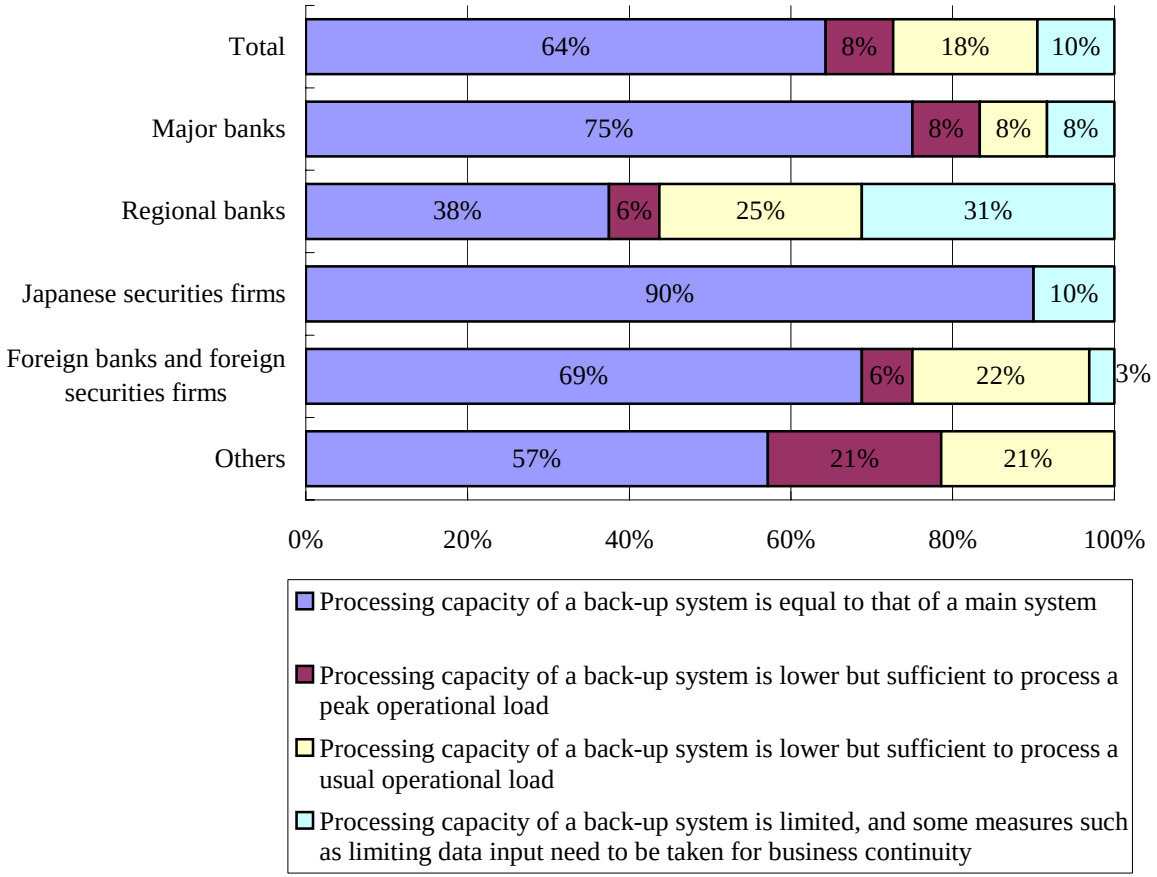
b. Time for Mirroring and Updating of Transaction Records[4]



■ Only 51 percent of the respondents answered that they "have estimated the time for both data mirroring and data updating and have also examined the compatibility with BCPs" in relation with starting up back-up systems.

4 "Data mirroring" refers to the mirroring of transaction records onto a back-up system using the back-up data. "Data updating" refers to the follow-up input of transaction records that are not in the back-up data as well as the identification and input of unsettled transaction records.

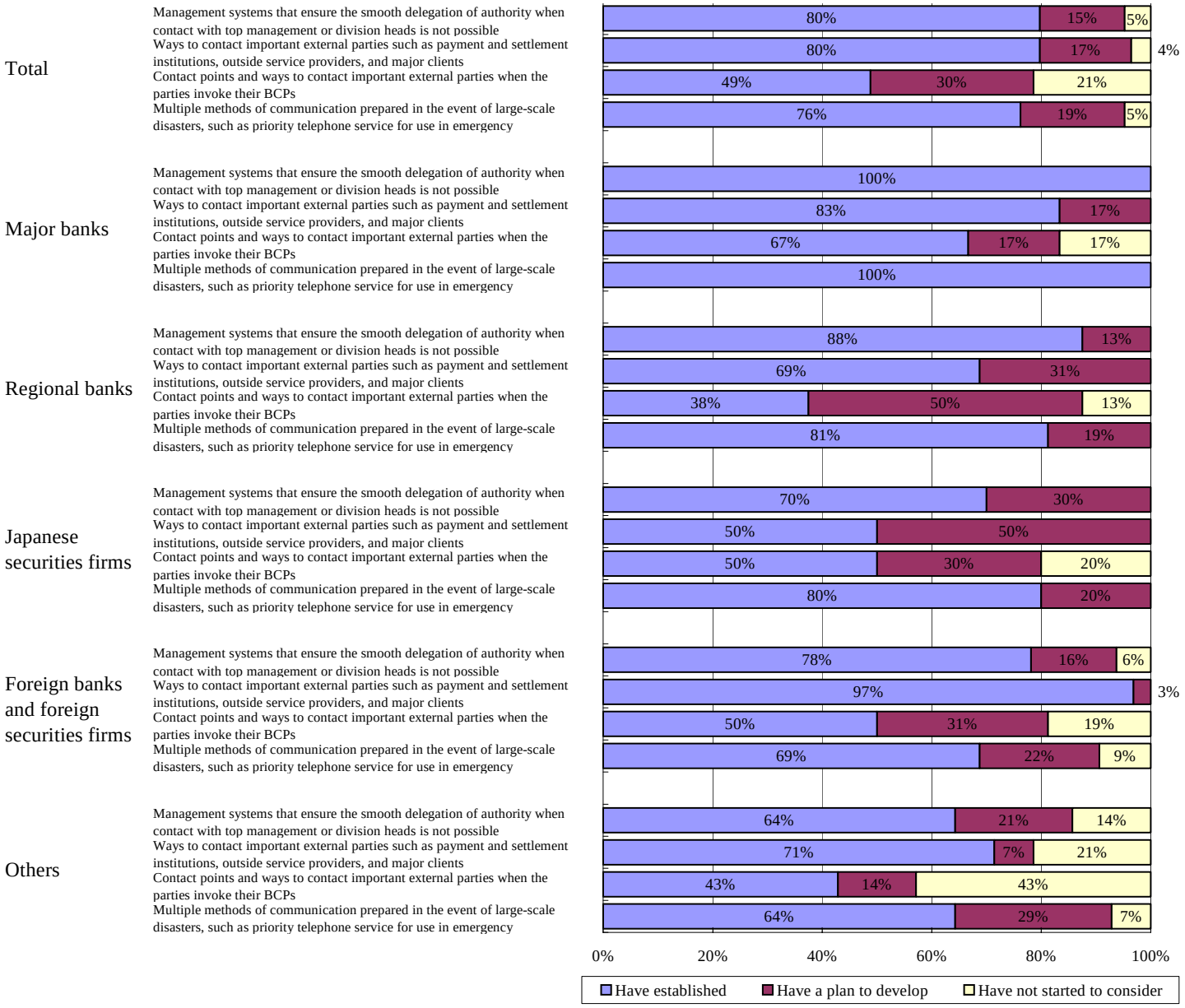
c. Processing Capacity of Back-Up Systems Compared to Main Systems



■ 64 percent of the respondents answered that "processing capacity of a back-up system is equal to that of a main system."

■ By type of financial institution, 75 percent of major banks and 90 percent of Japanese securities firms responded that "processing capacity of a back-up system is equal to that of a main system."

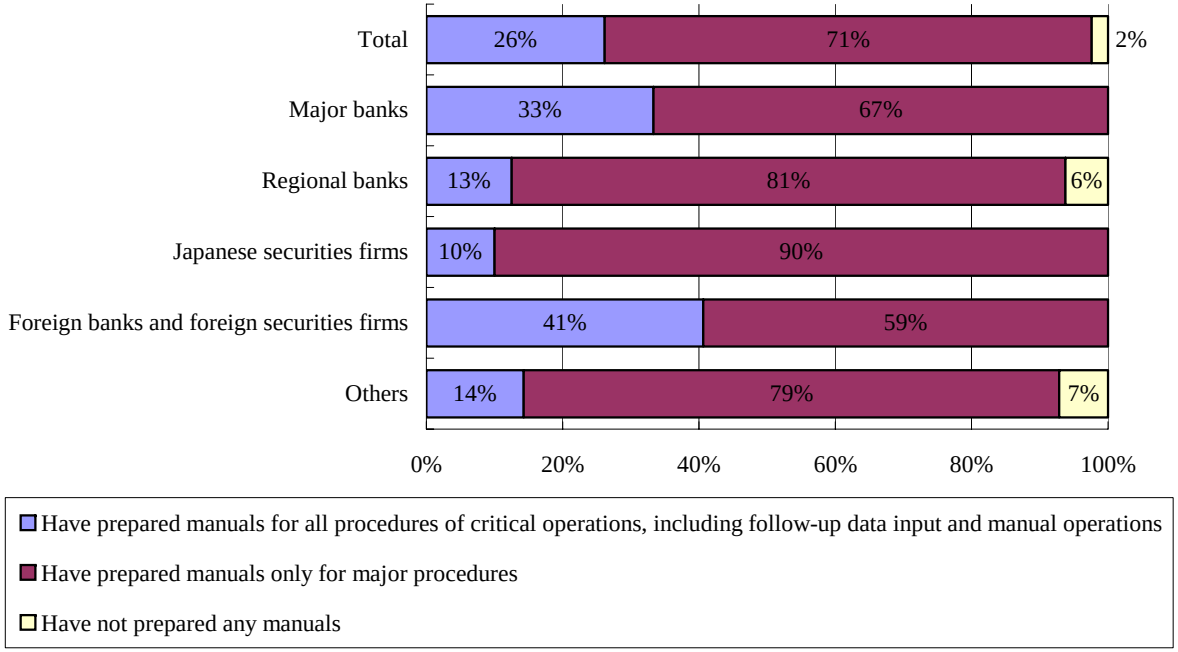
5. Decision-Making Procedures and Communication Arrangements for BCP Implementation



■ 80 percent of the respondents answered that they "have established" "management systems that ensure the smooth delegation of authority when contact with top management or division heads is not possible" and "ways to contact important external parties such as payment and settlement institutions, outside service providers, and major clients." Meanwhile, only 49 percent of the respondents answered that they "have established" "contact points and ways to contact important external parties when the parties invoke their BCPs."

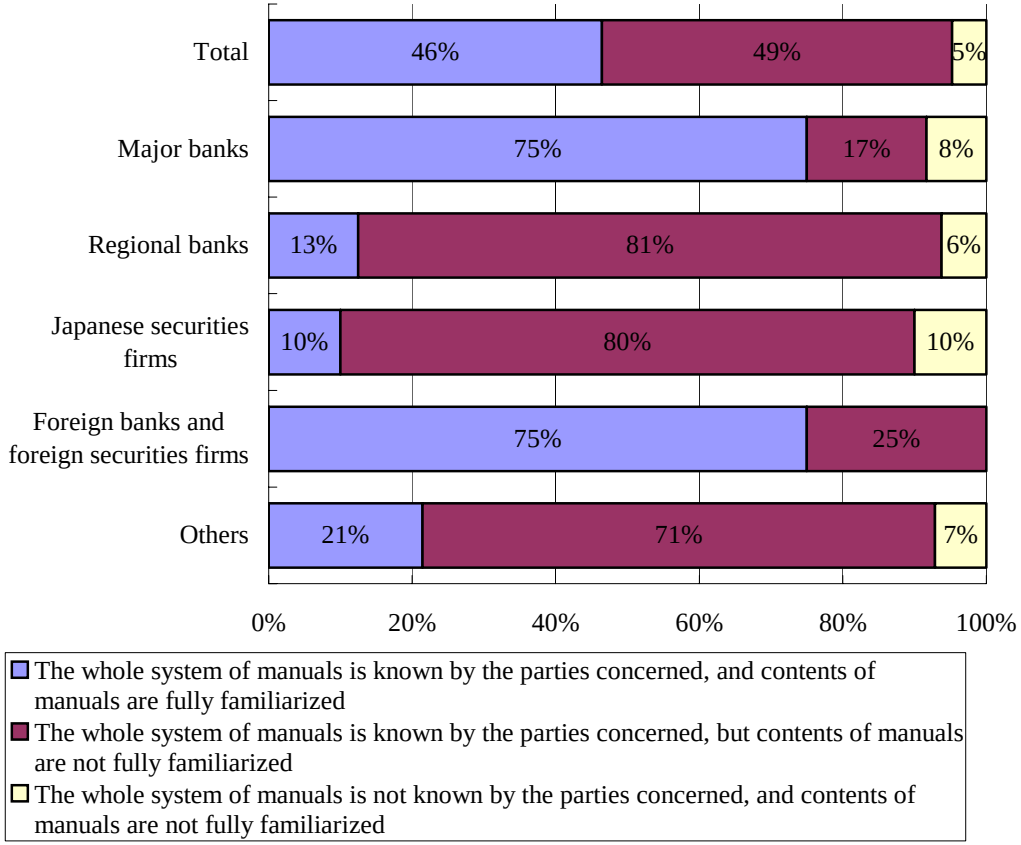
6. Manuals for BCP Implementation

a. Manuals for Critical Operations



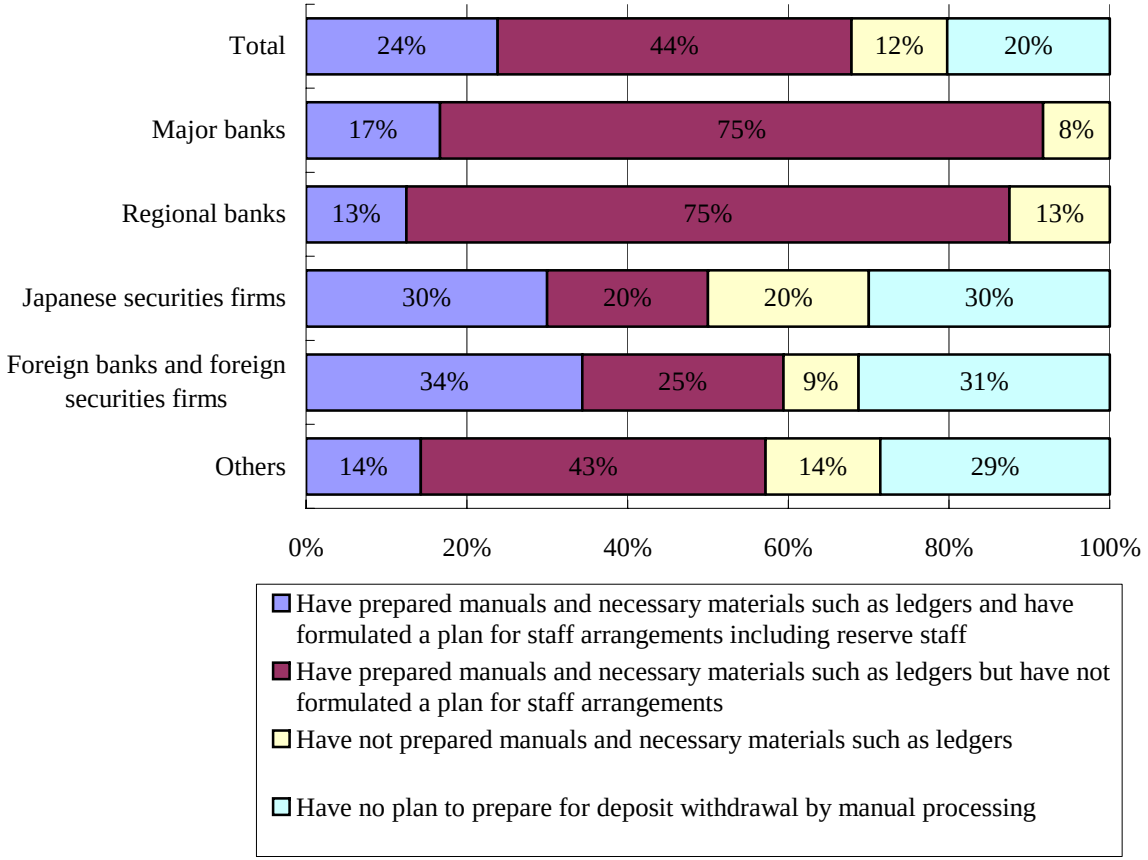
■ Only 26 percent of the respondents answered that they "have prepared manuals for all procedures of critical operations, including follow-up data input and manual operations." 71 percent of the respondents answered that they "have prepared manuals only for major procedures."

b. Awareness of Manuals



■ Only 46 percent of the respondents answered that "the whole system of manuals is known by the parties concerned, and contents of manuals are fully familiarized."

c. Deposit Withdrawal Operations by Manual Processing

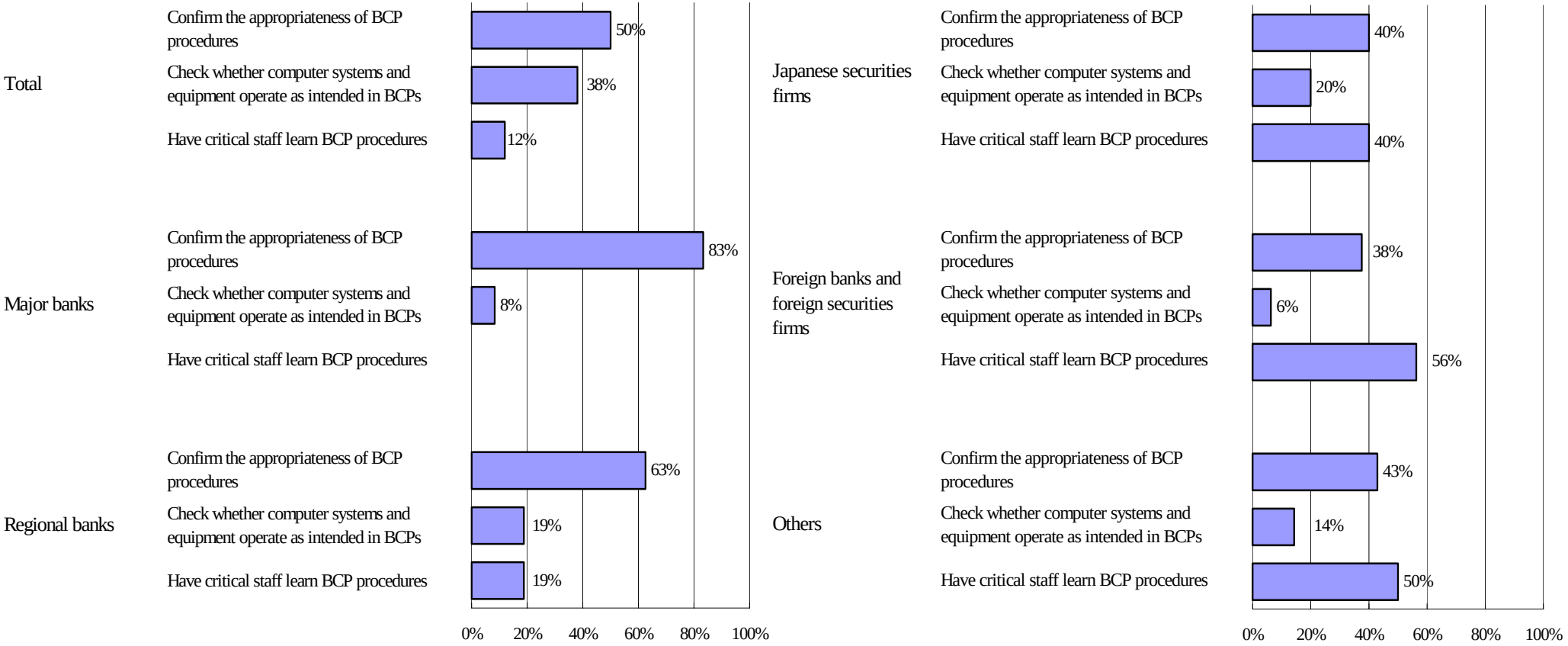


■ Only 24 percent of the respondents answered that they "have prepared manuals and necessary materials such as ledgers and have formulated a plan for staff arrangements including reserve staff" for deposit withdrawal operations by manual processing immediately after a disaster. 56 percent of the respondents answered that they "have prepared manuals and necessary material such as ledgers but have not formulated a plan for staff arrangements" or "have not prepared manuals and necessary material such as ledgers."

C. Exercises and Reviews of BCPs

1. Exercises

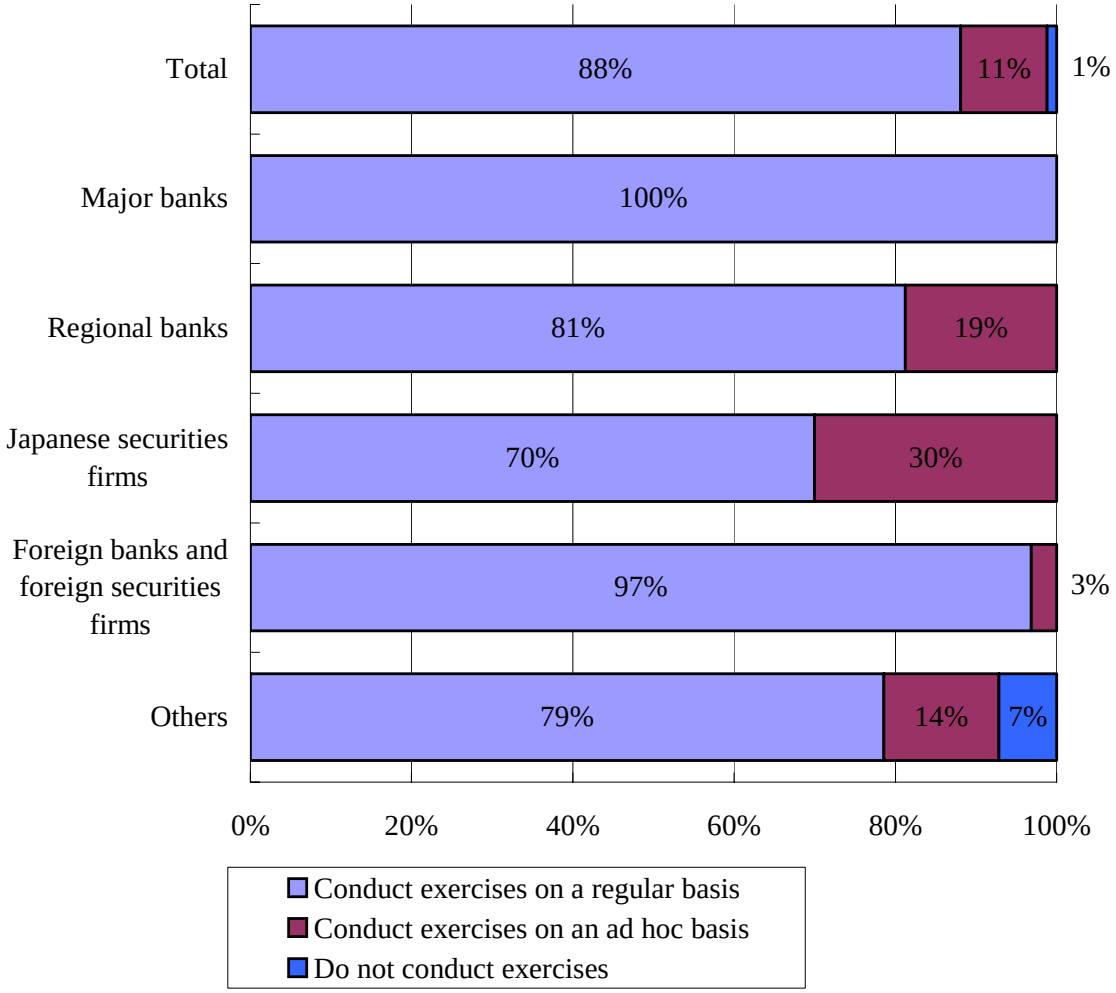
a. Objectives of Exercises[5]



■ 50 percent of the respondents answered that they "confirm the appropriateness of BCP procedures," and 38 percent of the respondents answered that they "check whether computer systems and equipment operate as intended in BCPs" as the most important objectives of exercises.

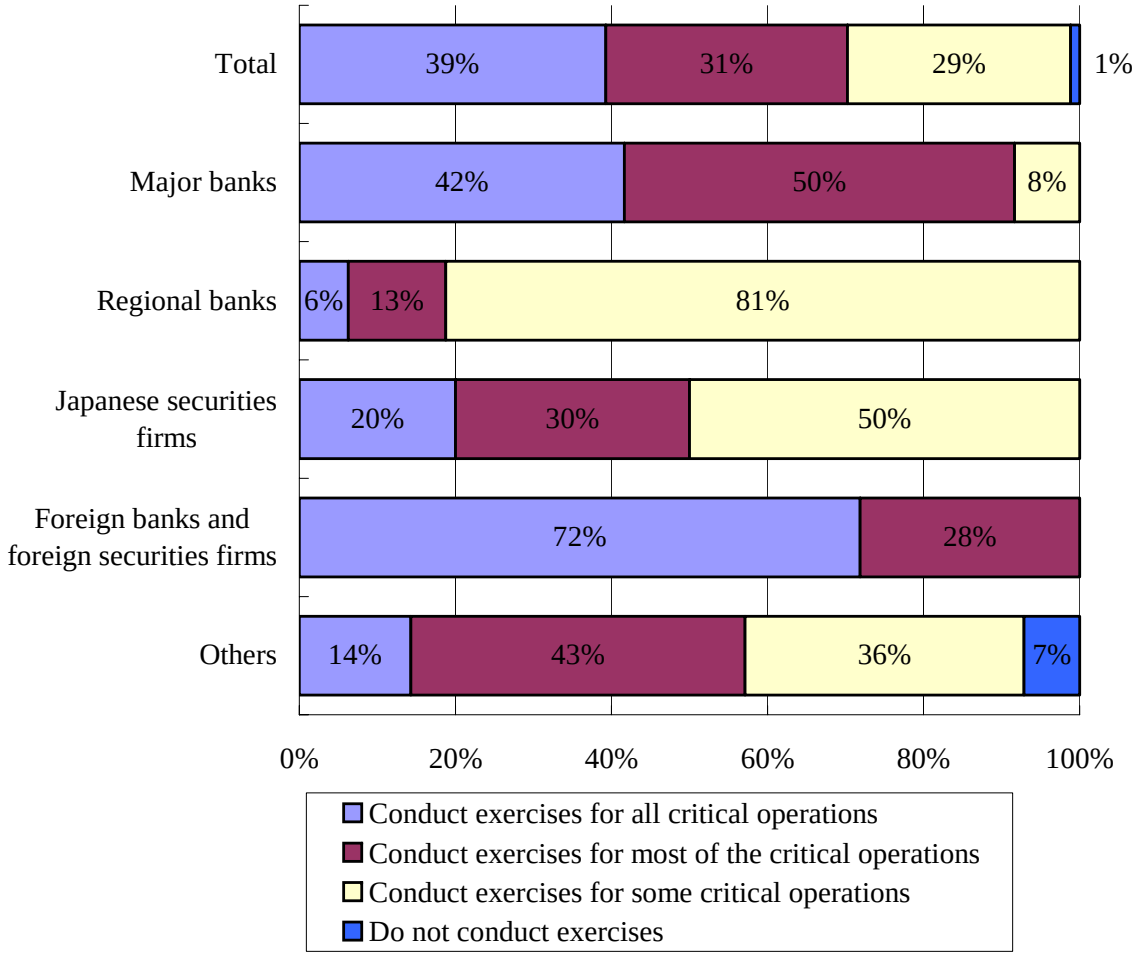
[5] Multiple answers were allowed.

b. Frequency of Exercises



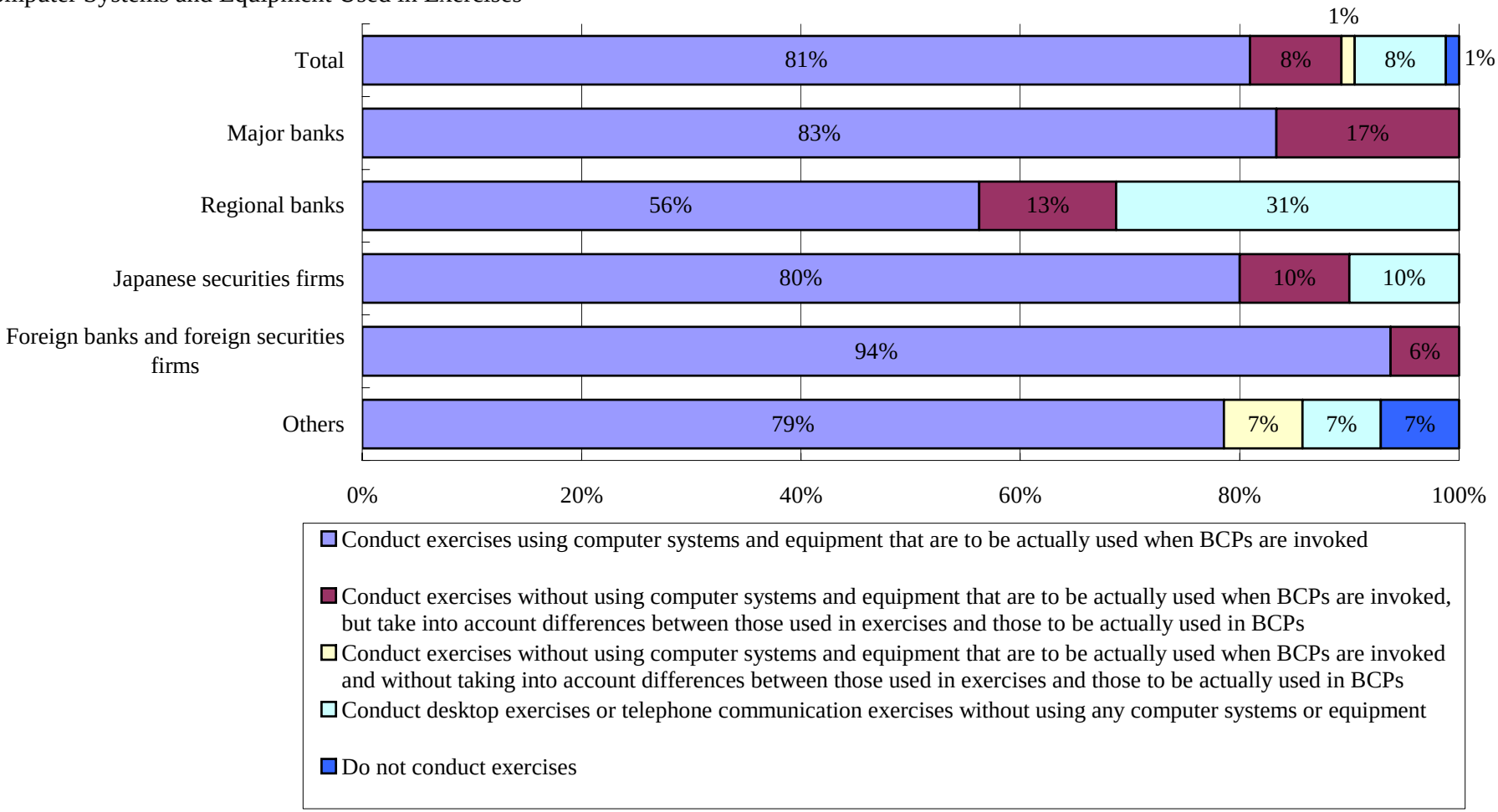
■ 88 percent of the respondents answered that they "conduct exercises on a regular basis."

c. Critical Operations Covered by Exercises



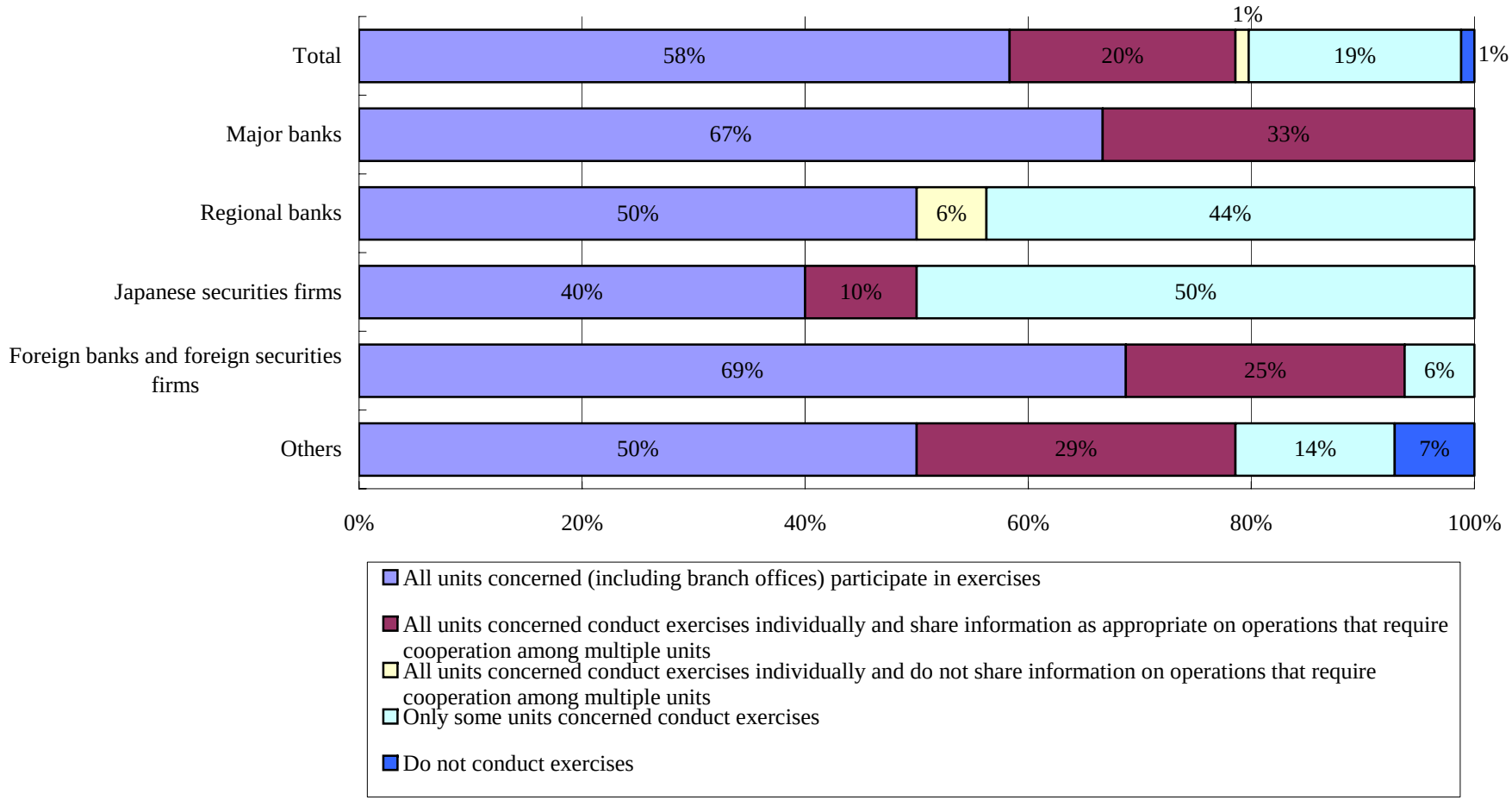
■ 39 percent of the respondents answered that they "conduct exercises for all critical operations."

d. Computer Systems and Equipment Used in Exercises



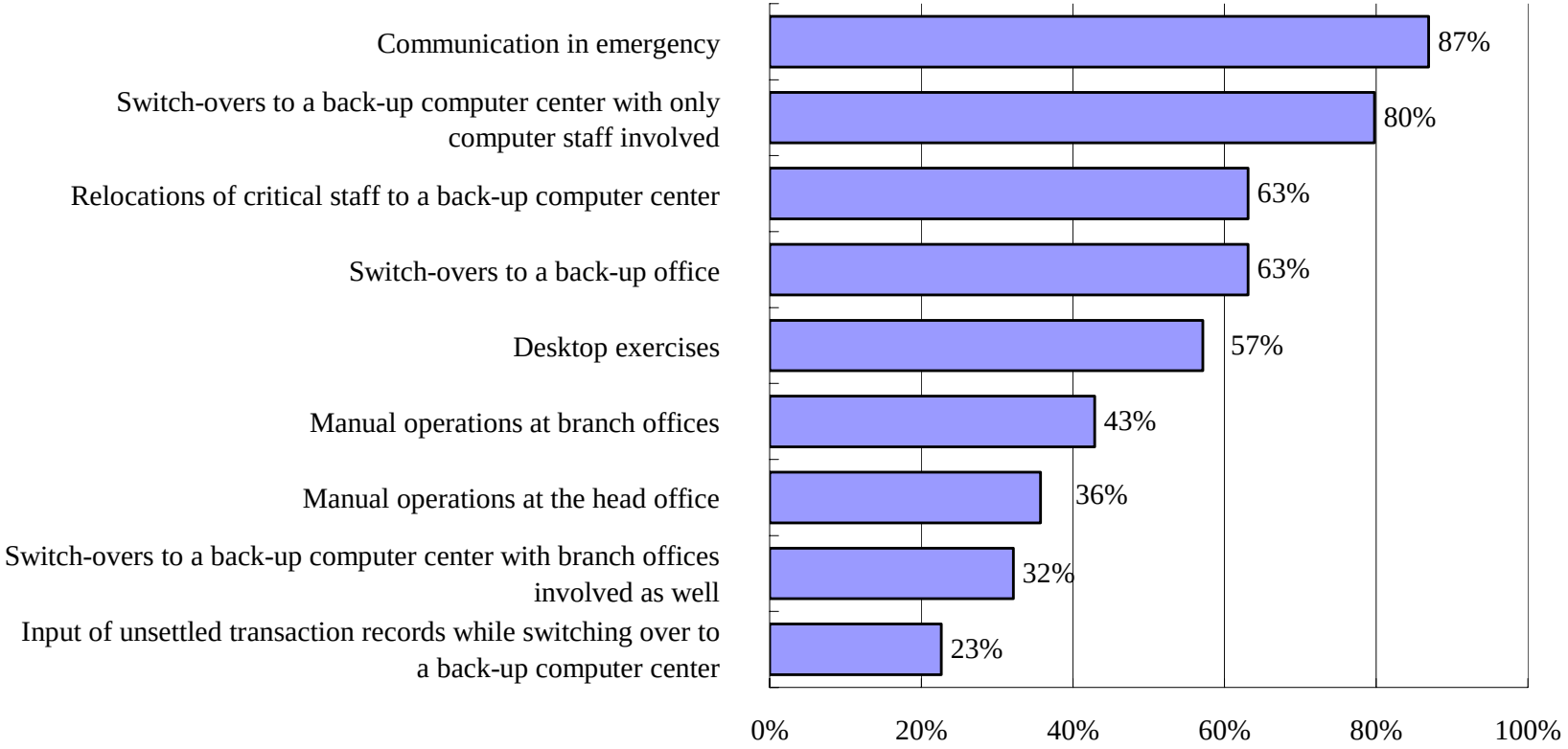
■ 81 percent of the respondents answered that they "conduct exercises using computer systems and equipment that are to be actually used when BCPs are invoked."

e. Participants in Exercises



■ 58 percent of the respondents answered that "all units concerned (including branch offices) participate in exercises."

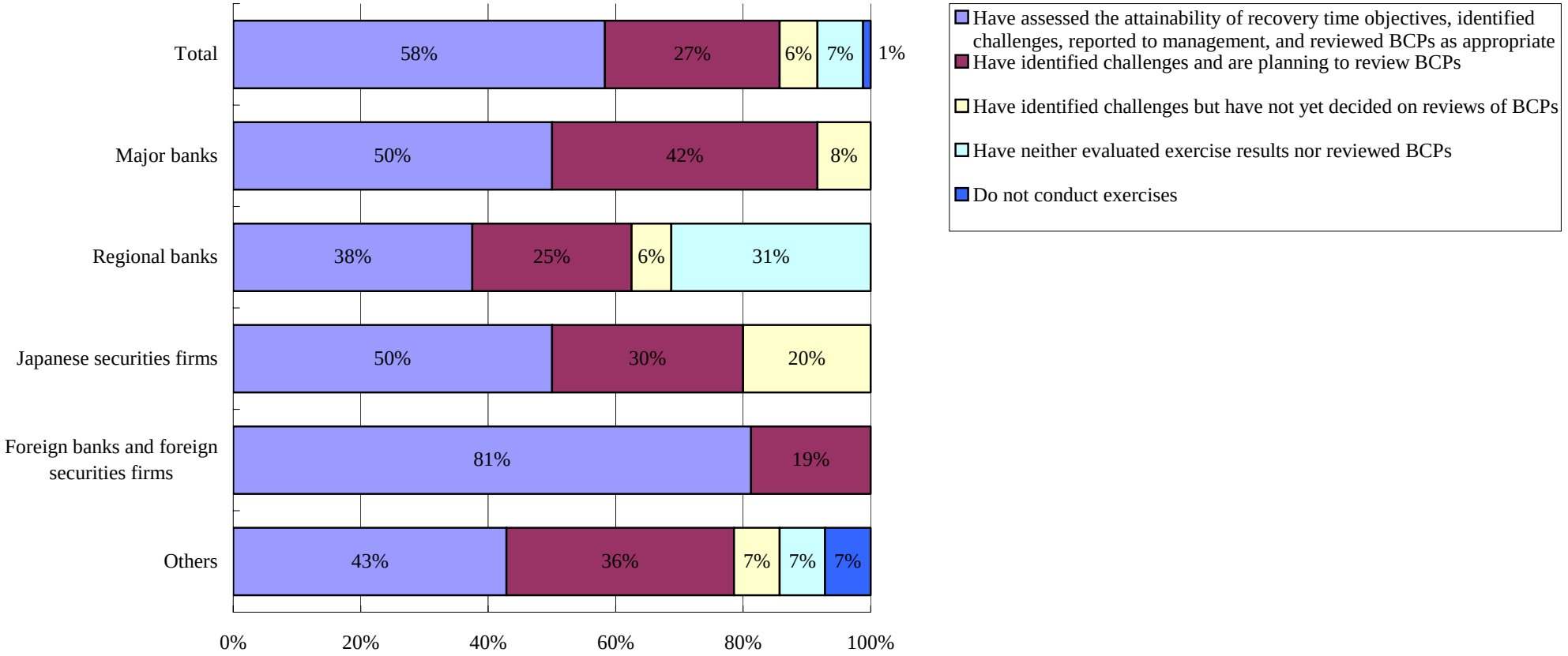
f. Types of Exercises



■ 87 percent of the respondents answered that they conduct "communication in emergency," and 80 percent of the respondents answered that they conduct "switch-overs to a back-up computer center with only computer staff involved."

■ Meanwhile, only 32 percent of the respondents answered that they conduct "switch-overs to a back-up computer center with branch offices involved as well," and only 23 percent of the respondents answered that they conduct "input of unsettled transaction records while switching over to a back-up computer center."

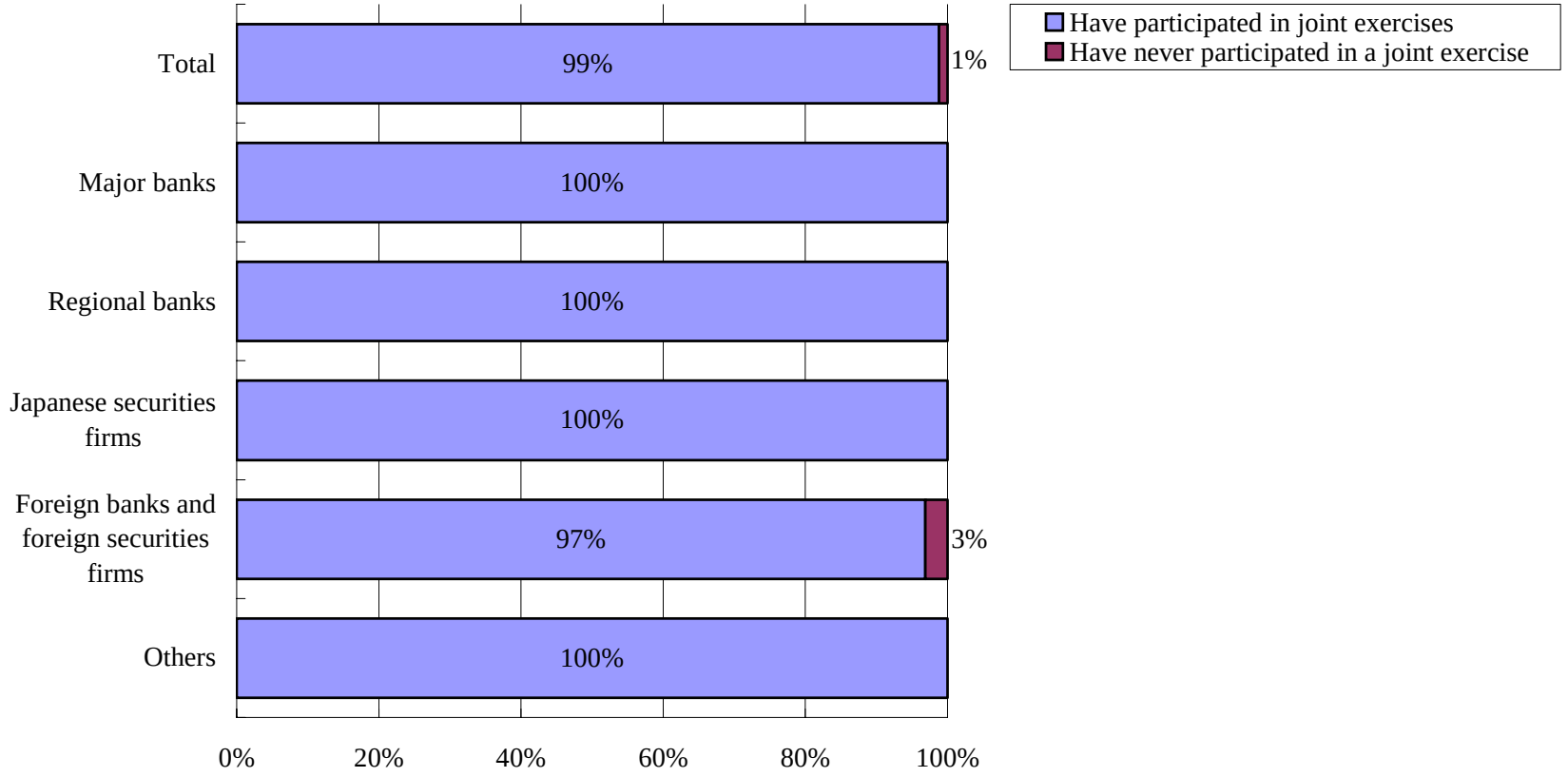
2. Exercise Evaluations and Reviews of BCPs



■ 58 percent of the respondents answered that they "have assessed the attainability of recovery time objectives, identified challenges, reported to management, and reviewed BCPs as appropriate."

3. Joint Exercises Organized by Other Financial Institutions

a. Participation in Joint Exercises

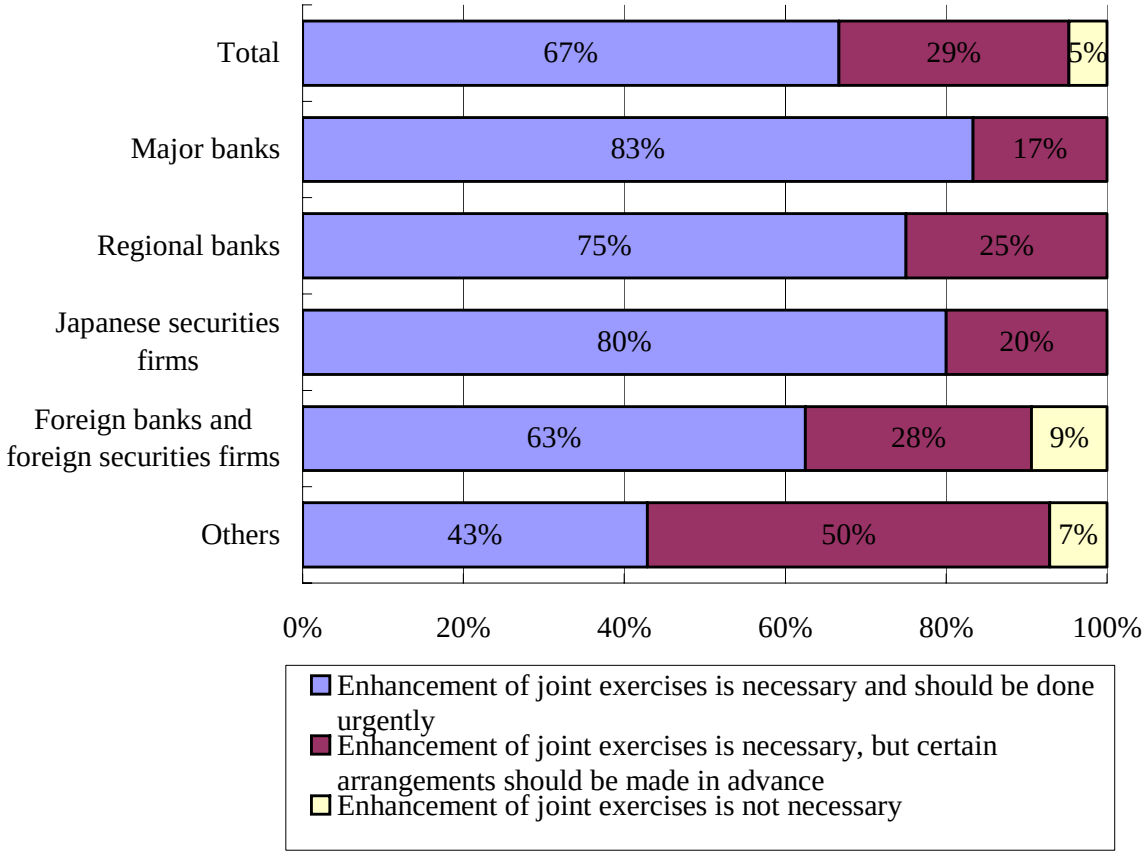


■ 99 percent of the respondents answered that they "have participated in joint exercises" organized by other financial institutions.

▼ Joint exercises the respondents have participated in included the following:

- Joint exercises for switching over to the back-up computer center for the Bank of Japan Financial Network System (organized by the Bank of Japan)
- Joint exercises using a BCP-dedicated web site for the money market (organized by Japanese Bankers Association)

b. Enhancement of Joint Exercises

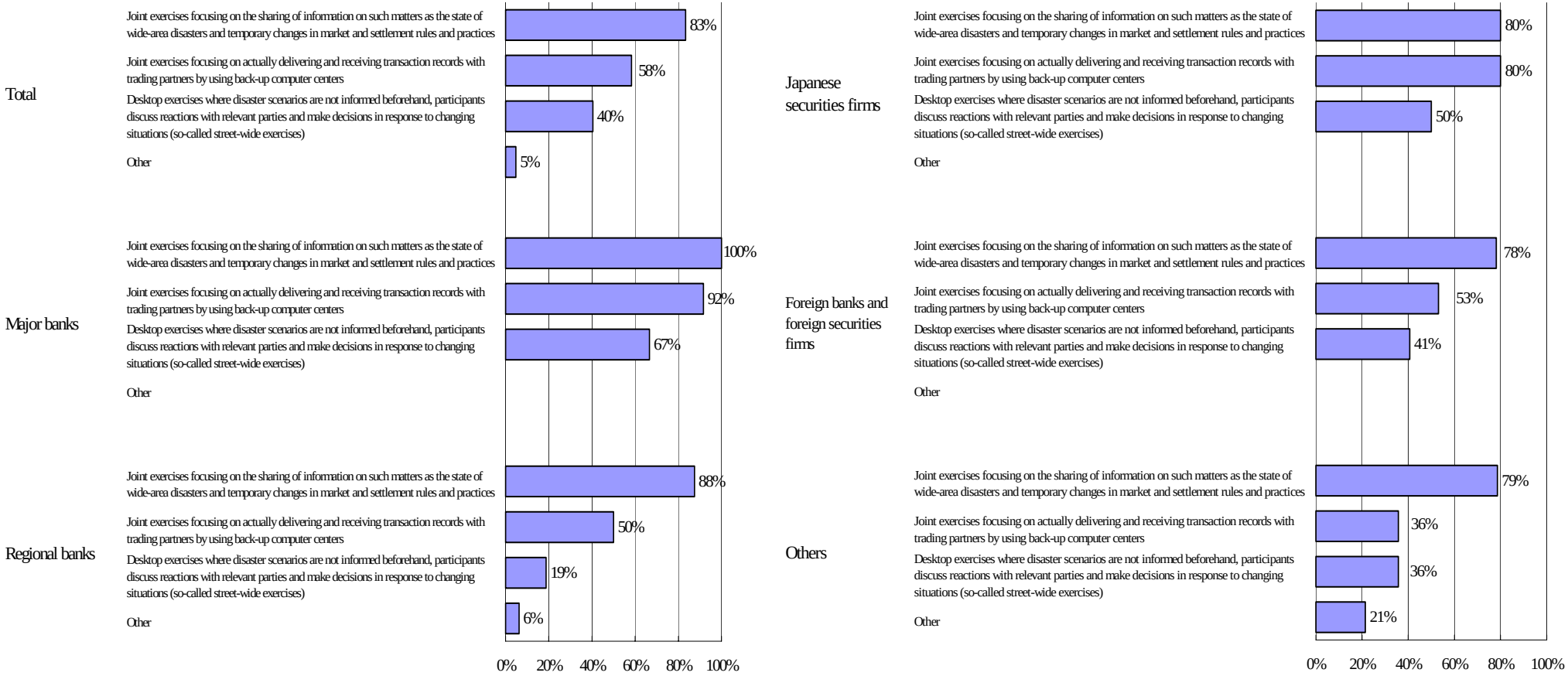


■ 67 percent of the respondents answered that "enhancement of joint exercises is necessary and should be done urgently."

▼ Conditions raised by respondents who answered that "enhancement of joint exercises is necessary, but certain arrangements should be made in advance" include the following:

- Date, method, and coverage (operations and staff)
- Clarifying objectives
- Making consensus regarding disaster scenarios
- Broad coverage (e.g., across markets with the participation of more than one payment and settlement system)
- Considering constraints of computer systems

c. Areas of Joint Exercises That Need to Be Enhanced[6]



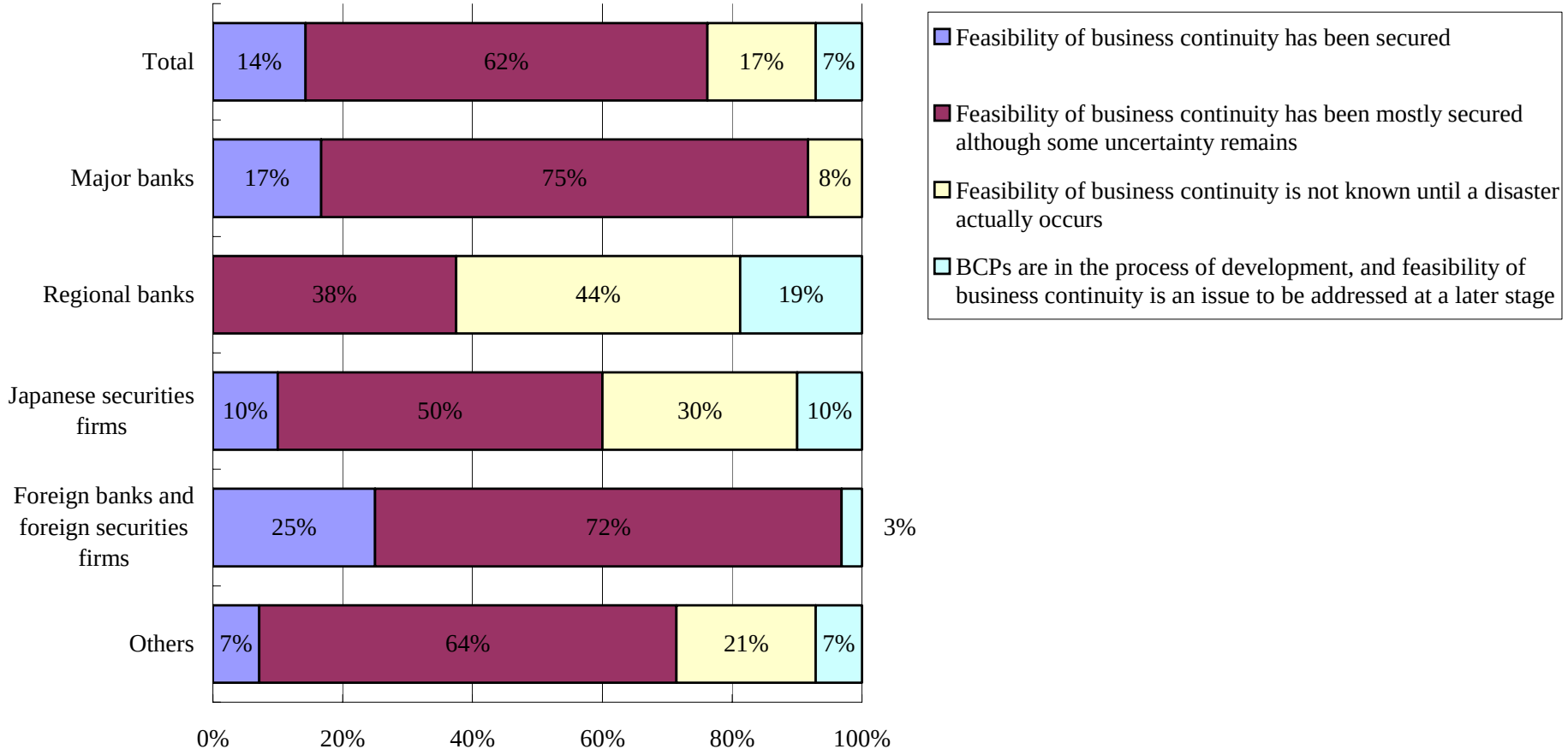
■ 83 percent of the respondents answered that they should enhance "joint exercises focusing on the sharing of information on such matters as the state of wide-area disasters and temporary changes in market and settlement rules and practices," and 58 percent of the respondents answered that they should enhance "joint exercises focusing on actually delivering and receiving transaction records with trading partners by using back-up computer centers."

▼ Other responses included answers such as "usage of a BCP-dedicated web site," "cooperation with payment and settlement system institutions," and "expansion of operations covered by exercises."

[6] Multiple answers were allowed. This question was asked to the respondents who answered the previous question that "enhancement of joint exercises is necessary and should be done urgently" or "enhancement of joint exercises is necessary, but certain arrangements should be made in advance."

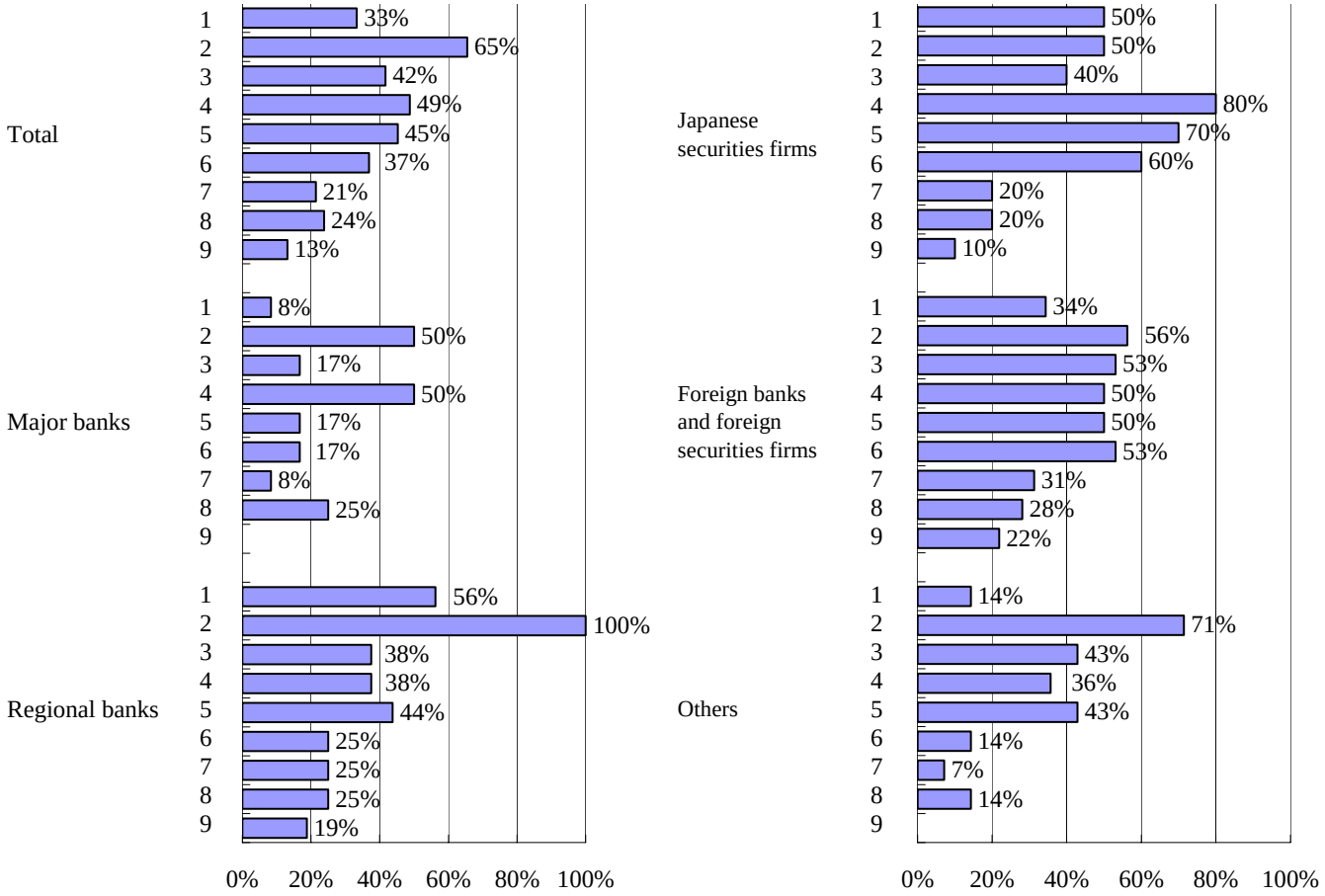
D. Overall Assessment

1. Feasibility of Business Continuity



■ Only 14 percent of the respondents answered that "feasibility of business continuity has been secured," and 62 percent of the respondents answered that "feasibility of business continuity has been mostly secured although some uncertainties remain."

2. Critical Issues to Be Addressed[7]



1	Enhance awareness among top management and employees
2	Expand or refine BCPs
3	Enlarge the scope of disaster scenarios, considering, for example, new type of pandemics such as avian flu
4	Improve back-up facilities
5	Improve exercises
6	Improve education and training
7	Strengthen control of outside service providers by such measures as confirming their readiness for business continuity
8	Make BCM more adapted to guidelines such as "High-Level Principles for Business Continuity" by the Joint Forum and "The Guideline for Countermeasures against a Severe Earthquake in the Tokyo Metropolitan Area" by the Central Disaster Management Council
9	Strengthen auditing

■ 65 percent of the respondents answered that they should "expand or refine BCPs," and 49 percent of the respondents answered that they should "improve back-up facilities."

■ By type of financial institution, all regional banks responded that they should "expand or refine BCPs," and 80 percent of Japanese securities firms responded that they should "improve back-up facilities."

[7] Multiple answers were allowed.