MONASH UNIVERSITY
13 MAY 1998
DONALD COCHRANE LIBRARY
ECONOMICS

Evidence of Australian Bank Exposures to Operational Disaster

by

Christopher W. Viney*

*Department of Accounting and Finance,
Monash University, Caulfield Campus, Victoria, 3145, Australia.
Phone: (03) 9903 2585; Fax: (03) 9903 2422
Email: Chris.Viney@BusEco.monash.edu.au

May 1998

WORKING PAPER NO. 59

Not for quotation
Comments welcome.

The author would like to acknowledge contributions of Professor Michael Skully, Michael Vincent and Kathy Avram.

ABSTRACT

The loss of a bank's critical business operations due to a physical, technical or natural disaster may have a catastrophic effect on the ultimate survival of the institution and may even threaten the overall stability of the financial system.

This paper reports and analyses the results of an extensive survey of the disaster recovery planning practices of Australian banks. Banks are grouped as major, regional and foreign banks. Data analysis considers specific organisational disaster recovery planning issues within broad categories of organisational commitment; development and maintenance of formal planning and response processes; and Reserve Bank regulatory requirements.

Results clearly demonstrate that Australian banks, as a group, have not fully implemented disaster recovery planning within their organisations, and are generally only in the formative stages of the process.

The paper concludes that banks are not adequately prepared to respond to, or recover from, a significant event that may impact upon the provision of critical business functions. Given the importance of the banking sector, particularly the major banks, to the stability of the Australian financial system, it is further concluded that there is a substantial level of associated systemic risk.

1 DISASTER RECOVERY PLANNING PERSPECTIVES

1.1 Introduction

Mr G. J. Thompson, Deputy Governor of the Reserve Bank of Australia, stated;

> "...banks are increasingly reliant on computers for information-processing and control. As a result, they are exposed to various kinds of operational risk.
>
> For a bank active in derivatives trading, a breakdown in computer systems for even a relatively short time could be disastrous - preventing it from monitoring its changing market positions and disrupting its capacity to trade and to settle outstanding transactions. I recently heard a keen observer predict that the next big banking disaster would come from a (hypothetical) major international bank losing track of its derivatives positions for 24 hours.
>
> To protect against such events, banks invest heavily in the integrity of their computer systems, as well as in back-up and disaster recovery facilities."[1]

This paper investigates the disaster recovery planning practices of Australian banks. The survey considers both organisational disaster recovery planning practices and those limited only to computer centre operations and treasury operations.

An institution with a comprehensive organisational disaster recovery plan will have a greater chance of survival, and minimise the cost of that survival, in the event of a disastrous business disruption. "Companies that plan for the possibility of a disaster, that formulate strategies for recovering critical business functions, and that train employees to implement those strategies, generally do survive disasters." (Toigo 1989:3)

Organisational disaster recovery planning is the planned development of specific strategies which, in the event of a disruption to business operations due to a physical or natural disaster, will enable an institution to resume critical business operations in the shortest possible time-frame and facilitate the resumption of normal business operations in an efficient, structured and prioritised manner.

A disaster is an evolving or immediate event which significantly disrupts the normal business operations of an institution, in particular its critical business functions. Critical business functions refer to minimum operational requirements necessary to meet an institution's current commitments, maintain customer relationships and minimise financial loss. Physical and natural disasters are operational disasters. Physical disasters may be further categorised as technical or human, and include sabotage, terrorist acts, loss of power, water, communications, employee errors and actions. Natural disasters may include flood, fire, hurricane, earthquake, snow storm.

---

[1] Thompson, G.D., (1997), "The Many Faces of Risk in Banking", *Bulletin*, Reserve Bank of Australia, Sydney, July, p.15

1.2 Disaster Recovery Planning - The Traditional Focus

The rapid development of technology and the integration of information systems throughout an organisation, and the universal dependence on technology and information systems, means that a disruption of limited duration could cause severe financial loss and even threaten corporate survival. (Christensen 1992:35)

The traditional focus of disaster recovery planning over the past twenty years has therefore primarily centred around the business computer centre. However the concept of organisational disaster recovery planning is now recognised as an essential element of risk management as technology has become totally integrated into business operations. The emphasis in disaster recovery planning has moved from a blinkered focus on the computer centre, to an all encompassing organisational risk management process that incorporates all business units within an organisation.

1.3 Disaster Impacts - Selected Surveys and Statistics

Arnell (1990:2) presents data based on a 1979 University of Minnesota study and his own observations in 1990. In 1979 a 48 hour down-time would create a serious impact, whereas in 1990 a similar impact would occur with a down-time of 24 hours. He notes that for the finance sector a significant contraction to less than 24 hours in the maximum allowable downtime of computer supported services before the organisation will be heavily impacted with regard to finances, competitive position, contractual implications and penalties. Technology advances coupled with globalisation of international financial systems has further increased the time sensitivity of financial institutions to even limited access to critical business operations.

A further study conducted by the University of Texas in North American shows that organisations suffer significant and increasing daily revenue loss over elapsed time after a major disaster (Woodcock 1992:2). A University of Minnesota study (Toigo 1989: 4-6) also clearly demonstrates a critical relationship of time to successful disaster recovery for a financial institution.

With the Newcastle [Australia] earthquake that occurred in 1989, 50% of businesses that were isolated in the central business district for twelve (12) days have subsequently failed financially. Banks were fortunate in that their critical business operations were not exposed to this earthquake.

Results of a nationwide study in the United States of America by the Center for Research on Information Systems at the University of Texas at Arlington (UTA), and reported in Chantico (1991:4) shows that:

- as the length of the outage increases, loss of functionality and integration of functions worsens.
- reverting to manual backup methods accomplishes only part of normal functions. The backlog increases.
- co-ordination of information among the functions and departments is decreased, resulting in errors in order commitment and loss of sales and profit.
- computer outages initiate actions that cause the business to incur additional expenses.
- the largest intangible loss is cash-flow interruption.

- continued loss of customers, competitive edge, and image might prove more damaging than the temporary loss of revenue and additional costs.

A further USA study reported by Chantico (1991:3,4), conducted by Contingency Planning Research, Inc., cites disaster risk exposure by industry. **The finance industry has the highest risk exposure.**

1.4 Need for this Study

Existing research (Blair 1991; Ford 1990; Arnell 1990; Toigo 1989) clearly identifies a high risk exposure of financial institutions to events of business disruption due to a natural or physical disaster. Australian banks operate within a global market and are subject to both international and domestic business continuity demands of government (economic and social objectives); regulators (financial system stability and monetary policy objectives); customers (public confidence); other institutions (interrelationships and dependencies); and shareholders (business survival).

Banks are the predominant institutions within the Australian financial system, representing over 70% of total assets, and as such their survival is critical to overall system stability and efficiency. Furthermore the banks are essential to the functioning of the real economy.

Given the critical need for Australian banks to maintain continuous operation, this research surveys their disaster recovery planning practices in an endeavour to draw some conclusions on the level of preparedness of the banks to respond to, and recover from, a significant event of business disruption.

1.5 Methodology

Australian banks have been categorised on the basis of size and origin into major, regional, and foreign banks.

The research methodology adopted included a combination of literature review and content analysis; mail questionnaires; and standardised, scheduled interviews. Data was analysed using standard frequency distributions, asset weighted distributions, and rank order.

The data relates to research conducted in 1994 of the total Australian bank population of which 72% of banks (4 major, 10 regional, 11 foreign banks) responded to questionnaires, and 60% of banks (4 major, 8 regional, 9 foreign banks) were interviewed.

2 RESULTS - BANK DISASTER RECOVERY PLANNING PRACTICES

2.1 Introduction

The theory of the organisation contends that the risk management process derives from an organisation's need to survive. Therefore, organisational disaster recovery planning should actively reside within all bank management decision structures; that is, ideally, the risk management process will ensure that all critical exposures to business disruption are identified and managed through a structured decision process.

However, operational imperatives, or constraints of the institution, may limit the extent of the risk management process. The institution may place constraints on, or even ignore, the pre-emptive management of risk exposures and develop an ethos of reactive risk management.

The purpose of this survey is to examine the organisational disaster recovery planning practices of Australian banks. Organisational disaster recovery planning is a detailed and complex process comprising a multitude of variables, each of which may be at a different stage of development. Survey and interview questions focus on a range of specific elements of the organisational disaster recovery planning process. To afford a more meaningful analysis, questions are categorised into:

(a) the level of organisational commitment,
(b) the *planning* process,
(c) the *response* process, and
(d) Reserve Bank of Australia requirements.

Absolute numerical and percentage results are tabulated and analysed by bank sub-groupings of major, regional and foreign banks. An indication of the level of systemic risk is sought by applying percentage asset weightings [in brackets] for all banks.

2.2 Organisational Commitment to Disaster Recovery Planning

The purpose of this section is to examine the organisational commitment to disaster recovery planning. Clear and unequivocal management direction and support is an imperative of an effective disaster recovery planning process. (Toigo 1989:5, Arnell 1990:10, Ford 1990:12, Rehesaar 1992:2, Wold 1992:29)

2.2.1 Disaster Recovery Plan Status

Table 1 reports the **organisational** disaster recovery plan status in each bank. Twelve percent of respondent banks (n = 3) have achieved an organisational disaster recovery planning status where a plan has been fully developed and documented; this includes only one major bank. Eighty percent (n = 20) are currently developing a plan, comprising seventy-five percent (n = 3) of major banks, ninety percent (n = 9) regional banks and seventy-three percent (n = 8) foreign banks. No regional bank has a completed plan, and ten percent have not commenced a planning process. One foreign bank has not commenced a planning process.

Table 1 Organisational Disaster Recovery Planning Status

	Major (n = 4)		Regional (n = 10)		Foreign (n = 11)		All Banks (n = 25)		
Organisational DRP fully documented	1	25%			2	18%	3	12%	[19%]
Organisational DRP being developed	3	75%	9	90%	8	73%	20	80%	[78%]
No organisational DRP documented			1	10%	1	9%	2	8%	[3%]

These statistics alone present a position of some considerable concern, particularly given that three of the four major banks are included in the majority that do not have fully documented organisational disaster recovery plans. Also of concern is the fact that two banks, one regional and one foreign, acknowledge the non-existence of a formal planning process.

The results of this question indicate a significant proportion of the banks are currently developing an organisational disaster recovery plan. The level of systemic risk is high, with [78%] of all banks only in the plan development phase. The stage of development of the organisational disaster recovery plans is not known, however analysis of further questions provides a clearer understanding.

Having regard to the almost absolute reliance of banks on computer systems, the next question (table 2) sought to determine the disaster recovery planning status with regard to computer centre operations. Sixty- four percent (n = 16) of all banks, including three of the four major banks and seven of the regional banks, maintain fully documented plans for their computer centre operations. One foreign bank has no plan.

Maintenance of computer centre operations is critical to interbank operations, and the higher weighted percentage of banks with computer centre recovery plans [72%] indicates a lower level of systemic risk.

These statistics reveal that bank management place a higher priority on the management of risk within the computer centre than critical business functions of the overall organisation. Interview comments and literature review (Arnell 1990) indicate that senior managers within the computer centre environment are, generally, more aware of the potential impacts of business disruption than are senior managers of other business units in an organisation.

Table 2 Computer Centre Disaster Recovery Planning Status

	Major (n = 4)		Regional (n = 10)		Foreign (n = 11)		All Banks (n = 25)		
Computer centre DRP fully documented	3	75%	7	70%	6	55%	16	64%	[72%]
Computer centre DRP being developed	1	25%	3	30%	4	36%	8	32%	[27%]
No computer centre DRP documented					1	9%	1	4%	[1%]

A further question directed towards the reason why two respondent banks have not commenced the development of a formal organisational disaster recovery plan elicited responses that both banks' management had not considered the issue.

Other questionnaire and interview responses indicate that a number of banks, which stated they are currently developing a disaster recovery plan, are significantly constrained as a result of low priority and limited resource allocation to the project.

With such a high proportion of banks indicating they are in the development phase of disaster recovery planning, it is necessary to consider the extent of the organisational policy commitment.

2.2.2 Policy

The formalisation of objectives and policy of a bank is the responsibility of the board of directors. Table 3 shows the results of a question of whether the board of directors of Australian banks have issued written policy documents specifying organisational objectives and policy in relation to disaster recovery planning.

Table 3 Written Policy Document Issued by Board of Directors

	Major (n = 4)		Regional (n = 10)		Foreign (n = 11)		All Banks (n = 25)		
Yes	3	75%	3	30%	7	64%	13	52%	[64%]
No	1	25%	7	70%	4	36%	12	48%	[36%]

Only fifty-two percent (n = 13) of all respondent banks have issued a written disaster recovery planning policy document. Given that ninety-two percent of respondent banks (table 1) have implemented, or are currently developing, an organisational disaster recovery plan, this result immediately raises concerns regarding the veracity of that response, the extent of the bank policy decision processes, and the functional direction of the decision process within Australian banks. Further analysis by bank grouping reveals an even lower level of policy documentation in the regional banks, with a reported thirty percent (n =3).

Analysis of the ninety-two percent (n = 23) of all banks currently developing, or with fully documented, organisational disaster recovery plans (table 1) with the fifty-two percent (n = 13) banks where the board of directors have issued a relevant written policy document indicates that there is a significant variance. Whilst neither variable is dependent upon the other, it suggests that, at best, the formal organisational disaster recovery planning risk management process is not being driven from the top of those organisations.

2.2.3 Priority

The effectiveness of organisational commitment is dependent upon the level of priority given to the planning process. Respondents were asked to consider that a bank must manage a number of financial risks and operational risks, and then determine whether the management of business continuity risk receives a high priority within the organisation relative to other areas of risk management.

A quite high proportion, fifty-seven percent (n = 12), indicate that the management of business continuity risk is not given a high level of priority. This is especially evident within the regional and foreign banks, with seventy-five percent (n = 6) and fifty-six percent (n = 5) respectively, expressing a negative opinion. Major banks indicate a higher level of commitment at seventy-five percent (n = 3). (table 4)

Comparative analysis of the ninety-two percent (n = 23) of all banks developing, or with fully documented organisational disaster recovery plans, to the much lower forty-three percent (n = 9) that acknowledge a high priority allocation, may be further evidence that in many of the banks, planning is progressing within significant constraints. Given the potential of a critical business disruption to threaten the survival of a bank, the overall low level of priority allocation raises concerns as to the understanding of, and commitment to, disaster recovery planning by executive management.

Table 4 Business Continuity Risk - Priority Relative to Other Risk Areas

	Major (n = 4)		Regional (n = 8)		Foreign (n = 9)		All Banks (n = 21)		
Yes	3	75%	2	25%	4	44%	9	43%	[61%]
No	1	25%	6	75%	5	56%	12	57%	[39%]

2.2.4 Awareness

Recognising that there are different levels of management within an organisation, the following two questions are directed towards determining commitment to organisational disaster recovery planning at the executive management level, and at the operational business manager level.

Seventy-one percent (n = 15) of all banks indicated an awareness and commitment to organisational disaster recovery planning, and with a further nineteen percent (n = 4) expressing a commitment with reservations. (table 5)

Table 5 Executive Management Awareness and Commitment

	Major (n = 4)		Regional (n = 8)		Foreign (n = 9)		All Banks (n = 21)		
Yes	2	50%	7	88%	6	67%	15	71%	[60%]
Yes (reservations)	2	50%			2	22%	4	19%	[36%]
No			1	12%	1	11%	2	10%	[4%]

This result however does not appear to be supported by the results obtained in previous questions, where only fifty-two percent have issued a policy document, and a low forty-three percent actually allocate a high priority to disaster recovery risk management. Similarly, a comparative analysis of results in table 7, shows that only a fifty-two percent (n = 13) of banks make a formal budget allocation.

Business manager commitment is much lower at the operational level of the organisation. Thirty-eight percent (n = 8) of all banks identify limited commitment and only twenty-four percent (n = 5) recognise commitment throughout the organisation. An analysis of commitment by bank grouping indicates only variable or limited commitment in one-

hundred percent of major banks; fifty percent (n = 4) of regional banks; and sixty-six percent (n = 6) of foreign banks. Weighted data indicates an even lower commitment by operational business managers to disaster recovery planning.

Such low levels of commitment by operational managers must raise significant concerns regarding the development, effectiveness and on-going maintenance of the planning process, in particular education and training programmes, and banks' preparedness to respond to a disastrous event of business disruption.

Table 6 Operational Business Manager Commitment to Disaster Planning

	Major (n = 4)		Regional (n = 8)		Foreign (n = 9)		All Banks (n = 21)		
Yes - throughout organisation			2	25%	3	33%	5	24%	[9%]
Yes - computer centre only			2	25%			2	10%	[5%]
Varies between business units	2	50%	2	25%	2	22%	6	29	[42%]
Limited commitment	2	50%	2	25%	4	44%	8	38%	[44%]

2.2.5 Resource Allocation

A measure of a bank's commitment to disaster recovery planning is its formal allocation of resources. Due to factors of confidentiality and competitive advantage, it was not possible to obtain actual budget expenditures, however questions asked whether the bank had a formal budget allocation for disaster recovery planning. Fifty-two percent (n = 13) of banks provide a formal budget allocation, however between bank groupings this figure varies significantly, with seventy-five percent (n = 3) major banks; sixty percent (n = 6) regional banks; and a low thirty-six percent (n = 4) of foreign banks. (table 7)

This question related only to a budget allocation for disaster recovery planning, rather than specifically organisational disaster recovery planning. A number of interviewees indicated that formal allocation was incorporated in the computer centre budget allocation only, therefore the budget allocation to organisational disaster recovery planning is significantly lower.

Table 7 Disaster Recovery Planning Formal Budget Allocation

	Major (n = 4)		Regional (n = 10)		Foreign (n = 11)		All Banks (n = 25)		
Yes	3	75%	6	60%	4	36%	13	52%	[68%]
No	1	25%	4	40%	7	64%	12	48%	[32%]

Personnel resource allocation is examined, and four variables used; full-time disaster planning personnel, part-time disaster planning personnel, line management function, or no formal allocation of responsibility. As indicated in table 8, a very low sixteen percent (n = 4) of all banks maintain full-time disaster recovery planning personnel; a further thirty-six percent (n = 9) maintain part-time personnel. Disaster recovery planning is a line management function for twenty-eight percent (n = 7) of all banks; including fifty percent (n = 2) of major banks. Two regional and three foreign banks allocate no formal task responsibility.

Table 8 Allocation of Disaster Recovery Planning Management Personnel

	Major (n = 4)		Regional (n = 10)		Foreign (n = 11)		All Banks (n = 25)		
Full-time DRP personnel	1	25%	2	20%	1	9%	4	16%	[22%]
Part-time DRP personnel	1	25%	3	30%	5	46%	9	36%	[28%]
Line management function	2	50%	3	30%	2	18%	7	28%	[42%]
No formal DRP allocation			2	20%	3	27%	5	20%	[7%]

This result raises issues of efficient resource allocation, prioritisation of critical business functions and co-ordination of both the planning and recovery processes, in an environment where there is no specialist disaster recovery planning risk manager, and having regard to the low level of commitment exhibited by operational business managers (table 6).

The particularly low level of organisational commitment of specialist personnel within the major banks is a concern, given the size and diversity of the major banks' national and international operations. Serious questions arise regarding their ability to respond to a disaster situation and implement recovery strategies in an efficient, co-ordinated, prioritised and timely manner.

2.3 Development and Maintenance of the Organisational Disaster Recovery *Planning* Process

2.3.2 Plan Development

The organisational disaster recovery process comprises a planning process and a response process. This section considers elements of the planning process.

There are a number of computer software packages available which provide a basis of a disaster recovery planning management tool. Twenty-four percent (n = 6) of all banks use such a package, but none of the major banks. Forty-four percent of all banks (n = 11) use a computer based word processing package to develop their own planning methodology, including all major banks (table 9). Again discrepancies exist between specific question responses. One bank indicated no computer centre disaster recovery plan documented (table 2), five banks have not used any documentation tool.

Table 9 Disaster Recovery Planning Documentation Process

	Major (n = 4)		Regional (n = 10)		Foreign (n = 11)		All Banks (n = 25)		
Specialist software package			4	40%	2	18%	6	24%	[11%]
PC word processor	4	100%	4	40%	3	27%	11	44%	[79%]
Hand written			1	10%	1	9%	2	8%	[3%]
Other					1	9%	1	4%	[1%]
Not applicable			1	10%	4	36%	5	20%	[6%]

Risk assessment and business impact analysis are an essential element of the plan development process. The next question sought to determine whether banks had carried out a business impact analysis to identify which business functions are critical to the organisation. (table 10)

Table 10 **Business Impact Analysis Completed**

	Major (n = 4)		Regional (n = 10)		Foreign (n = 11)		All Banks (n = 25)		
Yes	4	100%	8	80%	6	55%	18	72%	[91%]
No			2	20%	5	45%	7	28%	[9%]

Seventy-two percent (n = 18) of all banks, comprising one-hundred percent major banks, eighty percent (n = 8) regional banks, and fifty-five percent (n = 6) foreign banks, have completed a business impact analysis.

In table 1, ninety-two percent of banks stated they maintained, or were developing, an organisational disaster recovery plan, however this question (72%) indicates that twenty percent of those banks are in the formative stages of development, as they have not completed a business impact analysis. Table 11 responses provide an indication that the extent of business impact analyses conducted may be limited.

Each bank was asked to list in priority order its five most critical business functions. The weighted rank order distribution is presented in tables 11 (a), (b), (c), and (d).

Computer centre operations were identified by forty percent (n = 10) of banks as the most critical business function, followed by treasury operations at thirty-two percent (n = 8), and retail banking/customer services third at twelve percent (n = 3). Overall, ninety-six percent (n = 24) of banks included treasury operations; ninety-two percent (n = 23) included computer centre operations; and forty percent (n = 10) included retail banking/customer services in their list of critical business functions.

A comparative analysis of the critical business functions of all banks provides some interesting variations in the weighted rank order results, reflecting to some degree the past development and different market segments in which the banks operate. Treasury operations are ranked number one for the all banks grouping, whereas major and regional banks rank computer centre operations as their most critical business function. Treasury operations is ranked number two for major and regional banks.

Retail banking/customer service, whilst ranked number three overall, is not included in the five most critical business functions of major banks; is ranked number three for regional banks; and number six for foreign banks. Again, the fourth ranked business function overall, clearing operations, is not included in the listed major bank critical functions. International banking operations is ranked number three by major banks, but is not included in the regional banks' most critical business functions.

The very broad nature of the critical business function identification by respondent banks, raises serious concern regarding the extent of the business impact analysis carried out by the banks. The business impact analysis would normally be expected to provide a much more definitive identification of specific critical business functions. This concern is further supported by disparities in critical function identification, in particular, the major banks not recognising clearing and settlement operations as a specific critical function.

The extent of the business impact analysis process was further questioned at the interview stage, with a range of banks indicating that a systematic quantitative methodology was not used, but rather the experience method was adopted. Specific critical business functions were generally not identified.

Table 11 (a) Percentage Distribution by Average Rank Order of Critical Business Functions All Banks (n = 25)

Rank Order: 5 = most critical business function to 1 = lower ranked critical business function

Critical Business Function	5		4		3		2		1		Weighted Rank	
Treasury operations	8	32%	5	20%	8	32%	3	12%			3.60	1
Computer centre	10	40%	5	20%	2	8%	4	16%	2	8%	3.44	2
Retail banking services	3	12%	3	12%	1	4%	2	8%	1	4%	1.40	3
Clearing operations	1	4%	4	16%	2	8%					1.08	4
Telecommunications	1	4%	2	8%	1	4%	1	4%	1	4%	0.76	5
Corporate banking	1	4%	2	8%	1	4%			1	4%	0.68	6
International banking					4	16%	2	8%			0.64	7
Lending services			2	8%	1	4%	1	4%	2	8%	0.60	8
Retail cards operations			1	4%	1	4%	2	8%	3	12%	0.56	9
Executive/H.O. admin.	1	4%			1	4%			6	24%	0.56	9
Custodial services					1	4%	3	12%	2	8%	0.44	10
Other							3	12%	2	8%	0.32	11
General ledgers							1	4%	2	8%	0.16	12
Statutory reporting							1	4%	1	4%	0.12	13
No response			1	4%	2	8%	2	8%	2	8%		

Table 11(b) Percentage Distribution by Average Rank Order of Critical Business Functions Major Banks (n = 4)

Rank Order: 5 = most critical business function to 1 = lower ranked critical business function

Critical Business Function	5		4		3		2		1		Weighted Rank	
Treasury operations	1	25%	1	25%	1	25%	2	50%			4.00	2
Computer centre	2	50%	2	50%							4.50	1
Retail banking services												
Clearing operations												
Telecommunications									1	25%	0.25	6
Corporate banking												
International banking					3	75%	1	25%			2.75	3
Lending services												
Retail cards operations			1	25%			1	25%	1	25%	1.75	4
Executive/H.O. admin.	1	25%							1	25%	1.50	5
Custodial services												
Other												
General ledgers									1	25%	0.25	6
Statutory reporting												
No response												

Table 11(c) Percentage Distribution by Average Rank Order of Critical Business Functions Regional Banks (n = 10)

Rank Order: 5 = most critical business function to 1 = lower ranked critical business function

Critical Business Function	5		4		3		2		1		Weighted Rank	
Treasury operations	2	20%	2	20%	4	40%	1	10%			3.20	2
Computer centre	4	40%	3	30%					2	20%	3.40	1
Retail banking services	3	30%	1	10%	1	10%	2	20%			2.60	3
Clearing operations			2	20%	1	10%					1.10	4
Telecommunications	1	10%			1	10%					0.80	6
Corporate banking									1	10%	0.10	10
International banking												
Lending services			1	10%	1	10%	1	10%	1	10%	1.00	5
Retail cards operations					1	10%	1	10%	2	20%	0.70	7
Executive/H.O. admin.									2	20%	0.20	9
Custodial services												
Other							2	20%	1	10%	0.50	8
General ledgers							1	10%			0.20	9
Statutory reporting							1	10%			0.20	9
No response			1	10%	1	10%	1	10%	1	10%		

Table 11(d) Percentage Distribution by Average Rank Order of Critical Business Functions Foreign Banks (n = 11)

Rank Order: 5 = most critical business function to 1 = lower ranked critical business function

Critical Business Function	5		4		3		2		1		Weighted Rank	
Treasury operations	5	46%	2	18%	3	27%					3.82	1
Computer centre	4	36%			2	18%	4	36%			3.09	2
Retail banking services			2	18%					1	9%	0.82	6
Clearing operations	1	9%	2	18%	1	9%					1.46	3
Telecommunications			2	18%			1	9%			0.91	5
Corporate banking	1	9%	2	18%	1	9%					1.46	3
International banking					1	9%	1	9%			0.46	8
Lending services			1	9%					1	9%	0.46	8
Retail cards operations												
Executive/H.O. admin.					1	9%			3	27%	0.55	7
Custodial services					1	9%	3	27%	2	18%	1.00	4
Other							1	9%	1	9%	0.27	9
General ledgers									1	9%	0.09	10
Statutory reporting									1	9%	0.09	10
No response					1	9%	1	9%	1	9%		

2.3.3 Strategies

Having identified critical business functions of the Australian banks, data was gathered on the backup facility status of the banks, that is, the level of preparedness to recover an identified critical business function in the event of business disruption.

In analysing the responses to this question, it should be borne in mind that each business function has been identified as being ***most critical*** to the organisation, and as such would, by definition, need to be recovered in a very short time-frame to minimise the operational and financial impact upon the organisation.

Table 12 shows that twenty-four percent (n = 6) of all banks maintain hot sites for their most critical business function, and a further forty percent (n = 10) maintain warm sites. The percentage of banks with hot site backup facilities falls away as the ranking of criticality reduces, where, at the fifth most critical function, no hot site facilities are available and thirty-six percent (n = 9) warm sites are maintained. At the other end of the scale, identified critical business functions with no backup facilities range from twenty-four percent (n = 6) to a significant fifty-six percent (n = 14).

Within bank groupings there are important variances. When asset weightings are applied, the level of limited or no backup facilities for banks' most critical business functions is high; ranging through [26%], [13%], [18%], [14%] and [53%].

Table 12 Backup Facility Status by Critical Business Function - Ranking 1 to 5

Critical Function 1	Major (n = 4)		Regional (n = 10)		Foreign (n = 11)		All Banks (n = 25)	
Hot Site	1	25%	3	30%	2	18%	6	24% [25%]
Warm Site	2	50%	6	60%	2	18%	10	40% [49%]
Cold Site			1	10%	2	18%	3	12% [4%]
No	1	25%			5	46%	6	24% [22%]

Critical Function 2	Major (n = 4)		Regional (n = 10)		Foreign (n = 11)		All Banks (n = 25)	
Hot Site	1	25%	3	30%			4	16% [23%]
Warm Site	3	75%	4	40%	4	36%	11	44% [63%]
Cold Site			1	10%	2	18%	3	12% [4%]
No			2	20%	5	46%	7	28% [9%]

Critical Function 3	Major (n = 4)		Regional (n = 10)		Foreign (n = 11)		All Banks (n = 25)	
Hot Site	2	50%	1	10%	1	9%	4	16% [37%]
Warm Site	2	50%	4	40%	2	18%	8	32% [44%]
Cold Site					1	9%	1	4% [1%]
No			5	50%	7	64%	12	48% [17%]

Critical Function 4	Major (n = 4)		Regional (n = 10)		Foreign (n = 11)		All Banks (n = 25)	
Hot Site			1	10%			1	4% [2%]
Warm Site	4	100%	6	60%	3	27%	13	52% [84%]
Cold Site					2	18%	2	8% [2%]
No			3	30%	6	55%	9	36% [12%]

Critical Function 5	Major (n = 4)		Regional (n = 10)		Foreign (n = 11)		All Banks (n = 25)	
Hot Site							0	0% [0%]
Warm Site	2	50%	5	50%	2	18%	9	36% [47%]
Cold Site			1	10%	1	9%	2	8% [3%]
No	2	50%	4	40%	8	73%	14	56% [50%]

The data from this question provides some significant insight into the level of disaster preparedness of the banks. The five business functions listed in the survey responses are the most critical that the bank has identified, yet the overall capacity to recover that operation, within the very short time-frame necessary, is not high. Again concerns are expressed as to the actual level of organisational disaster recovery plan development, preparedness and capacity of banks, as a group, to recover from a major disaster.

Another essential element of a disaster recovery planning strategy is the off-site storage of critical data; electronic and hardcopy. Banks were questioned whether they had a structured programme in place for the off-site storage of critical data for either the total organisation, computer centre only, or computer centre plus limited other critical data. (table 13)

Table 13 Critical Data Off-Site Storage Programme

	Major (n = 4)		Regional (n = 8)		Foreign (n = 9)		All Banks (n = 21)	
Total organisation			4	50%	5	56%	9	43% [17%]
Computer centre only			1	13%			1	5% [3%]
Computer centre plus limited other data	4	100%	3	38%	4	44%	11	52% [80%]

All banks maintained some level of off-site storage. Fifty percent (n = 4) regional banks, and fifty-six percent (n = 5) foreign banks have an organisational programme in place. A further thirty-eight percent (n = 3) regional banks and forty-four percent (n = 4) foreign banks, plus one-hundred percent (n = 4) major banks, maintain a computer centre off-site storage programme with limited other critical data storage.

The next two questions consider the provision of power, an essential input to two of the identified critical business functions, the computer centre and treasury operations. Banks were asked if they maintained uninterrupted power supply (UPS) and backup generators for these critical business functions. Seventy-six percent (n = 16) and forty-eight percent (n = 10) of all banks maintain UPS and backup generators to their computer centre and treasury operations respectively (tables 14 and 15). Disturbingly, twenty-four percent (n = 5) and fifty-three percent (n = 11) respectively do not maintain backup generators, or do not know their current status. Based on asset weightings, computer centre backup power arrangements are robust at [91%], however treasury operation arrangements remain very low at only [48%].

Table 14 Computer Centre - Uninterrupted Power Supply and Backup Generator

	Major (n = 4)		Regional (n = 8)		Foreign (n = 9)		All Banks (n = 21)	
UPS & backup generator	4	100%	6	75%	6	67%	16	76% [91%]
UPS only			2	25%	1	11%	3	14% [7%]
Backup Generator only								
Neither					1	11%	1	5% [1%]
Unknown					1	11%	1	5% [1%]

Table 15 Treasury Operations - Uninterrupted Power Supply and Backup Generator

	Major (n = 4)		Regional (n = 8)		Foreign (n = 9)		All Banks (n = 21)	
UPS & backup generator	2	50%	3	38%	5	56%	10	48% [48%]
UPS only	2	50%	1	13%	2	22%	5	24% [39%]
Backup Generator only								
Neither			3	38%	1	11%	4	19% [9%]
Unknown			1	13%	1	11%	2	10% [4%]

This is of particular concern given the previously mentioned treasury operation risk exposures noted by Thompson (1997) and further support concerns regarding the extent of organisational disaster recovery planning in Australian banks.

2.3.4 Testing and Training

Plan testing and personnel training are essential phases in achieving the ultimate success of plan development and disaster response effectiveness. Banks were asked if a scheduled test programme had been implemented for existing disaster recovery plans. All major banks (n = 4), seventy percent (n = 7) regional banks and fifty- five percent (n = 6) foreign banks, representing sixty-eight percent (n = 17) all banks, indicated they implemented scheduled test programmes. (table 16)

Table 16 Scheduled Disaster Recovery Plan Test Programme

	Major (n = 4)		Regional (n = 10)		Foreign (n = 11)		All Banks (n = 25)	
Yes	4	100%	7	70%	6	55%	17	68% [89%]
No			3	30%	5	46%	8	32% [11%]

However this data does not indicate the type or extent of the test programmes. Comments made at interviews by a number of the banks indicated that a significant proportion of testing of disaster recovery plans relates specifically to the computer centre. A comparative analysis of the computer centre disaster recovery planning status (table 2) and the existence of a scheduled disaster recovery test programme shows a strong correlation between the two variables. However the proportion of banks with a scheduled test programme does not correlate with the proportion of banks that have fully documented, or are currently developing an organisational disaster recovery plan. (table 1) This further supports the view that the organisational disaster recovery planning process in a number of banks has not developed to a point where testing is feasible.

A further question identified the primary type of testing that the banks implement. As shown in table 17, computer centre testing predominates at forty-three percent (n = 9) of

all banks; this increases to sixty-three percent (n = 5) of regional banks. Nineteen percent (n = 4) of all banks have no specific type of testing.

Table 17 Disaster Plan Testing by Type

	Major (n = 4)		Regional (n = 8)		Foreign (n = 9)		All Banks (n = 21)		
Computer applications only	1	25%	5	63%	3	33%	9	43%	[34%]
Critical business functions	1	25%	1	13%	2	22%	4	19%	[22%]
Business unit specific	2	50%					2	10%	[34%]
Comb. operational/ simulation			1	13%	1	11%	2	10%	[4%]
None			1	13%	3	33%	4	19%	[6%]

The frequency of testing elements of the existing disaster recovery plan was examined. Sixty-eight percent (n = 17) of all banks test elements of their disaster recovery plan at least annually; twenty-eight percent (n = 7) semi annually; twenty-four percent (n = 6) quarterly; and four percent (n = 1) monthly (table 18). Twenty- eight percent (n = 7) of all banks, comprising twenty percent (n = 2) regional banks, and forty-six percent (n = 5) foreign banks, do not test, or do not have a plan to test.

Table 18 Disaster Recovery Plan Testing Frequency

	Major (n = 4)		Regional (n = 10)		Foreign (n = 11)		All Banks (n = 25)		
Monthly			1	10%			1	4%	[2%]
Quarterly			5	50%			5	20%	[11%]
Semi Annually			1	10%			1	4%	[2%]
Annually	3	75%	1	10%	6	55%	10	40%	[59%]
Various	1	25%					1	4%	[17%]
Never			2	20%	5	46%	7	28%	[9%]

Overall, the level of periodic testing of elements of the disaster recovery plan is low, and again may support an argument that Australian banks currently maintain a low level of disaster recovery planning commitment and preparedness.

An advanced form of plan testing, other than actual business interruption or a real disaster, is the full simulation test. The next question surveyed the number of banks that had conducted a full simulation test of their currently developed organisational disaster recovery plan. The data indicates twenty percent (n = 5) of all banks have conducted full simulation testing; comprising twenty-five percent (n = 1) major banks, ten percent (n = 1) regional banks and twenty-seven percent (n = 3) foreign banks. The results of this data relate to currently developed plans, which explains the variance between the three banks which have fully documented organisational disaster recovery plans (table 1) and the five banks which have carried out full simulation of their existing plans. (table 19)

Table 19 Full Simulation Testing of Current Disaster Recovery Plan

	Major (n = 4)		Regional (n = 10)		Foreign (n = 11)		All Banks (n = 25)		
Yes	1	25%	1	10%	3	27%	5	20%	[22%]
No	3	75%	9	90%	8	73%	20	80%	[78%]

With a clearer perspective of the disaster recovery plan testing practices of the Australian banks, each bank was asked, to the extent that they had developed a disaster recovery plan, which primary form of disaster recovery planning training, other than the testing programme, is used.

Six variables, represented in table 20, incorporate the major training techniques adopted by interviewee banks. Variables 2 and 3 relate to computer centre training only. Results indicate that disaster recovery training is particularly limited outside of the computer centre environment. Of the nineteen percent (n = 4) of banks that have used a training seminar, most comprised an introductory/broad concepts format, rather than specific applied training. Considerable time had elapsed since the seminars were conducted.

Thirty-three percent (n = 7) of all banks, comprising twenty-five percent (n = 2) regional banks, and fifty-six percent (n = 5) foreign banks, do not conduct any form of disaster recovery training.

Table 20 Primary Disaster Recovery Training Form

	Major (n = 4)		Regional (n = 8)		Foreign (n = 9)		All Banks (n = 21)		
Scenario role play	1	25%					1	5%	[17%]
Staff rotation/cross skilling	1	25%	3	38%			4	19%	[25%]
Computer centre training module	1	25%					1	5%	[17%]
DRP personnel role documentation	1	25%	1	13%	2	22%	4	19%	[22%]
Internal training seminar			2	25%	2	22%	4	19%	[8%]
No training conducted			2	25%	5	56%	7	33%	[11%]

The comparative analysis conducted on scheduled test programmes, the type of testing, frequency of testing, and training programmes support the view that Australian banks have significant scope in which to increase the testing and training elements of their organisational disaster recovery planning.

2.4 Development and Maintenance of the Organisational Disaster Recovery Response Process

2.4.1 Disaster Recognition

Disaster recognition shifts the focus of the organisation from the planning process to the disaster response; that is, where an event of business disruption is recognised as a disaster.

Particular types of disaster, that banks have identified as being an exposure to which they may be more vulnerable are presented in table 21. Fifty-seven percent (n = 12) of all banks, comprising one-hundred percent (n = 4) major banks, seventy-five percent (n = 6) regional banks, and twenty-two percent (n = 2) foreign banks, have not identified any disaster to which the bank may be more vulnerable. Of the banks that have identified a disaster vulnerability, fourteen percent (n = 3) nominated fire, followed by loss of communications and denial of building access, both at ten percent (n = 2).

Table 21 Perceived Disaster Vulnerability by Type

	Major (n = 4)	Regional (n = 8)	Foreign (n = 9)	All Banks (n = 21)
Aircraft crash		1 13%		1 5% [3%]
Loss of communications			2 22%	2 10% [2%]
Loss mainframe computer		1 13%		1 5% [3%]
Fire			3 33%	3 14% [4%]
Denial building access			2 22%	2 10% [2%]
None	4 100%	6 75%	2 22%	12 57% [86%]

Further discussion of this issue in the interview led to the conclusion that a large proportion of banks which had indicated, in the questionnaire, no particular vulnerability to disaster by type, had not considered the issue, and had not carried out a risk assessment or security impact analysis of their critical operations. Concerns are again raised about the extent of plan implementation. On an asset weighted basis, [86%] of banks had not identified or considered the disaster vulnerability of the bank.

Having surveyed the perceived vulnerability of the banks to disaster, questions sought to quantify past experiences of exposure to severe business disruption due to both natural disaster (e.g. fire or flood), or physical disaster (e.g. power loss or systems failure).

Two major banks are the only banks which have experienced a severe business disruption due to a natural disaster. (table 22) However a number of foreign banks indicated that their overseas parent banks had suffered from a natural disaster. The banks' experiences with physical disasters have been somewhat worse, with sixteen percent (n = 4) of all banks, one major bank, one regional bank and two foreign banks, acknowledging experiencing a physical disaster that had a severe impact on business operations. (table 23)

Table 22 Severe Business Disruption due to Natural Disaster

	Major (n = 4)	Regional (n = 10)	Foreign (n = 11)	All Banks (n = 25)
Yes	2 50%			2 8% [34%]
No	2 50%	10 100%	11 100%	23 92% [66%]

Table 23 Severe Business Disruption due to Physical Disaster

	Major (n = 4)	Regional (n = 10)	Foreign (n = 11)	All Banks (n = 25)
Yes	1 25%	1 10%	2 18%	4 16% [21%]
No	3 75%	9 90%	9 82%	21 84% [79%]

An observation, based on discussion at the interview, is that within banks generally a central data base of business disruption occurrences, and impact implications, is not maintained for the total organisation, and therefore the data provided relating to physical disaster disruption in particular, may significantly understate the extent of past experience. For example, there was a reluctance of computer personnel to quantify and report the frequency, operational and financial impacts of computer downtime.

Banks were asked if they had identified a disaster alert trigger point for each business function, that is, the point in time when an event of business disruption ceases to be a normal operational problem and requires the implementation of the disaster recovery plan.

Formal incorporation of the disaster alert trigger point in the disaster planning process for the total organisation is limited to nineteen percent (n = 4) banks, comprising one major bank and three foreign banks (table 24). Recognition of disaster alert trigger points is higher in the computer centre environment (variables 2 and 3), with thirty-eight percent (n = 8) of all banks; comprising twenty-five percent (n = 1) major banks, seventy-six percent (n = 6) regional banks, and eleven percent (n = 1) foreign banks. Recognition within the treasury operation (variables 1 and 3) is only twenty-four percent (n = 5) of all banks, which is surprising given its high critical business function ranking. (table 11)

Table 24 Disaster Alert Trigger Point Identified

	Major (n = 4)		Regional (n = 8)		Foreign (n = 9)		All Banks (n = 21)		
Total organisation	1	25%			3	33%	4	19%	[20%]
Computer centre only	1	25%	5	63%	1	11%	7	33%	[32%]
Computer and treasury operations			1	13%			1	5%	[3%]
No	2	50%	2	25%	5	56%	9	43%	[45%]

2.4.2 Response Infrastructure

The physical structure established for the central control of a disaster response plan, incorporating the then active elements of the organisational disaster recovery plan, may be variously referred to as a recovery control centre or an emergency operations centre. The recovery control centre becomes the management and administrative hub for the co-ordinated implementation of the disaster response for the total organisation.

Banks were asked if they had established predetermined recovery control centre/s. A high proportion of major and regional banks, one-hundred percent (n = 4) and eighty percent (n = 8) respectively, maintain established recovery control centres, but only thirty-six percent (n = 4) of foreign banks (table 25). A number of foreign banks indicated they would revert to a hotel suite, however it was recognised, by some, that critical delays would be experienced in establishing communications systems and providing equipment.

Table 25 Recovery Control Centre Established

Question 15	Major (n = 4)		Regional (n = 10)		Foreign (n = 11)		All Banks (n = 25)		
Yes	4	100%	8	80%	4	36%	16	64%	[89%]
No			2	20%	7	64%	9	36%	[11%]

Questions were directed to ascertain the proximity of the recovery control centre to existing executive management and the head office administration, and whether banks had established more than one recovery control centre. The location of the recovery control centre has strategic implications depending on the type of disaster experienced. A disaster that impacts upon the central business district (e.g. earthquake, chemical fire) may result in denial of access to the recovery control centre if it is located in the same geographic area of the organisational operation which it is to support.

Table 26 **Recovery Control Centre Strategic Geographic Dispersion**

	Major (n = 4)		Regional (n = 8)		Foreign (n = 4)		All Banks (n = 16)		
Within 10 Km	2	50%	6	75%	4	100%	12	75%	[61%]
Over 10 Km	1	25%	1	13%			2	13%	[20%]
Within 10 Km plus interstate	1	25%	1	13%			2	13%	[20%]

Seventy-five percent (n =12) of all banks with established recovery control centres, locate the centre within ten kilometres of their existing head office administration, but do not maintain a centre outside that perimeter. Thirteen percent (n = 2) have a single control centre outside the ten kilometre radius. Only thirteen percent (n = 2) of all banks have established a second recovery control centre as a fallback position in the event of a disaster, within the ten kilometre radius, impacting upon the primary recovery control centre. In each case the second recovery control centre is located interstate.

It should be noted that, with the major and regional banks, systemic risk in this instance, is lessened due to a natural geographic dispersion of critical business functions in various States. However, foreign banks are predominantly located in Sydney.

2.4.3 Media Liaison

Another essential element of the disaster response process is the organisation's media liaison or public relations strategy. Media liaison will represent the face of a bank in the event of disaster, and will adopt a pivotal role, particularly where a bank does not have an established recovery plan. This question sought to determine the preparedness of banks to respond publicly to a disaster situation through an established media liaison strategy.

Eighty-six percent (n = 18) of all banks, comprising one-hundred percent (n = 4) major banks, eighty-eight percent (n = 7) regional banks, and seventy-eight percent (n = 7) foreign banks, indicated that a disaster response media liaison or public relations strategy is in place (table 27).

Table 27 **Operational Disaster Media Liaison or Public Relations Strategy**

	Major (n = 4)		Regional (n = 8)		Foreign (n = 9)		All Banks (n = 21)		
Yes	4	100%	7	88%	7	78%	18	86%	[95%]
No			1	13%	2	22%	3	14%	[5%]

2.4.4 Response Testing

This section of the research sought to obtain data on the response capabilities of the Australian banks collectively. Due to the sensitivity of such information, the questions are purposely broad in perspective.

The bank computer centre is identified as a critical business function. Banks were asked, if a major disaster occurred at the computer centre, how long would it take to recover to an acceptable operational level using backup facilities. As shown in table 28, there is a wide dispersion in responses. Fourteen percent (n = 3) of all banks, comprising twenty-

five percent (n = 2) regional banks and eleven percent (n = 1) foreign banks, believe computer operations can be recovered in less than eight hours. A further forty-eight percent (n = 10), comprising fifty percent (n = 2) major banks, thirty-eight percent (n = 3) regional banks, and fifty-six percent (n = 5) foreign banks, believe computer operations can be recovered between eight hours and twenty-four hours.

The data would indicate that sixty-two percent (n = 13) of all banks are able to recover computer operations within the acceptable downtime proposed by Arnell (1990:2), but thirty-nine percent of all banks (n = 8) are not able, or do not know if they are able, to recover within that period of less than twenty-four hours.

Table 28 Computer Centre Recovery Time Scale

	Major (n = 4)		Regional (n = 8)		Foreign (n = 9)		All Banks (n = 21)		
Less than 8 hours			2	25%	1	11%	3	14%	[7%]
8 hours to < 24 hours	2	50%	3	38%	5	56%	10	48%	[48%]
24 hours to 48 hours	1	25%	2	25%	2	22%	5	24%	[25%]
More than 48 hours	1	25%	1	13%			2	10%	[20%]
Not known					1	11%	1	5%	[1%]

When asked if the computer centre recovery time had been fully operationally tested, only fifty-seven percent (n = 12) of all banks, comprising fifty percent (n = 2) major banks, seventy-five percent (n = 6) regional banks, and forty-four percent (n = 4) foreign banks, responded in the affirmative.

Therefore, whilst ninety-five percent of all banks have identified the time frame in which they could recover computer centre operations, only fifty-seven percent had actually fully operationally tested their current recovery response status. Care should be exercised in interpreting this data; during interviews a number of banks expressed strong reservations with regard to the estimated recovery times provided by their computer centre personnel.

Table 29 Computer Centre Recovery Plan Operationally Tested

	Major (n = 4)		Regional (n = 8)		Foreign (n = 9)		All Banks (n = 21)		
Yes	2	50%	6	75%	4	44%	12	57%	[55%]
No	2	50%	2	25%	5	56%	9	43%	[45%]

Treasury operations were also identified as critical. This question focused on the recovery of critical treasury data through the application of a disaster scenario. Banks were asked if they lost their treasury operations through fire (immediate evacuation, loss of site hardware and data), would they be able to recover both their intra-day positions and overnight positions.

Only forty-three percent (n = 9) of all banks, comprising fifty percent (n = 2) major banks, twenty-five percent (n = 2) regional banks, and fifty-six percent (n = 5) foreign banks, believe they are able to recover both positions. A further fourteen percent (n = 3), comprising twenty-five percent (n = 2) regional banks and eleven percent (n = 1) foreign banks, are able to recover their overnight position and some intra-day data. Another

nineteen percent (n = 4) of all banks are able to recover their overnight position (table 30).

Ten percent (n = 2), including one major bank and a regional bank, would not be able to recover their positions. A further thirty-three percent (n = 3) of foreign banks do not know if they are able to recover their positions.

Given the high level of criticality placed upon treasury operations by the banks, and its potential to incur a large and immediate financial impact upon the organisation, the vulnerability of the banks generally to a loss of critical treasury operations data is a serious concern. This data also implies a very high level of systemic risk at [45%] which potentially could impact financial system stability.

Table 30 Treasury Operations Recovery - Intra-day; Overnight

	Major (n = 4)		Regional (n = 8)		Foreign (n = 9)		All Banks (n = 21)		
Both positions	2	50%	2	25%	5	56%	9	43%	[45%]
Overnight /some intra-day			2	25%	1	11%	3	14%	[7%]
Overnight only	1	25%	3	38%			4	19%	[25%]
None	1	25%	1	13%			2	10%	[20%]
Not known					3	33%	3	14%	[4%]

2.5 Reserve Bank of Australia Regulatory and Prudential Requirements

The Reserve Bank of Australia (RBA) is the central bank of Australia and, at the time of this survey, the regulatory and prudential supervisor of banks. The RBA currently has particular responsibilities for promoting stability within the overall financial system and, by definition, a responsibility for the stability of the banking system.

Banks were asked whether the RBA requires them to develop and maintain an organisational disaster recovery plan. Two regional banks responded in the affirmative, the remaining ninety-two percent (n = 23) indicating the RBA does not require the development and maintenance of an organisational disaster recovery plan (table 31). During later interviews, three foreign banks advised they had confirmed their negative response with the RBA.

Table 31 RBA Organisational Disaster Recovery Planning Requirement for Australian Banks

	Major (n = 4)		Regional (n = 10)		Foreign (n = 11)		All Banks (n = 25)		
Yes			2	20%			2	8%	[4%]
No	4	100%	8	80%	11	100%	23	92%	[96%]

A further question sought to determine if the RBA required banks to develop and maintain a computer centre disaster recovery plan. The same negative responses were received.

The RBA acknowledges there is no formal requirement for banks to develop and maintain disaster recovery plans for either their computer centre operations, or the total organisation. The RBA refers to its on-going consultative process, where it has stressed,

to banks, the need for appropriate disaster recovery plans, however the data indicates that not all banks have responded to this aspect of the RBA's consultative process.

3 CONCLUSIONS

Any contention that Australian banks have fully developed and maintain a comprehensive organisational disaster recovery planning process in their risk management practices is not supported by the data. Furthermore, such a contention cannot be supported for any of the sub-groupings of major banks, regional banks or foreign banks.

The results of the research clearly demonstrate that banks, as a group, have not fully implemented disaster recovery planning throughout their organisations and are still in the formative stages of the process. Survey responses indicate a general recognition of organisational disaster recovery planning, however an overall low level of organisational commitment is constraining development of the planning and response processes.

This study found that Australian banks, as a group, have not fully developed an organisational disaster recovery plan and are not adequately prepared to respond to a significant event that may impact upon the provision of critical business functions. Major banks appear to have progressed further with the development of the organisational disaster recovery planning processes than the regional and foreign banks. However, some individual major banks have not reached a point where they could confidently claim that they are prepared to recover critical business functions in the event of a disaster.

Given the importance of the banking sector, particularly the major banks, to the stability of the Australian financial system, it is further concluded that the consequent levels of systemic risk are of concern.

The RBA advised that it does not have a specific requirement, but encourages banks, through its consultative processes, to implement organisational disaster recovery planning. This is not evident in the practices of the banks. All banks stated the RBA did not monitor the level of either organisational, or computer centre, disaster recovery planning preparedness.

The systemic risk of a major disaster in the banking system is significant and should also be addressed by the RBA. One alternative may be to adopt a reporting regime similar to that existing in the United States of America, whereby bank management must certify annually that a comprehensive disaster recovery planning process has been documented and implemented throughout the organisation, and is periodically tested and actively maintained and reviewed.

Serious questions are raised as to the level of preparedness of Australian banks to respond effectively to a significant event of disruption to critical business operations. The operational and financial impacts of business disruption should concern government, the RBA, bank management, customers, suppliers, other associated organisations and shareholders.

The ramifications for the banking industry and the financial system of a disastrous event on a particular bank, or group of banks, should be addressed. Whilst individual banks are ultimately responsible for their own management and survival, external interrelationships and dependencies mean systemic risk must also be considered. The dominance of the four major banks in Australia in particular increases significantly the level of systemic risk directly associated with those banks.

REFERENCES

Arnell, A., (1990), *Handbook of Effective Disaster/Recovery Planning A Seminar/Workshop Approach*, Technical Editor: Davis, D.G., McGraw-Hill Publishing Company, New York

Blair, G., (1991), "Corporate Security and Contingency Planning Survey", Coopers & Lybrand and Price Waterhouse Contingency Planning '91 Conference, Sydney, 28 -29 November

Christensen, S., (1992), "Surveying, and Salvaging, the Aftermath of Outage", *Computerworld*, 2 October, p.35

Chantico Publishing Company, Inc., (1991), *Disaster Recovery Handbook*, TAB Professional and Reference Books, Blue Ridge Summit, PA.

Ford, M.H., (1990), *Disaster Recovery Planning: How to Develop and Write a Plan*, American Bankers Association, Florida

Rehesaar, H., (1992), *Secrets of Successful DRP Project Management and Insurance*, fourth edition, Harper Collins Publishers Inc., New York

Thompson, G. J., (Deputy Governor) Reserve Bank of Australia, (1997), "The Many Faces of Risk in Banking", *Bulletin*, Sydney, July, p. 15

Toigo, J.W., (1989), *Disaster Recovery Planning - Managing Risk and Catastrophe in Information Systems*, Yourdon Press, Prentice-Hall, Inc., New Jersey

Wold, G.H., (1992), "The Disaster Recovery Planning Process - Part I of III", *Disaster Recovery Journal*, Volume 5, Number 1, January, February, March, p.p. 29-34

Woodcock, D., (1992), "Organisation-Wide Contingency Planning", Coopers & Lybrand and Price Waterhouse Contingency Planning '92 Conference, Melbourne, 2-3 April