Monash University

Department of Banking and Finance
P.O. Box 197
Caulfield East Victoria 3145
Telephone: (03) 9903 2585
Facsimile: (03) 9903 2292
Email: Chris.Viney@BusEco.Monash.Edu.Au

9 September 1996

The Secretary
Financial System Inquiry
Treasury Building
PARKES ACT 2600

Dear Sir/Madam,

Submission to the Financial System Inquiry
Organisational Disaster Recovery Planning

This submission relates to a single issue, but one which may potentially impact upon the survival of an individual financial institution, and importantly the stability of the financial system; that is, organisational disaster recovery planning.

Please find attached, as part of this submission, my paper which puts forward the proposition that disruption to critical business operations of a financial institution from a natural, technical or physical disaster represents a negative externality that may seriously impact the overall stability of the banking system and financial system generally.

It is argued that the level of organisational disaster recovery planning varies significantly between banks and as such is an uncompensated risk within the financial system. This conclusion is drawn from a detailed examination of bank disaster recovery practices conducted in 1994 by the writer.

A survey of selected international bank supervisors of their practices for the regulation of organisational disaster recovery planning indicates a divergence of practices. Of note is the regulatory requirement within the United States of America for financial institutions to develop, test and maintain comprehensive disaster recovery plans. These must be signed-off annually by the board of directors, and are subject to audit by regulatory examiners. The Reserve Bank has not implemented a prudential standard for organisational disaster recovery planning within banks. The Insurance and Superannuation Commission has implemented some standards for superannuation funds.

In conclusion, banks are absolutely dependant upon technology based information, product delivery and support systems. Studies indicate institutions must recover critical operations within 24 hours to ensure survival. Loss of a [major] financial institution within Australia must have financial system stability implications. Banks, as a group, are not adequately prepared to respond to an event of disruption to their critical business operations.

It is recommended that the prudential regulator(s) of the Australian financial system establish prudential guidelines on organisational disaster recovery planning for financial institutions.

Yours sincerely,

Chris Viney
Director, Australian Banking Research Unit

REGULATION OF BANK ORGANISATIONAL DISASTER RECOVERY PLANNING: A FINANCIAL SYSTEM ISSUE

ABSTRACT

Financial institutions manage a range of financial and operational risks. Within the banking sector, regulatory reporting requirements impose a level of transparency upon a number of these risks, however it is argued that uncompensated risks still exist. This paper puts forward the proposition that organisational disaster recovery planning, that is the management of business continuity risk, remains an uncompensated risk.

The loss of critical business operations due to a physical, technical or natural disaster by a bank potentially may have a catastrophic effect on the ultimate survival of the institution and may even extend to the overall stability of the financial system. Acceptance of this proposition raises the issue of the level of regulatory control and supervision of organisational disaster recovery planning for banks.

A survey was conducted of the regulation of bank organisational disaster recovery planning by the Reserve Bank of Australia (RBA) and other international bank regulatory authorities, including a focus on the South East Asia Region. Finally, Australian banks were surveyed to ascertain their perception of RBA requirements, and the extent of their development of organisational disaster recovery planning.

The paper concludes that bank supervisory authorities generally have not established disaster recovery guidelines; exceptions being the United States of America, Hong Kong and Thailand. Reserve Bank of Australia practices are generally consistent with other major and regional financial centres, indicating that the potential adverse consequences of this form of operational risk to the stability of the financial system remain both an international and domestic issue.

1. INTRODUCTION

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

The proposition that underlies this paper is that a bank with a comprehensive organisational disaster recovery plan in place will have a greater chance of survival and of minimising the operational impact and financial cost of recovery, and will pose a lesser threat to overall financial system stability, in the event of a disastrous event of business disruption.

This paper examines the regulation of bank disaster recovery planning from the perspective of selected international bank regulators and the Australian bank regulator and prudential supervisor, the RBA.

2. REGULATORY INTERVENTION - A FINANCIAL SYSTEM ISSUE

"The overall goal of bank regulation .... is to maintain public confidence in the banking system. On the microeconomic level, the focus is upon limiting the risk exposure of *individual* banks ...." (Sinkey 1985:349,350)

The use of the regulatory process to establish boundaries on public risks is usually presumed to be based on a valid perception of these risks, and of their relative importance in the spectrum of public exposure to all risks. The regulatory process obviously deals with future events, and thus suffers from the well-known limitations of any prediction. Ideally, risk regulation should be based on a statistically significant history of similar risk events which are reasonably measurable and which disclose the relevant cause-effect relationships. Unfortunately, such a professionally satisfying analytical basis seldom exists, and most risk regulation is unavoidably embedded in large uncertainties. (Starr 1987:537,538)

Prudential supervision of banks varies. Within the United Kingdom, Japan and Australia, prudential supervision of banks is a central bank function, whilst in the United States of America, Germany and Canada supervision is carried out by agencies which are not part of the central bank. Associated regulation also varies considerably between countries. The United Kingdom and the United States of America, both major financial centres, maintain a more informal approach to regulation with elements of discretion and self regulation; whereas countries such as France, Italy and Belgium are more tightly regulated. (Di Cagno 1990:1,2)

Within Australia, financial institutions are divided into bank and non-bank sectors. The Reserve Bank of Australia (RBA) is responsible for the regulation and prudential supervision of the banking sector; the Australian Financial Institutions Commission, building societies and credit unions; and the Insurance and Superannuation Commission, insurance companies and superannuation funds.

Regulation of banks results, in part, from risk management inefficiencies, or market imperfections, in a competitive market that is reluctant to disclose information on risk levels adopted by an institution. Marquardt argues that "Ordinary market devices, such as pricing risk, do not allocate risk appropriately, because depositors cannot charge a bank for risks they do not know about." (1987:7) He further argues (1987:10) that if the financial system has a significant market in interbank deposits, then each bank is exposed directly to risks taken by the management of banks where deposits are made. If these risks are unknown, then they are uncompensated risks banks, as depositors, should want to avoid. If each bank is at times a depositor at other banks, there will be incentives for some form of explicit or implicit agreement among banks that they will voluntarily refrain from placing uncompensated risks on each other.

It is the process by which this *agreement* is achieved that requires further development. It may be argued that bank managers should fully represent the interests of bank shareholders against their own interests, and therefore banking risks affecting shareholders should be fully taken into account in bank management decisions. In addition, Marquardt highlights the probability that negative externalities exist in banking, and that the cost of this form of risk is not taken into account when making business decisions. (1987:6,7-9)

Countries with central bank regulatory controls attempt to ensure *agreement* is reached in managing otherwise uncompensated risks of an institution by the application of standards to be observed by participants. That is, the regulatory body may be set up and given discretion to control conflict of interest between banks, shareholders, depositors, borrowers and government which may not otherwise be resolved by co-operative agreement. The implementation of capital adequacy standards is an example of such regulatory authority intervention.

An organisational disaster may be regarded as a potential negative externality which may not have been included in the decision making process. The specific level of planning and commitment to disaster recovery planning within a bank is information that generally is not available to other market participants, and therefore may represent significant uncompensated risk. It may well be argued therefore that the management of business continuity risk should fall within the ambit of the central supervisory body. This is supported by the argument that ".... regulation has a basic objective to improve the soundness of the banking system. .... The rationale given for any restrictions imposed on the banking system, usually points to the lower probability of failure that results when these constraints are binding." (Di Cagno 1990:8,9)

This raises the following questions in relation to regulatory supervision of banks:

(a) are banks required by a central authority to develop, test and maintain organisational disaster recovery plans?

(b) does the central authority actively monitor the organisational disaster recovery planning process within banks under its prudential supervision?

(c) if the central authority does not require banks to develop and maintain organisational disaster recovery plans, is a lesser level of disaster recovery planning required?

The Bank for International Settlements (BIS), primarily representing the Group of 10 countries (United States of America, United Kingdom, France, Italy, the Netherlands, Germany, Belgium, Canada, Sweden, Switzerland and Japan), has evolved into a central bank for many of the world's central banks. BIS monitors developments in the international financial markets, and has instigated a number of operating standards and conventions for participants in the markets; including the capital to risk weighted assets standards. There is no international standard applied to the management of business continuity risk (disaster recovery planning).

3. INTERNATIONAL REGULATORY AUTHORITY DISASTER RECOVERY PLANNING REQUIREMENTS FOR BANKS

A survey of selected international banking regulatory authorities was conducted. Selection of the sample was based upon the sophistication of the financial markets of a country; size of the market; international diversity and dispersion; together with geographic proximity (South East Asia market) to Australia. Seventeen international authorities were forwarded a survey letter. Banking regulatory and supervisory authority respondents are listed in table 1. Twelve authorities responded to the survey, representing 70.59% of the sample.

Table 1 International Banking Regulatory Authorities - Sample Respondents

Country	Authority
Canada	Office of the Superintendent of Financial Institutions Canada
Germany	Deutsche Bundesbank
Hong Kong	Hong Kong Monetary Authority
Indonesia	Bank of Indonesia
Malaysia	Bank Negara Malaysia
New Zealand	Reserve Bank of New Zealand
Singapore	Monetary Authority of Singapore
Thailand	Bank of Thailand
The Philippines	Central Bank of The Philippines
United Kingdom	Bank of England
United States of America	Federal Reserve System
United States of America	Comptroller of the Currency

A summary of each respondent country's disaster recovery planning requirements follows.

3.1 Canada - Office of the Superintendent of Financial Institutions

Banks are required by the Office of the Superintendent of Financial Institutions to maintain a business continuity plan and a disaster recovery plan for systems information. "....the Office does allow institutions the flexibility in deciding the scope and details of these plans, provided the plans are developed within the framework of prudent business practices. Flexibility is allowed because each institution has different needs." (Heyes, J.W., Office of the Superintendent of Financial Institutions Canada, Toronto, 12 April 1994)

The Office of the Superintendent of Financial Institutions uses a risk-based approach in the examination of financial institutions. Therefore, the extent of review of an institution's business continuity and disaster recovery plans will vary between institutions, depending on their risk profile.

3.2 Germany - Deutsche Bundesbank

The Federal Banking Supervisory Office is responsible for banking supervision in Germany. "....as part of the proper conduct of business pursuant to section 6 of the Banking Act, German banks also have to take precautions against natural or physical disasters." (Maurer, C., Deutsche Bundesbank, Frankfurt, 30 March 1994)

The Federal Banking Supervisory Office does not issue formal instructions regarding disaster recovery planning to institutions under its supervisory control.

3.3 Indonesia - Bank of Indonesia

Banks are not required by the central bank of Indonesia to maintain organisational disaster recovery planning.

Bank of Indonesia receives reports on banks' current electronic data processing platform and environment, and performs its own risk assessment in order to gain an understanding of risk management techniques and controls implemented by the banks.

"As banking EDP risk has increased domestically and globally, we will definitely be requiring all banks to increase their internal control on EDP matters (e.g. Contingency Planning) so that they would be able to manage the risk identified more properly." (Sudibyo, W., Bank Indonesia, Jakarta, 8 April 1994)

3.4 Hong Kong - Hong Kong Monetary Authority

Deposit-taking institutions authorised under the Banking Ordinance are required by the Hong Kong Monetary Authority to maintain adequate and effective internal control systems, which are subject to regular review. This includes contingency plan arrangements for mitigating and containing damage caused by disaster. (Luk, R., Hong Kong Monetary Authority, Central, 22 March 1994)

The Hong Kong Monetary Authority is empowered to commission audit reports or conduct on-site examination. Guidelines are issued and cover the following areas:

(i) Objectives - mitigate the effect of business disruption and ensure the orderly continuance of operations

(ii) Key control techniques and procedures

(a) A formal contingency plan should identify:
- critical business functions
- key personnel
- essential premises, equipment, files and documentation

(b) Responsibilities for development, maintenance, testing and implementation of the disaster recovery plan should be clearly identified

(c) Backup and/or off-site storage procedures for computer files and key documentation should be established

(d) Formal training programmes established

(e) Testing programme to verify adequacy of plan

(f) Service provider agreements should be established

(g) Periodical testing of external backup and standby arrangements

(h) Periodical adequacy review of insurance arrangements

3.5 Malaysia - Bank Negara Malaysia

Bank Negara Malaysia does not require banks to maintain organisational disaster recovery plans. Banks and switch companies which provide automatic teller machine network sharing between institutions are required to maintain computer disaster recovery backup arrangements.

Bank Negara Malaysia permits institutions to set up their own backup site; establish mutual sharing arrangements; or subscribe to approved disaster recovery backup providers. The disaster recovery plan "....should cover the whole computerised banking operations and include security and recovery capabilities necessary to ensure continuity of operations and data integrity....[they]....should also be approved by the management and should be reviewed from time to time...." (Hussin, A.A., Bank Negara Malaysia, Kuala Lumpur, 30 March 1994)

Strict compliance controls are established to ensure the confidentiality and integrity of customer information. Banks and disaster recovery backup companies are required to:

(i) test plans twice a year at the backup site and report to Bank Negara Malaysia for an adequacy review,

(ii) advise Bank Negara Malaysia when backup facilities are activated for any recovery exercise,

(iii) [disaster recovery backup companies] submit a certified financial audit report to Bank Negara Malaysia, and

(iv) [disaster backup recovery companies] provide an annual list of bank and non-bank financial institution subscribers to their computer backup facilities.

3.6 New Zealand - Reserve Bank of New Zealand

Banks registered in New Zealand are not required by the central bank supervisor, the Reserve Bank of New Zealand, to maintain organisational disaster recovery plans.

The Reserve Bank of New Zealand notes that many banks do maintain a disaster recovery plan, and that the adequacy of banks' disaster recovery planning is often included in audit reports to bank management. (Dawe, S., Reserve Bank of New Zealand, Wellington, 4 March 1994)

3.7 Singapore - Monetary Authority of Singapore

Banks in Singapore are not required to maintain organisational disaster recovery planning.

Whilst the Monetary Authority of Singapore has not issued formal guidelines or regulation, banks in Singapore are expected to maintain disaster recovery plans for their computer centre operations. Such plans are reviewed by the banks' external auditors and Monetary Authority of Singapore examiners to ensure their adequacy. (Lau, L., Monetary Authority of Singapore, 10 March 1994)

3.8 Thailand - Bank of Thailand

Commercial banks in Thailand are required to maintain contingency plans which must be submitted to the Bank of Thailand. Contingency plan guidelines issued by the Bank of Thailand cover the total organisational contingency plan and the computer system plan:

(i) Planning principles
- the planner must be qualified with a good working knowledge of the banking operations,
- the plan must be in writing, and distributed to relevant personnel,
- testing (occasional) of the plan is required.

(ii) Assumptions
- identification of disaster scenarios, impact analysis, protective measures

(iii) Scope of authority and chain of command throughout the organisation

(iv) Personnel - records, training, communication, rotation, welfare

(v) Office - alternative sites for offices, equipment and communication systems

(vi) Cash and financial resources - security, diversification of sources

(vii) Asset keeping - identification and prioritisation of assets, storage, security safety equipment, training

Furthermore, computer centre contingency plan guidelines cover:

(i) Safety systems - duties, responsibilities, documentation, system control, personnel safety, insurance, safety control and damage protection for buildings, equipment and hardware

(ii) Emergency plan and computer backup system
- emergency plans must be maintained
- computer backup system should be 'far' from the main computer centre
- commercial banks may share computer backup facilities, or establish joint venture companies to provide a mutual backup service

"Since 1990, commercial banks are not allowed to stop servicing customers for reason of the commercial bank's computer system failure longer than a working day, except where a permission to act otherwise has been granted by the Bank of Thailand." (Phuvanat-naranubala, T., Bank of Thailand, Bangkok, 20 April B.E. 2537 (1994))

3.9 The Philippines - Central Bank of The Philippines

The Central Bank of The Philippines requires bank examiners to complete a questionnaire designed to determine compliance by banks with prescribed internal control standards. One questionnaire relates to "....Bank's formulation of an emergency preparedness program to provide for the protection of personnel continuity management reconstruction of records...." (Encarnacion, L.T., Bangko Sentral ng Pilipinas, Maynila, 25 March 1994)

The questionnaire relates primarily to immediate emergency response actions and records protection and reconstruction. The questionnaire does not cover comprehensive issues of computer centre or total organisational disaster recovery planning.

3.10 United Kingdom - Bank of England

The Bank of England has not issued a formal notice specifically requiring banks to maintain organisational disaster recovery planning. However a guidance note has been issued incorporating computer environment disaster recovery planning.

The guidance note addresses issues of physical security, standby systems, recovery management, data backup, and electronic systems business interruption planning. Institutions are required to commission an accountant's report, which includes in part, comment on the adequacy of the computer disaster recovery plan. The report is forwarded to the Bank of England.

"....following bomb explosions in the "City" in 1992 and 1993, the focus on disaster recovery is now much more widely drawn....the Bank [of England] would expect an institution to maintain a disaster recovery plan for the total organisation and not just for the computer operation." (Blackburn, M., Bank of England, London, 9 March 1994)

3.11 United States of America - Federal Reserve System
- Comptroller of the Currency

The revised version of banking circular BC177, dated 12 July 1989, issued by the Comptroller of the Currency, and adopted by all financial institution regulators, under the auspices of the Federal Financial Institutions Examination Council (FFIEC), requires institutions to maintain corporate wide contingency planning. (Coonley, D.G., Comptroller of the Currency, Washington, 17 March 1994) Detailed guidelines are issued by the regulators to support the planning process. Co-operative agreements are specifically not acceptable; a hot site is required.

Direct responsibility for business continuity rests upon the management of the institution. (Toigo 1989:10) (Ford 1990:11) "It is the responsibility of the board of directors and senior management of financial institutions to ensure that a comprehensive contingency plan for the entire organization is developed, maintained and tested. Failure to comply with the policy could result in an enforcement action against the financial institution...." (Vinnedge, D., Federal Reserve System, Washington, 28 March 1994)

The Comptroller of the Currency (OCC) states that examiners strictly enforce the requirement for an annual board of directors review of the contingency plan. "The OCC, Federal Reserve Board and Office of Thrift Supervision examiners review an institution's recovery program .... there are no volume and/or dollar thresholds for compliance that must be met before the policy on recovery planning will be enforced." (McCarthy 1991:52)

A further banking circular, BC187, extends bank management responsibility for developing and implementing a contingency plan in the event of a service bureau outage.

The Federal Reserve performs periodic examinations of banks and EDP service bureaus to verify compliance with the policy. The frequency of the examinations is based on the condition of the organisation according to the most recent full scope examination, periodic visitations and progress reports.

4. AUSTRALIAN REGULATORY AND SUPERVISORY DISASTER RECOVERY PLANNING REQUIREMENTS FOR BANKS

The RBA is the central bank of Australia and is the regulatory and prudential supervisor of Australian banks. It derives its legislative powers primarily from the Banking Act 1959 (Cwth) and the Reserve Bank Act 1959 (Cwth) and associated Regulations.

"The Reserve Bank has particular responsibilities for promoting stability in the banking system, and a more general responsibility for the financial system as a whole. Those responsibilities are exercised in ways which are intended to minimise the risks of the systems encountering serious problems, but they do not extend to preventing individual institutions from making losses or even failing." (Reserve Bank of Australia 1993:24) The RBA, by its own statement, has responsibility for stability of the banking system, and therefore, the integrity of bank management and operating systems that underlie market perception and public confidence in banks.

A survey letter was mailed to the RBA seeking to determine whether banks under its regulatory control are:

(a) required to maintain a disaster recovery plan for the total organisation,
(b) required to maintain a disaster recovery plan for the computer centre operation, or
(c) not required to maintain a disaster recovery plan.

A response from the RBA stated that: "A basic principle in the Reserve Bank's approach to bank supervision is that the primary responsibility for a bank's sound operation rests with that bank's own management and board of directors. Although there are some aspects of banks' operations where the Reserve Bank is more intrusive and has instituted prudential guidelines, to date it has not done so in respect of disaster recovery plans. Nevertheless, in its regular consultations with banks, the Reserve Bank has stressed the need for appropriate disaster recovery plans." (Egan, B.M., 29 June 1994)

A mail questionnaire was forwarded to the Australian banking population (N = 35). Responses were received from 25 banks, representing 71.43% of the population. [note: the survey results used in this paper are from a detailed examination of the disaster recovery planning practices of Australian banks conducted in 1994.]

Banks were asked specifically whether the RBA requires them to develop and maintain an organisational disaster recovery plan. Two regional banks only, responded in the affirmative, the remaining ninety two percent (n = 23) of all banks indicated the RBA does not require the development and maintenance of an organisational disaster recovery plan. (table 2)

Table 2 Reserve Bank of Australia Requirement for Banks to Develop and Maintain an Organisational Disaster Recovery Plan

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

When questioned further on their affirmative responses, the two regional banks advised the RBA requirement was issued with the granting of each banking authority. Both banks were asked if the RBA monitored this conditional requirement of the banking authority. Each answered in the negative.

The questionnaire also sought to determine if the RBA required banks to develop and maintain a computer centre disaster recovery plan. Identical responses were received to those shown in table 2.

A further question sought to determine the status of **organisational** disaster recovery planning 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. Eighty percent (n = 20) are currently developing a plan, comprising seventy five percent (n = 3) of major banks, ninety percent (n = 9) of regional banks and seventy three percent (n = 8) of foreign banks. Analysis of table 3 demonstrates some disparity between various bank groupings. Whilst ninety percent (n = 9) of regional banks are developing an organisational disaster recovery plan, none has achieved that objective, whilst ten percent (n = 1) have not commenced a planning process. Nine percent (n = 1) of foreign banks have not commenced the planning process; seventy three percent (n = 8) have commenced, and eighteen percent (n = 2) have fully documented plans. The level of systemic risk is reflected in [brackets] by applying asset weighting to the data.

Table 3 Australian Bank 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%]

The results of this question indicate a significant proportion of 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 extent of development of the organisational disaster recovery plans is not evident from this question, but is analysed further in Viney (1994).

These statistics alone present a position of some considerable concern regarding the potential exposure of individual banks to a disastrous event of business disruption, and more importantly the potential risk to the stability of the Australian financial system. 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 plan.

The RBA acknowledges there is no formal requirement for Australian banks to develop and maintain disaster recovery plans for either their computer centre operations or the total organisation. The RBA does make clear reference to its on-going consultative process, where it has stressed the need for appropriate disaster recovery plans, however conclusions that may be drawn from the above data indicate not all banks have recognised, or responded to, the RBA's consultative process in this matter.

4. CONCLUSION

Modern organisations, and in particular financial institutions, are more than ever exposed to business continuity risk. The elapsed time between when a disaster results in the loss of a critical business function and when recovery of that function is essential to ensure organisational survival is generally accepted as being less than twenty four hours for banks. (Arnell 1990; Wold and Shriver 1990) Banks are fundamentally reliant upon technology to support their information systems and deliver their products and services. Coupled with this absolute dependency on technology is an exposure to public confidence and market sentiment.

Of the twelve bank regulatory authority respondents; three issue guidelines relating to organisational disaster recovery planning to banks under their control. A further three authorities issue guidelines in relation to computer centre operations, whilst another five authorities adopt a much less formal approach to disaster recovery planning for banks. One authority issues no guidelines or controls. A summary comparative analysis of the results of the survey is presented in table 4.

Table 4 Bank Regulatory and Supervisory Authority Issuance of Disaster Recovery Planning Standards or Guidelines - by Country

Country	Organisational DRP Guidelines	Computer Centre DRP Guidelines	Other DRP Arrangements
Australia	No	No	Yes
Canada	No	Yes	
Germany	No	No	Yes
Hong Kong	Yes	Yes	
Indonesia	No	No	Yes
Malaysia	No	Yes	
New Zealand	No	No	
Singapore	No	No	Yes
Thailand	Yes	Yes	
The Philippines	No	No	Yes
United Kingdom	No	Yes	Yes
United States of America	Yes	Yes	

With the exception of the United States of America, Hong Kong and Thailand, respondent bank regulatory authorities do not impose organisational disaster recovery planning standards or guidelines upon banks within their jurisdiction. This includes the RBA which does not directly address the potential consequences to an individual bank, or the financial system as a whole, of a significant event of disruption to bank critical business functions.

Banks are exposed to potential financial and operational risks due to negative externalities, both within the domestic and international financial markets. Failure of bank regulatory authorities to establish organisational disaster recovery standards indicates that the potential consequences of this form of operational risk to the financial system remains both an international and domestic issue. The existence of this uncompensated risk increases the level of systemic risk within the global financial system.

This paper sought to determine the practice of the Australian bank regulator (RBA) and international banking regulatory authorities regarding the issuance of formal disaster recovery planning guidelines. The results raise concerns about the financial system ability to recover from a severe business disruption. This in turn raises questions relating to the appropriate role of regulatory authorities, both in Australia and overseas, in the context of disaster recovery planning.

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.

Davis, K. and Harper, I., editors, (1991), *Risk Management in Financial Institutions*, Allen & Unwin Australia, North Sydney.

Di Cagno, D., (1990), *Regulation and Banks' Behaviour Towards Risk*, Dartmouth Publishing Company, Aldershot, Hants.

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

Marquardt, J.C., (1987), *Financial Market Supervision: Some Conceptual Issues*, BIS Economic Papers No. 19, May, Bank for International Settlements, Basle.

McCarthy, A.M., (1991), "Disaster Recovery Programs: Small Banks Can't Afford Not to be Protected", *Bank Management*, Vol. LXVII, No. 2, December, pp. 52-53.

Reserve Bank of Australia, (1993), *Report and Financial Statement 1993*, Sydney.

Rotberg, E.H., (1992), *Risk Taking in the Financial Services Industry*, Organisation for Economic Co-Operation and Development, Paris.

Sinkey, J.F.Jnr., (1985), "Regulatory Attitudes Towards Risk", *Handbook for Banking Strategy*, Aspinwall, R.C. and Eisenbeis, R.A., editors, John Wiley & Sons, Inc., New York.

Starr, C., (1987) "Dealing with Uncertainty in Risk Regulation", *Risk Assessment and Management*, Lave L.B., editor, Plenum Press, New York.

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

Viney, C.W., (1994), *Organisational Disaster Recovery Planning: An Examination of Australian Banks*, Masters Thesis, Monash University, Melbourne.

Wold, G.H. and Shriver, R.F., (1990), *Disaster Recovery Planning Manual for Financial Institutions*, Bankers Publishing Company, Chicago, Illinois.