Informing IT Managers – Why the Bank for International Settlements is Establishing a Capital Charge Guideline for Operational Risk: the Australian Evidence

Christopher Viney
Deakin University, Melbourne, Australia

cviney@deakin.edu.au

Abstract

IT managers within financial institutions must understand and be able to respond to the operational, financial and regulatory impacts that will result from a loss of critical business functions. The *Basel Committee on Banking Supervision*, through the Bank for International Settlements (BIS) has circulated a consultative paper which, if eventually adopted by nation-state bank supervisors, will impose an operational risk capital charge on banks as part of the new Capital Accord. Banks will also be required to record and report operational risk occurrences or events. This paper presents data on aspects of the disaster risk management practices of banks operating within the Australian financial system. The data indicate that banks, as a group, do not maintain effective disaster risk management practices and are not adequately prepared to recover a loss of critical business functions. The results clearly support the necessity of the BIS initiatives.

Keywords: operational risk, disaster risk management, financial institutions capital accord

Introduction

Why do IT managers in banks need to understand the nature of operational risk and the purpose of disaster risk management in the maintenance of the continuity of a bank's critical business functions? Three over-arching reasons are evident; these are (1) operational, (2) financial and (3) regulatory. Operational issues relate to the impact on an organization of a loss of critical business function capacity. Financial impacts relate to the cost of recovering normal business operations, plus consequential losses associated with reduced business output. Regulatory issues evolve from the requirements of bank prudential supervisors.

Major events that result in a loss of critical business functions of financial institutions do occur! This was clearly demonstrated on September 11, 2001 when terrorist attacks in New York exposed the reality of disaster. The US financial system was severely tested as financial institutions and markets closed and struggled to recover their critical business operations. The direct and consequential operational and financial losses associated with this disaster are significant and extend beyond the domestic US markets to incorporate the global financial system.

IT managers should be cognisant that technology advances, coupled with globalisation of the international financial system, has increased the time sensitivity of financial institutions to even limited disruption to critical business operations. This is particularly evident in derivatives transactions, foreign exchange trading and payments system settlements. A nation-state's financial system may be described

as the life-blood of the real economy. For an economy to grow, and maintain that growth, it must be supported by a highly developed and efficient financial system (Viney 2000). The modern global financial system comprises a range of institutions and markets that are reliant on complex interrelationships and dependencies for the efficient conduct of financial transactions to support economic trade in goods and services, plus the flow of funds between nation-states.

Within the context of this paper, 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 operational and financial survival of an institution. Operational risk contagion is a further real risk to which nation-state financial systems are exposed. The contagion effects may even threaten the overall stability of the global financial system. Disaster risk management requires the development and maintenance of specific strategies that enable an institution to recover and resume disrupted critical business operations.

The importance of maintaining business continuity in an information technology based business environment has been established for over a decade by Chantico (1991, p.4). That research shows, in relation to information systems, that:

- as the length of an outage increases, loss of functionality and integration worsens,
- with a loss of critical business functions, reverting to manual backup procedures is totally inadequate,
- the management decision process deteriorates as horizontal and vertical coordination of business functions decreases markedly,
- computer outages initiate actions that cause the business to incur additional expenses,
- the largest intangible loss is cash-flow interruption, and
- continued loss of customers, competitive edge, and image might prove more damaging than the temporary loss of revenue and additional costs.

Existing research, including Hiatt, 2000; Myers, 1999; Wold, 1992; Ford, 1990; and Arnell, 1990, clearly identifies the high-risk exposure of financial institutions to events of business disruption due to a natural, physical or technical disaster. Major 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 (service and public confidence); other institutions (interrelationships and dependencies); and shareholders (profitability and business survival).

The implications of the above are that banks must manage their exposures to business continuity risk. As a result, the Bank for International Settlements (2001) has adopted a position that regulatory intervention is necessary and is developing international guidelines for the measurement of operational risk and the application of minimum capital charges.

Regulatory Operational Risk Responses

An objective of this paper is to highlight the necessity for IT managers to be aware of the impacts of a loss of business continuity may have upon the ultimate survival of a bank and therefore the vital importance that should be placed on the education and training of bank personnel in disaster risk management. IT managers must understand the operational and financial impacts of both the form and timing of their disaster recovery planning and response. In seeking to maintain financial system stability, bank regulators may impose regulatory requirements on banks in relation to the maintenance of business continuity. However, regulatory practice varies between nation-states.

For example, the Reserve Bank of Australia (RBA) is the central bank of Australia with specific responsibilities for the soundness of the payments system and overall financial system stability. The Australian Prudential Regulation Authority (APRA) is the bank supervisor. The RBA and APRA impose only limited specific prudential standards for banks to develop and maintain strategies and procedures to manage business continuity for either their computer centre operations, or the total organisation. One important area of potential operational risk where the RBA and APRA have taken an active approach is the introduction of real time gross settlement (RTGS) within the payments system. With the introduction of RTGS, each bank was required to establish backup systems and procedures to ensure their continuous participation in the payments system.

The United States of America provides the most comprehensive example of the regulation and supervision of business continuity risk. The Comptroller of the Currency (OCC), and other financial institution regulators under the auspices of the Federal Financial Institutions Examination Council (FFIEC), require institutions to maintain corporate-wide contingency planning. Direct responsibility for business continuity rests with the board of directors and senior management of banks. They must ensure that a comprehensive contingency plan is developed, maintained and tested for the entire organisation. Failure to comply with this policy could result in an enforcement action against the bank. OCC examiners strictly enforce the requirement for an annual board of directors' review of the contingency plan. Bank management responsibility for developing and implementing a contingency plan is extended to include service bureau and outsourced business functions.

The Basel Committee on Banking Supervision operates a secretariat within the Bank for International Settlements (BIS) and comprises senior supervisory representatives from the United States of America, United Kingdom, France, Italy, the Netherlands, Germany, Belgium, Canada, Sweden, Switzerland and Japan. The committee 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 adequacy accord. There currently are no international guidelines for the management of operational risk.

The BIS has issued its *Core Principles for Effective Banking Supervision* (1997) which comprise twenty-five basic principles that represent a minimum prerequisite for effective prudential bank supervision. Principle 13 (iii) states that supervisors "should ensure senior management puts in place effective internal control and auditing procedures; also, that they have policies for managing or mitigating operational risk (e.g., through insurance or contingency planning). Supervisors should determine that banks have adequate and well-tested business resumption plans for all major systems, with remote site facilities, to protect against such events."

A survey of the operational risk policies of international banks by the Basel Committee on Banking Supervision (1998) notes that "managing such risk is becoming an important feature of sound risk management practice in modern financial institutions." The committee interviewed thirty major banks from different member countries on the management of operational risk. The report focused primarily on policy and management processes and did not explore the detail of specific risk management practice. In summary, the report found that:

- awareness of operational risk among bank boards and senior management is increasing,
- while all banks surveyed had some operational risk management framework, many indicated that they were only in the early stages of development,
- identification of operational risk as a separate risk category is relatively new,
- few banks currently measure and report this risk on a regular basis, and
- limited institution historical data is available to develop empirical risk management models.

It should be remembered that the banks in this survey are major international banks. If these banks do not adequately manage operational risk, then what lesser standards are practiced by other banks; both within nation-state financial systems, and the global financial system?

The BIS (January, 2001) is proposing a regulatory framework for the incorporation of a capital charge for operational risk in its new *Basel Capital Accord*. The BIS is currently gathering data to support the development of three approaches to measuring an operational risk capital charge; that is, the Basic Indicator Approach, the Standardised Approach and the Internal Measurement Approach. Operational risk is categorised as internal fraud; external fraud; employment practices and workplace safety; clients, products and business practices; damage to physical assets; business disruption and system failures; and execution, delivery and process management.

Given the proposed BIS operational risk capital charge, and the critical need for bank IT managers to maintain continuous business operations, this paper analyses the disaster risk management practices of banks within the Australian financial system in an endeavour to:

1. draw conclusions and compare the practices of Australian banks in the practice of disaster risk management, and
2. explain the motivation for the initiatives of the *Basel Committee on Banking Supervision* to develop an international standard to measure operational risk exposures and apply a related capital charge on banks.

IT Practice in Disaster Risk Management – Australian Evidence

The BIS definition of operational risk is very broad. Therefore, this paper focuses on critical aspects of operational risk associated with disaster risk management. A bank with a comprehensive IT business continuity plan will minimize the cost of recovery and will have a greater chance of survival in the event of a disastrous business disruption. As stated by Toigo (1989, p.3), organisations that plan for a disaster, formulate recovery strategies for critical business functions, and educate and train their personnel to plan for, and effectively respond in a disaster situation, generally will survive.

Operational disaster risk management facilitates the development of specific disaster recovery planning and disaster response processes. In the event of a disruption to business operations due to a natural, physical or technical disaster, these processes will enable a bank to resume critical business operations within a defined period and facilitate the efficient, structured and prioritised resumption of normal business operations.

A disaster is an evolving, or immediate, event that may significantly disrupt the critical business functions of a bank. Critical business functions are minimum operational requirements necessary to meet an institution's current commitments, maintain customer relationships, ensure market confidence, maintain cashflows and minimise financial loss. Natural, physical and technical disasters are operational disasters. Natural disasters may include flood, fire, hurricane, earthquake and snow-storm. Physical and technical disasters may include employee error, sabotage, terrorist acts, loss of power, loss of computer systems and applications, and failure of communication systems. Disaster risk management requires the identification, measurement and management of these operational risk exposures. For example, if the Treasury function of a major bank lost access to its communication systems, this would create uncertainty within the market, make it difficult for the bank to execute and settle transactions, and would lead to significant financial loss.

The rapid development and institutional integration of IT, including information systems, product delivery systems and communication systems, has created an environment in which a disruption to critical business functions of a limited duration potentially could cause severe financial loss, and ultimately may

even threaten corporate survival (Hiatt, 2000, p.76; Christensen 1992, p.35). IT managers need to appreciate that technology integration throughout an organization means that the focus of disaster risk management must incorporate all business units within an institution, that is, IT managers must extend the risk management process beyond the computer center and include all technology based systems across the bank.

Within the Australian financial system, banks are the dominant financial institutions. Banks within Australia may be differentiated between the four major banks (National Australia Bank Limited, Commonwealth Bank of Australia Limited, ANZ Banking Group Limited, and Westpac Banking Corporation Limited), regional banks, such as St George Bank Limited and Suncorp-Metway Limited, and foreign bank subsidiaries and branches. Data was gathered through questionnaires forwarded to the bank population within the Australian financial system, plus scheduled interviews conducted with bank disaster risk managers. Twenty-five of banks, representing 71.43% of the population, responded to the questionnaire, while interviews were conducted with twenty-one banks.

Disaster risk management is a complex process that incorporates many variables. The data in this paper focuses on a range of specific IT elements of the disaster risk management. The data differentiates the disaster risk management practices of the major Australian banks, regional Australian banks and foreign banks. The reason that the banks are categorised as major, regional or foreign derives from the nature of banking development in Australia which has been impacted by wide geographic dispersion and historic heavy regulation. The major banks (National Australia Bank Limited, Commonwealth Bank of Australia Limited, ANZ Banking Group Limited and Westpac Banking Corporation Limited) clearly are the most significant financial institutions and therefore it is useful to consider their practices with out the possible distortion of the impact of the practices of the regional and/or foreign banks. It is also interesting to consider whether the practices of the Australian banks differ from those of the foreign banks. The 'all banks' data enables conclusions to be draw on the preparedness of banks within the Australian financial system to respond to, and recover from, a disruption to critical business operations. Absolute numerical and percentage results are tabulated and analysed by bank sub-groupings. An indication of the level of systemic risk is sought by applying percentage asset weightings [in brackets] for all banks.

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

	Major	**Regional**	**Foreign**	**All Banks**
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%]

Table 1: Organisational disaster recovery planning status

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. This result indicates 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.

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 bank computer centre operations. Sixty-four percent of all banks, including three major banks, seven of the regional banks and six foreign banks, maintain fully documented plans for their computer centre operations. One foreign bank has no plan. Maintenance of computer centre operations is critical to inter-bank 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 IT managers place a higher priority on the management of operational risk within the computer centre than managers of other business functions of a bank. Interview responses also indicated that IT 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.

	Major	**Regional**	**Foreign**	**All Banks**
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%]

Table 2: Computer centre disaster recovery planning status

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 on whether the boards of directors of Australian banks have issued written policy documents specifying organisational objectives and policy in relation to disaster risk management.

	Major	**Regional**	**Foreign**	**All Banks**
Yes	3 75%	3 30%	7 64%	13 52% [64%]
No	1 25%	7 70%	4 36%	12 48% [36%]

Table 3: Written policy document issued by board of directors

Only fifty-two percent of all respondent banks have issued a written disaster recovery planning policy document. Given that ninety-two percent of respondent banks (table 1) indicated they 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 a very low level of policy documentation in the regional banks, with a reported thirty percent.

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

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

Table 4: Disaster recovery planning formal budget allocation

Risk assessment and business impact analysis are essential elements of the disaster risk management process. The next question (Table 5) sought to determine whether banks had carried out a business impact analysis to identify which business functions are critical. The business impact analysis facilitates an analysis of each identifiable business function, and provides a detailed understanding of the financial and operational impacts of experiencing business disruption, and highlights both internal and external interrelationships and dependencies. The business impact analysis is, to a large degree, the basis upon which the organisational disaster recovery plan is built, in that it provides management with the empirical evidence with which an informed business decision may be made regarding the allocation of resources to the development of a plan.

	Major		Regional		Foreign		All Banks		
Yes	4	100%	8	80%	6	55%	18	72%	[91%]
No			2	20%	5	45%	7	28%	[9%]

Table 5: Business impact analysis completed

Seventy-two percent of all banks, comprising one-hundred percent major banks, eighty percent regional banks, and fifty-five percent foreign banks, have completed a business impact analysis. Again, 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 very early formative stages of development, as they have not completed a business impact analysis.

Banks identified treasury operations and computer center operations as their two most critical business functions. Both these functions are totally reliant upon, and supported by, IT operations. Data was gathered on the type of backup facility banks maintained for these critical IT functions. A backup facility refers to an alternate site available to an institution for relocation of business operations in the event of disruption of operations at the primary site (e.g. computer centre, treasury operations). Backup facilities are generally described as being a cold site, warm site or hot site.

A cold site backup facility is one where no provision of resources or equipment has been made. A computer centre cold site should however incorporate raised flooring and environmentals (e.g. power, telecommunications, air-conditioning), however, all other equipment and resources required to duplicate existing facilities are only installed if the backup site is activated. A warm site is a facility where resources and equipment are available, but a period of time will elapse before the facility can be made operational; for example, the down-loading of current data. A hot site is a backup facility that provides sufficient du-

plication of the primary site to allow near immediate and continuing operation of critical business operations until the recovery of normal operations is achieved.

In analysing the responses to this question, it should be borne in mind that treasury operations and computer center operations have been identified as being the most critical to a bank, and as such would need to be recovered in a very short time-frame to minimise the operational and financial impact upon the organisation.

Table 6 shows that only twenty-four percent of all banks maintain hot sites for their treasury operations, and a further forty percent maintain warm sites. Thirty six percent of banks maintain cold sites or have no backup arrangements in place. The loss of treasury operations would have a significant operational and financial impact upon a bank, yet the level of preparedness to respond to a disaster is clearly inadequate.

	Major		Regional		Foreign		All Banks	
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%]

Table 6: Treasury operation backup facility type

A bank's ability to recover computer center operations is also constrained by the type of computer centre backup facilities that are in place. Only sixteen percent of banks have a hot site facility, and a further forty-four percent a warm site. The preparedness of the remaining forty percent of banks also appears inadequate.

	Major		Regional		Foreign		All Banks	
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%]

Table 7: Computer centre operation backup facility type

The data from this question provides some significant insight into the level of disaster response preparedness of the banks. These two business functions are the most critical functions identified by the banks, yet the overall capacity to recover those operations, within the very short time-frame necessary, is not high. Again concerns are expressed as to the actual level of disaster recovery plan development, preparedness and capacity of banks, as a group, to recover from a major disaster.

The next two questions consider the provision of power, an essential requirement for computer centre and treasury operations. Banks were asked if they maintained uninterrupted power supply (UPS) and backup generators for these critical business functions. UPS, supported by a generator system, provides a backup source of clean power (i.e. voltage irregularities are removed) which will allow the continued and uninterrupted operation of equipment and facilities. UPS will generally support the institution's computer centre and other identified critical business operations, such as treasury.Only forty-eight percent of banks maintain UPS and backup generators to their treasury operations, while seventy-six percent maintain UPS and

backup generators to their computer centre operations (Tables 8 and 9). Disturbingly, fifty-three percent and twenty-four percent 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%] and certainly represent increased systemic risk.

	Major	Regional	Foreign	All Banks
UPS & backup generator	2 50%	3 38%	5 56%	10 48% [48%]
UPS only	2 50%	1 12%	2 22%	5 24% [39%]
Backup Generator only				
Neither or unknown		4 50%	2 22%	6 28% [13%]

Table 8: Treasury operations - uninterrupted power supply and backup generator

	Major	Regional	Foreign	All Banks
UPS & backup generator	4 100%	6 75%	6 67%	16 76% [91%]
UPS only		2 25%	1 11%	3 14% [7%]
Neither or unknown			2 22%	2 10% [2%]

Table 9: Computer centre - uninterrupted power supply and backup generator

The next question surveyed the number of banks that had conducted a full simulation test of their currently developed disaster plans. A simulation test involves the planned conduct of disaster recovery plan strategies in a manner consistent with actual operating conditions. Initial simulation tests may test individual components of the recovery plan, but will progressively incorporate more business functions until management is confident that the institution can respond effectively in a real disaster situation. The data indicates only twenty percent of all banks have conducted full simulation testing; comprising twenty-five percent major banks, ten percent regional banks and twenty-seven percent 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 10). Testing is a critical element of the disaster risk management process. The low level of testing implies banks cannot afford to be confident in the robustness of their disaster recovery strategies.

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

Table 10: Full simulation testing of current disaster recovery plan

Banks were asked, if a major disaster occurred at their computer centre, how long would it take to recover to an acceptable operational level using backup facilities. As shown in Table 11, there is a wide dispersion in responses. Fourteen percent of all banks, comprising twenty-five percent regional banks and eleven percent foreign banks, believe computer operations can be recovered in less than eight hours. A further

forty-eight percent, comprising fifty percent major banks, thirty-eight percent regional banks, and fifty-six percent foreign banks, believe computer operations can be recovered between eight hours and twenty-four hours.

The data indicates that sixty-two percent of all banks are able to recover computer operations within the 24-hour acceptable downtime proposed by Arnell (1990), however, thirty-eight percent of banks are not able to do so. In the interviews, significant reservations were expressed as to the reliability of the computer center recovery times.

	Major	Regional	Foreign	All Banks
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 12%	1 11%	3 14% [20%]

Table 11: Computer centre recovery time scale

The next 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 of all banks, comprising fifty percent major banks, twenty-five percent regional banks, and fifty-six percent foreign banks, believe they are able to recover both positions. A further fourteen percent, comprising twenty-five percent regional banks and eleven percent foreign banks, are able to recover their overnight position and some intra-day data. Another nineteen percent of all banks are only able to recover their overnight position (Table 12). Twenty-four percent, including one major bank, one regional bank and three foreign banks, would not be able to recover their positions.

	Major	Regional	Foreign	All Banks
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%	3 33%	5 24% [24%]

Table 12: Treasury operations recovery - intra-day; overnight

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

Conclusion

The events of September 11, 2001 have reinforced the unpredictable nature of operational risk exposures, and have again confirmed that indiscriminate disasters can happen that may significantly disrupt the critical business operations of a financial institution. Bank IT operations are particularly exposed to opera-

tional risk, incorporating business continuity risk. The elapsed time between when a disaster causes the loss of critical business functions, and when recovery of that function is essential to a bank's survival, is typically accepted as being less than twenty-four hours for a bank's computer centre operations. However, some critical IT supported functions, such as foreign exchange trading, derivatives dealing and payments system settlements, are time sensitive within minutes. Banks are fundamentally reliant upon IT to support their information systems, product delivery systems and communication systems.

The Bank for International Settlements has recognised that the systemic risk that may eventuate from a major disaster in the banking system is significant. The Australian evidence raises serious concerns as to the level of preparedness of banks operating within the Australian financial system to respond effectively to a significant event of disruption to critical business functions, in particular IT supported functions. 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 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 governance, management and survival, external interrelationships and dependencies mean systemic risk is an issue. The evident level of systemic risk that may eventuate from a major disruption to critical business functions in the banking system has been recognized by the BIS through the Basel Committee on Banking Supervision. The reluctance of most nation-state bank supervisors to implement specific operational risk management guidelines has prompted the Committee to move to develop international guidelines and encourage nation-state bank supervisors to adopt specific standards to measure operational risk and apply an operational risk capital charge. IT managers must be cognisant of the operational, financial and regulatory impacts of a disaster on critical IT functions, and must ensure policies and procedures are implemented that encourage the practice of effective disaster risk management.

References

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

Bank for International Settlements. (1997). *Core Principles for Effective Banking Supervision*, Basle, Bank for International Settlements.

Basel Committee on Banking Supervision. (2001). *Overview of the New Basel Capital Accord*, Consultative document, Basle, Bank for International Settlements, January.

Basel Committee on Banking Supervision. (1998). *Operational Risk Management*, Basle, Bank for International Settlements, September, paper No.42.

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

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

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

Hiatt, C.J. (2000). *A Primer for Disaster Recovery Planning in an IT Environment*, Hershey, PA, Idea Group Publishing.

Myers, K.N. (1999). *Manager's Guide to Contingency Planning for Disasters: protecting vital facilities and critical operations*, second edition, New York, John Wiley & Sons.

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

Viney, C. (2000). *McGrath's Financial Institutions, Instruments and Markets*, third edition, Sydney, McGraw-Hill Book Company.

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.

Biography

Christopher Viney is a senior lecturer with the Department of Accounting and Finance at Deakin University, Melbourne, Australia. He is the author of the text *McGrath's Financial Institutions, Instruments and Markets*, third edition, McGraw-Hill Book Company, Sydney. This is the recommended finance text adopted by the majority of Universities within Australia in the study of the operation and functions of a modern financial system. Chris has overseas teaching experiences in a number of countries; he is also the Director, of the University's finance international study program. He has conducted major research projects within industry and government. Prior to moving to academia, Chris had 27-years experience in the banking industry.