The Conceptualisation Of Operational Risk Management Models

Christopher Viney, (Email: cviney@deakin.edu.au), Deakin University, Australia

ABSTRACT

Operational risk is evolving as a specialist field of risk management that must be practiced within all organisations, but currently has a particular relevance to banks. The Basel Committee on Banking Supervision has circulated a consultative paper which, if adopted by nation-state bank supervisors, will impose an operational risk capital charge on banks as part of a new Capital Accord. The definition of operational risk is wide-ranging and creates some unique issues related to the development of appropriate risk management models. This paper conceptualises two distinct operational risk management models; being a predictive model that will result in a known outcome upon its implementation, and a pre-emptive operational risk management model which prepares an organisation in the event that a future risk occurrence results in a disruption to critical business operations.

INTRODUCTION

Major operational risk 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. Direct and consequential operational and financial losses associated with disaster are significant and extend beyond the domestic financial institutions and markets to incorporate the global financial system.

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 (BIS, 2001a). All types of business organisations and government departments are exposed to operational risks, however, this paper will consider operational risk within the context of financial institutions, in particular banks.

Operational risk is not a new risk exposure that organisations must manage, but it may well be argued that operational risk has not been predominant in the risk management practices of organisations in the past. However, operational risk management has certainly gained prominence in recent times, especially with significant operational risk losses being experienced by a number of high profile international organisations. One such example, that precipitated the move to a greater understanding of operational risk, was the significant loss experienced by the treasury operations of Barings Bank. Most recently, increased terrorist activities have highlighted the need to develop expertise in operational risk management.

Therefore, banks need to understand the nature and purpose of operational risk management within the context of maintaining the continuity of a bank's critical business functions. Three over-arching objectives become evident; these are operational, financial and regulatory. Operational objectives relate to the impact on an institution of a loss of critical business function capability. Financial impact objectives relate to the cost of recovering normal business operations, plus consequential financial losses associated with reduced business output. Regulatory objectives evolve from the requirements of bank prudential supervisors.

Bank 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. For example, 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 2003). 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. Operational risk management requires the development and maintenance of specific strategies that enable an institution to recover and resume disrupted critical business operations within pre-determined time frames.

THE BIS AS A DRIVER OF OPERATIONAL RISK MANAGEMENT POLICY AND PRACTICE

Existing research, including Hiatt (2000) and Myers (1999), 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); regulators (financial system stability and monetary policy); customers (service and public confidence); other financial institutions (interrelationships and dependencies); and shareholders (profitability and business survival).

The theory of the organisation contends that the risk management process, in part, derives from an organisation's need to survive. Therefore, operational risk management should be expected to actively reside within all management decision structures; that is, 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 and constraints restrict the extent of the risk management process. An organisation may place limits on or even ignore the pro-active management of operational risk exposures and develop an ethos of reactive risk management. Examples of failures within an organisation's operational risk management process may derive from a lack of understanding of this risk by the board of directors and executive management, inadequate budget allocations, poor risk management leadership and procedures, and weak or non-existent education and training programs.

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.

In 1997 the BIS published the *Core Principles for Effective Banking Supervision* which comprise twenty-five basic principles that represent a minimum prerequisite for effective prudential bank supervision. Principle 13 (iii) states that nation-state bank supervisors should ensure banks implement effective internal control and auditing procedures and that they have policies stating how the institution will manage or mitigate operational risk. Supervisors should determine that banks have adequately documented and rigorously tested business resumption plans for all major systems.

In 1998 the Basel Committee on Banking Supervision conducted a survey of the operational risk policies of international banks. The subsequent report noted that operational risk must become an important feature of sound risk management practice. 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 of directors 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 historical data is available to develop empirical risk management models.

It should be noted 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?

Therefore the BIS (2001b) has adopted a position that regulatory intervention is necessary and is currently developing international guidelines for the measurement of operational risk and the application of minimum capital charges within a proposed new capital adequacy accord. The BIS 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.

While managers have become more aware of the nature of operational risk and have begun to allocate greater resources to this area of risk management, the role of the BIS in proposing that an operational risk capital charge be applied to banks within the context of a new capital adequacy accord has been a principal driver of evolving operational risk management policy and practice.

PREDICTIVE VERSUS PRE-EMPTIVE OPERATIONAL RISK MANAGEMENT MODELS

The BIS definition of operational risk is very broad. Operational risk exposures include internal and 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 (BIS, 2001a).

It is essential that bank managers understand that risk management policies and procedures must take account of the different natures of the wide range of operational risks. For example, policies, procedures and the practice of risk management may well differ significantly when managing the risk of fraud in a treasury dealing room versus a major loss of computer or communication systems. This introduces the concept of a predictive operational risk management model and a pre-emptive operational risk management model.

Predictive operational risk management model

The literature provides any number of risk management frameworks, each with its own level of sophistication and complexity, but essentially all adopt a structure of risk identification, risk evaluation, strategy selection and administration. Following is an applied institutional framework drawn from Campbell (1991) which has been adapted to reflect operational risk management requirements:

- identify all risk exposures – this first step is fundamental to the operational risk management process. It is not possible to effectively measure and manage a bank's operational risk exposures if those risks have not been identified and documented. Bank personnel must have a detailed knowledge of their business operations, cash flows and balance sheet structure, plus causal risk linkages that will be evident across business functions,
- analyse risk exposure impacts – bank personnel need to have the skills to be able to conduct a risk analysis and business impact analysis to determine the financial and operational extent of a risk exposure,

- assess the bank's attitude to each risk exposure – this will vary across business functions, and will be dependent upon the critical nature of a function. Importantly, this will ensure that a bank's decision processes have been applied to operational risk management, and that the risk consequences are understood,
- select appropriate risk management strategies, products and services – quantitative and analytical models may be used to compare the advantages of risk strategy choices. A bank's risk strategies will be constrained by policy options and budget resource allocations. Bank personnel must be trained to recognise the potential of internal risk management strategies; for example, using alternative existing bank resources. Relevant bank personnel needs to be aware of the range of specialist external risk management products and services that are available, and develop the skills to accurately determine their appropriateness to the bank's business operations,
- implement controls – before any risk management strategy can be implemented it is essential that appropriate operational and financial controls are established. For example, the authority and responsibility for strategy implementation, maintenance and monitoring needs to be in place. Computer systems need to be functional to support the strategy. New strategies must be compatible with existing risk management strategies and procedures. Funding and cash-flow requirements need to be approved and available. Reporting requirements need to be documented,
- implement the risk management strategy – only at this point is the bank able to confidently implement a new risk management strategy. Written authority must accompany the implementation, and
- monitor, audit and review all risk management strategies – risk exposures will alter as the bank's business responds to customer needs, policy initiatives, regulatory changes, shifts in economic activity and competitor influences. Therefore, a risk management strategy implemented today may need to be modified at a later date. Risk exposures and related strategies need to be audited to ensure they comply with the bank's policy directives and that they are appropriate. Policy should also stipulate periodic reviews of the bank's operational risk management practices.

A number of the operational risk exposures identified above may be successfully managed by applying the seven steps of the risk management framework. For example, an organisation may adequately increase the security of its computer centre by requiring all personnel to use an electronic access system, plus further security may be gained from security camera monitoring and alarm trigger systems. A bank may significantly reduce the chance of internal fraud in its treasury operations with the implementation of clearly documented procedures and the application of sophisticated computer reporting systems that generate exception reports immediately authorised procedures or limits are breached by personnel.

In each of the examples, a risk management model is applied that should result in a determinable outcome. The management of these risk exposures may be graphically shown in figure 1 with a predictive operational risk management model. Within this model the organisation identifies its operational risk exposures within the business environment, gathers information, investigates risk management products and strategies, establishes controls and makes an appropriate decision for implementation. In this risk management model a predictable business outcome occurs.

However, there are other operational risk exposures that are not fully managed within the above predictive operational risk management model. This necessitates the application of a pre-emptive operational risk management model.

Pre-emptive operational risk management model

An area of operational risk where the predictive operational risk management model is inadequate is disaster risk management; that is, situations whereby the normal day-to-day operations of a business are significantly disrupted. Operational disaster risk management facilitates the development of specific disaster planning and disaster response processes. In the event of a disruption to normal business operations due to a natural, physical or technical disaster, these processes will enable a bank to resume critical business operations within a defined time-period and facilitate the efficient, structured and prioritised resumption of normal business operations.

Figure 1. Predictive operational risk management model

A disaster is an evolving or immediate event that may significantly disrupt the critical business functions of an organisation. Critical business functions are minimum operational requirements necessary to meet an institution's current commitments, maintain customer relationships, ensure market confidence, maintain cash-flows 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 sabotage, terrorist acts, a cut in power supplies, loss of computer systems and applications, or a failure of communication systems. Disaster risk management requires the identification, measurement and management of these operational risk exposures. For example, if the treasury division of a major bank was to loose access to its communication systems, this would create uncertainty within the financial markets, make it difficult for the bank to execute and settle transactions, and may lead to significant financial loss.

The rapid development and institutional integration of technology based 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; Christensen, 1992). An institution with a comprehensive organisational business continuity plan will have a greater chance of survival, and minimise the cost of that recovery, in the event of a disastrous business disruption (Viney, 1994).

The objectives of disaster risk management are identified by Myers (1999) and Wold (1992) as:

- minimising the occurrence of disaster events,
- protecting an institution in the event that its critical operations are disrupted,
- establishing a structured and coordinated disaster response process,
- providing confidence and security to shareholders, management, regulators, customers, creditors, personnel and associated parties,
- minimising operational risk delays,
- minimising cash-flow disruptions and financial impacts,
- guaranteeing the reliability of disaster risk management strategies,
- providing a documented and measurable standard for testing a plan, and
- minimising management decision-making during a stressful disaster situation.

Within the broad definition of operational risk it is apparent that disaster risk management extends beyond the determinable outcome of the predictive operational risk management model and also incorporates a critical disaster response process. Grove and Moffitt (2001) and Viney (1994) propose that disaster risk management is a dual process of planning and response; that is:

- the business resumption plan; being the planning and management decision process necessary for the development and maintenance of the disaster recovery preparedness and capability of a bank, and
- the disaster response plan; being the action process necessary for the implementation of appropriate elements of the organisational business resumption plan in the event of a disaster disrupting business operations.

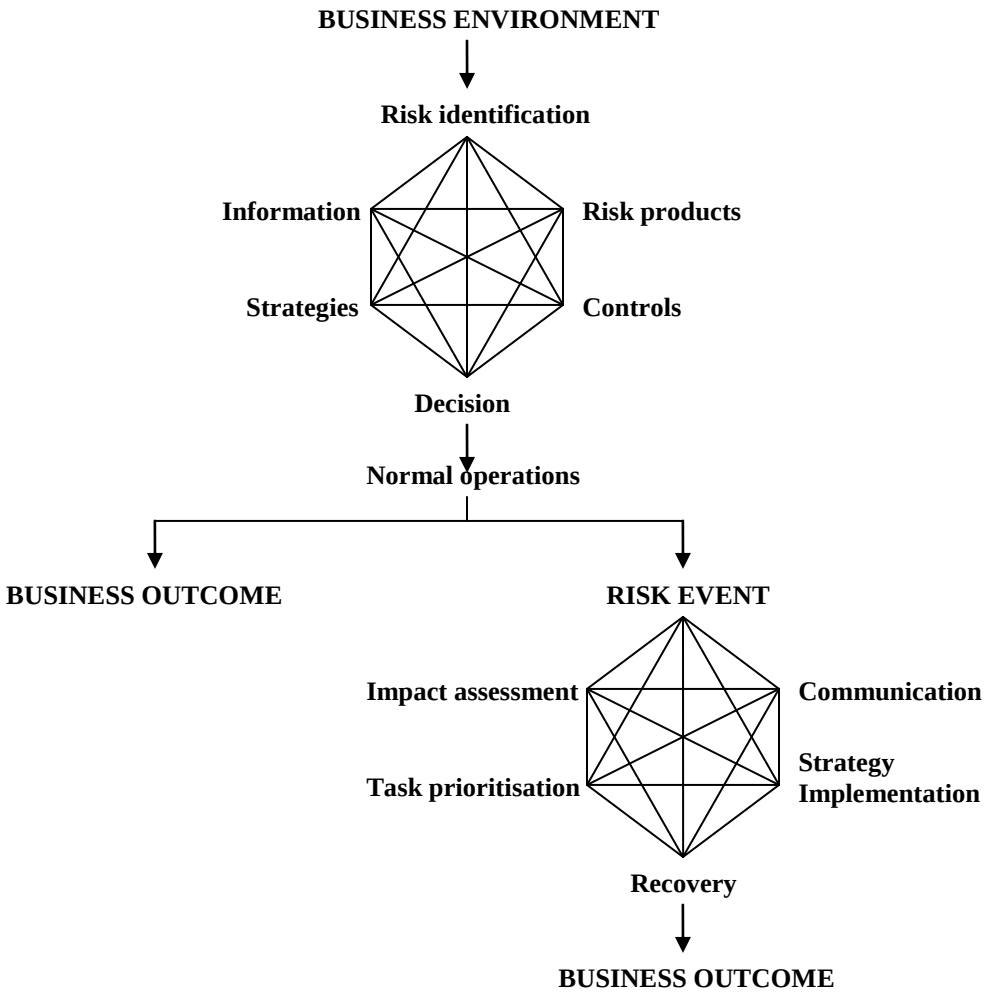
Not all operational risk management strategies result in a single predictive business outcome. It is quite probable that the full implementation of a risk management strategy may ultimately be dependent upon the occurrence of some uncertain future risk event. The risk event may, or may not, occur. Irregardless, the operational risk management strategy is in place. The risk management process may then be described as being pre-emptive. For example, a bank will typically identify its computer operations as being critical to its ongoing business operations. The bank may adopt a number of alternative strategies to manage this risk exposure. The bank could enter into an agreement with a back-up computer centre provider that allows the bank access to necessary computer facilities in the event that its primary computer centre site fails. Alternatively the bank may decide to build its own secondary computer site. In either case it will only be necessary to action the disaster response plan if the primary site experiences a disaster and is no longer operationally functional.

This concept is demonstrated in Figure 2, where the first phase of the risk management process prepares the organisation for the possible eventuality of a risk event. At this point in the model a strategy is in place, but normal business operations continue. However, should a risk event occur, management will assess the impact on the organisation of the disruption, establish lines of communication (internal and external), determine current priorities for the management of the situation, and implement predetermined recovery strategies to ensure the on-going operation of the organisation.

The pre-emptive risk management model allows for the situation of two alternative business outcomes, depending on the continuance of, or disruption to, normal business operations. That is, once the first phase of the model is implemented normal business operations continue, but should a disaster situation eventuate then the second phase of the model is activated. Therefore, the pre-emptive operational risk management model may be described as a dichotomy, whereby there is a planning process and, if necessary, a response process. Organisational disaster risk management is an example of the application of the pre-emptive risk management model.

The pre-emptive operational risk management model can be applied to a bank's computer centre operations. Banks are totally reliant upon their technology based information and product delivery systems. As such, a bank cannot afford to loose its computer operations for more than a limited time-period. A bank may decide to build a secondary computer facility as a back-up strategy in case it should operationally loose its primary computer facility. This is the first phase of the model where a strategy is put in place and normal business operations continue. If, at a future date, the bank was to experience an operational disaster it would immediately assess the impact of the disaster and determine whether it was necessary to activate the secondary computer site. If the site is activated then the bank would need to advise the board of director, executive management and other related personnel. The pre-determined response strategies would be implemented. Depending on the nature of the disaster, it may also be necessary to advise authorities, shareholders, the media and others of the situation. Within the context of the particular disaster, the organisation would prioritise the recovery of critical business functions and progressively implement recovery strategies. Both the prioritisation of recovery tasks and the application of appropriate recovery strategies should be derived from the organisation's documented business resumption plan. Successful recovery of business operations should be the expected outcome.

Figure 2. Pre-emptive operational risk management model



CONCLUSION

Financial institutions are exposed to operational risks that must be measured and managed within the context of an institution's overall risk management strategies. While the understanding of operational risk management is increasing within banks, regulatory drivers, initiated through BIS proposed changes to the Basel Capital Accord, will necessitate the development and review by bank managers of their operational risk management policies and practices.

The BIS definition of operational risks is wide-ranging and perhaps all encompassing. Risk managers need to be aware that one risk management model is not suitable for the management of all operational risks. This paper has developed the concept of a predictive operational risk management model and also a pre-emptive operational risk management model.

The predictive operational risk management model identifies a risk exposure within a current business environment, gathers information in relation to the operational and financial impact of that exposure, researches and considers a range of risk management products and strategies, establishes management controls of authority,

responsibility, reporting, systems, audit and review, and then instigates the risk management strategy to achieve a determinable business outcome.

The pre-emptive operational risk management model recognises that a determinable business outcome is not always the final outcome of an operational risk management strategy. Particularly in relation to disaster risk management, the risk management process is a dichotomy of disaster planning and, if necessary, disaster response. The pre-emptive model adopts the components of the predictive model, but then extends to a second phase that will be activated if a disruption to critical business functions occurs. In the event of a disaster the second phase of the model will recognise the risk event and assess the operational impact of the disaster on the organisation. Internal and external communication systems will be activated to mobilise and inform necessary parties. Having regard to the documented business resumption plan developed in the first phase of the model, managers will prioritise the recovery of affected critical business functions and initiate pre-determined recovery strategies. The structured application of the business resumption plan will facilitate the timely recovery of normal business operations and minimise the operational and financial impacts of the disaster.

REFERENCES

1. Bank for International Settlements, 1997, "Core Principals for Effective Banking Supervision", BIS, Basel
2. [BIS] Basel Committee on Banking Supervision, 1998, "Operational risk management", Bank for International Settlements, Basel, September, paper No.42
3. [BIS] Basel Committee on Banking Supervision, 2001(a), "Operational Risk", Consultative Document, Bank for International Settlements, Basel, January
4. [BIS] Basel Committee on Banking Supervision, 2001(b), "Overview of the new Basel Capital Accord", Consultative Document, Bank for International Settlements, Basel, January
5. Campbell, C., 1991, "The seven stages of risk management success", *Decisions*, National Australia Bank, John Fairfax and Sons, Melbourne, Volume 3, Number 3, August
6. Christiansen, S., 1992, "Surveying and salvaging the aftermath of outage", *Computerworld*, October, p.35
7. Grove, J. and Moffitt, C., 2001, "Success: Coming together as an industry", *Disaster Recovery Journal*, Volume 21, pp.473-496
8. Hiatt, C.J., 2000, *A Primer for Disaster Recovery Planning in an IT Environment*, Idea Group Publishing, Hershey, PA
9. Myers, K.N., 1999, *Manager's Guide to Contingency Planning for Disasters: protecting vital facilities and critical operations*, second edition, John Wiley and Sons, New York
10. Viney, C., 1994, "Organisational Disaster Recovery Planning: An Examination of Australian Banks", Unpublished Thesis, Monash University, August
11. Viney, C., 2003, *McGrath's Financial Institutions, Instruments and Markets*, fourth edition, McGraw-Hill Australia, Sydney
12. Wold, G.H., 1992, "The Disaster Recovery Planning Process", *Disaster Recovery Journal*, Volume 5, No. 1, pp.29-34, No 2., pp.32-34, No. 3, pp.36-38