6

RISK MANAGEMENT

Background

6.1 Risk management is 'the systematic application of management policies, procedures and practices to the tasks of identifying, analysing, assessing, treating and monitoring risk'.[1] Risk management helps to mitigate against adverse events occurring. This includes taking action to avoid or reduce exposures to the costs or other effects of events occurring rather than reacting after an event has taken place. Risk management, if conducted effectively, will help to achieve more effective corporate performance. MAB/MIAC states that prudent risk management will give:

- a more rigorous basis for strategic planning as a result of a structured consideration of the key elements of risk;
- no costly surprises because agencies are identifying and managing undesirable risks;
- better outcomes in terms of program effectiveness and efficiency;
- greater openness and transparency in decision making and ongoing management processes; and
- a better preparedness for and facilitation of positive outcomes from subsequent internal/external review and audit processes.[2]

6.2 In recent times, risk management techniques are being applied in both the private and public sectors as a means of focusing on cost, quality and financial performance.

---

1 MAB/MIAC Report No.22, October 1996, p. 52.

2 MAB/MIAC Report No.22, October 1996, p. 12.

6.3 The Australian National Audit Office (ANAO) suggested that a greater focus on risk management 'will come with the advent of the move to electronic commerce and the greater use of the internet for business purposes.'[3]

6.4 Ultimately, risk management is the responsibility of the GBE board. It is the role of the board to ensure that appropriate risk management processes and plans are in place throughout the entity to identify and manage risk. This includes setting acceptable levels of risk.

6.5 The Commonwealth faces a range of risks associated with the operations of GBEs, including financial, operational, political and reputational risks. GBEs are increasingly operating in more open markets and are therefore exposed to higher degrees of business risk.

6.6 The Commonwealth, as the major shareholder of GBEs, is particularly sensitive to business risk due to the operations of GBEs being either explicitly or implicitly guaranteed by the Commonwealth.[4] As a result, the governance arrangements have allowed shareholders to 'set limits on activities of GBEs in some circumstances'.[5] The governance arrangements require GBEs to 'provide details of their risk management framework in their corporate plans'[6] in addition to informing their shareholder minister(s).

6.7 The audit committee of a GBE plays an important role in risk management. The directors of GBEs are required 'to establish an audit Committee to monitor compliance with the CAC Act requirements' as well as providing a 'forum for communication'.[7] It is important for the audit committee to liaise with the organisation's management, the internal and external auditor, as well as to report to the board and disclose appropriate information to the board and the responsible minister(s).[8] The internal audit process and external risk reviews are recent innovative processes that have been recognised by some GBEs as effective tools for risk management.

---

3 Australian National Audit Office, Corporate Presentation to the Defence Audit and Program Evaluation Committee, Canberra, 28 July 1998.

4 The Auditor–General Audit Report No. 2, 97-98, *Government Business Enterprise Monitoring Practices*, p. 42.

5 Department of Finance and Administration, *Submission*, p. S5.

6 Humphry, R., *Review of GBE Governance Arrangements*, p. 53.

7 Australian National Audit Office, Principles and Better Practices, *Corporate Governance in Commonwealth Authorities and Companies, Discussion Paper*, 1999, p. 26.

8 Australian National Audit Office, Principles and Better Practices, *Corporate Governance in Commonwealth Authorities and Companies, Discussion Paper*, 1999, p. 26.

Current Arrangements

6.8 Part 4.9 of the 1997 Governance Arrangements discusses guiding principles for managing risk. It states:

- directors should establish processes and practices within the GBE to manage all risks associated with the GBE's operations;
- directors should keep the Shareholder Ministers informed of risk management strategies by outlining them in corporate plans and progress reports, and other reports where necessary;
- in addition, corporate plans and progress reports should contain a statement from the Board which states that the Board has appropriate risk management policies and practices in place and that adequate systems and expertise are being applied to achieve compliance with those policies and procedures;
- as a result of the Government, as shareholder, being sensitive to commercial risk, the following limits may be set on the activities of particular GBEs, eg. on liabilities and / or financial exposures:
  - ⇒ in normal circumstances, a GBE should only use derivative financial instruments for the purpose of hedging exposures;
  - ⇒ shareholder Ministers may require the Board of a GBE to provide a risk management plan, the contents to be agreed on a case-by-case basis;
- as a general rule the Government will not provide formal guarantees of GBE liabilities:
  - ⇒ guarantees provided in the past continue to apply to existing borrowings until they mature, in order to protect the interests of investors;
  - ⇒ the enabling legislation of public financial enterprises currently provide for statutory guarantees of most of the obligations of those enterprises.[9]

6.9 The Department of Finance and Administration (DoFA) is responsible for assessing the risk management strategies of all GBEs. If, at any stage, DoFA has concerns with any risk management strategies, they 'go back and raise them with the GBEs.'[10]

---

9 *Governance Arrangements for Commonwealth Government Business Enterprises, June 1997.*

10 Ms Megan Coombs, Department of Finance and Administration, *Transcript*, p. 92.

6.10 Throughout the inquiry, witnesses were asked to address key components of their agencies' risk management framework and strategies. This included outlining the structure of the board, the role of the audit committee and the benefits of external risk reviews.

6.11 In addition to addressing the above key components of risk management, Medibank Private and Employment National (EN) informed the Committee that they conduct risk management training and education strategies for their employees. EN stated:

> There is an education and training strategy that goes down through the organisation to ensure that people are attuned and aware. We have 215 sites, and individuals within those sites need to be very much aware of the profile risk that the company works within.[11]

6.12 The Department of Communications, Information Technology and the Arts (DoCITA) recognised that risk management strategies were important and discussed the issues with their GBEs. They now ask their GBEs to indicate their approaches to risk management in their corporate plans.[12] DoCITA also holds regular briefings with their GBEs in which issues of risk analysis and management often feature.

6.13 The Committee received submissions from a range of GBEs and Commonwealth government departments who shared the view that the present corporate governance arrangements were satisfactory in terms of risk management.

- Telstra submitted that 'the present arrangements for management of risk provide a proper and adequate safeguard'.[13]
- Defence Housing Authority stated that 'There are no areas of risk management governance which, in our view, need to be strengthened through additional requirements'.[14]
- Sydney Airports Corporation Limited (SACL) considered that 'the current risk management governance arrangements are satisfactory'.[15]
- The Department of Health and Aged Care stated that 'Risk management principles as outlined in the governance arrangements

11 Mr Rodney Halstead, Employment National, *Transcript*, p. 19.

12 Mr John Neil, Department of Communication, Information Technology and the Arts, *Transcript*, p. 80.

13 Telstra, *Submission*, p. S84.

14 Defence Housing Authority, *Submission*, p S120.

15 Sydney Airports Corporation Limited, *Submission*, p. S19.

are appropriate and maintain a balance between board autonomy and Government control'.[16]

6.14 Overall, DoFA was 'generally happy' that the GBE risk management strategies in place were effective.[17] From their point of view, the process of the board reporting to shareholder Ministers on key risks and management strategies were operating well.

Audit Committees

6.15 Audit committees have a key role to play in risk management. They are established in order to 'improve management reporting by oversighting audit functions, internal controls and the financial reporting process'.[18] Chapter Two of the ANAO's Better Practice Guide, *Corporate Governance in Commonwealth Authorities and Companies*, noted that an audit committee 'is usually constituted as a sub-committee of the Board'.[19]

6.16 Section 32 and 44[20] of the CAC Act require directors of Commonwealth authorities and wholly owned Commonwealth companies to establish an audit committee with functions that include:

- helping the authority/company and its directors to comply with obligations under the CAC Act and (for companies) the Corporations law; and
- providing a forum for communication between the directors, the senior managers of the authority/company and the internal and external auditors of the authority/company.[21]

6.17 The ANAO, in its Better Practise Guide, proposed that an audit committee should have a charter that is approved by the board. The ANAO proposed that the audit committee charter should include a 'suitable risk management and internal control framework.'[22] In addition, the ANAO

16 Department of Health and Aged Care, *Submission*, p. S110.

17 Ms Megan Coombs, Department of Finance and Administration, *Transcript*, p. 92.

18 Australian National Audit Office, Principles and Better Practices, *Corporate Governance in Commonwealth Authorities and Companies, Discussion Paper*, 1999, p. 12.

19 Australian National Audit Office, Principles and Better Practices, *Corporate Governance in Commonwealth Authorities and Companies, Discussion Paper*, 1999, p. 12.

20 Section 32 refers to Commonwealth Authorities and section 44 refers to Commonwealth Companies.

21 *Commonwealth Authorities and Company Act 1997.*

22 Australian National Audit Office, Principles and Better Practices, *Corporate Governance in Commonwealth Authorities and Companies, Discussion Paper*, 1999, p. 27.

suggested that audit committees 'should approve and monitor policies for reporting, risk management and internal control.'[23]

6.18 The ANAO commented that when audit committees are properly structured and given a clear mandate they can 'provide considerable benefit to organisations'.[24] However, a 'one size fits all' model does not exist for audit committees. The function of the committee will 'depend on the particular circumstances of each organisation, including its size, complexity and nature of operations'.[25]

6.19 In its Better Practise Guide the ANAO suggested that the audit committee 'should have unlimited access to both internal and external auditors and to senior management and all employees'.[26] The Australian Society of Certified Practising Accountants also supported this notion and commented that 'audit committees should work in partnership with both the external and internal auditors'.[27]

6.20 During the inquiry, Telstra discussed the benefits of incorporating risk management functions into the role of internal audit. They informed the Committee that their internal auditors assess 'the risks inherent in all the various lines of business within Telstra and assists those business units in developing risk mitigation strategies'.[28]

6.21 Australia Post informed the Committee that they have recently recruited a new chief internal auditor with a particularly strong background in risk management. They commented that the audit area had significant responsibility for carrying out risk management within the business, however, it was 'not itself responsible for risk management'.[29]

6.22 Medibank Private discussed the way in which the 'internal audit area drove the initial roll out of risk management and the philosophy of risk management across the organisation'. [30] Medibank Private has also recently built into their strategic internal audit plan a review of risk

23 Australian National Audit Office, Principles and Better Practices, *Corporate Governance in Commonwealth Authorities and Companies, Discussion Paper*, 1999, p. 27.

24 Australian National Audit Office, Principles and Better Practices, *Corporate Governance in Commonwealth Authorities and Companies, Discussion Paper*, 1999, p. 12.

25 Australian National Audit Office, Principles and Better Practices, *Corporate Governance in Commonwealth Authorities and Companies, Discussion Paper*, 1999, p. 12.

26 Australian National Audit Office, Principles and Better Practices, *Corporate Governance in Commonwealth Authorities and Companies, Discussion Paper*, 1999, p. 27.

27 Australian Society of Certified Practising Accountants and the Institute of Chartered Accountants in Australia, *Submission,* p. S94.

28 Mr John Stanhope, Telstra, *Transcript,* p. 101.

29 Mr Gerry Ryan, Australia Post, *Transcript,* p. 123.

30 Mr Michael Wheelan, Medibank Private, *Transcript,* p. 58.

assessment.[31] Their risk management framework requires them to 'integrate risk management and risk identification components into all operational strategies'. [32]

6.23 SACL has established four sub committees to deal with safety, security, environment and health matters. SACL informed the Committee that they also have an 'audit committee that has a wider ambit than just audit'.[33] SACL indicated, in evidence to the Committee, that its audit committee was holding discussions with the internal auditors to formalise the actual structure of how risk is addressed.

6.24 Snowy Mountains Hydro Electric Authority (SMHEA), is a Statutory Authority, and their risk management issues are now being dealt with through the Authority's Audit Committee.[34]

6.25 Similarly, the Australian Government Solicitor, a Commonwealth Authority, has adopted an audit committee (in accordance with section 32 of the CAC Act) which serves an important risk management function.[35]

External Risk Review

6.26 An external risk review requires an independent person to assess the risk management strategies of the organisation. The ANAO reported that appropriate risk management systems and processes may include the organisation 'submitting itself to periodic external and internal risk reviews'.[36]

6.27 The Committee found that external risk reviews were not commonly commissioned by GBEs. However, Australia Post and Medibank Private, were two GBEs who did conduct external risk reviews.

6.28 Australia Post annually reviews the effectiveness of the corporation's risk management policies and procedures as well as periodically commissioning an external risk review.[37]

---

31 Mr Michael Wheelan, Medibank Private, *Transcript*, p. 59.

32 Mr Michael Wheelan, Medibank Private, *Transcript*, p. 58.

33 Ms Caroline Archer, Sydney Airports Corporation Limited, *Transcript*, p. 7.

34 Snowy Mountains Hydro Electric Authority, *Submission*, p. S3.

35 Australian Government Solicitor, *Submission*, p. S91

36 Australian National Audit Office, Principles and Better Practices, *Corporate Governance in Commonwealth Authorities and Companies, Discussion Paper*, 1999, p. 16.

37 Australia Post, *Submission*, p. S161.

6.29 The external review includes a thorough review of the whole corporation of all the risks, where they are itemised, contextualised, given a ranking as to how they were managed and then reported directly to the board.[38] Australia Post stated that the 'board has found that it gives a great deal of assurance about the integrity and the thoroughness of the whole risk management area within the corporation'.[39]

6.30 Medibank Private informed the Committee that the ANAO, who are responsible for the external audit activity for Medibank Private, contracted the service out to Arthur Anderson. As part of the audit, an independent review of risk assessment was carried out. This process involved validating the risks that were identified by Medibank Private and reviewing the risk management process.[40] This provided management and the audit committee with some 'considerable comfort as to the quality and substance of those arrangements'.[41]

6.31 A number of GBEs raised concerns about being required to conduct external risk reviews. They commented that governance arrangements relating to GBE risk management should be no greater than the requirements in the private sector. For example, SMHEA emphasised that an appropriate balance must be struck between the requirements imposed on public sector organisations where competition exists between two sectors. They stated that 'Risk management requirements imposed on the public sector should not operate to the detriment of those bodies, particularly in circumstance where competitive neutrality vis a vis similar private sector bodies is concerned'.[42]

38 Mr Michael McCloskey, Australia Post, *Transcript*, p. 124.
39 Mr Michael McCloskey, Australia Post, *Transcript*, p. 124.
40 Mr Michael Whelan, Medibank Private, *Transcript*, p. 58.
41 Mr Michael Whelan, Medibank Private, *Transcript*, p. 58.
42 Snowy Mountains Hydro Electric Authority, *Submission*, p. S3.

Conclusions

6.32 The Government is exposed to many risks through its ownership of GBEs, including financial, operational, political and reputational risks. Therefore, the Government considers it is essential to ensure that the risk management strategies of all Commonwealth GBEs are operating effectively. The board of a GBE is wholly responsible for identifying, monitoring and controlling all risk that may affect the operations of a GBE.

6.33 Risk management issues were discussed during the inquiry. GBEs and government departments demonstrated to the Committee that risk management, as part of the governance arrangements are, at present, operating satisfactorily and effectively. The Committee was pleased to note that all GBEs, who appeared at the inquiry, recognised the importance of risk management.

6.34 Audit committees are playing an increasingly important role in corporate governance, and more specifically, in the area of risk management. The Committee notes that Telstra's internal audit function is conducting a risk management assessment function. The Australian National Audit Office, in its better practice guide, proposed that audit committees should have a role in risk management including approving and monitoring policies for reporting risk management and internal control.

6.35 The 1997 Governance Arrangements devote a section to managing risks although there is no mention of the role of audit committees in this process. The Committee, therefore, recommends that the risk management responsibilities of audit committees be included in the Governance Arrangements for Commonwealth GBEs, under Part 4, *Managing Risk*.

6.36 The Committee lastly touched upon the merits of external risk reviews. Such reviews involve an independent assessment of the organisation’s risks. Australia Post and Medibank Private discussed the benefits of carrying out periodic external risk reviews. Both GBEs informed the Committee that an external risk review provided their management with assurance that they had suitable risk management strategies in place. Other GBEs, however, expressed concerns regarding external risk reviews. They did not wish external risk reviews to become part of the governance arrangements as they believed it would be an additional requirement that the private sector did not have to adhere to. The Committee acknowledges the advantages of external risk reviews, however, it does not consider they should be obligatory for all Commonwealth GBEs.

Recommendation 7

6.37 **That the Minister for Finance and Administration amend Part 4, *Managing Risks,* of the 1997 *Governance Arrangements for Commonwealth GBEs* to include requirements setting out the risk management responsibilities of audit committees.**

Bob Charles, MP
Chairman
8 December 1999