1

Introduction to Performance Strategy

Introduction to Performance Strategy

1

Learning Outcomes

After completing this chapter you should be able to:

- Understand the inter-relationship between the elements of the *Performance Strategy* syllabus.
- Have a broad appreciation of risk management, governance, internal control and audit.
- Understand how financial risks (e.g. interest and foreign exchange risk) and non-financial risks (e.g. information systems) are particular examples of risk management, governance and internal control, that are emphasised in the *Performance Strategy* Syllabus.

1.1 Introduction

Two key issues underpin P3 *Performance Strategy*:

1. What risks does an organisation face?
2. How can those risks be managed and controlled?

The main purpose of this chapter is to help candidates see *Performance Strategy* as an integrated subject. Whilst the syllabus (see *The CIMA Learning System* that precedes Chapter 1) has five separate elements, each with its own learning outcomes and syllabus content, to understand *Performance Strategy* properly is to see all the elements of the syllabus as inter-related.

1.2 Risk management in 2009

This chapter is being written early in 2009 as the effects of the global financial crisis affect most organisations and individuals. Share markets have suffered major falls, the value of pension funds has fallen as a result. There is little confidence in the regulators of financial markets, or in the large investment banks (some of which have failed) or in credit rating

agencies. Huge companies like General Motors and Chrysler have asked for funds from the US government to keep them afloat. Individuals are concerned about the falling values of their homes, whether they will keep their jobs and many economies have fallen into recession. Commentators argue that this is the most serious financial crisis to face the world since the Great Depression that commenced in 1929 and continued well into the 1930s.

1.2.1 Case study: Global financial crisis

The global financial crisis commenced in 2007 and continued into 2008 as a result of falling US house prices and defaults on 'sub-prime' mortgages. The sub-prime market supported loans to those with poor credit histories. These loans enabled US homeowners to borrow up to the full value of their homes, with low initial repayments. However, homeowners were unable to refinance when interest rates increased and the fall in US housing prices led to many homeowners being unwilling or unable to repay their mortgages. In the US, the structure of these loans was that owners could walk away, return their keys to their lender, and avoid responsibility or repay their debts (a practice which is impossible in the UK and most other countries). The subsequent sale of houses at a loss led to further falls in the housing market.

The impact on global financial markets has been to a large extent a result of the securitisation of debts like these. Securitisation involves the pooling of debts, making them available to a wider range of investors, which in turn provides more money for lending. The resulting security often received a higher credit rating, and attracted a lower rate of interest. The portfolios of many financial institutions contained investments with assets derived from bundled home mortgages which had received overly favourable credit ratings. A congressional committee in the US has claimed that credit rating agencies were fully aware that their conflicts of interest were giving unduly high scores to risky assets, threatening the stability of the entire financial system.

Part of the securitisation package was the creation of derivatives known as Credit Default Swaps (or CDS). A CDS is like an insurance policy, under which a buyer makes a payment (a kind of premium) to a seller, and receives an amount of money if there is a default in the underlying debt repayment. Many commentators have argued that the financial system was vulnerable because of the use of these derivatives. There has been criticism of the US Treasury, Federal Reserve, and the SEC for being opposed to increasing regulation of derivatives trading.

Derivatives are very powerful methods of risk management (Chapters 11–14 of the Learning System covers financial risks like these in detail) but can be misunderstood and misused. In an interview with the BBC in 2003, Warren Buffett, one of the world's most astute – and successful – investors, said that "the rapidly growing trade in derivatives poses a 'mega-catastrophic risk' for the economy … such highly complex financial instruments are time bombs and 'financial weapons of mass destruction' that could harm not only their buyers and sellers, but the whole economic system."[1]

The effects of the sub-prime crisis were subsequently felt throughout the world in terms of reduced credit availability and higher interest rates. In response, governments and central banks announced interest rate cuts, capital injections, and lending guarantees to restore liquidity.

---

[1] http://news.bbc.co.uk/2/hi/business/2817995.stm

In September 2007, Northern Rock plc experienced a bank run by its customers with the UK government providing 'lender of last resort' funding and guarantees for the bank's depositors. In 2008, Northern Rock was nationalised by the UK government.

Bear Stearns, one of the largest US brokers and investment banks collapsed and was subsequently sold to J P Morgan Chase. The US Government intervened by imposing a 'conservatorship' to protect mortgage giants Fannie Mae and Freddie Mac from insolvency. Lehman Brothers filed for bankruptcy after the Federal Reserve Bank refused to provide it with financial support and J P Morgan subsequently took over part of their business. Similarly, Merrill Lynch was sold to Bank of America. American Insurance Group (AIG) also suffered a liquidity crisis and had to be supported by the US Federal Reserve. Washington Mutual Bank, the sixth largest bank in the US closed and went into receivership, making it the largest bank failure in US history.

In Europe, Fortis was broken up and Hypo Real, Germany's second largest mortgage lender, was bailed out by the government. In the UK, Bradford and Bingley also had to be nationalised.

Even whole countries were affected. Iceland was especially affected due to its banks' debts being six times that country's gross domestic product. Iceland's three largest commercial banks were taken over by the Icelandic government to avoid their collapse. Interest rates were increased to 18% under the terms of a loan provided by the International Monetary Fund. The result has been a serious impact on the country's economy with sharp falls in the value of its currency and the suspension of its foreign currency exchange market. The Icelandic stock exchange has fallen in value by over 75%.

Stock markets around the world have fallen, as the global economy faces recession and unemployment in what many commentators have called the most serious financial crisis since the Great Depression. The US government passed the Emergency Economic Stabilisation Act and many European central banks injected capital into their banking systems. The Troubled Asset Relief Program (TARP) enabled the US government to purchase what have become known as 'toxic assets' from financial institutions. In November 2008, TARP was scrapped with funds being reallocated to help relieve pressure on consumer credit, including car and student loans, and credit cards. At the time of writing there are major concerns for the car industry, especially General Motors, Ford and Chrysler in the US who have called on the US government for assistance.

1.3 The emergence of risk, governance and control

Risk management has evolved from various separate functional areas: occupational health and safety; insurance; the hedging of financial risks (foreign exchange and interest rates); credit risk; and project management. The first two were largely the focus of risk managers in organisations, whilst the third and fourth were the province of financial and treasury managers, the fifth being the responsibility of operational managers. Risk management also had links with quality management and the international standard ISO9000.

There have been two major developments in risk management as it affects accountants:

1. Sarbanes-Oxley legislation
2. The Basel Committee on Banking Supervision

The introduction of the US Sarbanes-Oxley (SOX) Act in 2002 was the legislative response in the US to the financial and accounting scandals of Enron and WorldCom and the misconduct at the accounting firm Arthur Andersen. Its main aim was to deal with issues of transparency, integrity and oversight of financial markets. SOX as it is called requires the certification of annual and quarterly financial reports by the chief executive and chief financial officer of all companies with US securities registrations, with criminal penalties for knowingly making false certifications. SOX is criticised for having increased corporate costs as a result of the greater emphasis on internal controls and the audit of financial reporting.

The notion of risk in relation to financial derivatives in the banking industry was first formulated by the Basel Committee on Banking Supervision (1994). For banks and regulated financial institutions, the Basel Committee has had an important impact, particularly as it affects risk and internal control. Part of the Bank for International Settlements, the objectives of the Basel Committee include enhancing the understanding of key supervisory issues and improving the quality of banking supervision worldwide. Basel II is the second group of Accords from the Basel Committee. It contains international standards for banking laws and regulations aimed at helping to protect the international financial system from the results of the collapse of a major bank or a series of banks. Basel II established rigorous risk and capital management requirements to ensure each bank holds reserves sufficient to guard against its risk exposure given its lending and investment practices.

Risk came to be seen on a much wider basis through the publication of books such as *Risk Society* (Beck, 1986, 1992 in translation); *Risk* (Adams, 1995) and *Against the Gods* (Bernstein, 1998). These books highlighted the social and cultural aspects of risk management.

In the UK, high profile corporate failures led to a series of reports, beginning with that by Sir Adrian Cadbury on corporate governance (Cadbury Code, 1992) and culminating in the Combined Code on Corporate Governance (Financial Reporting Council, 2003). In Australia, the first risk management standard was produced in 1999 as AS4360.

In the US the Treadway Commission produced *Internal Control – Integrated Framework* (Commitee of Sponsoring Organizations of the Treadway Commission (COSO), 1992) but the critical legislation impacting organisations, particularly in relation to risks associated with financial reporting, followed the scandals of Enron and WorldCom and the enactment of the Sarbanes-Oxley Act (SOX) in 2002. Chapter 4 describes the background of corporate governance in detail.

The relationship between risk and reward, with risk coming to be seen both in terms of upside and downside is now well established (International Federation of Accountants, 1999). As risk management became more widespread and took on the mantle of enterprise risk management (Commitee of Sponsoring Organizations of the Treadway Commission (COSO), 2003; see Chapter 5), the role of internal audit, previously an essentially accounting role became transformed into a broader risk-based audit, with the Institute of Internal Auditors becoming the predominant body, rather than the accounting profession. Risk-based approaches have also been adopted by external auditors, particularly those subject to SOX. Chapter 7 describes the internal audit in detail.

Management controls have always existed, in order to control the behaviour of employees with the purpose of ensuring that organisational objectives are achieved. Many of these controls were accounting controls, such as budgets, standard costs, variance analysis, etc. (discussed in detail in Chapter 3). As organisations became more sophisticated, non-financial controls were added. These controls included targets such as quality, waste, delivery lead time, customer satisfaction, etc. When other controls, such as those in respect of personnel, information systems, corporate policies, working practices, etc. are added, the

result is a system of management control, although often the components of the 'system' lead to different behaviours. Chapter 6 describes internal control in detail.

Good governance (e.g. Financial Reporting Council, 2003) requires that boards of directors review the effectiveness of internal controls in response to the risks facing the organisation. The risk-based approach to control, as for audit, should lead to the development of controls that are a response to risks, rather than being developed incrementally over time (International Federation of Accountants, 2006) often for political purposes unrelated to risk.

Standards for risk management are now international, and remarkably consistent in their focus (Commitee of Sponsoring Organizations of the Treadway Commission (COSO), 2004; Institute of Risk Management, 2002; Standards Australia, 2004). As Michael Power explains in his recent book *Organized Uncertainty* (Power, 2007), risk has become very important in the language of managers and a major element of accountability.

The relevance of risk to accountants has been reflected in CIMAs *Performance Strategy* syllabus. *Performance Strategy* is a strategic level subject that brings together enterprise risk management, governance, internal control and audit in relation to both financial and non-financial risks. The title 'Performance Strategy' is important, because the syllabus is not just concerned with what things might go wrong – so-called downside risks but also with the risk of not achieving the organisational strategy and goals, that is, the risk of not achieving the desired level of performance. Governance, internal control and audit should therefore be directed at achieving performance goals through using risk management as an important tool.

1.4 What is corporate governance?

Corporate governance is the system by which companies are directed and controlled. Boards of directors are responsible to their shareholders and have a stewardship function for the governance of the company. The responsibilities of Boards include setting the company's strategic goals, providing the leadership to put those goals into effect, supervising the management of the business and reporting to shareholders. This role involves the management of risk and the review of the effectiveness of internal control. Corporate governance is covered in Chapter 4.

CIMA has produced a model of enterprise governance (Chartered Institute of Management Accountants and International Federation of Accountants, 2004) that emphasises the importance of the two dimensions of conformance and performance. Conformance is about satisfying good governance, whilst performance focuses on strategy to improve shareholder value.

1.5 What is risk management?

Risk management is the process of understanding and managing risks that the organisation faces in attempting to achieve its objectives. Perhaps the best definition of risk management is that in relation to enterprise risk management (or ERM, discussed in Chapter 5). ERM aligns risk management with business strategy and embeds a risk management culture into the business. It encompasses the whole organisation and sees risks as opportunities as much as hazards.

In managing risk, organisations should follow a well-established process, although the level of detail they go into may vary quite significantly. While there are different models

for risk management (discussed in detail in Chapter 5), the following 7 step process contains the essential ingredients:

1. *Identify the risk*: Risks are an everyday part of life, so organisations need a system to identify all the risks they face. This involves collecting information from a variety of sources: individuals, reports, observation and environmental assessments. Common methods of collecting data that identify risks include workshops, scenarios, brainstorming, surveys, etc. These may be linked with consultations with stakeholders, environmental analyses, strategic plans, etc.
2. *Assess the risk impact*: Once risks have been identified, some assessment needs to be made of their likely impact. This involves quantifying the risk in some way. We might carry out market surveys, computer simulations, cost–benefit analyses, use a Delphi technique or apply probabilities, statistical tests or sensitivity analysis. Alternatively, we may rely on subjective judgements.
3. *Risk mapping*: This involves prioritising the most critical risks by mapping the likelihood (or probability) of the risk eventuating against its consequences (or impact) if it does eventuate. Organisations may use a simple high–medium–low scale for both likelihood and consequences or map risks against a more complex scale. Whichever method is used, prioritisation is important because organisations will typically face hundreds or even thousands of risks, and only the most significant ones can be managed.
4. *Record risks in a risk register*: The risk register contains a listing of risks that have been identified, together with the likelihood and consequence of the risk occurring. This is a comprehensive register that ensures that risks are continually evaluated and managed, with most emphasis given to the greatest risks.
5. *Risk evaluation*: Risks are evaluated against the organisation's appetite for risk. This appetite is a balance between risk and return and must ultimately be a judgement that is made by the board of directors. This is really a question of setting the parameters for whether particular risks should be accepted, rejected or managed in some way.
6. *Risk treatment*: Also called risk response, this involves decisions as to whether particular risks should be avoided, reduced, transferred or accepted. Avoidance involves exiting from high risk activities. Risk reduction involves mitigating either the likelihood or impact of risks by introducing various internal control mechanisms. Sharing or transferring risk can take place through methods such as outsourcing, insurance or hedging while the acceptance of risk implies that no action is necessary in relation to risks evaluated as low.
7. *Risk reporting*: Risk reporting will explain the method of risk management, how risks are identified and assessed. The highest risks (in terms of likelihood and consequences) will be reported rather than all those in the risk register and the risk response will be identified for each. Risk reports should show both the gross risk (before controls are introduced) and the net risk (after the effect of controls is taken into account) to demonstrate the cost effectiveness of those controls.

1.6 What is internal control?

Internal control is the whole system of financial and other controls established to provide reasonable assurance of effective and efficient operation; internal financial control and compliance with regulation. An internal control system comprises five elements: a control environment, risk assessment, control activities, monitoring, and information and communication.

The control environment is the attitude and awareness of the Board and managers regarding the importance of internal controls and comprises culture and values – the background against which specific controls are introduced. Risk assessment was described in Section 1.5 above. Control activities are the policies and procedures that help ensure that objectives are achieved. Importantly, these controls are not just accounting controls but include quantitative (but non-financial) controls as well as qualitative (i.e. non-numeric) controls (see the discussion of management controls in Section 1.3 above). Monitoring continually evaluates the whole control system. Reviewing the effectiveness of internal control is one of the Board's responsibilities. Information and communication includes the need to capture relevant information about the organisation's environment and to communicate this information within the organisation. Internal control is covered in Chapter 6.

1.7 What is audit?

Audit is a systematic examination of the activities and status of an organisation based primarily on investigation and analysis of its systems, controls and records. The main types of audit are the external audit, the primary function of which is to form an opinion on the truth and fairness of financial statements; and the internal audit, the role of which is to examine and evaluate, add value and improve the operations of the organisation. It does so by helping an organisation achieve its objectives by improving the effectiveness of risk management, control and governance processes.

The audit committee is a committee of the board of directors, the primary function of which is to review the system of internal control, the external audit process, the work of internal audit and the financial information provided to shareholders. The role of audit is covered in Chapter 7 whilst the audit committee is covered in Chapter 4.

1.8 A model of governance, risk and control

It is important to understand the links between governance, risk management and internal control and the interaction between the board of directors, the audit committee, external and internal auditors, as this is the foundation of the *Performance Strategy* syllabus. This relationship is shown in Figure 1.1.

The Reading to Chapter 7 provides a case study of ABC, an example of these relationships.

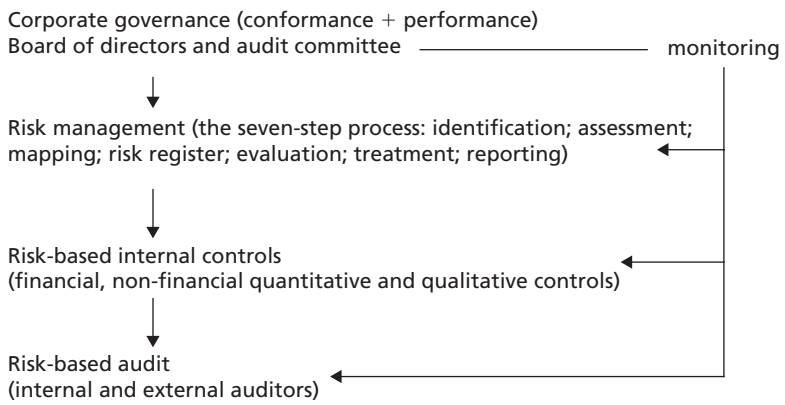

Figure 1.1 A model of governance, risk and control

1.9 Fraud, information systems and financial risk

The preceding discussion does not differentiate between different types of risk. However, the *Performance Strategy* syllabus addresses three specific risks: fraud (Chapter 10); information systems (Chapters 8 and 9) and financial derivatives (interest and exchange rate risks, covered in Chapters 11–14). Information systems risk comprises 15% of the syllabus and financial risk 35%. It is important therefore, to understand not only the general principles of governance, risk and control in Chapters 1–7 but also the specific risks covered in Chapters 8–14. Importantly, all the general principles apply to the specific risks, as well as to all other risks that are not identified in the syllabus. These unspecified risks therefore represent about 50% of the syllabus. It should also be remembered that many organisations will face general risks as well as specific information systems and financial risks. In interpreting Figure 1.1 therefore, it is important to remember that risks may be general, information systems or financial.

1.10 Summary

- The links between governance, risk management and internal control and the interaction between the board of directors, the audit committee, external and internal auditors is the foundation of the *Performance Strategy* syllabus.
- Corporate governance is the system by which companies are directed and controlled.
- Risk management is the process of understanding and managing risks that the organisation faces in attempting to achieve its objectives. Enterprise Risk Management aligns risk management with business strategy and embeds a risk management culture into the business, seeing risks as opportunities as much as hazards.
- Internal control is the whole system of financial and other controls established to provide reasonable assurance of effective and efficient operation; internal financial control and compliance with regulation. It comprises five elements: a control environment, risk assessment, control activities, monitoring, and information and communication.
- Audit is a systematic examination of the activities and status of an organisation based primarily on investigation and analysis of its systems, controls and records. The role of internal audit is to examine and evaluate, add value and improve the operations of the organisation, by helping an organisation achieve its objectives by improving the effectiveness of risk management, control and governance processes.
- The audit committee is a committee of the board of directors, the primary function of which is to review the system of internal control, the external audit process, the work of internal audit and the financial information provided to shareholders.
- The *Performance Strategy* syllabus addresses three specific risks: fraud, information systems and financial derivatives (interest and exchange rate risks). Information systems risk comprises 15% of the syllabus and financial risk 35%. Unspecified risks represent the balance of about 50% of the syllabus. Many organisations will face general risks as well as specific information systems and financial risks.

References

Adams, J. (1995), *Risk*. London: UCL Press.

Basel Committee on Banking Supervision (1994), *Risk Management Guidelines for Derivatives*. Basel: Bank for International Settlements.

Beck, U. (1986, 1992 in translation), *Risk Society*. London: Sage.

Bernstein, P.L. (1998), *Against the Gods: The Remarkable Story of Risk*. New York: John Wiley.

Cadbury Code (1992). Report of the Committee on the Financial Aspects of Corporate Governance: The Code of Best Practice, London: Professional Publishing.

Chartered Institute of Management Accountants and International Federation of Accountants (2004). Enterprise Governance: Getting the Balance Right. New York: CIMA/FIAC. http://www.ifac.org/MediaCenter/files/EnterpriseGovernace.pdf.

Committee of Sponsoring Organizations of the Treadway Commission (COSO) (1992). Internal Control – Integrated Framework. New York: COSO.

Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2003). Enterprise Risk Management Framework. New York: COSO.

Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2004). Enterprise Risk Management – Integrated Framework. New York: COSO.

Financial Reporting Council (2003). The Combined Code on Corporate Governance.

Institute of Risk Management (2002), *A Risk Management Standard*. London: IRM.

International Federation of Accountants (1999). Enhancing Shareholder Wealth by Better Managing Business Risk. *Rep. International Management Accounting Study No. 9.* New York: IFAC.

International Federation of Accountants (2006). Internal Controls – A Review of Current Developments, Professional Accountants in Business Committee, New York.

Power, M. (2007), *Organized Uncertainty: Designing a World of Risk Management*. Oxford: Oxford University Press.

Standards Australia (2004). Australian and New Zealand Risk Management Standard AS/NZS 4360:2004, 3rd edition. Sydney: Standards Australia.