



## SMEs — the risk of failing to manage risk

By **James Field**, Director, CompliSpace Pty Ltd

- *The failure to effectively implement a risk management program presents an extreme risk for thousands of SMEs*
- *For those that don't comply there awaits a 'perfect storm' of regulators, litigation lawyers, class action lawyers and directors' and officers' insurers*
- *With commitment to the risk management process, and by following some basic steps, SMEs can find shelter from the storm whilst adding considerable value to their business*

The latest round of corporate collapses in Australia has highlighted some inherent weaknesses in the corporate governance systems of many of Australia's leading businesses. High on the casualty list are many of Australia's major corporate brand names such as MFS, Centro, ABC Learning Centres and Allco. While David Coe of Allco may blame the 'perfect storm'<sup>1</sup> risk professionals nod knowingly wondering how it is that such highly regulated businesses did not see the storm coming. After all, that is what the risk professionals are paid to do.

Those in the know are talking about a 'perfect storm' of a different kind. This perfect storm involves the coming together of an increasingly complex regulatory environment, an under-resourced small to medium enterprise (SME)<sup>2</sup> sector, litigation funders, class action lawyers, directors' and officers' (D&O) insurers, a burgeoning professional services industry, and a media pack that is becoming hungrier and more knowledgeable by the day.

This article examines the emergence of risk management as the governance tool of choice for Australia's regulators, the key challenges that SMEs face in implementing risk management systems effectively, the benefits of embracing technology

solutions to manage risk and finally the confronting reality that lies ahead for businesses that fail to manage their risks effectively.

### Emergence of risk management as the regulators' management tool of choice

Peter Bernstein in his 1996 book *Against the Gods: The Remarkable History of Risk*<sup>3</sup> traces the origins of modern concepts of risk back to the 13th and 14th centuries. It is a simple fact that we all practise risk management every day, both as private individuals and as business managers, whether it be insuring an asset or simply weighing future options against a set of events we believe may occur. So if we are all practising risk management, what's the fuss about?

To understand what all the fuss is about you need to understand the evolution of risk management within the corporate world and how expectations and obligations with respect to risk management have changed markedly over the past five to ten years.

The 'big end of town' has, for a long time, known the considerable benefits that can be gained from implementing risk management programs. While they initially focused on finance based risks and insurable hazards, over the years other sub-disciplines of risk began to be recognised, leading to the emergence, in the late 1990s, of what is now referred to as enterprise risk management (ERM). As the name suggests, ERM involves consideration of risk on an enterprise-wide level extending well beyond the traditional risk categories to encompass every facet of an organisation's operations from the board room to the shop floor.

With other management processes such as total quality management (TQM) and process re-engineering being written off as fads, experienced managers may well have had some justification for arguing that risk management generally, and ERM in particular, would meet a similar fate. Then a strange thing happened. Law makers and regulators started to create obligations for organisations to implement risk management programs.

Prior to the commencement of the *Financial*

**Table 1: Laws and regulations requiring organisations to implement risk management systems**

Key laws, regulations and guidance notes	Applies to:	Risk management obligations
<i>Financial Services Reform Act 2001</i> <i>Corporations Act 2001</i> , s 912A(1)(h) ASIC Regulatory Guide 104	All non-APRA regulated financial services licensees including financial planners, stockbrokers, fund managers and insurance brokers	ASIC expects licensees to have a structured and systematic process for identifying, evaluating and managing risks. For guidance, ASIC refers to AS/NZS 4360
Numerous pieces of legislation imposing obligations on specific industry groups	All APRA-regulated financial services licensees including authorised deposit taking institutions, general insurers, registerable superannuation trustees, life insurance companies and credit unions	APRA has developed specific risk management guidelines for regulated entities based on their industry types
ASX Listing Rule 3.10 ASX Corporate Governance Council Principles (2003 and 2007)	All ASX listed entities	ASX-listed entities must implement risk management programs or disclose why they have not done so in their annual reports. For guidance the ASX refers to AS/NZS 4360
<i>Anti-Money Laundering and Counter-terrorism Financial Act 2006</i>	The first tranche of this legislation covers approximately 19,000 entities including financial services providers and the gaming industry  The second tranche (due late 2008 or early 2009) is expected to extend the obligation to lawyers, accountants, jewelers and real estate agents	AUSTRAC expects regulated entities to have a structured and systematic process for identifying, evaluating and managing risks relating to money laundering and terrorist financing. For guidance AUSTRAC refers to AS/NZS 4360

*Services Reform Act 2001* on 11 March 2002, (with the exception of workplace safety laws, which require all employers to undertake workplace hazard risk assessments), the vast majority of SMEs in Australia did not have a positive legal obligation to implement a risk management program. Since 2002 there has been a virtual avalanche of laws, regulations and guidelines requiring organisations to implement a risk management systems requiring them to do so (see Table 1).

It is estimated that approximately 21,000<sup>4</sup> organisations are now either required to implement a risk management program or, in the case of ASX-listed entities, to provide reasons why they have not done so. The commencement of the second tranche of the AML/CTF Act is likely to see this number at least double. The end result is that by this time next year it is likely that over 40,000 organisations in Australia will have a legal obligation to implement a risk management program. The vast majority of these organisations will be SMEs.

Risk management has now become a major legal and regulatory compliance issue for tens of thousands of SMEs.

### Defining the risk management obligation

In simple terms, risk management is a business methodology that assists individuals to predict

future events which may affect their organisation's activities (either positively or negatively) and to use structured processes to take appropriate actions to address the impact of these events.

There are currently two major international standards for risk<sup>5</sup>, the Australian Risk Management Standard AS/NZS 4360 and COSO.<sup>6</sup> AS/NZS 4360 is referenced by various regulators including ASIC, AUSTRAC and the ASX<sup>7</sup> as the guideline to follow when implementing a risk management program.

What is significant from an SME perspective is that AS/NZS 4360 itself, together with the accompanying handbook, and the large volume of regulatory guidelines and commentaries that have been published over the past five years, leave little room for doubt as to what is expected of regulated entities when implementing a risk management program.

Those organisations following AS/NZS 4360 are required to follow the seven-step methodology set out in Figure 1. In very simple terms this involves:

- establishing a risk management framework through consultative processes
- identifying risk events
- analysing the likelihood of each risk event occurring and the potential consequences of the event should it occur
- establishing controls and treatment plans designed to manage or mitigate each risk and

- monitoring each control and treatment plan to ensure they are effective.

Each part of the process needs to be documented and failure to carry out any part of the process may result in an organisation being in breach of its legal & regulatory obligations.

**The SME compliance challenge**

Anyone who has ever been involved in the management of an SME will immediately recognise the compliance challenge. By their very nature SMEs do not have either the human or financial resources of larger organisations. Rarely do they have internal lawyers. Often they do not have resources dedicated to manage other key functional areas such as human resources or technology. As a result, time-poor general managers, finance officers and company secretaries are often forced to add risk management to their never-ending list of daily responsibilities.

Once they scratch the surface of risk management, they quickly realise that it is simply one component of their overall governance framework. Because risk management by its nature demands that an organisation analyses its internal inadequacies, if the other components of the governance framework are missing the SME quickly comes to the realisation that not only must it implement risk but it must also develop an internal control (compliance) framework, as well as a governance infrastructure which will allow it to effectively document its policies and procedures, train its staff and monitor its performance across a range of areas.

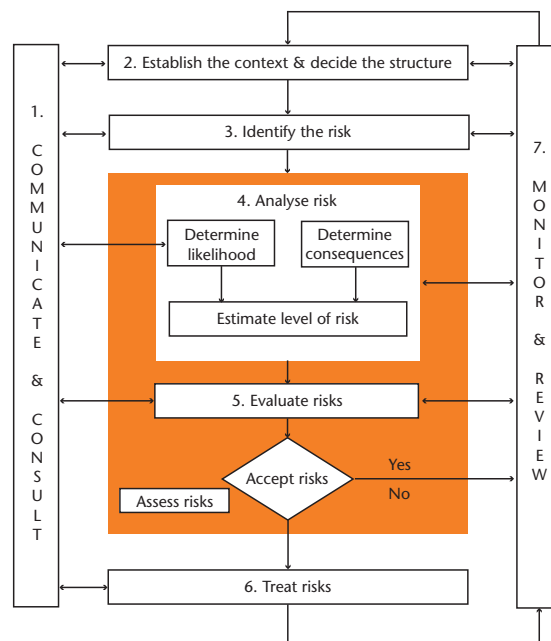
Rather than approaching the risk management process through consultation and communication

as recommended in Step 1 of AS/NZS 4360, many SMEs find themselves seeking a quick fix. This quick fix often comes in the form of asking an internal staff member to put together a risk 'document' with the hope that this document will at least show that they have tried to do the right thing. Sometimes the risk 'document' comes with a basic risk register. However rarely does the risk program extend to the point that controls and treatment plans have been established. Rarer still does the risk program extend to the point where these controls and treatment plans are being monitored to ensure their effectiveness.

There is a good reason for this. The risk management process does not come naturally to most people. It certainly was not taught at business school when the majority of today's managers were being educated. The concept of identifying individual risk events and analysing these in terms of likelihood and consequence is difficult for most people to follow and the process of monitoring all these controls and treatment plans requires an investment in people and infrastructure which most SMEs are not prepared to make without seeing a clear return on investment.

It is common to hear those empowered to implement risk programs talking about the frustrations they experience in gaining cultural acceptance for the process at board and senior manager level. Trade publications and conferences abound with stories of highly experienced managers and consultants struggling, often for years, with this very issue. Sadly without commitment at director and senior executive level any attempt to implement a risk program will be doomed from the outset.

**Figure 1: AS/NZS 4360 risk management standard**



The reality is that the majority of directors and senior managers of SMEs still do not understand what is expected of them when implementing a risk management program. Many simply see risk management as a compliance obligation and take a tick-box approach to implementation. Sadly not only will these organisations never experience the competitive advantages that they could achieve if they were to do the job properly, they are also leaving themselves wide open to regulatory intervention, fines, penalties and civil claims.

### Ten tips for developing a risk management program that works

The good news is that ERM is expected to be an \$US80 billion a year industry\* within a few years. With massive growth in the ERM market comes improved thinking as to how to satisfy the demand for simple solutions in the SME market and new technologies designed to deliver these solutions quickly, simply and within realistic budgets. For those struggling with the risk management concept the following tips have been drawn from over ten years of experience assisting SMEs develop practical governance solutions.

#### 1. Develop a compelling business case

In order for a risk management program to be successful, the board and senior management team must be committed to, and willing to resource, the process. The best way to obtain this commitment is to present a compelling business case that highlights the benefits of risk management in terms of return on investment, while simultaneously demonstrating both the legal and commercial consequences of failing to properly implement a risk program. SMEs are unlikely to properly implement a risk program unless there is a perceived commercial advantage in doing so.

#### 2. Embrace the ERM approach

For most SMEs there is little point in addressing one category of risk without addressing risks across the whole of their business. Embracing ERM allows all managers to understand the 'big picture' of key issues affecting their business and to create a structured and manageable continual improvement process. It is this continual improvement process that ultimately leads to the business obtaining significant commercial benefits and a return on its investment.

#### 3. Recognise the relationship between risk and compliance (internal control)

While a compliance program can live without a risk program, a risk program cannot succeed without an effective compliance system to back it up.

#### 4. Avoid paper-based policies and procedures

At the heart of any business are the policies and procedures that have been developed in order to

manage the business efficiently. These policies and procedures must be written in plain English and must be readily available for staff to reference as and when they are needed. Establishment of an intranet with an online content management system that streamlines the publication and maintenance of policies and procedures creates the platform for the implementation of an effective risk management program.

#### 5. Create a common risk language

The creation of a common risk language (or set of defined risk categories) is critical to aid the initial risk identification process and to ensure that there is an ongoing reference point for communications and reporting. An effective risk categorisation methodology should be broad enough to differentiate between key functional areas within an organisation and to capture key external stakeholders as well as external risk events such as changes in economic conditions and acts of nature.

#### 6. Develop a positive corporate culture

To manage risk effectively, an organisation needs to be able to openly recognise its strengths and weaknesses and undertake constructive debate around what may often be sensitive issues. To this end, directors and senior managers must work proactively to develop a corporate culture which encourages participation in the risk management process and transparency in its outcomes.

#### 7. Remember that ERM is not an exact science

Risk management is all about trying to predict the future. It is not an exact science. While it is important to clearly identify an organisation's risk appetite through its chosen risk matrix, and likelihood and consequence definitions, it is also important to recognise that we are dealing with human beings and there will always be a degree of variation in interpretation throughout the process. Recognising that risk management involves dealing with shades of grey, rather than black and white scenarios, will assist in creating positive outcomes.

#### 8. Recognise what you do well

One common mistake that occurs in implementing risk management programs is to focus on all the things that an organisation does badly. This inevitably gets a negative reaction from management, who are generally well aware of these shortcomings and already working towards developing appropriate solutions. Recognising the things that management does well helps break down any resistance to change (for example, the introduction of the risk management program). It also encourages management buy-in which ultimately will facilitate the acceptance of individual responsibilities and proactive participation in the process.

### 9. Embrace workflow technology

Even a relatively simple business will have 100 or so key risks. Given that each of these risks must have at least one control and given that many of these controls may need to be monitored monthly or quarterly, the task of managing risks, controls and treatments quickly becomes very difficult. The use of paper-based checklists is highly labour-intensive and rarely works well in practice. There are now many cost-effective technology solutions on the market designed to manage risk and compliance workflows and to provide streamlined reporting to management.

### 10. Remember that risk management is a journey

As with most things in life, the planning and initial set-up phase is crucial in determining the ultimate success of the project. Built on the right foundations and appropriately resourced and managed, a risk management program will deliver significant competitive advantages to those organisations that make the commitment to the process.

### Risk of not managing risk — the perfect storm?

Here is a warning to those organisations that have a legal obligation to implement a risk management program but are not willing to make the commitment to the process. There are storm clouds looming which involve the coming together of regulators, litigation funders, class action lawyers, D&O insurers, professional service providers and the media.

Recent market volatility has highlighted the inadequacies of corporate governance systems within many financial services and ASX-listed entities. Hardly a day goes by without another media headline putting the spotlight on those organisations (and directors and executives) that have failed to meet their obligations. Media focus increases pressure on politicians and on regulators to act to protect consumer interests.

It would appear however that for most organisations the regulators are not the major concern. As soon as a story breaks the litigation funders and class action lawyers move in, ready to pounce. The *Australian Financial Review*<sup>9</sup> recently reported that leading litigation fund IMF (Australia) Limited is banking on a claim of up to \$200 million for a successful class action against Centro with a further \$50 million from claims against MFS and Allco Finance. Aristocrat Leisure settled out of court in May 2008 for an undisclosed amount estimated to be \$130 million.

Unfortunately for SMEs, class actions are not confined to the big end of town. In November 2007, a class action was lodged against the former

executive chairman of Evans & Tate claiming just \$4 million. There are numerous other examples of claims around the \$5 million mark.

To make matters worse for those organisations that choose not to commit to implementing an effective risk management system, the Federal Court has recently announced its intention to overhaul its procedures for class actions to make them quicker and cheaper.

To highlight the trend it was recently reported that the Federal Court is planning to overhaul its procedures for class actions to make them quicker and cheaper.

D&O insurers have been quick to see the trend with recent reports that the D&O insurance market is rapidly tightening. It is now common within D&O applications that insurers require applicants to disclose whether or not they have a risk management system in place.

All this activity seems to be pointing in one direction. It is now becoming both a legal and a commercial imperative for regulated entities to ensure that their risk management programs are in place and working effectively. The danger for those that do not comply is that, if an adverse risk event occurs, they will be exposed to reputational damage as well as the threat of possible actions by regulators and class action lawyers.

*James Field can be contacted on (02) 9299 6105 or via email at [james.field@complispace.com.au](mailto:james.field@complispace.com.au).*

### Notes

- 1 *Australian Financial Review*, 4 March 2008, p 1
- 2 While there is no fixed definition for SME in Australia, the usual measure is by number of employees with 500 employees being a common upper limit. The author believes that SME is more appropriately defined by management's state of mind
- 3 P Bernstein (1996) *Against the Gods: The Remarkable History of Risk*, John Wiley and Sons
- 4 AUSTRAC refers to a figure of approximately 19,000 organisations that are required to comply with the AML/CTF Act. This figure includes the vast majority of AFSL holders. To this figure we can add approximately 2,000 ASX-listed entities that are not financial services licensees
- 5 A new international risk standard (AS 31000) is due to be published in 2009 and will replace AS/NZS 4360
- 6 Committee of Sponsoring Organizations of the Treadway Commission: see <<http://www.coso.org>> [18 June 2008]
- 7 The ASX refers to both AS/NZS 4360 and COSO for guidance with respect to the implementation of risk management and internal control systems
- 8 P Teuton (2005) 'Enterprise Risk Management and Where It Stands Today', *John Liner Review*, Fall 2005, Vol 19 No 3, pp 7-19
- 9 *Australian Financial Review*, 1 May 2008 ●