Risk Management Today

2011 . No 10

Contents

Risk Management Today

Is published monthly and is available in two formats: hardcopy and online. Feedback and suggestions regarding content is welcome and should be directed to the editor, **Kerrie Tarrant**, at kerrie.tarrant@lexisnexis.com.au.

Information contained in this newsletter is current as at May 2011

LexisNexis Butterworths

Getting risk management right to drive business success!

Richard Gossage *and* ***Tara Joyce*** *PRICEWATERHOUSECOOPERS*

If the global financial crisis (GFC) has taught us anything, it is that failing to manage the risks you take can lead to corporate and personal failure. But is this just the case in financial services? Is it only the nicely suited investment bankers who are the problem? History clearly shows that the answer is no! Ask any graduate who has studied business management and they will highlight a simple fact: over the last century, and specifically in the last 20 years, the root cause of the majority of corporate failures was a failure to manage risk.

Iconic examples of getting risk management wrong

The failure of General Motors (GM) is perhaps one of the most studied examples of an organisation getting risk management wrong. Failure to understand the consequences of fundamental changes in business models, new entrants to core markets, poor quality products, excessive production costs and poor union management were all contributors to the company's demise. This failure to understand and manage GM's changing risk profile over a sustained period of time led to one of the oldest and most respected icons in the United States becoming one of the world's largest corporate restructuring projects.

Not dissimilar to the demise of GM is the story of Kodak, a key player in the imaging, photographic and optical equipment/supplies industry, which showcases another significant example of getting risk management wrong. The consequences for Kodak were severe: a significant drop in sales and revenue, leading to its current struggle for survival and the loss of millions of dollars in brand and stock values. Key causal factors in the company's demise include a failure to understand changes to social and economic trends and customer behaviours, an inability to model the financial impacts of business model and product change, and a failure to align organisational culture with business strategy.

These are two well-publicised case studies, but there are many other examples across all industries.

What made the GFC so special is that the failure to manage risk was not limited to individual financial institutions, but was within the global financial system itself.

So, let's set down three basic principles from which we build our thinking.

1. Business management and risk management are two sides of the same coin.
2. Boards have ultimate responsibility for risk management, and this is delegated to the CEO to discharge.
3. Optimising enterprise value requires talking, holding and managing risk.

In this article, we build on these three fundamental risk management principles and explain how you can integrate the principles into your business management approach. The article concludes by reinforcing the benefits of implementing long-term risk management practices within your organisation.

How do business management and risk management interrelate?

The first step to the successful management of risk is to gain an understanding and appreciation of the interrelationship of business management and risk management.

A good definition of business management is:

> Business management is the operationalising of the business's strategy; the direction and scope of an organisation over the long-term which achieves advantage for the organisation through its configuration of resources within a challenging environment, to meet the needs of markets and to fulfil stakeholder expectations.[1]

Conversely, risk management is the systematic application of management policies, procedures and practices to the tasks of identifying, analysing, evaluating, mitigating and monitoring risk or uncertainty — risk being a potential event or scenario that is assessed as having a positive or negative impact on the achievement of an organisation's objectives.

So, how do these concepts interrelate? And why does this matter?

Risk management forms an integral part of the business management process. It is a key component for consideration when shaping an organisation's strategic planning — from one year through to, in some cases, 50 years. Many industries realistically work to three or five years; the financial services industry would be typical of this. Oil and gas companies and mining companies could work up to 10 to 25 year horizons. Governments can operate up to 50 years. Regardless of the number of years set by an organisation, risk management should not be divorced from the strategic planning process of an organisation.

So how do you integrate the fundamentals of risk management into your business?

There are seven fundamental stages in the generic risk management process, as outlined in Diagram 1.

Diagram 1: Risk framework

The **Risk Strategy** is the high level statement that sets out the broad policy as to how risk will be taken and managed by the enterprise to achieve its strategic objectives

The **Risk Profile** identifies, assesses and evaluates key risks facing the enterprise against a number of facets including probability and impact

The **Risk Appetite** sets out both at the Board and Executive, the level of risk tolerance the enterprise is willing to take and hold to achieve its short term (1 year) and medium term (1 – 3 year) aims

Risk Mitigation is the sum of the actions undertaken by management and the risk function to actually manage the risks identified in the risk profile to the tolerance determined by the enterprise's Risk Appetite. This includes the design and implementation of policies, processes and procedures

Performance Optimisation is the process of balancing the totality of risk across the overall enterprise. This includes optimising the use of capital and effort against each risk category. Portfolio management principles apply particularly for FS Enterprises

Ongoing **Monitoring and Reporting** of the extent to which risk mitigation has maintained risk exposure within limits established by the enterprise's Risk Appetite

The process of **Analysing the reason behind Variances** between predicted and actual performance. Where the variation is significant, it is important to develop remedial strategies to return performance to the expected range

Risk strategy

Essential to getting risk management right is deciding, at the highest level, what risks the organisation is prepared to take — ie, the risk strategy. The risk strategy is the high level statement that sets out the broad policy as to how risk will be taken and managed by the organisation to achieve its strategic objectives.

Risk profile

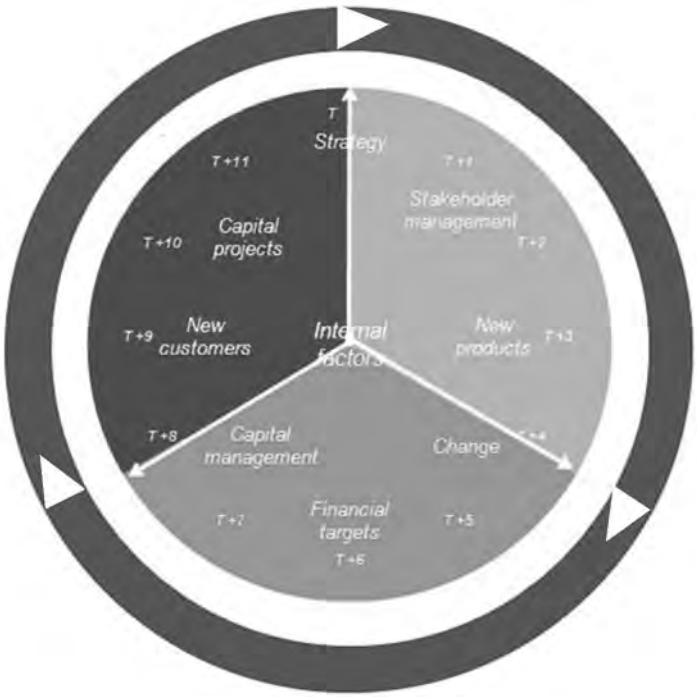
Having established a broad risk strategy as part of the business management planning process, the next step to getting risk management right is to understand your organisation's risk profile. The risk profile identifies, assesses and evaluates key risks, drivers and events facing the enterprise against a number of facets, including probability and impact. This assessment includes evaluation of both internal and external drivers and factors.

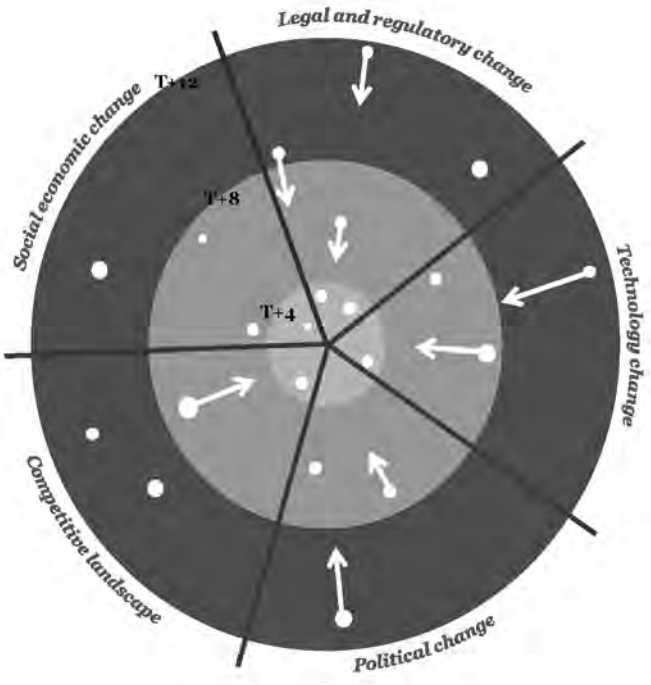
However, as the GFC demonstrated, sometimes events occur which by their very nature are hard to predict — for example, the collapse of Lehman Brothers being a catalyst for a loss of market confidence, contributing to the failure of the inter-bank markets.

Organisations need to continuously develop their scenario analysis to identify and model potential systemic shocks, and to run correlated event stress tests to help shape the organisation's resilience to unpredicted shock. In the financial services industry, such stress tests focus primarily on market, credit and liquidity risks. New thinking is emerging on linking the impacts of these areas, and also taking into account the impacts of operational and regulatory risk failures. Macroeconomic and correlated event stress test limits have formed part of the risk appetite statements of several banks for a number of years. However, traditionally the focus has been on the short term, and there is an increasingly recognised need to extend this assessment horizon.

So, how do you assess the internal and external drivers which inform your risk profile? We propose a number of internal and external drivers for consideration over a 36-month rolling risk assessment process. The time period can be longer, but a period of 36 to 60 months appears to work well for many organisations.

Diagram 2: Internal and external drivers for consideration





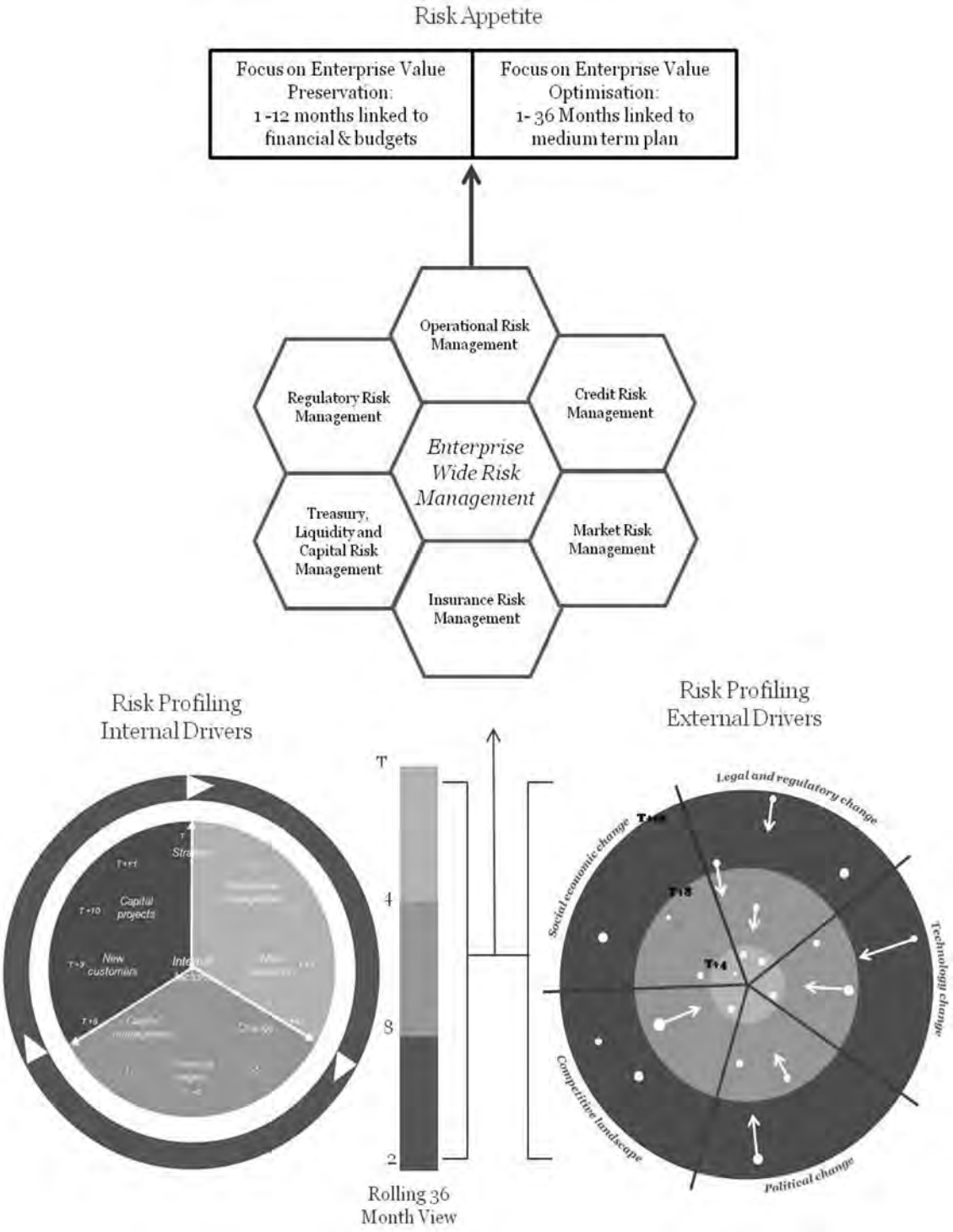
T = 3 months

The categories of drivers set out in Diagram 2 are illustrative — the drivers for your organisation may be different and your list will be more comprehensive. However, by analysing these drivers, your organisation can gain an understanding of the influential factors affecting your future business management strategies, which will shape your organisation's risk appetite and risk management approach.

Risk appetite

The next step is to define your organisation's risk appetite. Setting the correct risk appetite is essential and is informed by your risk profile (see Diagram 3). The risk appetite sets out for the board and executive the level of risk tolerance the enterprise is willing to take, and to hold, to achieve its short-term (one year) and medium-term (one to three years) aims. A short-term focus highlights an organisation's dedication to "enterprise value preservation" (EVP), a period of one to 12 months, which is linked directly to the financial plans and budgets. A medium-term focus showcases a higher level of dedication to "enterprise value optimisation" (EVO), over a period of one to 36 months, linked directly to medium-term planning.

Diagram 3: Relationship between risk profile and risk appetite



Where appropriate, you should also consider and implement an EVO-based approach to risk management planning, based upon a risk profile and appetite which goes beyond the medium term to the long term, post 36 months.

The changing nature of business risk management focus over time

In Diagrams 4, 5 and 6, we set out the subtle changes to the contributions made by business managers and risk managers when looking forward 12 months, 36 months and beyond.

Diagram 4: Operational planning — the next 12 months

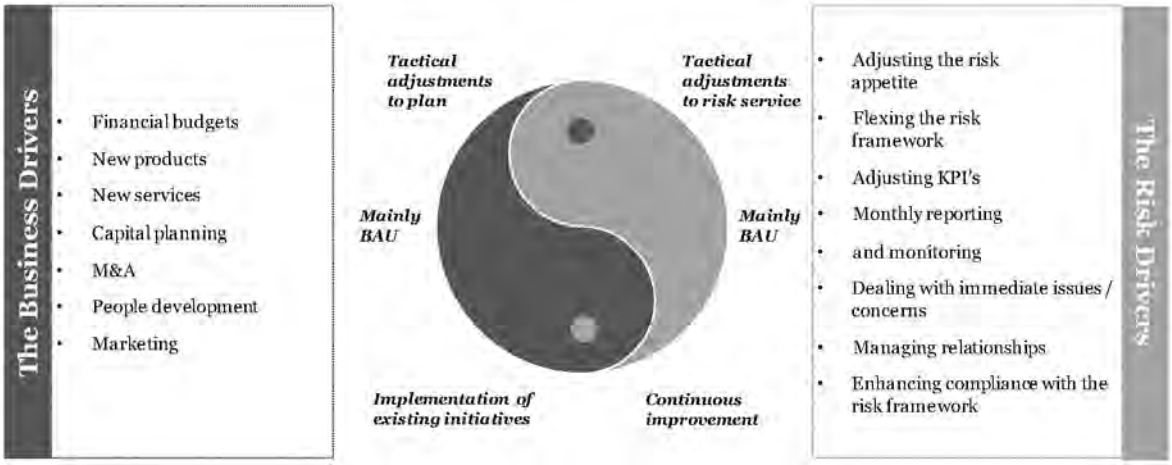


Diagram 5: Medium-term planning — the next 36 months

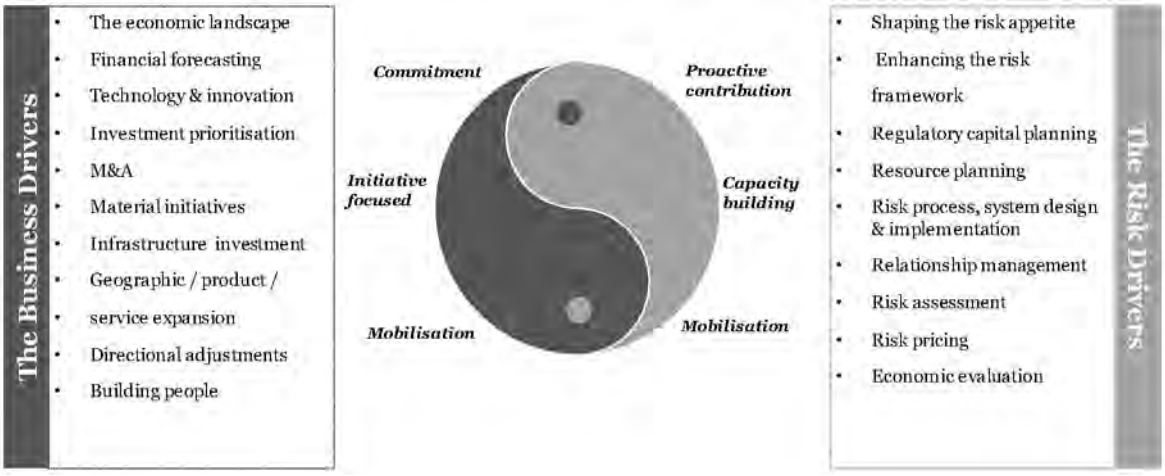
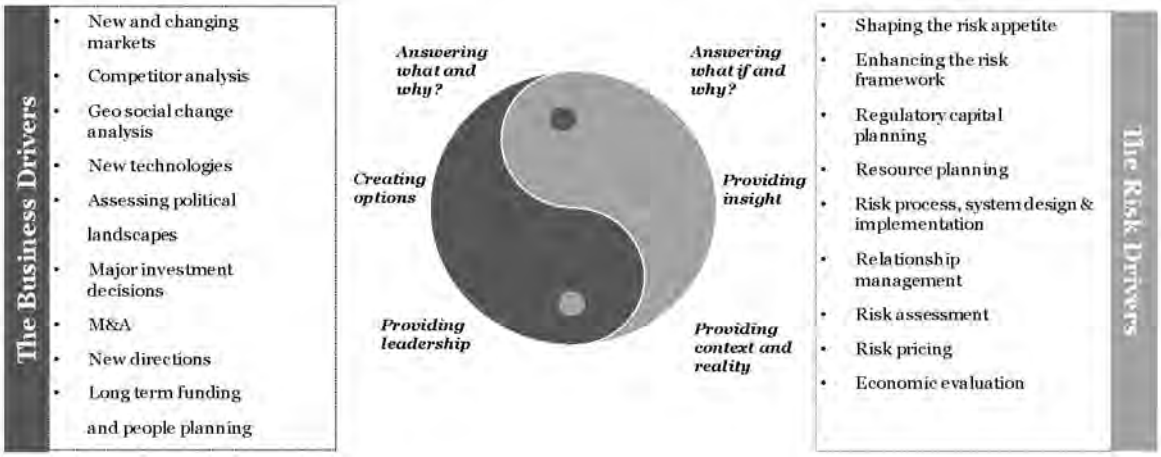


Diagram 6: Strategic planning — the next 60 months to 50 years



As can be seen from these diagrams, the nature of the risk management activity shifts from an "identify, assess and mitigate" process to an "identify, evaluate and model, and decide" process. This shift becomes more pronounced the longer the time horizon is.

By combining your organisation's focus on EVP approach (one year) with an EVO approach (one to three years, or longer), the organisation is better positioned to respond to new and changing markets, undertake competitor and geo-social change analysis, invest in new technologies, make major investment decisions, and undertake long-term people and funding planning. From a management perspective, your organisation is better able to shape a long-term risk appetite, and build the resilience to help weather the seas of uncertain times.

In this article we have focused primarily on the first three elements of the generic risk management framework (Diagram 1). However, this is only part of the solution. Your organisation needs to implement risk mitigation, monitoring reporting and causal analysis of variances strategies to cover the complete spectrum of risk management fundamentals.

Risk mitigation is undertaken by the organisation to actually manage the risks identified in the risk profile to the tolerance determined by the organisation's risk appetite. Unless this is done well, much of the earlier investment is wasted.

Ongoing monitoring and reporting of the extent to which risk mitigation has maintained risk exposure within limits established by the organisation's risk appetite must also be implemented.

Finally, a process of analysing the cause of the variances between predicted and actual performance must be implemented. When variances have been identified, it is essential to develop remedial strategies to return performance to the expected range.

Conclusion

We started this article with a simple fact: over the last century, and specifically in the last 20 years, the root cause of the majority of corporate failures was a failure to manage risk. If history teaches us anything about risk management, perhaps one lesson is that we have short memories. We often fail to apply the learnings from those who made mistakes before us. We believe that things are different now, and we know better. While the nature of world we live in is constantly changing, the basic principles of business and risk management remain constant. We just need to constantly strive to develop better ways of applying them and to challenge our understanding of existing and emerging risks.

Richard Gossage,
Partner — Risk & Capital Management,
PricewaterhouseCoopers,
Email: richard.gossage@au.pwc.com; and

Tara Joyce,
Senior Consultant — Risk & Capital Management,
PricewaterhouseCoopers,
Email: tara.joyce@au.pwc.com;
www.pwc.com.au.

Footnotes

1. Johnson G and Scholes K, ***Exploring Corporate Strategy*** (1998) Pearson Education (5th edn.)

Risk culture surveys — do they get it right?

David Goodsall *SYNGE & NOBLE*

We all know that a good risk culture is important not only in achieving sound risk management, but also in running a successful business. Measurement of risk culture is becoming increasingly common. You can download lots of surveys from the internet, but are we looking at the right things to get the true picture? I suggest not.

The ISO 3100 principles for managing risk state the following.

- "Risk management is based on the best available information."
- "Risk management takes human and cultural factors into account."[1]

Application of these principles requires a good risk culture, and trying to measure it effectively is a given. Although attitude to risk is fundamental to a successful business, I believe risk is generally assessed badly. I say this because I have had the opportunity to see the results of these assessments and work alongside the businesses to see what goes on in practice.

The traditional wisdom of business process management is to look at "people, processes and systems", but in my experience all the attention is on "processes and systems", with the "people" aspect being dealt with by role descriptions and procedures rather than a real consideration of how people behave.

Risk culture assessment seems to be done in the same way. But why does this matter?

If you look at any failure, the root causes generally boil down to human error at an individual or a group basis. Many equipment failures result from human error in design, manufacturing or servicing. As the global financial crisis has taught us, systemic problems can be brought about by people, and by a herd mentality. Even where this is recognised, the solution that's generally proposed is more processes and more systems. Why? Because these are easy to put in place and monitor, and people are seen to be doing something. The problem with this is an often ignored implicit assumption that people will follow those processes and run those systems properly, and this has not been tested.

Case study — the danger of following systems and processes alone

To illustrate, here are just a couple of examples.

- A large well-regarded company had very extensive controls, with a comprehensive control self-assessment process signed off through several levels of management and ultimately going to the board. This was an impressive and weighty set of documentation demonstrating good risk management and compliance. The surveys showed that the company had good controls and everyone knew what they had to do, so everyone relied on the self-assessment process. No one thought that processes may not be followed, or that staff wouldn't answer the self-assessment correctly. Unfortunately, despite this, a key business process was not performed for several years, and led to significant embarrassment for those responsible for signing off on the controls, along with significant cost for remedial action. I should point out that staff members may well have answered the self-assessment questions honestly in their view, even though they weren't correct.
- Another company entered into a transaction that breached a regulatory limit, resulting in action by the regulator. The incident policy was promptly put into action and, after much thought, the solution was to put in place a control to prevent a similar transaction occurring again. This overlooked the real cause, which was not a lack of control but a lack of awareness of the regulatory environment. This was a problem throughout the organisation. More importantly, the senior management involved either didn't know or weren't prepared to say they didn't know what the rules were, and they couldn't make an informed decision.

Poorly designed surveys can result in misleading results

So how do you gain an understanding of what staff members feel and how they are likely to behave? Many organisations conduct surveys to measure and monitor the risk culture. In my experience, these surveys are well intentioned but poorly designed, as they ask staff members questions that they are often not qualified to answer, they ignore human nature in the way people respond to surveys, and they tend to lead to a potentially false positive response.

A survey carried out in a large organisation, given to about 15% of staff members, found that they agreed that:

- risk management learnings were applied and shared within the business;
- staff members had adequate resources to manage risk effectively;
- the company's documented procedures and policies clearly described how staff members need to do their jobs;
- roles and responsibilities for risk management were documented appropriately and included within job descriptions; and
- the risk appetite for the company and tolerances were clearly defined, documented and communicated.

When you go to the appendix of the report to see the detail (and we all know that the appendices are always read in detail!) you find that only about 11% of the total staff answered the survey. There was no indication of the level of these staff members or the areas in which they worked, and there was no discussion of the consequences of about one in four respondents disagreeing with the statements! How would you feel about dealing with an airline where one in four staff members didn't think they managed risk well? Yet this is not an uncommon result and I often see directors not challenging these sorts of results.

Irrelevant questions

Digging a bit further into the appendices, respondents were asked to indicate whether they strongly disagreed, disagreed, agreed or strongly agreed with over 50 statements. The answers to these were collated and summarised to reach the above conclusions.

So, let's look at some of the statements staff members were asked to comment on.

- A risk management policy that is supportive of strategy and objectives has been developed.
- The company has clearly explained that policies and procedures are important to manage risk.
- I understand how the company's policies and procedures support my business unit in achieving its objectives.
- We have sufficient resources to manage risk effectively.
- The risk evaluation process considers the defined risk tolerance levels when making decisions.
- The interdependence of risk and the causes of risk are considered during risk analysis.
- Both the positive and the negative consequences of risk are taken into account.
- The level of risk found during the analysis process and the established risk criteria are compared when evaluating risks.
- Reporting to the audit, risk and compliance committee is independently reviewed before being used in decision making.
- The information provided to the audit, risk and compliance committee is appropriate in both content and detail.
- ***We have an honest and open culture where people are confident to speak up about risks.***

The survey was answered either by people involved in the risk management process, who will tend to agree with the statements because it's their responsibility, or by people who aren't involved in the risk management process, who, frankly, won't be in a position to answer the questions. (How many people in your company know the difference between a good and a bad risk management statement, know what resources are in place to manage risk, or know what is in the audit, risk and compliance committee papers?) Because the response "I don't know" is not an option and staff members have been told how important all this is to the company, employees will tend to assume that it is being done properly and will agree with the statements.

The end result is a feel-good outcome that is likely to miss the real attitudes of staff, and in this particular case the observed behaviours of staff often did not match the results.

The last statement above, in bold italics, is trying to get at attitudes, but it's also flawed because it asks if people are confident that they can speak up about risks — which is very different from asking if they actually do it.

A different approach

So, imagine how the results might vary if the survey had explored attitudes from a different perspective, such as the following.

- I feel the company rules make it hard to do my job.
- There so many rules, I don't always know what they are or even have time to read them.
- I often see managers ignore the rules.
- I don't tell anyone when this happens because I think it might impact my performance review.
- I sometimes take a few shortcuts in order to get the work done.
- Some people in my area don't have the skills or experience to do the job properly.
- I don't really know where my job fits in the overall business.
- I'm not interested in where my job fits in the overall business.

I'll leave it to you to decide which set of questions is more likely to give the more useful insight into the staff.

Now, I'm not suggesting it's as easy as substituting a new set of potentially confronting questions in a survey. However, in my experience, if you ask the right questions in a safe, constructive environment, people are very forthcoming and you can address these sorts of topics to gain a much better insight into your staff and uncover issues that don't normally see the light of day.

Conclusion

Although in this article I have been critical of the usefulness of the standard risk culture surveys, I commend a company that uses them as they are on the risk management journey. The challenge is to resist complacency and improve the understanding of your people — your most valuable resource.

David Goodsall,
Director, Synge & Noble,
Email: dgoodsall@SyngeAndNoble.com,
www.SyngeAndNoble.com.

David is a former partner of Ernst & Young who now consults to the financial services industry through his firm, Synge & Noble. He is also Senior Vice President of the Institute of Actuaries of Australia.

Footnotes

1. International Organization for Standardization, ISO 31000:2009: *Risk management — Principles and guidelines,* available at www.iso.org.

Resilience — from theory to practice

Tim Janes *BUSINESS CONTINUITY INSTITUTE AUSTRALASIAN CHAPTER*

Introduction

There have been many articles in recent years on the subject of resilience. Many have been from an academic or theoretical perspective, which reflects the nascent state of development of resilience concepts. Yet if these resilience concepts are to deliver to organisations the potential that they promise, the ideas must move from theory to a practical and implementable level.

This article aims to consider the realities of that change — what might be required to develop resilience concepts that are useful for everyday realities — and discusses some of the challenges that stand in the way. It will also offer some personal thoughts about possible outcomes as these models of resilience continue to evolve.

Background

I come to this discussion from a business continuity background which, depending on your point of view, may make me more or less biased in the ongoing resilience debate.

Any perceived hostility towards resilience from the business continuity community is misplaced. One of the few truisms I rely on from the last 20 years of business continuity practice is that change has been one of the few constants. With its roots in technology, business continuity has grown to be a business-focused management activity, gathering sophistication, complexity and multiple name changes along the way. It is unrealistic to imagine that this mutable behaviour will cease, or even slow.

This pattern of persistent transformation raises the question: Does the rise of resilience require a major revolutionary rethink of business continuity practices, or can it be accommodated simply as a natural evolutionary progression — just another step in the journey?

It can be argued that business continuity has traditionally been inward looking, focused on an organisation's own priorities and activities. This "self-absorbed" approach is necessary to truly understand the organisation itself and to prepare effective continuity responses. But it could mean that organisations ignore the external element, the significant part of the world outside the office glazing or factory gate. For some time, good practice business continuity methodologies have acknowledged this, and encouraged organisations to understand and address their external risks and dependencies as well as their internal ones.

The global financial crisis (GFC) was a notable example of how external risks and dependencies could bring seemingly well-run organisations to grief — the systemically contagious disruption caused by the failure of Lehman Brothers was felt globally. Closer to home, the problems encountered by RAMS, Centro and ABC Learning in 2008 and 2009 caused ripples that were felt beyond the financial markets.

The GFC was not a "traditional" business continuity event, in that it caused no physical disruption to premises, IT systems or people. However, it did cause significant operational disruption, and some organisations used business continuity principles and established procedures to respond to the chaos and disorder created.

One good example was the approach taken by Euroclear Bank[1] in London to manage the disarray generated by the collapse of Lehman Brothers in September 2008. Due to the scale and speed of events, Euroclear's business-as-usual procedures were felt to be inadequate to deal with the situation. The crisis management team was activated in virtual mode, as its members were dispersed across several cities in Europe. Euroclear used the response team structures, procedures and tools developed and exercised under its business continuity program to respond to the threat posed by the collapse of Lehman Brothers.[2]

This adaptability in an extreme situation, applying established techniques and procedures to an unexpected evolving threat, is one of the hallmarks of a resilient organisation.

To me, this shows that the well-established principles and practices of business continuity are not made redundant under a resilience mindset. They can be adapted to accommodate a potentially broader perspective.

Three levels of resilience

So, business continuity principles and methods can be adapted to accommodate resilience concepts, but is this the end product we are seeking? Essentially, what is meant by "resilience", and what is required for an organisation to implement these ideas?

When considering the first part of the question, there is a plethora of literature defining and explaining ideas about resilience. The following are just a few of the better-known and more accessible examples: the work of Hamel and Välikangas in 2003;[3] the research by Dr Erica Seville at the University of Canterbury; and the output of the Australian Resilience Expert Advisory Group (REAG), formerly the Resilience Community of Interest. More recently, the Australian federal and state governments, via the Council of Australian Governments (COAG), have adopted the National Strategy for Disaster Resilience.[4]

Undoubtedly, a substantial effort has been put into defining and describing the concepts of resilience. There are many common threads in the conclusions that are drawn that relate to values such as adaptability, culture, leadership and interdependency. At the same time, there is an interesting degree of diversity that exists in the interpretation of resilience, as expressed by academics, stakeholder groups and individuals. Understanding this diversity is important when considering how the concepts of resilience might be practically applied.

It seems that resilience might be described at three levels: as a philosophy, as a set of principles, or as a process. These three levels are explained in Table 1.

Table 1: Three levels of resilience

Level	Explanation	Reference examples
Philosophy	A holistic belief system about how to live or how to deal with a situation	Happiness, ethics
Principles	A set of general rules concerning the function of a complex system	Health, government
Process	A defined and repeatable procedure or series of practical acts intended to achieve an expected outcome	Safety, business continuity management

Philosophy

For some, resilience is best described as a philosophy, a set of beliefs that support a positive outcome but which are open to very broad reading. Take happiness. All but the most curmudgeonly would agree that happiness is a desirable and beneficial outcome. However, as many holidays and Hollywood films have taught us, what makes one person blissfully happy can make another entirely miserable.

At this level, resilience might be comparable to aesthetics or faith, or other ineffable activities, subject to personal interpretation based on an enormously variable set of criteria. As such, a philosophical approach to resilience would be inherently unsuitable for implementation in any practical manner by organisations that enabled comparison or benchmarking.

Set of principles

An alternative view treats resilience as a more fully formed set of principles or a set of rules that can be applied in a comprehensive manner. This second option provides better clarity of understanding but retains scope for interpretation. As an example, some basic requirements for good health can be readily defined, such as good diet, exercise, rest and social interaction. However, the degree to which these elements are needed at the individual level, and in what combination, are immensely variable, influenced by genetics, environment, lifestyle and so on.

Equally, we could define a set of resilience principles, but how they are applied might depend on an organisation's or individual's environment, circumstances, size and complexity. A principles-based approach could allow a degree of freedom in deciding what resilience is and how to achieve it. As a consequence, there might be many differing interpretations and approaches, making comparisons of resilience capabilities between organisations more challenging.

However, this approach reflects a view that resilience should be able to mean different things for different organisations. Resilience can be described at the level of a nation, community, organisation or individual. Consequently, resilience is likely to have quite distinct meanings for the citizens of Sendai City or Christchurch, compared to the managers of a global bank or to a farmer in a drought-prone region of Australia.

Process or system

The third level is where the most detail exists. Here resilience is defined as a management process or system with clear objectives, requirements, stages and outcomes. There is certainty about describing what is required for organisations to be resilient and how to go about achieving it. This degree of confidence leads naturally to setting out a resilience methodology. While this does not need to be a one-size-fits-all methodology, it is likely to be prescriptive to a degree that allows auditable comparison between organisations based on an accepted benchmark.

This is where resilience enters the realm of management systems and international standards. Whether the goal of a true resilience standard has been reached to date is open to question. There are already published resilience standards, such as ASIS SPC.1-2009, and the International Standards Organisation (ISO) has commenced the development of an ISO Resilience Standard.[5]

A resilience standard

If the world is to adopt a resilience standard, what form should it take? A good number of the published standards or guidelines that directly or obliquely link themselves to resilience actually look much like existing benchmark documents for closely related disciplines, such as business continuity or emergency management.

This creates a danger that resilience is seen simply as a rebranding exercise, where one or more established management practices are simply retitled. This approach is a good way to lose credibility with management and practitioners, generate false comfort, and destroy belief in the capabilities of a true resilience framework.

It is desirable that a resilience standard is produced, but if it is to be accepted and add value, it needs to demonstrate unambiguously how it is differentiated from the already interrelated disciplines such as business continuity, risk, security and emergency management. Fundamentally, how will resilience change what we already do? Will it move the "story" forward, or simply give it a new cover?

Given the diversity of opinion over what resilience should mean for nations, communities or individuals, accepting the variety of environments around the world and the assorted scale and complexity of organisations, is a single all-encompassing standard obtainable?

In the face of this multiplicity, a highly prescriptive management system type of resilience standard may struggle to appease all the factions. If the scope of a resilience standard is limited to certain stakeholder groups and conditions, then perhaps a rigorous, auditable benchmark document is achievable. But then we may finish up with multiple standards aligned to separate industries and nations that merely perpetuate the confusion and disputes.

Perhaps the solution lies in the middle ground, with a principles-based resilience standard. The natural trend for an aspirant standard as it slowly climbs the slopes of "Mount ISO" is to move towards simplification and commonality. The target is universal applicability. This happened in 2009 with the journey of various national risk management standards that evolved into ISO 31000.

To quote from ISO 31000, "it provides principles and generic guidelines; that can be used by any public, private or community enterprise, association, group or individual". An effective resilience standard might sensibly take the same approach.

Tim Janes,
President,
Business Continuity Institute Australasian Chapter, and
Director, Fulcrum Risk Services,
Email: tim.janes@thebci.org.au,
www.thebci.org.au.

Footnotes

1. Euroclear Bank is a leading provider of settlement services for domestic and international bond, money-market, equity and fund transactions. Euroclear Bank's clients comprise over 1400 financial institutions, located in more than 80 countries. The total value of securities transactions settled by the Euroclear group is in excess of €570 trillion per annum, while assets held for clients are valued at more than €18 trillion.
2. More information about the Euroclear case study can be found at the Business Continuity Institute website at www.bcipartnership.com/BCICaseStudy_Euroclearfinalversion.pdf.
3. Hamel G and Välikangas L, "The quest for resilience" (2003) 81(9) *Harvard Business Review* 52–63.
4. National Emergency Management Committee, *National Strategy for Disaster Resilience*, December 2009, available at www.coag.gov.au/coag_meeting_outcomes/2011-02-13/docs/national_strategy_disaster_resilience.pdf.
5. ISO/WD 22323: *Organizational resilience management systems — Requirements with guidance for use*, available at www.iso.org/iso/iso_catalogue.htm.

Australasian Business Continuity Summit 2011

Sofitel Sydney Wentworth Hotel 8–10 June 2011

Summit highlights

- The Summit is the only business continuity conference in Australia with a program developed by subject matter experts.
- The Summit program combines diverse presenters and topical subjects to address contemporary issues of concern to practitioners of business continuity and related disciplines.
- Presentations from over 20 expert speakers from diverse public and private sector organisations including Suncorp, Qantas, the ABC, Australian and New Zealand Federal Government agencies and the Universities of Canterbury and NSW.
- Hear multiple case studies presentations covering recent incidents such as the Queensland Floods and the Christchurch earthquakes, the Qantas A380 event and the BP Gulf Oil spill.
- Participate in interactive Mini-workshops focused on Running a Scenario Exercise or Effective Business Impact Analysis.
- Attend detailed Workshops covering Organisational Resilience (full day) or Managing the media in a crisis (half day).

The Australasian Business Continuity Summit 2011 is organised jointly by the Business Continuity Institute Australasian Chapter and Continuity Forum.

Australasian Business Continuity Summit 2011 Overview

The Australasian Business Continuity Summit 2011 is the principal annual business continuity conference in Australia and New Zealand. The Summit combines two conference days, Wednesday 8th and Thursday 9th June, followed by Workshops on Friday 10th June.

The Summit is planned by subject matter experts to combine diverse presenters and topical subjects into a program that addresses contemporary issues for practitioner of business continuity and related disciplines. Key themes to be covered at the 2011 Summit include:

- Case studies of organisations disrupted by recent natural disasters in Christchurch and Queensland
- How Qantas responded to a serious incident affecting it A380 fleet
- Seeing an incident through the eyes of the media to help your organisation protect its reputation.
- Updates on Organisational Resilience from academics and practitioners
- Experiences on the practical application of business continuity software applications by end users.
- Implementing business continuity practices in organisations during a time of significant change.
- How emerging technologies are affecting business continuity.
- Practical workshops demonstrating how to conduct effective Scenario Exercises or Business Impact Analysis.

The BCI Australasian Chapter is an approved local Chapter of the Business Continuity Institute (BCI) representing the local interests of BCI members, and raising business continuity awareness and understanding in Australia and New Zealand.

For more details about the conference topics and presenters, visit: www.thebci.org.au.

BULLETIN BOARD

NEW BULLYING LAWS — WHAT DO THEY MEAN FOR EMPLOYERS?

In April this year, the Victorian Parliament proposed new legislation, "Brodie's Law", to make it clear that serious bullying is a crime carrying a penalty of up to 10 years in prison.

The introduction of the Crimes Amendment (Bullying) Bill 2011 (Vic) (the Bill) is a response to the Café Vamp case, in which WorkSafe Victoria successfully prosecuted an employer and three employees under the Occupational Health and Safety Act 2004 (Vic) (OHS Act) for the systematic bullying of another employee, Brodie Panlock, causing her to commit suicide.

Traditionally, liability for bullying in the workplace has been dealt with under the OHS Act. The new legislation will provide protection against bullying in many circumstances and will not be limited to the workplace (unlike the obligations under the OHS Act). However, employers and employees will need to be aware that the new laws will extend to serious cases of workplace bullying, in addition to existing obligations under the OHS Act.

The Bill amends the current stalking provisions in the Crimes Act 1958 (Vic), making it clear that a person can apply for an intervention order against another person who engages in the following type of behaviour:

- makes threats or uses abusive or offensive words in the presence of the victim;
- performs abusive or offensive acts in the presence of the victim; or
- directs abusive or offensive acts towards the victim.

The above type of behaviour commonly falls within the spectrum of what can amount to bullying in the workplace.

For employers, the new laws have the effect of, once again, putting the spotlight on bullying behaviour, including in the workplace. This may mean that there will be a spike in allegations of bullying, and employees may readily use the protection of an intervention order against other employees who are bullying them. If this does happen, employers will need to act carefully in response to such allegations and any intervention orders made.

Employers can manage the risks associated with workplace bullying by having in place up-to-date policies on appropriate workplace behaviour, by educating staff on appropriate workplace behaviour, and by making clear the consequences for employees if they engage in bullying conduct.

*Contact:**Alison Baker,***
Partner, Hall & Wilcox,
Email:
alison.baker@hallandwilcox.com.au.

NATURAL DISASTERS SPARK NEED FOR EXPANDED RISK REVIEWS

The recent spate of devastating natural disasters has highlighted that preparation for a catastrophe should be part and parcel of any prudent business's risk management strategy, according to Gary Anderson from Protiviti.

"The trend in past years has been for businesses to cut costs by consolidating their activities and reducing their suppliers, even for critical inputs. This has sadly come back to bite many tech companies that are over-dependent on Japanese specialised parts manufacturers, which have now shut down indefinitely. Similarly, the Queensland floods have interrupted supplies of agricultural inputs and are sending businesses scrambling to find other cost-effective sources, on the hop."

Mr Anderson explained that for a business to be prepared for the unexpected, the traditional approach to operational risk, which focuses on gaps in internal processes and systems, should be extended far beyond the four walls of the business.

Risk management strategy should take in all parts of the business value chain. It should look upstream to supplier relationships and downstream to channels and customer relationships, and should also factor in vital inputs such as the labour force, transport systems, infrastructure and lines of credit.

"Management should then ask what would happen if any of these elements was taken away? What would be the implications of a shortage, disruption or quality problem in an input or output? What if major customers were to fail or important contracts not be renewed? How long could the company continue operating?"

Mr Anderson recommended that to determine the size of these risks, management should consider additional factors, such as how quickly the disruption in the value chain would impact the company, the severity and expected duration of the negative impact, and the resilience of the company. These assessments would help identify critical areas where the company's preparedness was not up to scratch.

"A world-class response to a crisis is vital to a company's ability to recover from it. Sooner or later, every business will face a crisis that cannot be prevented. Response readiness in the face of such dire events will be the real test of whether a business will sink or swim," added Mr Anderson.

Questions to evaluate your company's operational risks

- Where does the company sit within the "extended" value chain?
- Can the loss of any critical component of the value chain occur without warning?
- How quickly will it take for the loss to impact the company?
- How severe would the implications of the loss be for the company?
- How quickly can the loss be replaced?
- How resilient or prepared is the company to respond to that loss?
- Are there any uncompensated risks the company faces across the value chain, such as increased warranty costs, product recalls, and environmental or OH&S exposures?

Protiviti (www.protiviti.com.au).

INDEX — Authors and articles, issues 1–10

Page numbers in issues 1–10 correspond to the following issues:
Issue 1 — pp 1–16
Issues 2&3 — pp 17–40
Issue 4 — pp 41–60
Issue 5 — pp 61–76
Issue 6 — pp 77–92
Issue 7 — pp 93–112
Issue 8 — pp 113–28
Issue 9 — pp 129–48
Issue 10 — pp 149–68

Table of articles

This index lists alphabetically by author all articles appearing in issues 1–10 of Risk Management Today.

EDITOR: Kerrie Tarrant MANAGING EDITOR: Veronica Rios SUBSCRIPTION INCLUDES: 10 issues per year SYDNEY OFFICE: Locked Bag 2222, Chatswood Delivery Centre NSW 2067 Australia DX 29590. For further information on this product, or other LexisNexis products, PHONE: Customer Relations: 1800 772 772 Monday to Friday 8.00am–6.00pm EST; EMAIL: customer.relations@lexisnexis.com.au; or VISIT www.lexisnexis.com.au for information on our product catalogue. Editorial enquiries: kerrie.tarrant@lexisnexis.com.au.
ISSN 1448-3009 Print Post Approved: PP 349181/00244. This publication may be cited as (2011) Issue 10 ARM.