

MARCH 2000

An Australian View of Risk Management

 **ERNST & YOUNG**

FROM THOUGHT TO FINISH.™



Proud Sponsor of the
Australian Olympic Team

A wireframe globe is the central element, with its grid lines visible. Several autumn leaves in shades of brown, orange, and yellow are scattered across the globe, some partially obscuring the grid. The background is dark and out of focus.

An Australian View of Risk Management

The current pace of technological change coupled with the internet revolution have created many opportunities for Australian companies to expand their operations into new markets and to develop new ways of doing business. But equally this rapidly changing business environment is creating a raft of new risk factors which businesses are being forced to consider on a day to day basis from managing exposure to the 'millennium bug' to the increasingly prominent threat of eRisk.

In this report we examine corporate risk management in Australia in the context of this new technological paradigm. We also measure current perceptions about risk issues against perceptions recorded some twelve months ago. This report represents the views of more than 150 large to medium sized Australian companies and pinpoints the different approaches various industry groups are taking to risk management. It examines the level of resources different business sectors devote to this critical function and provides valuable insight into three topical issues which have significant risk management implications for Australian business, being eCommerce, business interruption and fraud.

Australian business must recognise that now more than ever it is essential that companies employ business risk management strategies which are dynamic and flexible. Without these characteristics, many of the risk management strategies employed by Australian companies may be inadequate in this time of unprecedented corporate change.

As part of a global network of firms advising business in the area of risk management, Ernst & Young Australia is working with Australian businesses to implement the leading edge practices that will help our organisations manage their risk and secure their future. We trust this report will further assist corporate Australia to come to grips with the dynamic issue of risk management.



Terry Richards
National Director
Business Risk Consulting
Ernst & Young Australia

Contents

Key Findings	3
Risk—the state of play	4
Risk—who is accountable?	5
Risk—the new order	6
Risk—the emergence of eRisk	8
Risk—a new focus on information security	11
Risk—when business is interrupted	13
Risk—the link between ethics and fraud	14
Risk—lessons from the Titanic	16
Risk—key steps for management	18
Risk—an expert approach from Ernst & Young	19



Key findings

The amount of time and resources devoted by Australian organisations to the risk management function has improved in the past year with 90 per cent of companies indicating they employ one or more people in a risk management-related role. Notwithstanding this:

- More than a quarter of organisations believe their risk management function is either partially effective or not effective and 20 per cent of those with a documented risk management policy are not confident that the policy is being followed.
- Risk management issues are now a regular item on the agenda at Board level but more than a quarter of the organisations surveyed said their board/audit committee placed only a moderate to low level of importance on the identification, assessment and management of risk.
- The ‘expectation gap’ between what organisations say they are doing in the area of risk management and how effectively they believe their organisation is managing risk, reveals a significant

change in corporate perceptions about risk issues with factors such as corporate structure, leadership and environment now viewed with greater concern.

- Although most organisations believe a number of aspects of their business are affected by eCommerce, 40 per cent of companies do not have an eCommerce strategy, potentially exposing them to a significant new area of risk.
- Among the different risks associated with eCommerce, information security tops the list of concerns with 72 per cent of respondents worried about this aspect of the new business channel.
- The issue of fraud is still not well understood by companies. Although 94 per cent of respondents indicated that their organisations had an ethical framework in place as a means of minimising fraud, only half have allocated resources to control fraud.

40 per cent of companies do not have an eCommerce strategy, potentially exposing them to a significant new area of risk.

Risk—the state of play

The great majority of Australian organisations surveyed (90 per cent) have a designated risk management function, however the level of resources devoted to the risk management function varies widely. Most companies employ just one person to fulfil their risk management requirements. Some 15 per cent employ more than 10 staff in their risk management function while 18 per cent allocate more than A\$1 million a year to their risk management activities.

We found a big improvement in the level of importance placed on risk management in some industry sectors (see Table 1). This improvement was

most noticeable for those companies in the mining, energy and utility sector. This is perhaps not surprising given the operational problems these sectors have been exposed to in recent times and the fact that these industries have inherently higher risk profiles.

In our previous risk management survey, less than 50 per cent of mining companies rated risk management as a very important consideration, compared with 80 per cent in the current survey. In our latest research we found 93 per cent of utilities rated risk management as very important compared with 78 per cent in the previous survey.

Once again the most risk-conscious enterprises were in the banking and financial services industry sectors which have a long history of sound risk management practices. At the other end of the scale, organisations in the government, manufacturing and transport sectors have traditionally not had extensive risk management programs and their low profile in this analysis is perhaps to be expected.

Table 1
Sector ratings of the importance of risk management

50% to 69%	70% to 90%	More than 90%
Manufacturing	Mining	Banking and Financial Services
Retail	Energy	Utilities
Transport	Technology	
Government	Telecommunications and Media	

Risk—who is accountable?

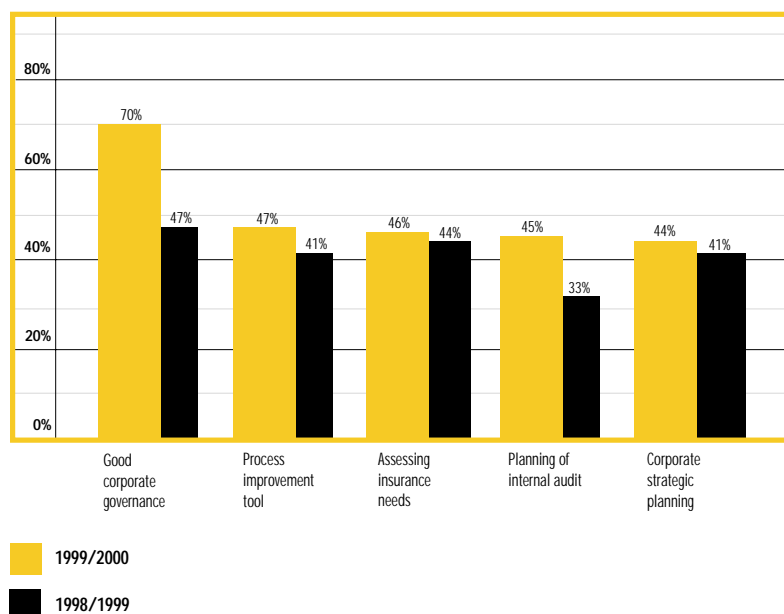
In Australian business, the risk management function typically reports to the managing director. However, in another strong indication that risk management has become a more critical issue for senior management, 40 per cent of respondents indicated their risk management function now also reports at the board/audit committee level, compared with just 14 per cent in the previous survey. In addition, 92 per cent of companies reported that risk management issues were now on the agenda at board level or at audit committee meetings, compared with 61 per cent of companies in our previous report.

Another comforting aspect of the latest survey is the more important role the risk management function appears to be playing in assisting companies in areas such as strategic planning and internal audit (see Graph 1). The contemporary definition of risk management incorporates corporate governance objectives that are also far more strongly reflected in the current survey.

The proportion of organisations with a documented risk management policy rose to 79 per cent from just 60 per cent in the previous poll. While 80 per cent of respondents say they are confident their risk management policy is being adhered to compared with 61 per cent previously, it remains a concern that one in five companies are dissatisfied with the level of compliance to risk management policies.

There is strong evidence that risk management has become a more critical issue for senior management.

Graph 1 Risk management applications



Risk—the new order

A look at the key issues

Our previous survey estimated the level of corporate concern about different risk factors and contrasted those concern levels with corporate estimates about how well those risks were being managed. This latest survey allows us to benchmark corporate perception on risk issues and also to monitor how well companies believe those issues are being managed.

For the purposes of both studies, survey participants were polled as to their perceptions in relation to a range of external, strategic, operational and financial risk issues (listed in Table 2 below).

All these issues were ranked according to the level of importance assigned to each issue by respondents and then according to greatest gap in confidence between respondents’ level of concern for these risks and their perceptions as to how well their organisations were managing those risks.

In terms of the level of importance, the top ranking risk in both surveys was the ‘millennium bug’. There is an argument that the limited impact of the millennium bug could lead to complacency about IT risk issues on an ongoing basis. But perhaps what is more relevant is the elevation in the current survey of other concerns such as risks associated with legal and regulatory issues and competitors: in general, respondents to the latest survey were more concerned about external and strategic risks rather than operational and financial risks.

Table 2
List of risk
issues surveyed

External	Strategic
New markets	Leadership
Competitors	Product life cycle
Legal and regulatory	Image
Economic	Valuation
Industry factors	Planning
Natural disasters	Communications
Political	Company structure
Technology	Performance measurement

A change in perceptions

This apparent shift in corporate mind-set reflects a more sophisticated view of risk management which is evident in many of the survey's results. External and strategic risk are of course inherently more challenging to manage because they are more difficult to control than operational or financial risk. Clearly it is not possible for a company to avoid external and strategic risk, a fact underlined by the actions of company analysts in the US who are starting to measure hidden value assets such as the management skill sets

which enable companies to stay out of legal and regulatory trouble.

Although concern levels are a useful gauge of changing corporate perceptions about risk factors, the gap between the level of concern and how well companies believe those risks are being managed offers an even more valuable insight into the risk management function.

The largest confidence gap in the latest survey is environmental risk. This issue was not on the radar screen in the

previous survey and reflects growing awareness by companies of the importance of becoming better corporate citizens. Evidently company executives are taking a new look at environmental risk factors as investors demand higher standards from companies in terms of environmental and social reporting.

Australian companies are also increasingly aware of potential risks posed by emerging markets and competitors, arguably a reflection of the inexorable globalisation of business.

Operational	Financial
Environmental	Liquidity
Customer profitability	Derivatives
Business portfolio	Credit
Health and safety	Fraud
Human resources	Data integrity
Production capacity	Financial reporting
Product/service failure	Budgeting
Product development	Superannuation
Suppliers	Taxation
Business interruptions	Currency
Brand erosion	Commodity prices
Customer satisfaction	
Project management	
Y2K	
Information security	

Risk—the emergence of eRisk

Business embracing eCommerce

The eCommerce revolution is reshaping the global business environment and changing the way many companies transact business on a business-to-business basis and a business-to-consumer basis. While eCommerce is no doubt offering significant new business opportunities, it is also posing a raft of new risks associated with a new business channel, some of which are unique to this technology.

Australians are enthusiastic adopters of new technology and our report reveals

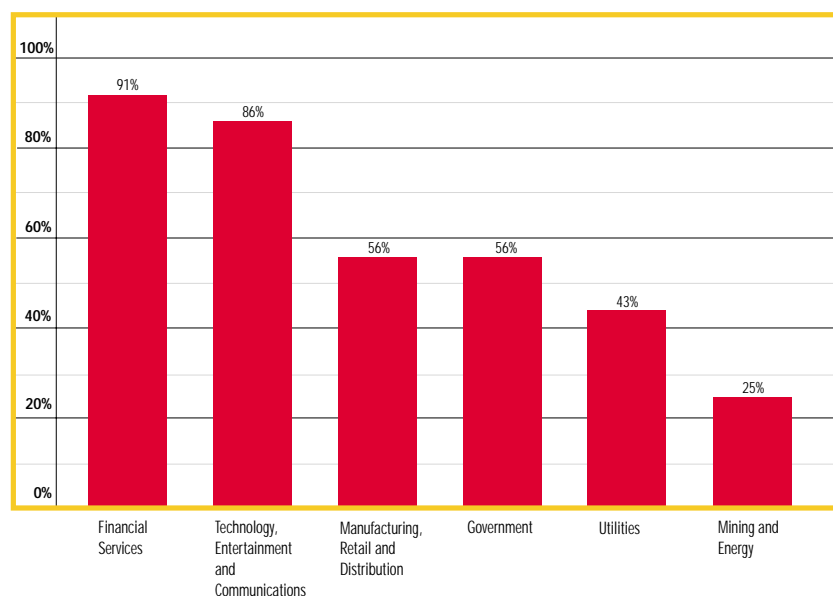
that the majority of Australian companies (60 per cent) have already developed an eCommerce strategy. The companies leading the development of business strategies need to ensure that eCommerce strategies are aligned with their corporate mission and business/technology plans. Those organisations that do not have an eCommerce strategy are likely to be exposing themselves to significant risks such as new competitors who use the internet as a delivery channel or order mechanism for their products and services (see Graph 2).

The survey found that larger companies are slightly more attuned to eCommerce with 63 per cent having a strategy in place compared to just 53 per cent of medium sized firms. An industry breakdown is more revealing with the financial services industry the most prepared in an eCommerce sense (91 per cent) and the mining and energy industries the least prepared (25 per cent).

The financial services industry is at the forefront of the eCommerce revolution in Australia with financial transactions currently accounting for nearly one third of total transactions over the internet. Additionally, the prospective emergence of a super brand in dealing with on-line bill payments, ebrokerage and einsurance have encouraged financial institutions to become experts in this new business channel.

Parts of the entertainment industry are still reeling from the impact and popularity of the internet. Given the dynamic state of the media and movie industries, the high number (86 per cent) having in place an eCommerce strategy is understandable.

Graph 2 Industry breakdown of companies with an eCommerce strategy



New channels—new risks

The lack of a business strategy for companies where eCommerce is impacting only one key aspect of their business is currently a topic generating much debate. One school of thought is that one-off projects should be considered as simply another channel for delivering business plans to customers and therefore only the method of delivery has changed, not the strategy. An alternative argument is that over time all business will be delivered electronically and one-off projects are just the first step in a much larger change in the way business will be transacted. Therefore, developing eCommerce as stand alone projects may result in a fragmented approach which fails to recognise the full impact of eCommerce and achieve the potential benefits of delivering new products through efficient channels to a wide customer base.

Most commentators agree that business planning in the connected economy needs to combine flexibility, speed and self-imposed corporate governance to enable companies to be responsive to technological development, whilst not being stagnated by government regulation.

Hotspots for change

Although 40 per cent of respondents indicated their company did not have an eCommerce strategy in place nearly every respondent anticipated at least one key aspect of their business would be affected by eCommerce. The key areas identified were:

- the supply chain (69 per cent);
- customer service and support (67 per cent) and;
- procurement (65 per cent).

The use of eCommerce is widely anticipated to have a significant bearing on the supply chain. Disintermediation of players, particularly in the manufacturing sector, and the rise of the integrated supply chain will impact the way in which companies interact with their channels to market. Also, the move to outsource procurement and technology to external service providers enables or requires these external providers to develop internet delivery channels, achieve efficient business solutions and attract a growing client base. The risk issue here is that as companies become increasingly reliant on external service providers they have less control of the end-to-end business process.

As companies become increasingly reliant on external service providers they have less control of the end-to-end business process.

Risk—the emergence of eRisk (continued)

Much of the euphoria surrounding business-to-business interaction over the internet is largely based on the benefits of eProcurement and its ability to seamlessly integrate the procurement process electronically. eProcurement is likely to help reduce process costs, improve inventory management and enhance the strategic value of the purchasing function. The benefits are significant but they are difficult to quantify and there is very little focus on the related risks of security, business privacy and management of external service providers.

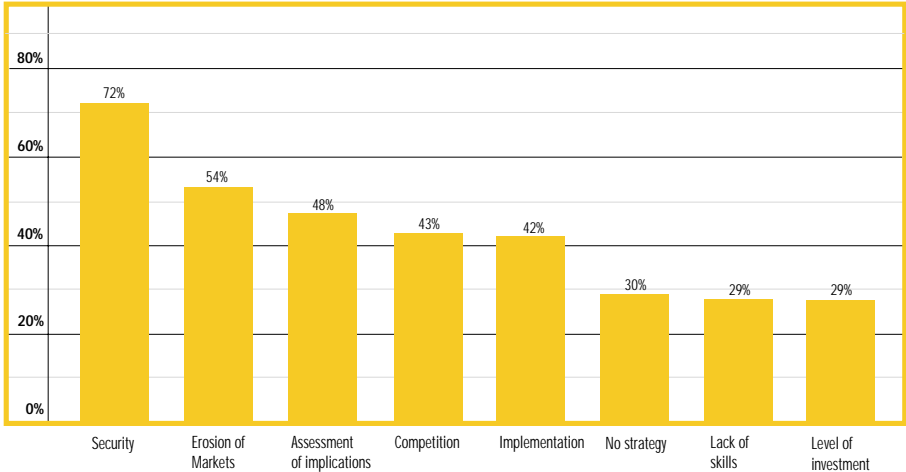
Traditional retailers have realised that they need a virtual presence on the internet as compelling as a store front. This is perhaps even more important in the financial services sector, where electronic delivery channels are competing with traditional branch networks. The big winners will be the financial institutions that combine cost-effective on-line delivery with business-to-consumer relationships to

reach a large mass of customers while at the same time enabling them to personalise the offering. The benefits of both reach and richness mean that eCommerce will affect marketing as well as customer self-service.

The survey asked companies to indicate their level of concern about different risks associated with eCommerce (see Graph 3). Security topped the list of concerns and this issue is discussed in the next section of the report.

While businesses acknowledged the advent of a new business channel would bring with it additional segments that were previously unreachable, this perceived benefit was outweighed by the feared loss of customers to new players using the eCommerce channels. More than half the respondents (54 per cent) were concerned their customer base would be cannibalised by this new business channel.

Graph 3 Company ranking of eCommerce risks



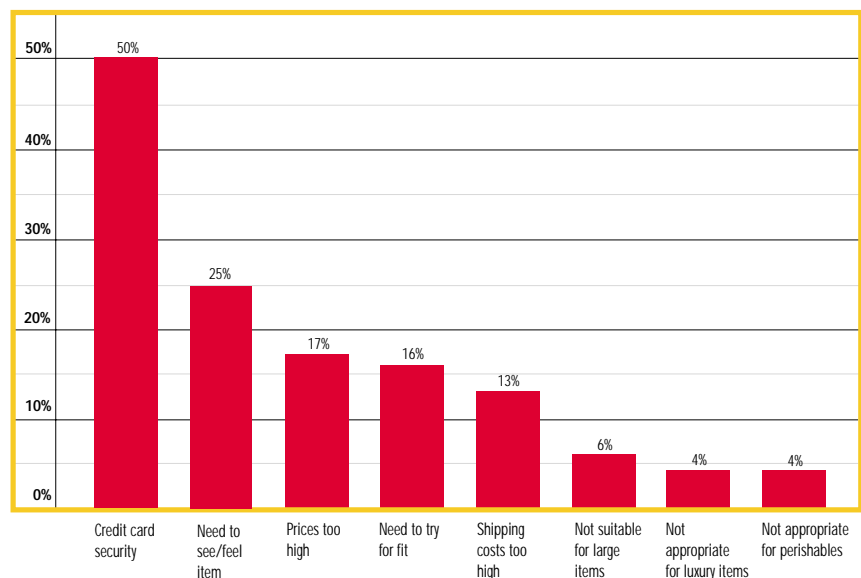
Risk—a new focus on information security

Senior management needs to accept a level of risk associated with rapid technological development to achieve business leadership. At the same time management needs to learn how to control the new significant risks created by eCommerce. The survey respondents clearly identified security as the biggest concern for Australian business and this reflects similar concerns identified amongst consumers in the recent Ernst & Young Special Report on Internet Shopping in Australia. The Internet Shopping report found 50 per cent of on-line shoppers cited credit card security on the internet as their prime concern (See Graph 4) compared to 19 per cent in the US and 24 per cent in the UK.

The recent infiltration by hackers of cduniverse.com's database that allegedly exposed up to 300,000 credit card numbers shows that company and consumer fears about security are not groundless. Because eCommerce revolves around dynamically-enabling business models, for these models to succeed, an organisation must establish an environment of trust and understanding

within the enterprise and with its customers, business partners and shareholders. Our experience and research show that addressing issues of risk, security, reliability, trust and assurance is critical to success in the marketplace.

Graph 4 Concerns of Australian on-line consumers



Risk—a new focus on information security (*continued*)

Lack of action and, in many cases, a misunderstanding of where the main threats lie, are exposing companies to serious financial losses. Chief executives need to recognise security as an enabler of business growth and opportunities, not a restraint and to assume control of the issue.

The initial size of an eCommerce start-up business has allowed informal governance and control procedures to operate reasonably effectively, whilst enabling the business to meet competitive pressure with respect to ‘speed’ of business development. However, the growth of eCommerce businesses has been much larger than predicted. In many cases business strategies and budget forecasts have quickly become outdated and the

supporting governance and risk management practices have not been implemented as originally contemplated.

Ideally management should adopt project management disciplines to ensure the delivery of internet business plans and initiatives. This encompasses an ongoing review of business strategies and budgets to ensure that resource levels, systems capacity and the capability of external service providers reflect the increased business growth.

Risk—when business is interrupted

As most organisations have invested in the development of Y2K contingency plans, they now have the opportunity to enhance and expand these into ongoing enterprise-wide business continuity plans (BCPs) in order to reap some continuing benefit. The time to act on this is now, while senior executives and staff still have the importance and understanding of contingency planning fresh in their minds.

An expected new driver for BCP is eCommerce. Because of the changes in operating rules that eCommerce presents (e.g. blurred geographical boundaries, reconstruction of value chains, promotion of networks of affiliation and compression of cycle times), most existing BCPs will need to be reassessed and adjusted to address the resulting changes in time-critical business processes and technology.

The survey prompted respondents to identify from a list of business interruption events, which ones had seriously impacted their organisation in the past five years. The five most significant interruptions were:

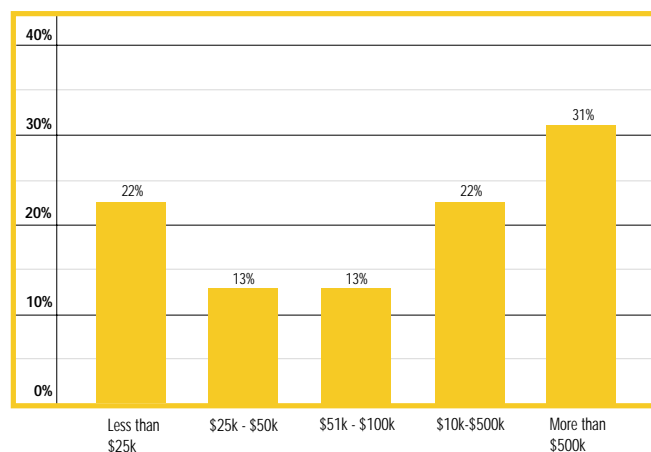
- computer software problems (54 per cent);
- power/gas outage (51 per cent);

- human error (50 per cent);
- facilities move (39 per cent); and
- computer hardware failure (38 per cent).

The high level of occurrence of utility outages seems to be a reflection of the current utility service provision in most states and should alert companies to the importance of having adequate risk management and business continuity planning processes in place. Perhaps surprisingly high is the response of business interruption caused by human error. This appears to be an area overlooked by organisations who may not be focusing enough attention towards ensuring adequate training or skill levels are in place.

Graph 5 below demonstrates how business interruption can have a significant financial impact on an organisation, particularly when litigation results. Other financial impacts may include loss of revenue, penalties, interest on borrowed funds and extraordinary expenses required during the interruption. Further analysis reveals that the industry sectors worst affected by interruptions were mining, energy, utilities and manufacturing while the least affected sector was government.

Graph 5 Cost to business of interruptions in the past year



Risk—the link between ethics and fraud

Fraud is a continuing and growing threat to business. It is a business risk which is largely unrecognised in the broader analysis of enterprise-wide risk in any organisational profile.

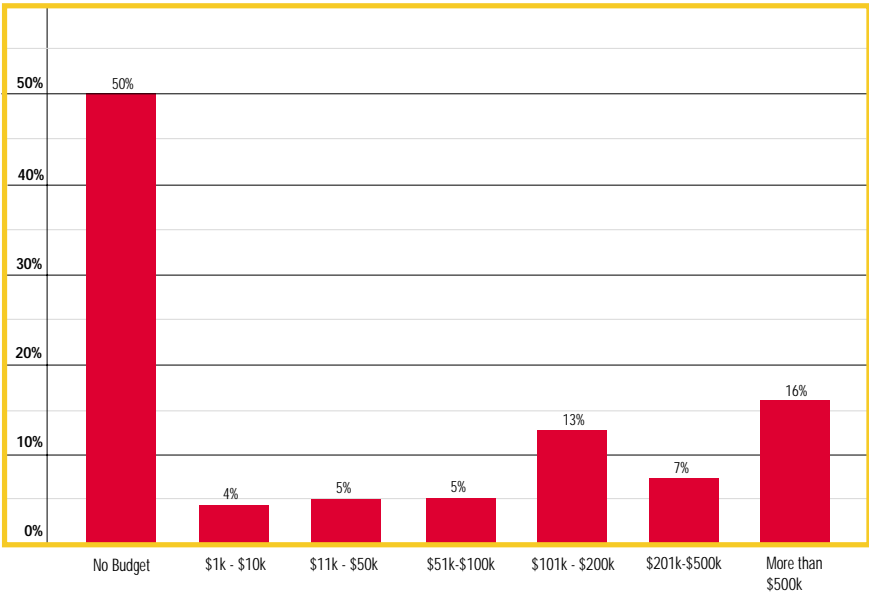
Fundamental to managing risk of fraud is the active promotion of a business culture which will prevent and detect fraud—a culture of honesty, vigilance and, if necessary, exposure and punishment. The great majority of respondents (94 per cent) said they had an ethical framework in place to minimise the instance of fraud. This response was encouraging, however, when we asked companies to indicate their level of budgeted resources for fraud control we found that only half in fact allocate funds to mitigate this serious risk (see Graph 6).

This result is disturbing because it indicates that a significant number of organisations do not recognise that managing the risk of fraud is a dynamic process which requires resources. It also suggests that many companies may consider that having an ethical framework in place is the only protection they can have against fraud—an apparent acceptance of defeat in the battle to control or reduce fraud.

Further analysis reveals that the industry sector with the biggest budget for fraud is financial services. A standout in the 'no budget' category is the manufacturing sector although this group is split with manufacturers also well represented in the high budget category.

Is this a cause for concern? Referring to the most recent Ernst & Young international report into the effect of fraud on business, 'Fraud—the

Graph 6 Business budget for fraud



Unmanaged Risk', during the past five years, more than 75 per cent of the international business respondents had been subject to fraud. The Australian response showed 70 per cent of respondents had been defrauded and 30 per cent had experienced five or more frauds in a single year.

In addition more than 80 per cent of respondents said they were concerned that a significant fraud could occur in their organisation. Despite these fears, more than half the respondents said their organisations had not done as much as they could cost-effectively do to protect themselves against fraud.

If the fraud survey is a general snapshot of the spend on fraud risk—what is at stake as we move to a connected economy?

Risk—lessons from the Titanic

Risk management is not a fad issue. Its application as a management tool is just as relevant today as it was 100 years ago. The following analysis of the ill-fated maiden voyage of the Titanic provides a good illustration of the sort of risk issues that still exist in organisations today.

The Titanic was a state-of-the-art transatlantic liner and the company that owned it, the White Star Line, was among the best in the world. Its captain, E.J. Smith, a veteran with the company, was reputed to be the best captain in the White Star Line.

The liner was equipped with wireless receivers to get information from shore and other ships in the area. Should damage occur, the ship had a mechanism to seal off the problem area, thus preventing flooding in one compartment from spreading to others. The ship could stay afloat if any two of the 16 compartments flooded, and even four if they were the smaller compartments at the bow of the ship. If all else failed, the ship had lifeboats.

The ship departed on 10 April 1910 in calm seas for its well-publicised voyage with a passenger list containing a who's who of the rich and famous. On the night of 14 April, it hit an iceberg and sank, killing more than 1,500 passengers and crew. These are the events that led up to the disaster:

Responsibilities not clear

The new ship had a crew that had not worked together before; as a result, they did not know each other, nor were their individual responsibilities clear.

Incentives not aligned with risk management

The captain was trying to beat a speed record for the transatlantic crossing. Competitive pressures to cut costs and improve customer convenience resulted in the elimination of some of the safety features that engineers had included in the design of earlier ships. Instead, relying on a new, untried technology, the designers thought the ship was safe enough.

Information not monitored timely or sufficiently

Iceberg warnings from other ships were received by the radio operator, who put them aside in order to deliver radio messages to the passengers. Lack of binoculars for the lookout resulted in visual sightings of the iceberg after it was too late to avoid it.

Information not analysed

The iceberg warnings showed a pattern that indicated the ship was in the middle of a rectangular patch of icebergs. Had the iceberg warnings been reviewed and assessed, the pattern would have been apparent and the ship's speed could have been slowed to reduce the impact of a hit, or the ship's direction could have been changed to avoid the hit altogether. Even after the ship hit the iceberg, the magnitude of the damage was not understood and evacuation of the ship was delayed.

Senior management not informed

The radio messages regarding the icebergs were not given to the captain.

Failed back-up safety measures

The sealed compartments were not effective in controlling the damage. More damage occurred than was thought possible.

Inadequate contingency plans

To save costs and to allow for more deck space, the ship had only half the number of lifeboats it needed in view of its passenger load. Further, procedures were not followed to ensure that the lifeboats that were available were completely filled. Many left the sinking ship partially empty.

According to historians, the disaster could have been prevented—and the manner of prevention sounds very much like the integrated risk management framework being adopted by leading edge corporations.

If the captain had in place a process to:

- Identify risks—he would have been aware that the icebergs in the area were a significant threat. Icebergs are highly likely in the Atlantic Ocean in the spring. He should have understood the difference between ‘unsinkable’ and a very high probability that the ship was unsinkable.

- Set objectives relative to risk—the ship could have set a speed record on another crossing. What drove the objective to set a speed record with untried technology in iceberg season?
- Measure and monitor risks—the radio operator would have captured the information and given it to the appropriate crew to assess.
- Communicate risk tolerances—the crew would have raised the red flag to the captain.
- Control risk—the captain would have slowed and turned the ship—and would have made sure the safety measures had been thoroughly tested and that the contingency plans were viable.

If a pro-active integrated risk management process had been in place, Captain Smith’s reputation as the best captain in the best fleet would have remained intact, the Titanic would have carried passengers across the Atlantic for years to come and, most importantly, hundreds of lives would have been saved.

The Titanic is a sad lesson in failed risk management.



Risk—key steps for management

With virtually all aspects of commercial life uncertain, organisations must be in a position to assess their risk position and take action in accordance with their preferred risk tolerance. They must be able to ensure that a common and coordinated approach to risk extends down through their enterprise, guiding the evaluation of opportunities and the implementation of responses to them.

They must also be able to demonstrate to existing and potential investors that they have achieved and can sustain the best possible balance of risk, cost and reward—and that this contributes to a genuine, sustainable advantage in the marketplace and hence will contribute in a positive manner to business prosperity and shareholder value.

For boards, audit committees and management keen to address the issue of risk management there are several key steps that require attention:

- Risk management needs to address whole-of-business risk, not just insurable or auditable risks.
- Risk management systems must report the emergence of new risks and the impact on existing risks of changing business conditions.
- The entire management team needs to take responsibility for the identification and assessment of risk rather than delegating it to a risk manager or internal audit.
- A common definition of what constitutes acceptable risk needs to be developed for each organisation to ensure consistent understanding.
- What constitutes an acceptable level of risk for each organisation needs to be defined—some will be more risk averse than others.
- Risk management systems need to be capable of reporting risks that fall outside acceptable criteria.
- Risk management needs to be an ongoing concept, not something that is addressed periodically.
- Risk management policies should be developed and communicated throughout the organisation.

Risk—an expert approach from Ernst & Young

A critical attribute of a successful business is the effectiveness of its risk management process. It is increasingly recognised that the better the risk management capability, the more certainty there is of prosperity and potential long-term competitive advantage. In Australia and around the globe, Ernst & Young works with leading businesses to:

- **Design and improve risk management capability**—By working with senior executives, we help them to understand their tolerance for risk and co-develop their strategy for managing key risks. In addition, we work with them to assess the business's current capability to manage risk and, if appropriate, implement a robust risk management process. This will lead to better control on the part of senior management and provide increased confidence as to how to successfully balance risk and reward. This can enhance a business's ability to reduce its cost of capital and can lead to reduced or more effective spend on risk management activities.
- **Provide innovative solutions to specific risk management challenges**—In certain situations, there is a need for concentrated consideration of the impact of change on the risk profile of the business and a need to design the future risk and control architecture. In these situations, we have worked with organisations during business transformation programs, the establishment of shared service centres and during the implementation of major systems changes. Through the timely involvement of business risk specialists, an organisation can be more certain that change will not create undesired exposure in the future and that day-to-day activity will not be adversely affected.
- **Deliver wider assurance**—Ernst & Young is a leader in the development of innovative internal and external audit approaches which focus on providing management with assurance against their key business risks and ideas on how to manage them better as opposed to purely assessing the system of financial control. Clients benefit from wider assurance through the adoption of a dynamic approach incorporating process reviews, leading edge business analytics, best practices and benchmarking.



A wireframe globe is the central element, with thin lines representing latitude and longitude. It is partially covered by several autumn leaves in shades of brown, orange, and yellow. The leaves are scattered across the globe, with some appearing to be falling or resting on its surface. The background is a soft, out-of-focus bokeh of light and dark spots, suggesting a shallow depth of field.

Ernst & Young Business Risk Consulting Group

Contacts

ADELAIDE

Ian Painter
91 King William Street
Adelaide SA 5000
Tel (08) 8233 7111
Fax (08) 8231 8050
ian.painter@ernstyoung.com.au

BRISBANE

Ian Rodin
1 Eagle Street
Brisbane QLD 4000
Tel (07) 3011 3333
Fax (07) 3011 3100
ian.rodin@ernstyoung.com.au

CANBERRA

Geoff Knuckey
51 Allara Street
Canberra ACT 2601
Tel (02) 6267 3888
Fax (02) 6257 2648
geoff.knuckey@ernstyoung.com.au

DARWIN

Les Harley
9-11 Cavenagh Street
Darwin NT 0800
Tel (08) 8982 1444
Fax (08) 8982 1400
les.harley@ernstyoung.com.au

MELBOURNE

Terry Richards
Peter Moloney
120 Collins Street
Melbourne VIC 3000
Tel (03) 9288 8000
Fax (03) 9654 6166
terry.richards@ernstyoung.com.au
peter.moloney@ernstyoung.com.au

PERTH

John Copp
152 St Georges Terrace
Perth WA 6000
Tel (08) 9429 2222
Fax (08) 9429 2436
john.copp@ernstyoung.com.au

SYDNEY

Bill Rock
Peter Matruglio
321 Kent Street
Sydney NSW 2000
Tel (02) 9248 5555
Fax (02) 9262 6565
bill.rock@ernstyoung.com.au
peter.matruglio@ernstyoung.com.au

ERNST & YOUNG

www.ey.com

© 2000 Ernst & Young.
All Rights Reserved.
Ernst & Young is a registered trademark.

© Ernst & Young Australia 2000

This communication provides general information current as at the time of production. It is not intended that the information provide advice and should not be relied on as such. Professional advice should be sought prior to actions on any of the information contained herein.

Liability is limited by the Accountants' Scheme under the Professional Standards Act 1994 (NSW).
Business Development EYA (AABS0313)