

Contents

- page 170** **Survival of the learning organisation — the business organisation of the 21st century**
The prosperity and ultimate survival of businesses depend on the individual and collective decisions of boards and managers; those ill equipped to foresee and plan for the future will be cast aside. A successful business of the future will have the ability to be aware of its environment and will have the adaptability to develop forward-thinking plans to ensure survival.
Michael Vincent MONASH UNIVERSITY
- page 175** **A framework for IT controls**
In recent times, some spectacular IT system failures have impacted the ability of corporations to conduct business, maintain credibility and satisfy customer needs. These failings also raise questions as to how management and directors can be assured that their IT systems and applications are robust and can withstand both internal and external stresses.
Dean Sleight TABCORP and **Devan Naidoo** ECHO ENTERTAINMENT GROUP
- page 179** **Freezer risk management**
The tools of research are becoming increasingly significant within the university sector. This article reviews recent trends regarding the storage and loss of research materials in temperature-controlled environments, focusing on freezers and cool rooms. What once was an operational issue increasingly has strategic impacts, and should be viewed as a priority by both risk professionals and senior managers.
Harry Rosenthal REGIS AND PARTNERS

Commissioning Editor
David Wilkinson,
Principal, Risk on the Run

Expert Panel
Christine Lithgow,
Director, Contracts Australia
Jean Cross,
*Emeritus Professor of Risk Management,
University of New South Wales*
Todd Davies,
Todd Davies & Associates
Dr Carl Gibson,
*Director of the Risk Management Unit,
La Trobe University, and
Chair of the working group responsible for AS/NZS 5050: 2010*

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.

Survival of the learning organisation — the business organisation of the 21st century

Michael Vincent MONASH UNIVERSITY

Business has been in a state of change since its beginning: without change, there is no progress. The change pattern of the 21st century is the speed of the cycle of change. The demands for performance are increasing and the strains to perform are greater. Education is essential to understanding the forces that are dictating the structure and shape of organisations into the next several decades. We are in the middle of the technological revolution, it's just that most of us don't realise we are part of history.

This was the same for the people caught up in the industrial revolution of 200 years ago. They did not realise that the events that were changing and shaping their lives would change the very nature of the world we would inherit. The inability to understand the cycle and the events that are shaping our environment can lead to a wasted generation of people who are not equipped to be survivors.

Risk management is evolving within learning organisations to fill the void left by the elimination of middle management. Risk was managed as a process in the past because of the layers of management and the devolution of responsibility. Now there is no middle management, and risk must be managed in a directed sense. The only way for this to occur is for individuals to be skilled and the organisation to respect the quest for knowledge.

The business of the future is faced with choices, the selection of which will dictate success or failure. The basic choices are as follows.

- Embrace a learning environment that recognises and rewards individual and organisational excellence.
- Reinvent middle management to overlay the reinstatement of process, with all its associated costs.
- Allow technology to take over by adopting techniques that are not understandable or usable by the vast majority. This leads to an abrogation of managerial responsibility.
- Allow the business to descend into chaos and, ultimately, disappear.

As we face the future and consider the decisions that must be made under uncertainty, different pathways will lead to different requirements and different attitudes of staff towards success. Business practices once seen as eternal and unchanging are being cast aside, to be replaced with new mantras that, in their turn, will be replaced. Businesses that fail to embrace change and adopt a policy of transition will not survive.

A prosperous future and ultimate survival depend on the individual and collective decisions of boards and managers; those ill equipped to foresee and plan for the future will be cast aside. A successful business of the future will have the ability to be aware of its environment and will have the adaptability to develop forward-thinking plans to ensure survival.

Survival is not compulsory

Comfort zones need to be cast aside. Business needs to realise that it is hard work to survive and that an organisation has many stakeholders who depend on its success for their future. These stakeholders include:

- shareholders;
- the board of directors;
- executive management;
- management;
- workers;
- the families of all the above.

All business has access to the same information and advice, depending on the level of disposable funds. Some businesses move forward and prosper, but many will fall by the wayside and fail. Size is not necessarily the key success factor. There can be many reasons for failure and success, some of which can be attributed to the life cycle of the organisation. Other possible reasons include the following.

- **Individuals:** A well-educated and skilled workforce that embraces the corporate vision and has the empowerment to build success. A learning organisation develops a corporate ethos and maintains corporate memory that is the sum of the skilling of its staff.

- **Planning:** The ability of the organisation to identify the future direction or directions that increase the chances of survival, and having the breadth of vision not to be locked into the past. Planning enables an organisation to understand that ideas have a time, and that timing is the key success factor of change management.
- **Implementation:** The courage of the entity to embrace and implement its plans, which have been well thought out and constructed to ensure success. Implementation involves the understanding of timing and the potential effects on the organisation.
- **Right place at the right time:** Organisations need to embrace a philosophy that there is no such thing as good luck; rather, “luck” is the outcome of hard work. At times hard work is seen as good luck, but a successful organisation will develop an ethos that makes success look easy.

Remember, a business is not forced to survive; dictatorships tend to disappear after the first generational wave.

21st-century business environment

The future is about developing the skills to navigate the maze of the 21st-century business environment, which is characterised by turbulence. The major issues to be faced here are the following.

- **Social:** There is an ongoing process of the creation, in very stark terms, of the “haves” and the “have-nots”. This is happening at all levels and in all societies. The perception is creating the environment of protest and uncertainty; thus, the business dynamic is affected regardless of the truth of the matter. Business needs to develop the concept of the worth of the individual and translate this into a business success factor; importantly, it needs to communicate this philosophy more effectively to the developed and the under-developed worlds. All parties need to know the basic economic fundamentals that drive business decisions and how different levels of return to stakeholders in different environments can be fair and equitable. A successful business of the 21st century will address this risk as a matter of priority.
- **Political:** The political map of the world is changing, turbulence is the norm, old systems have been bypassed, and new systems are struggling to take hold. Business needs stability to grow and prosper, and herein lies the problem. Sometimes the status quo is the most favourable business environment,

but it is not in the long-term interests of the people. Business must get used to dealing in an uncertain political environment, even in established countries. Business needs to transcend the political environment, at the same time exacting a balance that allows it to grow as a good corporate citizen.

- **Technical:** Computer knowledge is growing at a doubling rate of less than two years. Equipment must be amortised more quickly and IT decisions must be carefully considered because of the cost of mistakes, let alone the cost of success. The key success factor is the application of IT power to enhance the business opportunity — in other words, the consumption of finite resources that results in a sustainable growth of the entity.
- **Economic:** Managers must embrace basic fundamentals and implement strategies and policies that create an environment for success. Major concepts are:
 - opportunity cost;
 - cost of risk;
 - concept of marginal costing and return;
 - time and externalities;
 - allocation of scarce resources; and
 - product time and diminishing returns.

Business success depends on successful managers who can cope with change. In order to do this, they must understand that business is made of a micro and macro environment. Those who successfully manage the external and internal environments will set the scene for survival. Even with all these aspects in play, it is not a guarantee that survival is compulsory.

Information technology

This is the ultimate conundrum in that IT is a major factor in survival and, at the same time, a major contributor to failure. Much has been written on IT; therefore, all that needs to be stated for the purposes of this article is that rapid evolution of knowledge and the even more rapid obsolescence cycle present unique threats to the survival of business. Never before in history has the decision-making process in one factor of a business process become so critical to survival.

The key factors to be considered under the IT banner are the following.

- **Hardware:** The choice of equipment and the cost of operation, as opposed to the amortisation within an acceptable level of return. The major issue is to know what you want the equipment to do, the costs involved, and the range of choices available. Note that the cheapest option is not always so.

Risk Management

Today

- **Software:** The platform must deliver the needs of the business. The basic choice is between off-the-shelf versus tailor-made. Cost is an issue here, as well as operational efficiency. The ability to upgrade at a smaller cost is critical to the ongoing survival of any system.
- **Networks:** Intra and inter are the basic choices, and each has its own risks and benefits. The implementer must know what they want from the network. Security issues and desired outcomes are the driving forces of decision making. The cloud is coming.
- **Workstations:** The design and integration of the stations for the identified tasks will create a sustainable and pleasant environment. Occupational health and safety issues must be paramount in the decision-making process.
- **Robotics and artificial intelligence:** Here lies the future. Companies that can harness successfully the resources that are coming on line will be the survivors of the next generation.

Change — the only known constant

Change is not an aberration; it is not an event that disturbs a normally quiet and stable world. A successful company recognises this fact and understands that there is no such thing as stability. Change is the constant and it is always happening. To an individual, change and the management of change can be a stressful task but, to a company, the challenge is to create an environment of constructive change that embraces the individual in an inclusive rather than exclusive sense. It is the environment of change that leads to advances; periods of perceived stability are the times of little progress or advancement. In a sense, we are a lucky generation because the pace of change is extreme; accordingly, we are in an exciting time with the prospect of huge advances to benefit the whole community.

We do know that there is resistance to change and, as humans, we prefer the status quo. However, when we embrace change as a philosophy, humans actually enjoy the challenges. A successful learning organisation creates an environment of constructive change that is embraced by its workforce. It could be said that a successful company in the future will harness the need for change with a method of change that is embraced by individuals. In other words, most people object not to change but rather to the perceived harsh methods utilised to achieve change.

Change will only work in the long term if it is viable and self-sustaining. Many corporations are crippling their future by the severity of change today in the quest for a greater return to shareholders. These companies are

forgetting that the business has a series of stakeholders and not merely shareholders. The successful learning organisation of the future will understand the needs of all its stakeholders and will be able to balance the competing needs for a sustainable and long-term growth curve.

Change must be planned and managed and not done in isolated pockets of an organisation; rather, it must be a macro application with micro results.

Forces on the learning organisation

The economies of the world are getting closer, the world is getting smaller in a global sense, and country borders are less relevant today than they were a decade ago. Forces of change are irreversible and irrevocable. Countries ignore these forces at their own peril. Some bigger economies can resist for a period but, in the end, the survival of the world economy is enhanced by embracing rather than resisting change. An organisational learning philosophy will enable companies and individuals to survive intact the winds of change. The major forces sweeping the world today are:

- globalisation;
- worldwide competition;
- productivity requirements; and
- access to knowledge.

Dimensions of the forces of change

The forces of change that are apparent and unstoppable around the world can be summarised as follows:

- increased role complexity caused by continuous change;
- managers need to cope with unclear lines of authority;
- changing accountability and authority;
- changing planning process and measurement systems;
- rapid technology infrastructure change; and
- management today may involve many revolving teams.

The above points dramatically demonstrate the worth of the learning organisation. Corporations will only prosper into the future by understanding and implementing the philosophy that sits behind the concept of organisational memory.

The risk planning process

Risk is a normal state in which losses are not only possible but also likely. An individual lives under uncertainty from birth to death. It is necessary to differentiate between pure and speculative risks.

- **Pure risks:** loss/ no loss.
- **Speculative risks:** loss/ no loss/ gain.

Planning adds the elements of forecasting and control. When planning for risk management, the following factors — in addition to the normal risk identification and mitigation process — will ensure that an effective organisation learning culture is developed.

- **Competitive potential:** What is the future position and potential, in a world sense, of our businesses? What do we need to do in order to release potential?
- **Business value potential:** The identification of the future value of the business to shareholders and other stakeholders.
- **Service level potential:** At what point do we grow beyond the existing resource base and need the deployment of extra resources to ensure growth?
- **Technology potential:** What is available to the entity in order to drive the business segments forward?
- **Review:** An ongoing process that brings together the entire planning process and ensures that potential is directed and unleashed.

Definition of a learning organisation

Argyris¹ defines organisational learning as the process of “detection and correction of errors”.² In his view, organisations learn through individuals acting as agents for them: “The individuals’ learning activities, in turn, are facilitated or inhibited by an ecological system of factors that may be called an organisation learning system.”³

Huber⁴ considers four constructs as integrally linked to organisational learning: knowledge acquisition, information distribution, information interpretation and organisational memory. He clarifies that learning need not be conscious or intentional. Further, learning does not always increase the learner’s effectiveness, or even potential effectiveness. Moreover, learning need not result in observable changes in behaviour. An entity learns if, through its processing of information, the range of its potential behaviours is changed.

Senge⁵ defines organisational learning as the organisation “in which you cannot not learn because learning is so insinuated into the fabric of life”.⁶ In addition, it is “a group of people continually enhancing their capacity to create what they want to create”.⁷

Therefore, a full definition could be “an organisation with an ingrained philosophy for anticipating, reacting to and responding to change, complexity and uncertainty”.

The effects of a learning culture

- Flatter organisations result, leading to more trust and the empowerment of individuals within the new structures of the 21st century.
- Layers of management and speed in decision making and reaction time are not compatible. The survivors of the future will be able to manage the innovation and process of their organisation within a flat structure and streamlined decision-making process.
- Because of the peeling away of the layers and the empowerment of the individual, potential is unleashed. As people accept more responsibility and accountability, decision making becomes faster and more reliable because empowered individuals make the decisions closer to the point of output.
- With empowerment comes the honesty to examine plans and change strategies where applicable.

Outcome of a learning culture

This is the key to the success of the learning organisation. The outcome in fact is the conundrum of the future, as it adds stress to the decision-making process. Workers need to be educated to understand the potential impact. In essence, as cycle times reduce there is more opportunity to learn. Every cycle is a learning opportunity; with shorter cycle times, you have more chances to learn. In other words, reaction times are compressed, enabling individuals and organisations that embrace the learning culture to learn on a reduced timescale, thus adding value in shortening cycles.

Why?

The following are the outcomes for an organisation that effectively implements organisation learning:

- superior performance;
- competitive advantage;
- avoid a decline;
- improvement in quality outcomes;
- understand risk and diversity;
- innovation;
- increase ability to manage change;
- energised workforce;
- interdependence; and
- because time demands it.

The risk management learning organisation

- **Strategic:** Risk of plans failing.
- **Financial:** Risk of financial controls failing.

Risk Management

Today

- **Operational:** Risk of human error or omission and equipment failure.
- **Commercial:** Risk of business interruption.
- **Technical:** Risk of physical assets failing.

Conclusion

Simply put, survival is not ordained or even encouraged in today's competitive environment. It takes hard work, a good culture and an understanding of the true value of risk management within an organisational setting.



Michael Vincent,
*Senior Lecturer, Department of Accounting
and Finance,
Monash University,
Email: Michael.Vincent@monash.edu,
www.buseco.monash.edu.au.*

Footnotes

1. Argyris C, *On Organizational Learning*, Blackwell Publishers Ltd, Oxford, 1999.
2. Above note 1, p 159.
3. Above note 1, p 157.
4. Huber G P, "Organizational learning: the contributing processes and the literatures" (1991) 2 *Organization Science* 88–115.
5. Senge P M, *The Fifth Discipline: The Art and Practice of the Learning Organization*, Doubleday, New York, 1990.
6. Above note 5, p 9.
7. Above note 5, p 42.

A framework for IT controls

Dean Sleigh TABCORP and Devan Naidoo ECHO ENTERTAINMENT GROUP

Businesses are becoming increasingly reliant on IT to drive shareholder value and streamline business activities. While using IT presents a number of opportunities to a business, it is not without its problems.

In recent times, there have been a number of spectacular IT system failures. Amazingly, these have been more common or more widely published in industries that place a high degree of reliance on IT to conduct their business. Examples include an airline's booking system that was down for 11 days, causing a \$15–\$20 million impact on pre-tax profit, and let's not forget the numerous bank payment and ATM system failures that have occurred over the last 12 months.

No doubt the majority of these entities impacted by IT failures had lofty statements in their annual reports and on their websites outlining the detailed framework in place to identify and treat the risks of the organisation. The reality is that *rhetoric is the poor cousin to action*.

How did these problems occur? The simple answer is poor IT controls.

The extent of these and other IT failings has impacted the ability of corporations to conduct business, maintain credibility and satisfy customer needs.

These system failings also raise the question as to how management and directors can be assured that their IT systems and applications are robust and can withstand both internal and external stresses.

For entities operating in highly regulated sectors, such as gaming, significant focus exists to ensure that such IT failures do not occur, because if they do it could be disastrous for the operations of the business. Often for these companies, one factor that impacts their licence is the adequate operation and reliability of their IT systems.

Is there a silver bullet to prevent IT failures? The answer is "no". What is required is a commonsense approach with the right people focusing on the right things.

One element that is critical for success is a well-resourced and capable internal audit function. Also, simple testing and review go a long way in telling a story

and providing some real answers. However, it is more often the case that the resources given to the internal audit team and their capability are not sufficient. The consequence of this is that the internal audit function fails to gain the necessary depth and coverage in its work to provide the assurance that stakeholders demand.

What coverage is adequate and what should the role of internal audit be? Also, how can management help bridge the gap if internal audit resources are fully committed on other activities?

The role of internal audit

An appropriately resourced internal audit team should have an annual audit plan that requires all major risks to be considered.

Latent in this is the need to review IT applications and key elements of IT infrastructure. In relation to IT applications, a high-performing internal audit team should be resourced and capable of conducting IT general controls (IT GC) testing against each and every critical IT application that the organisation relies upon to operate the business.

For nimble organisations, this population will be relatively small — perhaps up to 20 applications. For large diverse organisations with multiple lines of business, it would not be uncommon to have more than 100 applications (or separate instances) used across the business.

The scope of IT GC is not new and has been well defined over time. What is new is the risk associated with individual system failure and the growing proliferation of systems across organisations. The audit response needs to keep pace with this growth while not seeking to review each and every application. The risk of failure of a particular application needs to be assessed in order to determine the specific IT applications to be focused on.

Table 1 provides a simple summary of the scope of IT GC.

Risk Management

Today

Table 1: The scope of IT GC

Basic IT controls	Extended IT controls (examples)
Security and access <ul style="list-style-type: none"> • physical security • logical security • access rules and segregation of duties • environmental 	Performance and capacity Service desk and incident management Data management Third-party services IT continuity
Change management <ul style="list-style-type: none"> • authorisation and approval • testing • migration and implementation 	
Computer operations <ul style="list-style-type: none"> • job processing • backups and restoration • incident management 	

While Table 1 might suggest that a large amount of work is involved, for a well-organised IT audit team the extent of testing and disruption to management is far less than you would think. Based upon our experience, we estimate that each application should take less than 10 days to test — hardly an onerous commitment when considered against the possible cost to the business if one of these applications fails.

Management (both business and IT management) should easily be able to provide the evidence that is required to pass IT GC. It should be working to a standard well above basic IT GC compliance. Often, while management says it is doing this, testing reveals otherwise.

Experience indicates that the most common areas of weakness when testing IT GC are:

- systems access (password configuration and lack of user access reviews);
- change and release management controls; and
- backup and recovery processes.

It is also common to find issues relating to the maturity of processes for availability and capacity management, patching and virus management.

Regrettably, the ability of many IT audit teams to clearly articulate these weaknesses is compromised through reports that are overly technical and/or complex. In our experience, a simple summary chart outlining pass or fail criteria is a more effective way to present findings to management. An example is depicted in Table 2.

Table 2: Sample report summary chart

IT process	Security and access								Change management					Operations		
IT control	Information security policy	User creation and modification	User termination	Configuration of access rules	Password Configuration	Duplicate accounts	Review of accounts	Privileged users	Authorisation and approval	Testing	Migration of changes	Configuration changes	Emergency changes	Job processing	Backups and restoration	Incident management
App 1	✓	✓	✓	✓	✓	✓	x	x	✓	✓	✓	✓	✓	x	x	✓
App 2	✓	✓	✓	✓	✓	✓	x	x	✓	✓	✓	✓	✓	x	x	✓
App 3	✓	✓	✓	✓	✓	✓	x	x	✓	✓	✓	✓	✓	x	x	✓
App 4	✓	✓	✓	✓	x	✓	x	x	✓	✓	✓	✓	✓	x	x	✓
App 5	✓	✓	✓	✓	x	✓	x	x	✓	✓	✓	✓	✓	✓	x	✓

How can management help bridge the gap?

Management has far greater knowledge and intimacy regarding the systems than does the IT audit team. Management also has prime responsibility for ensuring that the risk appetite is being satisfied as it applies to IT applications.

The first contribution management can make is to recognise the need for IT GC to be the minimum standard. Building and enforcing policies to ensure that IT GC is met is a tangible way of demonstrating such commitment.

In simple environments, this can be easily achieved. In complex environments with multiple applications and often large elements outsourced, this requires active engagement and clear expectation setting with the outsource providers.

Many organisations outsource some part of their IT operations to third-party providers and rely on Statement of Auditing Standards No 70 (SAS 70) reports to provide assurance over IT controls for the outsourced services. The passive receipt of SAS 70 style comfort letters is often insufficient, as these are often unclear regarding:

- exactly what was tested — the controls selected and the extent of testing for the control objective may be insufficient to provide the level of assurance required; and
- scope and coverage — SAS 70 reports often cover multiple organisations and therefore it is important to understand if the same level of controls is applied by the third-party provider over your organisation's IT systems.

The second contribution management can make is to actively expect relevant members in management teams to accept that they have a role to play in IT GC. This emphasis can be used to push down the importance of IT

GC to those best placed to ensure it is met, and gives those team members the opportunity to spend the time required to ensure it is met. Many IT organisations have adopted elements of the COBIT maturity model¹ to assess the current state and define the target maturity level for IT controls. COBIT also provides a common language and can be mapped to international standards such as ITIL and ISO 27000.

When properly articulated, we have not seen a business owner argue against IT GC as being important!

The third thing management can do to support broader adoption of IT GC across the organisation is to reduce the expectation on external audit. The focus of external audit is on the financial statements. This responsibility will rarely extend to testing for IT GC across every major application; it may only extend to testing the key financial systems, and even this is not always clear. Reliance on external audit in relation to broad IT GC assurance is not wise.

The last thing management can do to support an improved environment is to advocate that internal audit has a comprehensive program of work to review IT GC for each material application. This advocacy may require a long-term commitment, but the rewards via a better-controlled environment and broader understanding of IT GC across the business will be well worth the effort.

Conclusion

As we increase our reliance on IT applications to execute everyday transactions, it is critical that we continue to evolve the control environment of the organisation. The rapid growth in customer-facing and customer-impacting applications is actually making the IT environment more complex and fragile.

To support managing these risks better, management needs to recognise the need to meet minimum control standards and internal audit needs to develop agile but comprehensive testing approaches covering all major applications.

Risk Management

Today



Dean Sleight,
Chief Audit Executive, Tabcorp,
Email: sleighd@tabcorp.com.au,
www.tabcorp.com.au;
and



Devan Naidoo,
Head of Audit, Echo Entertainment Group
Limited,
Email: Devan.Naidoo@echoent.com.au,
echoent.com.

Footnotes

1. COBIT is an IT governance framework and supporting toolset created by the Information Systems Audit and Control Association (ISACA); see www.isaca.org.

Freezer risk management

Harry Rosenthal REGIS AND PARTNERS

The role of research has never been greater in the Australian university sector. In many ways, “research activity” not only is defining the individual academic staff working in our sector, but also is used to describe the institutions themselves. This rush for research has significantly changed the landscape of the higher education sector and has affected the risk profile of our institutions.

For many years, freezer losses have been viewed as an operational risk issue, which the university addresses using standard procedures and processes. With the increasingly strategic importance of research, we are discovering that the tools of research are becoming increasingly significant. This article reviews the recent trends regarding the storage and losses of research materials in temperature-controlled environments, focusing on freezers and cool rooms. The purpose of the article is to highlight that what once was an operational issue increasingly has strategic impacts, and should be viewed as a priority by both risk professionals and senior managers.

An age of research intensity

It is truly a wonderful time to be working in the university sector; we have a front-row seat to one of the most transformative periods in history. For example, over the past 100 years, our life span has been extended by a factor of one-third, there are reduced infant mortality rates across the planet, and we have successfully eradicated some diseases that plagued our species for thousands of years. By many measures, we enjoy a quality of life that no previous generation could imagine, much less hope to experience, and we have every right to believe that such enhancements to the condition of our species will continue. The incubators of these improvements will, no doubt, be located on the grounds of the universities. This future will be accomplished by a growing number of professional researchers. As a matter of fact, the majority of all scientists who ever lived are alive today. It’s an amazing time, when vast financial and educational resources are being dedicated to research and the media is full of research-related articles. This future will be delivered by a better-educated workforce (with 40% of 24–35-year-old Australians having a tertiary degree by 2025) and will be key to sustaining the momentum of the past 20 years of

steady economic growth in Australia. Prominent researchers are even recognised in popular culture, winning awards such as Australian of the Year. Albert Einstein was *Time* magazine’s “Person of the Century for the 20th Century”, in spite of the fact that he did not play for any major sporting team at any point in his distinguished career.

Research activity is also shaping the face of education. It has succeeded in redefining universities, shifting our mission from creating “well-rounded citizens” to creating research engines that are designed to churn out intellectual property and innovation at an increased rate. The Australian university sector fervently believes that research will create the magnets for money, top students, and reputational fame and glory.

Finally, research is a cash cow par excellence. It’s a large, relatively predictable revenue fountain, which some sector senior managers feel they can control. Research revenues contribute to the financial viability of our universities. We see “increase in research quantum” as a key strategic goal and a common key performance indicator for Australian universities. Research cash flows are often used as barometers of university strength and self-identity. Is the research funding pie limitless, or is it a zero sum game?

The changing landscape

There are familiar changes in the wind regarding research funding. The global financial crisis continues to ripple across the economies of the Western world, and once-leading countries in scientific research are re-examining their commitment and their ability to deliver on academic-based research. The latest Organisation for Economic Co-operation and Development (OECD) data shows that both Australia and the United Kingdom spend less than the OECD average on science and technology as a percentage of gross domestic product.¹ We hear today clear signals that the UK and Australian governments are examining significant cuts to government-funded research. In Australia, this will affect future funding of both Australian Research Council (ARC) and National Health and Medical Research Council (NHMRC) grants. It is anticipated that over \$400 million may be cut over the next three years, as our government attempts to reduce the troubling budget deficit created by spending related to recovery from the global financial crisis. How

Risk Management

Today

will this impact our vision of the future? As less NHMRC funding is available, there will be lower success rates for general science and medical researchers. If we use simple models, at current funding levels the average researcher has a one-in-four chance of getting their project funded (to some extent); with the cuts, this is expected to reduce to one-in-six. The result will be increased time generating funding applications, less time for research (and teaching), and increased research frustration and discord. This will be characterised by more institutions chasing fewer research dollars. There will be winners and losers, but who would work for a loser?

Is this view too bleak? Not really. We have seen this in the recent past where, in the United States, funding changes to the National Science Foundation (NSF) resulted in years of “yo-yo” research funding, with budgets going up and down dramatically. Currently, a US researcher has a one-in-10 chance of getting NSF funding; as a result, there are many American accents on Australian university campuses. For Australia, this was regarded as a good thing, but if NHMRC and ARC budgets begin to yo-yo, other foreign universities will enjoy hearing Aussie accents in their hallways as much as we enjoyed hearing American accents in ours. There are 11 countries that the OECD reports have a greater domestic expenditure on science and research than Australia, not to mention the non-OECD countries. The past also illustrated that this trend most greatly impacts early-career researchers, who are only now building a research profile. These are the future of Australian university research capacity, and they comprise a segment of university staff that we can ill afford to lose.

Where would they go? At this time, both Singapore and China are offering significant incentives for foreign researchers to relocate. The siren call of new, purpose-built lab facilities, coupled with attractive wages, will prove hard to resist as Australian universities continue in financially austere times. They will prove to be the venues of the future, where our unsuccessful NHMRC grant applicants will go to get over their disappointment of not being awarded Australian grants.

Freezer and cool-room risk connection

So what does this have to do with freezer losses? A great deal, as there is a strong connection between operational losses, such as freezer and cool-room failures, and diminished research capability and reputation. Research reputation is a top strategic risk at most Australian universities. Senior managers believe that an increased research profile is key to their institution’s strategic destiny. In response to this view, across the sector, universities are gearing up for increased research capability. New labs are sprouting up like mushrooms,

as universities are enjoying an unprecedented growth in lab building. Unimutual, the sector’s largest risk financing entity, is aware of a single institution with over \$700 million in new research-related construction projects over the next three years. Many of these facilities contain wet labs, including physical containment (PC) PC2 to PC3 facilities, and are being built to achieve a strategic research-related goal. Operational losses to these structures can impact achieving such goals, and the need to reduce these operational losses is increasingly important as intense competition is inflating the “cost of getting it wrong”. As risk professionals, our work is relevant to both the operational and the strategic objectives of our universities, and there are few places where the nexus of operational and strategic meet more often than in the management of loss related to research freezers.

The challenge for risk and insurance today

If research capability is a key strategic pillar of our organisations, and we believe we play a role in assisting our universities achieve these objectives, then we must identify the significant perils we face. There’s little doubt that the two most significant ways to destroy research capability are to lose the services of key researchers, and to lose the key work itself. Temperature-controlled environment losses achieve the latter outcome, increasing the likelihood of the former coming to pass. In other words, a researcher losing years of research samples, specimens or other subjects of examination in a freezer loss may be more inclined to depart to an organisation with superior protection of its research assets. I make this point only to recognise that these losses of temperature-controlled environments are not issues only for facilities and maintenance divisions, insurance officers, procurement officers, IT staff, and so on, as currently viewed by those institutions taking a traditional siloed approach. Such losses impact the university on a number of levels, including HR (staff turnover), finance (increased risk-financing costs and costs to attract new researchers, as well as revenue stream interruptions), and the research office (“please explain” for delayed publications, grant applications, and so on). As these losses impact on so many levels of the university, perhaps it would be useful for risk and insurance professionals to approach this matter in a way that includes all these stakeholder groups, rather than as only a facilities or security issue. These apparent operational losses impact the strategic capability of the institution and, therefore, should be of concern to others, such as pro vice chancellor research, faculty deans, heads of schools, lab managers, researchers and others who have significant stakes in the strategic health of research in the institution.

Why is this important?

The problem of freezer losses will increase in the foreseeable future. The frequency of these losses, according to our data, indicates that the number of claims for freezer or cool-room spoilage is going up. While a disturbing trend, it is not completely unexpected, as our site reviews reveal that the number of temperature-controlled environments and devices is growing exponentially. This explosion of building on Australian campuses is resulting in rapid growth in freezer procurement, needed for the current or anticipated research. It is a challenge for our members to identify the number of freezers that they have on campus, but Unimutual's reviews indicate that a large percentage of freezers in the sector are not identified. Some members are undertaking a comprehensive freezer survey and discovering that up to 30% of the university's freezers were unknown before the review. This could mean that minimally managed maintenance systems are in place for a large percentage of freezers in the asset inventory.

In addition, our data indicates that the reported financial losses associated with freezers have increased to an average value of over \$300,000 per freezer. This is a considerable sum for the loss of one device with a replacement cost of around \$60,000. The drivers of this increase are unclear, but it may involve the growing awareness by researchers of the cost of placing all their eggs in one basket (or freezer) and the suddenness of losing all of the research samples, as well as the current and future financial impact of this loss. It also may be that the freezers have become key research instruments in themselves, storing chemicals, reagents and cell lines which in themselves are far more expensive than what was kept in cold storage in the past.

Whether there are greater values at risk or simply a greater appreciation of the values at risk, the insurance industry has noted this increase in average freezer loss costs and is taking corrective actions. Some insurers have introduced very specific requirements for indemnification, including back-to-base alarms and maintenance contracts. Without these, cover is denied. Others have introduced sublimits, which restrict the level of cover available unless the client can demonstrate that they are reporting freezer numbers and values accurately. Many universities are conducting freezer surveys to provide better underwriting information for their insurers, and they are discovering that the values which lie in freezers are significant. Individual freezers with contents valued at over \$1 million are becoming commonplace, and we are aware of a single freezer that has a reported contents value of \$6 million. We see in the United States, for example, that freezer claims are rare, but this is due to most universities taking higher excess

levels and betting on the effectiveness of their risk management program. There is some logic to this, as the vast majority of freezer losses are due to preventable causes that lend themselves very well to risk management programs.

Common contributions to freezer losses

Examining the records of the past six years of experience reveals numerous causes of freezer loss. Most losses can be placed into specific categories, such as the failure of monitoring systems, extended power failures, mechanical breakdowns, the actions or negligence of people, and the failure of maintenance programs.

- The failure of monitoring systems can include communications failures or an internal alarm that measures temperature extremes in only one direction. For example, many temperature alarms are designed to engage when the temperature in the monitored freezer becomes too warm; however, they will not act if the temperature in the monitored freezer becomes too cold.
- Extended power failures are one of the most significant causes of freezer loss. Interruptions in power occur with greater frequency as demands for power on university campuses increase and storms grow in frequency and intensity. Almost all universities experience a period of either short-term or long-term mains power loss, often as a result of construction or contractors on site. The failure of freezers to reactivate or to be reset after a power failure is a common source of freezer contents loss, and one which is highly preventable. Reliability of power sources is a key risk, well known and recognised to risk professionals; however, it still results in significant freezer losses to the sector every year.
- Mechanical breakdowns are also common occurrences and common causes of freezer loss. There is anecdotal evidence to indicate that mechanical failures of freezers are occurring at an increasing rate, and that the life expectancy of these devices has reduced from 30 years to around 10 years for today's newer models. Perhaps many readers still have refrigerators at home that were given to them as wedding gifts many years ago; however, the complexity and reliability of modern refrigeration units have resulted in a shorter life expectancy. This means that plans should be in place to repair or replace these units under a regular scheduled program, but many universities do not have such a program in place. Instead, new units are obtained as old units experience costly mechanical failures.

Risk Management

Today

The increasing incidence of failure of older machines can clearly be anticipated and replaced without resorting to significant research interruptions and loss of freezer contents to act as a trigger for upgrades.

- Actions of people include a wide variety of behaviour, including negligence, such as leaving freezer doors open or accidentally using lab emergency switches to turn off lights, or vandalism, where disgruntled employees use the destruction of research samples as a way to retaliate for some perceived injustice. Other significant loss-causing behaviours include failing to respond to temperature alarms and intentionally unplugging the freezer in order to use its power point for another device (such as a vacuum cleaner), resulting in an intentional compromise of the integrity of the freezer unit. Poor work practices, lack of adequate supervision, and a failure to understand the importance of research freezers result in people taking actions that compromise temperature-controlled environments and result in the loss of valuable research.
- The failure of maintenance programs also results in frequent losses, either through maintenance conducted by unskilled technicians or through irregular maintenance schedules that overall compromise the efficiency of temperature-controlled units. The maintenance of modern research freezers is a speciality skill and is generally conducted by a contractor. In many cases, universities have suffered losses due to research stored in freezers belonging to, and maintained by, a hosting agency, such as a hospital or institute. The failure to engage trained technicians has resulted in several losses of university research samples and unclear recovery actions due to relationships with the host organisation.

Final recommendations

Risk professionals are skilled people. Over the years, our profession has developed extensive skills in the identification, mitigation and management of risks faced by our organisations. There are standards, operating procedures, analyses and investigations which, as a result, have provided the risk profession with much insight into the management of university risk. For example, major sources of property loss, such as fires or building collapse, which still occur, are much less prominent than they were years ago. We have developed extremely good skills in operational loss prevention, and as a result fewer employees are injured or die at work than was the case in the past.

Common sources of operational risk are better controlled now than at any time in the past, which is a credit

to our discipline and illustrates that we have been successful in learning from the past. It is my view, however, that the track record of our discipline in managing strategic risks is less distinguished. There is much debate among insurance and risk professionals about whether we have a role to play in the management of strategic risks and, even if we do have the skills to contribute, whether senior staff will seek our assistance in the identification and management of these risks.

I could explore many of the operational risk mitigation approaches that are common in the university sector to address this matter of freezer and cool-room losses; however, it is not the intention of this article to be as granular. There is little doubt that, using our arsenal of operational risk treatments, the frequency and severity of freezer losses will be reduced. This approach, while possibly effective, fails to note the systemic issue of strategic risk identification and whole-of-university engagement that will be required to address this issue at the macro level, making freezer/cool-room risk management as much a part of the institutional research culture as are lab safety and the use of the scientific method.

I encourage all readers to take both an operational and a strategic approach to this issue, as a two-pronged approach will ensure that adequate resources are allocated. A peril facing a strategic objective of the university will be regarded as being far more important than is a perceived day-to-day operational issue. The operational approach is the reason frequent post-loss investigations into freezer losses result in reports where one business unit blames another business unit for not doing its job properly. Strategic losses are often the result of high-level systems failures and should command senior management concern and attention. To keep this issue operational is to fly below the radar of senior management and possible cultural change.

So, what are some risk actions we can take to ensure that the strategic dimension of this problem is as well recognised as the operational? Some recommendations are as follows.

- **Freezer inventory:** Whether a requirement of your insurer, mutual or other risk-financing organisation, it is important to know the extent of your exposure to freezer and cool-room loss. We know that “that which is not measured is not managed”, and there is great power in promoting risk management actions to researchers if they realise the value and criticality of their temperature-control assets and inventory. Nothing focuses one’s attention more than \$1 million worth of assets sitting in the hallway which no one has responsibility to maintain.

- **Business continuity planning (BCP):** Freezer/cool-room losses can be minimised with adequate BCP. Most universities are currently examining their BCP capabilities, and insurance and risk professionals should ensure that temperature-critical assets are included in such contingency planning so that research capability is not compromised as a result of cooling device failure.
- **Alarms:** As discussed above, many risk underwriters will either exclude or greatly reduce indemnification amounts for devices that are not alarmed. Our examinations indicate that the number of unalarmed temperature-controlled devices in newly constructed labs is astounding, and this is a practice that we must work to eliminate. It is mindboggling that a university can spend \$24 million for a new set of laboratories, but have no funds remaining to attach freezer alarms to building maintenance systems (BMSs). The attachment of temperature-controlled environments to a university's BMSs should become part of the original building fit-out plans and costs, as are fire panels and exit signs. They should not be viewed as after-construction modifications, which are left to the lab owner to pick up in their operational costs. Experience has shown that these lab owners can ill afford a cost of \$100 to \$300 per unit to attach the freezer to a BMS. As a result, there is little effective monitoring in place.
- **Share the news:** Establish the loss of research items as a category of reported loss to audit and risk committees. Research items should be incorporated into the committee's risk dashboard and reviewed on a regular basis. As discussed, research capabilities are a strategic objective, and the management of risks that imperil such significant key objectives should be reported to those with ownership of the strategic risk profile of the university.

In summary, freezer losses are more than simply an operational irritation which we must endure and try to manage when time allows. It is an increasingly frequent and expensive class of public asset loss. Many of us, by virtue of the roles we play in our employment, have a professional obligation to reduce the financial impact to our institutions, and those who fund them, by reducing the frequency and severity of these events. For some of us, it is our jobs. While saving universities money is in itself a worthwhile endeavour, as illustrated above, freezer and cool-room losses can seriously have strategic impacts on our institutions. Losses to these assets can change the course of research in a way that affects strategic goals and objectives. As risk professionals, the more effective we are at aligning our loss control programs with these strategic objectives, the quicker we will receive the resources we require and the recognition we deserve in order to deliver the risk management culture our universities need to realise their planned futures.



Harry Rosenthal,
General Manager, Risk Management Services,
Regis and Partners,
Email: harry.rosenthal@rmml.com,
www.regisandpartners.com.

Regis and Partners are managers of Unimutual Limited.

Footnotes

1. OECD, *OECD Factbook 2010: Economic, Environmental and Social Statistics*, OECD Publishing, June 2010.

8th Annual Risk Management Conference 2011
The building blocks of Risk Management:
Assessment, embedding & implementation
9 August 2011, Pre-conference workshops
10 – 11 August 2011, Two-day program
The Grace Hotel, Sydney

Register Today!
Visit: www.lexisnexis.com.au/pd

Program highlights

- Risk culture, cloud computing, social media
- Risk appetite and tolerance – dispelling the myths

Speakers

- Simon Sproule, Fraud Risk Manager, Singtel Optus
- David Drummond, National Partner in Tax Risk Management Services, KPMG
- Tip Huizenga, Group Manager OE & Risk, Caltex

Endorsed by:



Product of:



Risk Management

Today

EDITOR: Michelle Nichols 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: michelle.nichols@lexisnexis.com.au.

ISSN 1448-3009 Print Post Approved: PP 349181/00244. This publication may be cited as (2011) Issue 11 ARM.

This newsletter is intended to keep readers abreast of current developments in the field of risk management. It is not, however, to be used or relied upon as a substitute for professional advice. Before acting on any matter in the area, readers should discuss matters with their own professional advisers. This publication is copyright. Except as permitted under the *Copyright Act 1968* (Cth), no part of this publication may be reproduced by any process, electronic or otherwise, without the specific written permission of the copyright owner. Neither may information be stored electronically in any form whatsoever without such permission. Inquiries should be addressed to the publishers.

Printed in Australia © 2011 Reed International Books Australia Pty Limited trading as LexisNexis ABN: 70 001 002 357