Risk Management Today

2014 . Vol 24 No 4

Contents

Information contained in this newsletter is current as at May 2014

LexisNexis Butterworths

General Editor's note

Harry Rosenthal *REGIS MUTUAL MANAGEMENT*

In issue 24(3) of *Risk Management Today*, I reviewed the merits of recent developments in higher education, including the first generation of free, public access, online university courses. This resource is widely available to assist in the ongoing professional development of risk managers. One of the examples cited regarded a technology called massive open online courses (MOOCs), which features university courses designed and conducted by numerous universities across the globe, delivered by a distance learning tool accessible to all via the internet. Recently, I saw that the University of New South Wales had released its first MOOC, which had 20,000 students enrolled. There are currently thousands of courses to be found in the MOOC environment, and all can be accessed via companies operating as higher education content aggregators, providing a consistent format for the delivery of these diverse university distance learning opportunities. To participate in a MOOC, you need not be registered with any university, only with the MOOC aggregator, which provides access to the courses, free of charge, 24 hours a day. As I mentioned in the earlier article, I believe that this is one of the greatest innovations in higher education in a very long time. It has made access to university-quality material and knowledge open to all with access to the internet.

An example I cited concerned my experience while participating in a course run by the University of Pittsburgh on the education platform Coursera. The subject of the course was disaster preparedness, and it was my first foray into the world of MOOCS. I did not know what to expect, but was delighted with the overall experience. While the program did have its drawbacks, engaging in a higher education experience online, at the time of my choosing, was much more painless than anticipated.

My primary interest in test driving a MOOC was based upon a common complaint of risk managers: "lack of time for professional development". Many risk professionals tell me that they recognise the need to keep developing as professionals; however, they do not have the time to engage in any type of formal or structured educational programs. They blame busy work schedules, travel and work–life balance. Others report that they attempt to remain current by reading blogs, online newsletters or professional journals. All lead busy work and private lives, leaving very little spare time for structured education. I was interested in whether the inherent flexibility of MOOCs held an opportunity for the risk professional to continue building their credentials in a higher education context. As a result of my experience, I reported about this universe of free online education and how it is an efficient and effective method for risk professionals to sharpen their skills through ongoing professional development.

On a personal note, I also recalled one of the more poignant memories of the course. It regarded an online discussion forum where a US obstetrician reflected on his firsthand experiences while working in a hospital, responding to a disaster caused by Hurricane Sandy in October 2012. As many readers will know, this was the second-most-expensive storm to strike North America, with damage estimates currently around US$68 billion. Only Hurricane Katrina's damage bill of US$81 billion was greater. The exchange reminded me that there is more to a disaster than numbers. This particular forum was about not the financial outcomes but rather the personal costs and impacts of the storm on this individual responder, who was providing emergency medical care following Hurricane Sandy's landfall. He recounted the many long hours following the aftermath of the storm and its impact on him and his family.

While a good story, and one from which we took away many lessons, it reminded me of another exchange which occurred later in the course, during another online discussion forum, which I feel is also worthy of note.

For many who work in the field of emergency preparation and management, the story of Memorial Hospital in New Orleans during Hurricane Katrina is a well-known and often-cited incident. As well as being a topic of discussion regarding critical institutional response to a disaster and the legal liability for decisions made, the hospital's experience has been used as a case study for higher education programs on disaster response topics. It featured as a case study in the MOOC and led to interesting class discussions.

For those readers not familiar with the Memorial Hospital incident, it regarded a large metropolitan hospital located in New Orleans. The hospital was inundated when a levee was breached by Hurricane Katrina, driving floodwaters through much of the city. Memorial suddenly found itself in a classic disaster nightmare situation. To those of us who've lived in New Orleans, the Ochsner Baptist Medical Center is a well-known and long-established medical complex located in the uptown section of the city. Through a series of mergers with other hospitals, by the mid-1990s it was transformed from a not-for-profit medical institution to a for-profit entity, purchased by Tenant Healthcare and renamed Memorial Hospital. The original Baptist Hospital building itself was a city landmark, dating from the 1920s. It was a highly regarded, if not loved, focal point for medical treatment and research for the uptown community over many years.

The hospital gained international recognition as a result of Hurricane Katrina, which struck New Orleans on Monday, 29 August 2005, resulting in substantial damage, loss of life and widespread flooding. That much is known by most risk professionals. The hospital itself occupied one of the inland sea areas created by floodwaters, completely cut off from the rest of the city. As a result, with water entering the lower levels of the building where the emergency generators were housed, there was no electricity, no working utilities and no sanitation for several days. With inside temperatures reaching as high as 43 degrees Celsius, by Wednesday, the decision was made to evacuate the hospital and abandon the location. Several other hospitals in the city were also being abandoned at the same time, affecting over 2000 patients.

While all this sounds quite standard, the story of Memorial Hospital took an unanticipated twist. After the evacuation was completed, it was discovered that 45 patients had died on the premises, just prior to or during Katrina. Post mortem examinations on these Memorial patients indicated than many had unusually high levels of morphine and other drugs in their systems, which may have contributed to or caused their deaths. It was reported that many of the patients died in a short period of time. It was suspected by authorities that the patients were euthanised by members of hospital staff, prior to the scheduled evacuation via boat and helicopter. A protracted series of investigations and legal actions was undertaken, although no prosecutions resulted. However, there has always been a strong suspicion that hospital staff made the decision to conduct their own emergency triage and decided to terminate patients who, it was believed, would not survive the evacuation.

Over nine years later, this remains a very controversial case, with opposing views on what might have happened at the hospital in response to the disaster. I encourage interested readers to research the case for themselves. While examining the case during the MOOC, we discovered that one of the participants had worked in a hospital that was afflicted by remarkably similar circumstances to those experienced by Memorial. This class participant was a physician in the Philippines during the recent Typhoon Haiyan, and was dispatched to a hospital which, like Memorial, was isolated, had no electricity or utilities, and had a growing patient load. His situation analysis was summarised as follows:

> The events at the Memorial Hospital following the impact of Hurricane Katrina in New Orleans in 2005 is [sic] very tragic for me, being a part of our government's response efforts in the Eastern Vizayas Regional Medical Center (EVRMC) in Tacloban City following the onslaught of Typhoon Yolanda [Haiyan], I cannot but help draw from what I experienced and learned there …

While he went on to make many analytical points about the Memorial experience and his own, the most significant regarded his view of the clear lack of command and control systems in place to adequately prepare for the likely event of a severe storm. He stated:

> There doesn't seem to be a real hospital incident command system in place. Had they established one, with immediate action plans and hourly meetings, this would have ensured that all needs and actions were known to the incident commander and emergency management authorities. In Tacloban, the EVRMC was in the dark and with very little food and supplies for more than a week. They had no power for days, they were severely undermanned. They intubated in the dark with penlights and headlamps and manually bagged patients with the help of their relatives or volunteers. When we got there on the second week, there were still no working ventilators, suction machines, and defibrillators. Our doctors and nurses battled codes with meds and fluids and lots of chest compressions. When the generators were up and running, we had ECG machines printing strips in place of heart monitors during codes. We knew it was a losing battle and lost many patients, but we never gave up. How could we when the patients were still fighting to live even in those hot, stinking, dark conditions? How can we not when the doctors and nurses, most of whom were there from Day 1, were still in the fight?

For the class, this was a very vivid description of the scene, which helped us understand the challenges that staff at Memorial as well as at EVRMC had to endure. The difficulty of the response was brought home to all of us, across the globe, when our classmate revealed that the responders had paid a personal price as well. One of his fellow doctors had suffered a heart attack the day following their return from the tour of duty in the crippled hospital. He blamed the disaster for this loss and explained it this way to the class:

> We worked there for 10 days and he [the physician who suffered the fatal heart attack] was heard on several occasions to keep repeating in our dialect that we are

> responders, we have to be strong! It didn't occur to us until after his death that he might have been feeling something wrong then because he was always in good spirits even when tired. He fought hard to save lives, he did not leave the helpless behind or leave until the job's done. I like to think that I did too and will continue to do the same.

In summary, for me an unexpected and additional power of the MOOC method of education, aside from price and schedule flexibility, is that a well-run MOOC can put you in the picture of some of the most significant events of recent times, because it can connect you with eyewitnesses and participants to those events. To the risk professional, this is particularly valuable, as by the time many of these disaster reports reach our journals or online resources, they have been stripped of much of their human elements. Being aware of the human elements surrounding a large-scale disaster helps us as risk professionals in several ways.

First, it connects us with the greater global community. The global community is of growing importance to the risk professional, and should be developed and cultivated. The days of us being 100% focused on our own organisations is long over; we are much more interconnected today. Global MOOCs are a good way to align and introduce people with similar interests and skills.

Second, putting a human face on disasters should motivate us to perform our roles better, as we better understand the human impact of the incident under review. Often, we are very clear about the financial or economic prices that we pay in disasters, but are less aware of the social, cultural and human prices that we pay following a large loss. It's far more than numbers. Part of our professional motivation to improve our organisation's skills in disaster loss prevention should be to minimise not only the financial impact, but also the social and community impacts. These human stories keep us informed of those impacts.

Finally, being literate in the stories of eyewitnesses and those who were part of emergency response provides us with a better platform for ongoing risk communication. Humans are hardwired to love stories, and can more easily relate to the lessons and implications of events that are relayed in a narrative or story format. Such accounts of actual loss events have much greater impact than statistical or scientific reports. As we are constantly communicating with our stakeholders on the need for improved disaster and continuity planning, such stories are powerful tools in our arsenals. They promote improved risk cultures and help us motivate our stakeholders to buy into the programs we are developing.

I encourage all risk professionals to examine the world of MOOCs and other online education opportunities for themselves. Done well, and approached with the right attitude, they can assist the risk professional in remaining current and competitive in today's market and can provide the type of development that our profession requires. I wish you good studying.

Harry Rosenthal
General Manager, Risk Management Services
Regis Mutual Management
harry.rosenthal@rmml.com

Risk is risk — what's in a name? Or: Risk is risk — let's bring it together!

Greg Bolton *GOVERNANCE, RISK AND COMPLIANCE PROFESSIONAL*

Risk is risk

How many times have you heard the terms business continuity management (BCM), business continuity plan (BCP) and business continuity planning? All are terms used extensively by business continuity (BC) consultants and practitioners and they are terms that perpetuate the disassociation of BCM from risk management. This disassociation was recently highlighted by a client that was attempting to provide evidence of compliance with a complex piece of counter-terrorism legislation that required input from a range of disparate sources, including risk, physical security, emergency management and BCM disciplines. Problematic? Yes. Fixable? Yes, by adhering to some basic guidance and tips.

If you keep asking for what you have always asked for from a risk perspective, you will continue to get the same inferior results — fragmented outcomes, inefficiencies, ineffective controls and resource wastage through lack of control optimisation.

This article intends to highlight the criticality of a holistic risk management framework approach that meets business needs and provides the ability to manage all risks, including those that will disrupt the operations of the business.

Through the use of best practice principles, industry Standards and practical examples, my aim is to broaden your understanding and application of disruption-related risk.

Inconsistency of approach

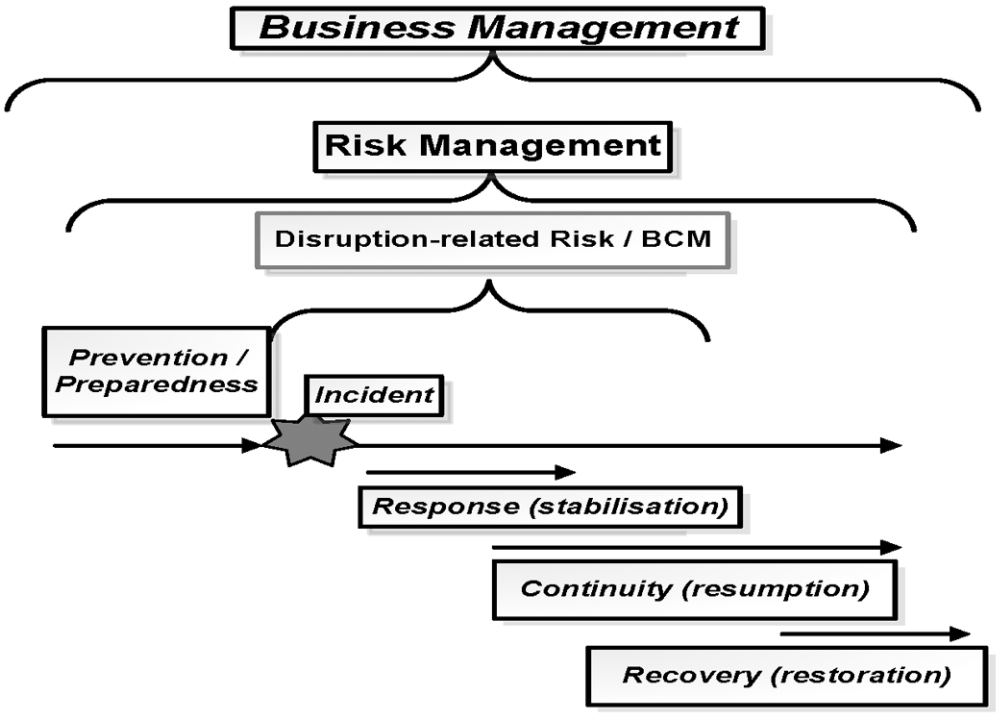
Safety, environment, security, BCM and project risk are all a subset of risk and they need to be managed under a common risk management framework with consistent processes that recognise and preserve discreet differences. Managing different areas of risk in a non-integrated manner does not make sense. It is inefficient and will result in missed opportunities.

The Business Continuity Institute (BCI) rightly points out that BCM is most effective when it exists in a *tightly bound interrelationship* with risk management. Reinforcing this are key elements from the *BCI Good Practice Guidelines* 2010 that state:

- BCM does not exist in a vacuum;
- it is necessary to determine where the application of BCM will bring value and how it fits in with other activities; and
- aspects of BCM have always been present in organisations, but under different names.

Figure 1 shows where BCM fits into the broader management disciplines — that is, a definite subset of risk management and, more broadly, business management.

Figure 1: Management/Discipline relationship



Note the linkage with the Emergency Management Australia (EMA) methodology, the Comprehensive Approach, also known as PPRR — prevention, preparedness, response and recovery. All stages of the PPRR methodology work closely together and cannot be treated in isolation of each other. Often, the outputs of an element are the inputs to the subsequent element. Note the strong requirement for integration, sequencing and feedback.

Risk is about doing the most with the available resources where this is most needed. Essentially, risk management is a resource optimisation activity with a key emphasis on controls — that is, the enablers (positives), the things that will facilitate success, and the achievement of organisational objectives.

It's all about the control environment

As outlined in AS/NZS 5050 *BC — Management of disruption-related risk*, treatment of disruption-related risk should be considered in terms of each of the organisation's risk criteria and requirements. For disruption-related risks, treatment options (controls) fall into the following two broad categories, both of which must be considered:

- proactive approaches involving prevention and protection measures that will influence the likelihood and scale of potentially disruptive events — that is, building resistance (robustness and hardening of assets and processes); and
- preventing or minimising operational impacts by either or some combination of:
  - — building contingent capability through the elimination or modification of the organisation's vulnerability to potentially disruptive events, such as increasing reliability, inbuilt flexibility of processes, contract terms and conditions, cross-skilling, and diversification of particular supplier dependencies; and
  - — developing contingency plans, such as disruption risk recovery plans and BC plans that stabilise the situation, continue critical functions and expedite restoration of normality in a timely and efficient manner — such plans may include communication with stakeholders, workarounds, and temporary reallocation of management responsibilities.

This systematic approach to control options highlights the importance of an integrated control environment with both breadth (variety) and depth (redundancy).

A clear indication of little knowledge on BCM is where the complete focus in on a BCP. A BCP is one of many controls. When developed and managed in isolation, it is meaningless and does not manage the risk effectively. It is *not just about having a plan* as shelf ware!

The bow-tie risk assessment technique (see fig 2) is a practical representation of a holistic risk control environment centred on a hazardous event. Managing controls separately and in isolation of each other is counterproductive, narrow in approach, inefficient and ineffective.

Figure 2: Risk bow-tie

Preventative, detective and mitigating controls equal a balancing act based on *context*. It is best to work from left to right in determining the optimum control environment, though it is often not possible or practical to have a balanced spread across the control continuum. Depending on the risk, context and changing circumstances, the distribution and focus of controls may vary greatly across the spectrum of preventative, detective and mitigating controls.

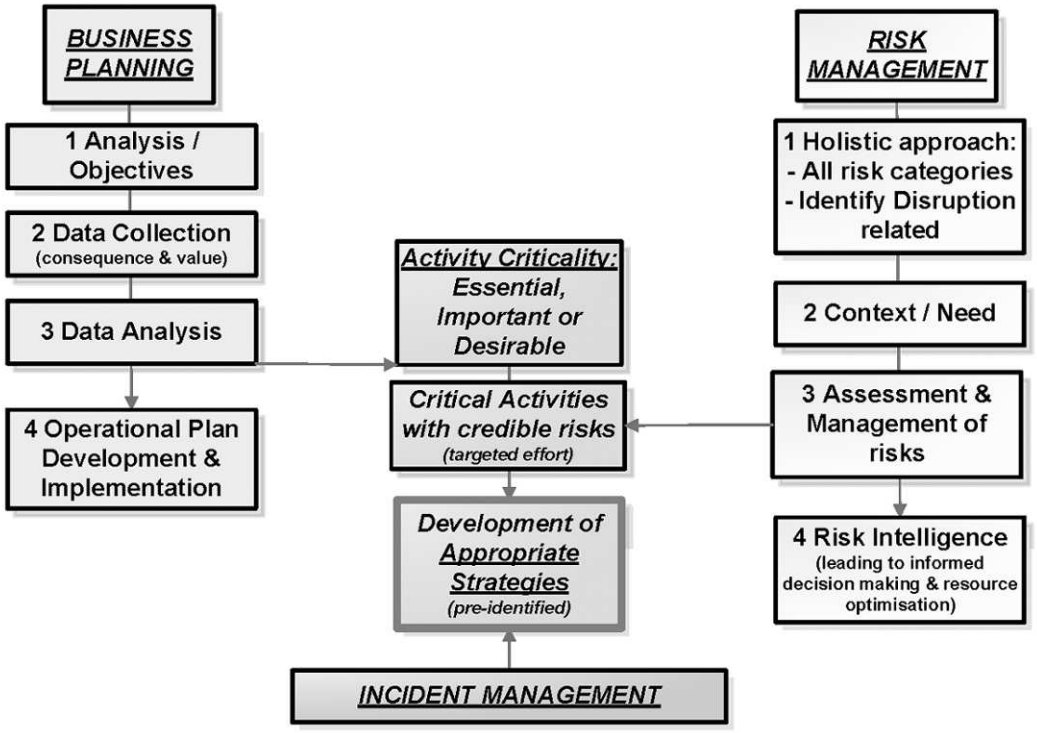
A key theme discussed earlier is the concept of control optimisation and where best to invest in controls from a BCM perspective — that is, essential business processes that are the most critical.

Business criticality

Business process criticality has always been a difficult question with very little literature or guidance available. It has always been problematic, as managers often view their business areas through rose-coloured glasses and think they are more important than others.

Integration of various disciplines — including business planning, risk, and incident management — provides the basis for a sound and logical answer to business criticality. See fig 3.

Figure 3: Business criticality



How do we determine the business criticality of a business process? Consider what would happen if the process were to stop. Ask the following key questions.

- Will it impact on core operational activities?
- Will staff/customers/public be injured or killed?
- Will the organisation be unable to meet contractual or legal obligations or requirements?
- Will it result in a loss of, or otherwise affect, accreditation or a licence to operate?
- Is it time critical — for example, what is the maximum acceptable outage?

Top tips for the management of disruption-related risk

- **Cherry pick:** When developing an integrated risk management framework, select what works for the organisation (it's all about context) from a variety of authoritative sources.
- **Get ahead of the game:** Early detection (slow-burn and fast-burn events) is essential.
- **The sum of the whole is greater than the individual parts:** Integration with other disciplines (sometimes by stealth) is important, including business planning, risk management and incident management.
- **Call a spade a spade:** Do not give false hope (assurance) — for example, do not portray that a BC plan will provide something that it will not in terms of capability, time to implement or sustainability
- **Pigeon pair:** Do not look at metrics in isolation — for example, maximum acceptable outage (MAO) must be assessed against recovery time objective (RTO).
- **Bend with the wind:** Develop workforce flexibility and business activity flexibility.
- **Don't make the same mistake twice:** Learn (have a process) from disruptions and focus on continual improvement.
- **Think with the end in mind:** Restore to a higher, more resilient state or fade away.

How do I commence the journey?

I am often asked how to commence this journey of building risk capability. As a starting point, I offer the following simple key actions.

- **Structure for success:** Understand the key linkages between management disciplines and structure the organisation accordingly — for example,

do not have risk practitioners and BCM practitioners functionally in different locations of the business. Risk is risk.

- **Use precise terms precisely:** Consistency of terminology drives understanding and application. Drive awareness across the business and ensure that a common language is being used.
- **Communicate, communicate, communicate:** Ensure that key internal stakeholders know who you are and what you do, and vice versa. This is particularly critical in large complex organisations where understanding those touch points/linkages is critical for success. Alternatively, run the risk of obscurity.
- **No register, no risk:** Ensure that all risks are managed in a risk register to facilitate targeted effort, awareness and effective management.

Organisation examples

Several real-world risk examples where a practical approach is applied to the management of disruption-related risk and their application within a heavy industry environment are outlined below.

Incident management capability

- Holistically, incident management includes incident, emergency, crisis and disaster management. Incident management mitigates most non-business-as-usual events. Having a readily adaptable capability is critical. Many resource organisations adopt this approach with tiered layers of incident management teams that seamlessly integrate together, able to respond to and manage a spectrum of scenarios. Again, flexibility in response highlights that planning is more important than plans — that is, the ability to bring the right people together quickly and to plan effectively.
- Incident management is particularly effective when it is designed and applied in line with the EMA methodology — all hazards approach. This approach concerns arrangements for managing the large range of possible effects of risks and incidents, regardless of source. As highlighted by a recent PWC Report,[1] an integrated incident management capability is becoming increasingly important in the management of BC. The ability to effortlessly move between and manage different stages of the PPRR methodology is present in more mature organisations — such as Qantas — in their management of events.

Doing nothing is a viable strategy

- At times, there is little if anything that can be done after the event has occurred. For example, consider a logistics/transportation organisation that moves high-volume commodities. When a disruption occurs and the primary means of transportation is not useable, the main effort is aimed at restoration of the affected assets as quickly as possible. There is often no viable resumption/continuity strategy that can be put in place in the interim.
- This approach highlights the importance of preventative and detective controls in managing the risk. Subsequent to this, it is all about addressing the backlog after the event, mitigated by suitable insurance, flexibility in business processes, and ability to ramp up rapidly for a sustained period.

Disruption to a complex system

- There are many interrelated variables: no disruption to a complex system is exactly the same. Variables include location, time of day, environment/context, other operations, customer expectations, and so on. This challenge to difficult scenarios is almost a *wicked problem*[2] due to the complex interdependencies. It also highlights the importance of a strategy or series of strategies that form the basis of any response to a disruption.
- A strategy serves as a starting point, but would be refined and enhanced prior to implementation based on the nuances of the event that has occurred. Examples of suitable strategies that can be used in isolation, combined or in hybrid form are outlined in Table 1.

Table 1: Strategy options

Focus	Strategy
Risk management	• Increase preventative and detective management controls — improving robustness or hardness of the activity or resources via resistance strategies • Build redundancy through alternative or extra resources • Eliminate/Manage any single points of failure (SPOFs) • Proactive supply chain management • Proactive workforce planning — recruitment and retention • Active management of critical staff — succession planning
Restoration	• Shorten the period of disruption by concentrating efforts on restoration of the resource (as compared to resumption of activity)
Resumption	• Redirect or reallocate the work to another internal/external area that has not been affected • Modify business activity/processes (do it differently or to a lesser level) • Reallocation of workforce • Manual intervention • Distributed processing via built-in arrangements that allow activities and processes to be performed in a distributed environment • Reprioritisation of workload • Reciprocal arrangements in place with other similar organisations • Relocate to an alternate premises • Implement a work-from-home policy that has been suitably recorded and routinely practised • Use alternative equipment • Amend stock-holding policies
Transfer/Share	• Transfer the disruptive risk
Accept	• Accept the disruptive risk and do nothing
Avoid	• Terminate or suspend the service, activity or process

Summary

An integrated methodology to risk management — in particular, managing risks of a disruptive nature — facilitates a mature approach to the management of risk. Focusing on BCM issues separately adds little value and, in fact, introduces additional challenges and risks.

An integrated approach will also facilitate a more resilient organisation — that is, an organisation that has developed the capability and capacity to:

- anticipate and plan for risk events;
- survive;
- adapt and thrive in the context of a changing and complex environment.

In adopting this integrated approach, I am suggesting that it is about *integration, not consolidation*, where differences are preserved, nuances are encouraged and all things work together. As long as we continue to do the same risk activities the same way, we will continue to get the same results. This is not optimal in a world of increasingly uncertainty in which there is a need to demonstrate due diligence.

Gregory Bolton
Governance, Risk and Compliance Professional
gmbolton@gmail.com

About the author

Gregory Bolton is accredited as a CPRM, MBCI and AACI. He is an active participant in a range of forums as both a speaker and a facilitator. Greg is also a sessional lecturer in risk management at Griffith University.

Footnotes

1. PricewaterhouseCoopers *Business Continuity Management 2022: Where We've Been; Where We're Going* March 2013, available at www.pwc.com.
2. A problem that is difficult or impossible to solve because of incomplete, contradictory and changing requirements that are often hard to recognise. The term "wicked" is used not in the sense of evil, but rather resistance to resolution.

What is the cost of feeling safe?

Adam Byrne *PROFESSIONAL SECURITY CONSULTANTS*

As we all recognise, the security industry is at its heart a service industry. Therefore, as you would expect, service quality and customer service are at the core of a successful client-provider relationship. Yet, in managing security risk and in consulting to clients looking for me to assist in managing theirs, the one question that is always asked first is this: How much will this cost me?

It is, more often than not, the case that decisions regarding the management of security risk are based on the lowest bid without considering service quality and therefore customer service.

Security is a big industry and is full of liabilities, yet so many of us continue to insist on budget as the defining consideration.

Whenever this conversation comes up, I ask my client what they expect from my service, and then what they are prepared to pay for feeling safe.

As a consultant, I recognise the reality that price can be a primary driver. In some cases, this is entirely appropriate.

If, for instance, a client exists in a low-risk environment — perhaps an industry with few criticalities and vulnerabilities, as well as little in terms of human or high-value assets that require protection — then I recommend they consider price as the most significant factor when assessing a request for quotation (RFQ) or request for tender (RFT).

That said, many clients have a limited understanding of the security environment that they exist in. Many spend only the bare minimum on security without any real thought to the value of quality equipment and how a properly trained and inducted team can benefit their organisational resilience. Their main focus is understandably on the core operations of their business. Security services are, at times, a necessary evil.

This is a perennial problem and is more acute in those countries in which the industry is not regulated at the government level.

Recently, I was asked by a client to conduct a security audit on their facilities. As part of the audit, I produced a report on the security cost of the facility and overall benefits/negatives of in-house versus outsourced security services.

Once completed, I drafted recruitment, training and ongoing-training requirements for both options of security services. One was cheaper but had limitations and risks for the client's business, while the other was more expensive but better suited to the client's needs.

The report assisted the client in recognising the probative value found in a professional service, that the lowest price is not the most useful indicator in assessing security tenders, and that a more qualitative assessment is needed.

Jan Carlzon, the former CEO of Scandinavian Airlines (SAS), stated in his book *Moments of Truth*: "We have 50,000 moments of truth every day." This was said at the start of the First Wave seminars to turn SAS around in 1982. Carlzon was referring to every time an employee of the company came into contact with a customer.

Relating this back to my clients, I often remind them that when a visitor arrives, the first person who meets them will be their security. It is this first impression — or moment of truth — that gives the visitor a lasting impression. Most importantly, with this in mind, while considering a low bid for services is fine, this does not mean that the cheapest bid ought to be accepted.

Most businesses are reluctant to spend money on a "non-revenue-generating" service and therefore commonly take a "we won't spend the money unless something happens" attitude.

Of course, such attitudes are short-sighted, given that it is security that so often protects the business from losses while ensuring the safety of staff and clients, as well as ensuring the integrity of intellectual property and reputation.

This said, competing with a superior service is most difficult in government, where value for money in a competitive environment has primacy.

Many of my clients who occupy security leadership roles in government bemoan the need to show fiscal responsibility through the correct management of taxpayer dollars and the consequences of having to justify why a better service at a higher cost was chosen over a cheaper service.

Here are the three main points why the lowest price often wins.

- **The client:** I'm not a security expert, but security is one of my responsibilities. What is really the risk? Nothing has happened ever, so why take security risk seriously?

- **The guard:** I'm on an average hourly rate, and I'm often not inspired or embraced in terms of psychology, emotion, career outcome, importance or value. Why would I do anything other than the bare minimum?
- **The guarding company:** My clients mostly focus on price, despite the quality service we provide. Is price so important? Why can't I seem to get clients to at least acknowledge that a quality service is worth spending more on?

It may well be that while we are good at selling the product, we fail at selling the message.

What I read recently in a blog was the need for "commercial cultural awareness communications of the view of those specialists in the security and protection industry".

Service is something that most businesses — even government — value as important. It can't be quantified, even if service is poor or it opens the door to danger or a continuity breach. If a client's business or reputation is not being given the proper service it deserves, then their own clients may not return.

There are many factors that can detract from or impact on the success of a business or government operation.

And it is the provision of a below-standard security guard force, chosen simply on price with no regard to service quality, that really is at the top of the list.

Adam Byrne
Director
Professional Security Consultants
adam@professionalsecurity.net.au

About the author

Adam Byrne is the Director of Campus Safety & Security at the University of Western Sydney. He has over 20 years of operational experience in law enforcement, security risk management and organisational resilience planning. A former Sergeant with the NSW Police Force and MBA qualified, Adam is a Sir Maurice Byers Fellow and an alumnus of Harvard University's Crisis Leadership in Higher Education Program.

Risk management in a world of dynamism of risks

Joshua Corrigan *MILLIMAN,* ***John Evans*** *AUSTRALIAN SCHOOL OF BUSINESS, UNSW and* ***Amandha Ganegoda*** *ANZ BANK GROUP*

In the previous issue of *Risk Management Today*,[1] we presented the case that all risks exist simultaneously in the three states of known, unknown and unknowable (KuU). We argued that to be effective, a risk management system needs to explicitly recognise the proportion of risks in each state. The question then arises, how do you design a risk management process that implicitly recognises this situation?

Historically, and mainly driven by regulatory compliance issues rather than business management, risk management in institutions has focused on quantitative modelling to assess capital requirements for particular levels of required survival of the institution.

The typical risk management process involved:

- risk identification;
- quantification;
- risk mitigation;
- provisioning of capital for net risks;
- monitoring and reporting, and management of risk events; and
- regular review of risks and risk mitigation.

Through quantitative modelling of historical events — whether taken from internal or external sources — implicitly it is being assumed that whatever weighting existed between the known, unknown and unknowable risks will continue in the future. Given the dynamics of most institutions, and the environment in which business operates, this is not a realistic assumption and can lead to not only misstatement of the risks, but also failure to ensure that appropriate risk mitigation is put into place.

If it is explicitly recognised that dynamism of risks exists, then for business management purposes the allocation of capital to the various risks needs to explicitly recognise how much exposure the institution has to known risks, unknown risks and unknowable risks. Regular review of the exposure to these states will then ensure that appropriate risk mitigation is in place, whether it be through risk transfer, risk monitoring or risk management.

By explicitly recognising the simultaneous existence of the various risk states, the business is able to understand what part of the risks it is reasonably comfortable with — that is, it knows the dynamics of risk through expertise, through experience or from historic observations; it can reliably transfer whatever part is required; and it can be confident of the internal processes to detect and manage the events as they occur. The business is also then able to explicitly recognise the exposure to that part of the risks that it doesn't have sufficient knowledge of, and thus concentrate on the appropriate form of risk mitigation, such as through risk transfer and/or seeking expert opinion to assist it in understanding and enhancing risk monitoring processes for any retained risks.

The explicit recognition of the simultaneous existence of the various risk states also brings into focus the possibility of exposure to possible unknowable events that exist through contract wording, enabling the risk to be appropriately managed to the extent possible. The other major unknowable risk exposure is to political and other external events, such as deliberate sabotage. While this is difficult to manage, at least the approach to risk recognition can highlight the possible exposure through focus group analysis, and management through lobbying can be an effective risk mitigation approach for political risk.

The recognition of the simultaneous existence of all three states of risk also assists with their assessment. By explicitly recognising the business processes where the business is reasonably comfortable with its knowledge of the risk events that could occur, quantitative modelling is then going to be more reliable by excluding processes where the business was less certain as to the risk events that could occur. While this approach may assist with more reliable models for known risks, it does not lead to more reliable models for the unknown risks, which by definition have risk events that the business cannot define or describe with any certainty. Quantitative modelling also is effectively useless for unknowable events.

The consequence of recognising the simultaneous existence of all three states of risk is that an alternative method of determining the risk events and the exposure

to them is required. The approach that fits best is to identify the processes historically where the business was comfortable with the identification of risk events, and the processes where it was not. Then it is necessary to identify the underlying causes, or "drivers", of each event, and to look for patterns in these drivers across time for both the known and unknown risk types. By identifying the causal drivers, the risk event identification process can then be changed to concentrate on detecting if one or more of these drivers exists, and implementing appropriate risk mitigation.

The risk management process then becomes:

- establishment of the business risk tolerance;
- identification of risk;
- identification of historical risk event drivers separately for known, unknown and unknowable risk events;
- identification of risk drivers and their emergent dynamics over time;
- risk event mitigation;
- assessment of remaining risks and establishment of appropriate capital to achieve risk tolerance;
- monitoring and management of risk events;
- review of emergent risk driver properties for input into scenario and stress testing; and
- review of exposure to known, unknown and unknowable risk events.

This process will then explicitly identify risk state exposure, allowing concentration on the management of those risks in the unknown category in particular, and also identifying where the quantitative modelling to achieve the risk tolerance of the business is going to be weakest.

An example of the "driver" approach is found in Neil Allen and Josh Corrigan's paper submitted to the Actuaries Institute Summit in May 2013.[2] The authors analysed the drivers for major operational risk events occurring over the past 10 years. Using phylogenetics, they were able to identify drivers that were common across several events which, if they reoccurred, should cause concern and lead to mitigation measures being put in place risk to avoid a further occurrence.

The process for identifying drivers of risk events is part art and part science. Being subjective, it requires constant review to ensure that the mapping process adopted between recorded causes of risk events and identification of the major drivers of risk events reflects the evolving nature of the causal drivers of risk.

"Driver" analysis of risks is also not appropriate for unknowable risks, but a similar process can be implemented through scenario analysis where the process involves a backward identification of drivers. This process requires an analysis of historical unknowable events, and an analysis of the drivers that lead to that event. By identifying these unknowable risk event drivers, business can begin to understand how these events build up — they are rarely, with the benefit of hindsight, single-driver events. This approach is also usable to identify some of the drivers for political risk.

A commitment to undertaking a driver approach to risk event analysis and prediction is not trivial. It requires a significant change in the culture of the risk management approach and the management of risks, but it does offer a sustainable basis that has eluded quantitative modelling-based methodologies to date.

By way of illustration of this process, take the case of a large diversified financial institution with a wealth management operation that has been selling relatively unsophisticated products to the retail market for some time. This institution decides for competitive reasons to introduce a hedge fund product with investment processes spread across the range of possibilities from long-short/market neutral to event-driven and arbitrage strategies. The risk drivers for this type of business are:

- failure to recruit adequately qualified sales and investment management staff;
- failure to train staff adequately;
- failure to align remuneration with required behaviour;
- failure to specify an appropriate asset management strategy;
- failure to understand changes occurring in the relevant capital markets;
- failure to understand the education standard of buyers; and
- failure to understand political issues involved.

These risk drivers can then lead to the following risk events:

- fraud;
- miss-selling;
- back-office errors; and
- breaches of regulatory requirements.

All of these can lead to:

- loss of capital;
- loss of operating licence; and
- reputational damage to the entire group.

Given that the institution has been operating for some time in the asset management industry selling relatively unsophisticated products, it is reasonable to assume that it has a good idea of what risk events can occur based upon past experience. It is likely that it has an established process to mitigate these risk events through insurance, staff selection and training processes, and internal audit and risk management analysis. Essentially, the business is operating in the "known" state. It is comfortable with its knowledge of the business risks involved, and thus the risk tolerance is acceptable.

But the introduction of the more sophisticated products creates a whole new unknown risk state that exists alongside the known risk state. Application of any quantitative modelling that was applicable to the known state is not going to be reliable for the emerging risks. The institution is facing the situation where it cannot be comfortable that it is staying within its risk tolerance. Simultaneously, unknowable risks continue to exist.

While the institution may well be comfortable with the risks inherent in the current wealth management business, at some stage even this business would have been in the unknown state. Analysis of the drivers that created risk events at that time will be instructive in assisting with identifying drivers for this emerging unknown state, which in turn will assist the business to direct resources for monitoring and mitigation of the emerging risks. It is, however, more art than science, as the environment will have changed. This needs to be recognised in deciding appropriate drivers to be cognisant of in the current situation. Diligence is required to see if there is any new behaviour emerging that has not been seen before.

The simple recognition of heightened risk through moving to an unknown state should in itself be valuable in alerting the institution to at least be aware that the risk tolerance of this area of business has increased and needs greater attention to manage it to within acceptable levels. It should also alert the institution to the fact that while the drivers for unknowable events may be vague, this risk state has also increased — particularly for the political and regulatory consequences of extreme unacceptable behaviour.

Without a driver approach, moving into new business activities will increase the risk of a business and by indeterminable levels, which is clearly unacceptable in a modern risk management environment.

Joshua Corrigan
Principal
Milliman
Joshua.corrigan@milliman.com

About the author
Joshua Corrigan leads Milliman's risk management services across the Asia Pacific region. He is a specialist in enterprise risk management, spanning a wide range of geographies and industries including insurance, banking and wealth management.

Joshua is a Fellow of both the Actuaries Institute of Australia and the Institute and Faculty of Actuaries in the United Kingdom, as well as being a CFA Institute Charterholder and a Chartered Enterprise Risk Actuary. He is an active contributor to the actuarial and risk professions, authoring numerous research papers, regularly speaking at conferences, and volunteering his time for professional committees such as the Actuaries Institute's Risk Management Practice Committee, which he chairs.

John Evans
Associate Professor
Australian School of Business
University of New South Wales
john.evans@unsw.edu.au

About the author
John Evans is Associate Professor in the Australian School of Business at the University of New South Wales, Chairman of Emerging Leaders Investment Ltd, and Chairman of several Risk and Compliance Committees for financial institutions. He was previously a Guardian of the New Zealand Superannuation Fund and consulted to several industry superannuation funds.

John lectures on risk management at both the Australian Business School and the Australian Graduate School of Management.

Dr Amandha Ganegoda
Operational Risk Manager
ANZ Banking Group
amandha@unswalumni.com

About the author

Dr Amandha Ganegoda is an Operational Risk Manager at the ANZ Banking Group, where he is currently working with a team of risk experts to develop a new operational risk capital model for the bank. Prior to joining ANZ, Amandha was a lecturer and a research assistant at the School of Actuarial Studies, University of New South Wales. He has many years of research experience in modelling financial risk, particularly in the areas of operational risk and superannuation.

Footnotes

1. J Corrigan, J Evans and A Ganegoda "Dynamisms of risks and their risk management implications" (2013) 36 *Risk Management Today* 316.
2. N Allen and J Corrigan "Emerging risk assessment — latest practice and innovations" paper presented to the Actuaries Institute Summit, May 2013.

How well do risk assessments inform decision-makers?

Chris Peace *RISK MANAGEMENT LTD*

Sometimes, it seems that every newspaper edition, news broadcast or news website carries yet another story about a disaster of some sort — an event that might have been avoided by better decision-making.

But do we ask whether such decisions were informed by risk assessments? And, if so, how effective were those risk assessments for informing the decision-makers about the risks? Which techniques were used in the risk assessments? Were the results presented in a way that made sense to the decision-makers? Do risk assessors follow a good process and so achieve some consistency in results, or do they just get lucky?

During the global financial crisis, questions were raised about the failures of risk management. Were there failures in how the risks were assessed? Were there any risk assessments at all? Were the decisions themselves faulty?

During the global financial crisis, questions were raised about the failures of risk management. Were there failures in how the risks were assessed? Were there any risk assessments at all? Were the decisions themselves faulty?

My research so far

A review of academic literature has found little research covering how well risk assessments informed decision-makers and — specifically — how decision-makers knew that they could rely on a risk assessment. There is some research touching on these questions, but it relates particularly to project management and software development. Yes, we have AS/NZS ISO 31000:2009, ISO 22301 and OHSAS 18001 — as well as the COSO enterprise risk management document, plus risk analysis documents — setting out guidance on how to carry out a risk assessment, but there seems to be little research investigating how, and how well, these work in practice. Do decision-makers get the information they need?

Similarly, there is some research covering risk techniques used in project risk management and IT risk management. At this point, you may say "But I use techniques A, B and C". The point is that there has been little research to find out which techniques are used by which groups of risk practitioners. Yes, we have an international standard IEC/ISO 31010:2010 *Risk management: risk assessment techniques* (now published in Australia and New Zealand as Handbook HB 89 Risk management: risk assessment techniques), which sets out 29 risk techniques, but my research has found more than double that number that are not in the standard (and you may know of and use still more).

So, questions arise. Do all risk assessments cover what ISO 31000:2009 calls the context? Do such risk assessments include risk criteria (or, for some practitioners, risk appetite)? Which techniques are used to decide with whom to communicate and consult?

And then there are the questions about risk assessment techniques. Which ones are actually used? About half the practitioners I meet use a mixture of professional judgment and some form of 5x5 consequence likelihood matrix. But my experience is limited, so what is actually being used in risk assessments?

The International Organization for Standardization is heading towards some commonality in the structure and language of management standards. By my count, there are 17 commonly used standards that relate to risk assessments and thus to decision-making. Who uses which ones?

Does it matter if we don't know who uses what? Perhaps not. But, if we don't know, how can standards-writers know which to include or exclude? How can educators and trainers know which to teach? And, perhaps most importantly, how can risk practitioners use the most appropriate techniques to gather the "best available information"?

You're probably a risk practitioner (such as a risk manager, emergency manager, risk adviser or safety practitioner), or a person who has to make decisions about or involving risk (such as a manager, director or insurance underwriter). I would really appreciate your help in answering some of my questions.

Help please!

You're invited to take part in a survey via which I aim to find some answers to these questions. The survey forms part of my postgraduate research. Approval to conduct this research has been granted by the Victoria University of Wellington Human Ethics Committee.

The survey is open to anyone whose work involves any part of decision-making, management or risk management. I hope you will find it professionally interesting and stimulating!

Your participation in the survey is voluntary and confidential. The survey should take about 20 minutes to complete. No information will be identifiable to an individual. **The survey closes on 31 May 2014.**

I hope to present the survey results at conferences. A working paper containing the results will be posted on the website of the Victoria University[1] or my professional website www.riskmgmt.co.nz.[2] I will also submit at least one paper for publication in an academic journal.

If you would like to contact me about this survey, please email me at christopher.peace@vuw.ac.nz.

I would really appreciate your participation. If you're ready to start, please follow this link: www.vuw.qualtrics.com.

Chris Peace
Principal Consultant
Risk Management Ltd
chris.peace@riskmgmt.co.nz

About the author

Chris Peace was born and educated in the United Kingdom. He has a BSc with Honours in Environmental Health and an MSc in Risk Management, both from Aston University, and is currently researching the effectiveness of risk assessments at Victoria University in Wellington.

Chris has gained wide experience as a consultant, risk manager and trainer in New Zealand, the United Kingdom, the United States and other countries. In 2003, he established Risk Management Ltd, an independent risk management consultancy. He taught risk management part-time at Massey University from 2007–2012.

Since 2007, Chris has been a member of the joint standards committee OB007, which wrote the original risk management standard and risk handbooks published by Standards Australia and Standards New Zealand. He now represents the New Zealand Institute of Safety Management on that committee and QR005 (dependability).

Footnotes

1. See www.victoria.ac.nz and follow the links to Research, then Working Papers.
2. See www.riskmgmt.co.nz.

The first four things: disaster volunteer

Steve Flohr *AUSTRALIAN BROADCASTING CORPORATION,* ***Chris Peace*** *RISKMANAGEMENT LTD and* ***Tony Harb*** *INCONSULT*

Editor's introduction

The media clearly know that disasters sell papers. Frequently, newscasts are filled with images of disasters unfolding across the planet, with footage of floods, fires, earthquakes, civil war and so on. It is natural that many watching these newscasts recognise that being a spectator to such events is not the only option. Never before in the history of mankind has information about events been so accessible. By using only our smartphones, we can become instantly aware of disaster events that occur in even the remotest corners of the planet. As a result, one of the unexpected outcomes of the convergence of easier transportation and increased knowledge is the growth in initiatives by individuals and newly created organisations in response to global events. No longer content to let global events be managed only by governments or professional agencies, it is now common for individuals to become personally involved in disaster relief and recovery. While many still contribute money to charities and relief organisations, an increasing number of individuals are flocking to volunteer with non-governmental organisations. Some are simply showing up at disaster sites, ready to work. Responding to disasters is becoming personal. Websites and organisations are rapidly growing to cater to this trend. In the future, this increase in global mobility and information technology could even affect our own organisation's ability to operate as normal.

The fictional case below is one such example. Inspired by good intent, a key person feels compelled to provide assistance in a very risky part of the planet. There are clear risks in this disaster response — to both the person and the employer. As usual, our panellists explain the first four things they would do when faced with this situation.

The case

You are the risk professional for a medium-sized financial services company located in Sydney. Your company services thousands of clients and is operated by a small but skilled team at the corporate headquarters. You learn that a large earthquake has struck off the coast of West Africa, resulting in a tsunami and shifting fault lines that cause substantial destruction to buildings, infrastructure and public institutions. The city of Abidjan, in the Côte d'Ivoire, was particularly hard hit by the disaster.

Later in the morning, after hearing about the disaster, your CEO comes into your office to seek your advice. Earlier in the day, Robert Hall, the chief actuary of your company, went to the CEO's office to inform her that he needed to leave immediately for Abidjan, as he is an active member of the disaster relief group Actuaries without Borders. Apparently, the Côte d'Ivoire is in immediate need of experienced actuaries and Robert, as an executive in this global volunteer relief organisation, must leave immediately for Abidjan to provide assistance and to help coordinate the response from Actuaries without Borders.

While supportive of providing assistance, the CEO is very concerned about letting Robert have leave at this time for a number of reasons. It is very close to the end of the annual reporting period and financial reports must be submitted to the regulator in the near future. Also, Robert is regarded as a key employee of the firm. If he should suffer a misadventure in his emergency volunteer role, the company would clearly suffer. Finally, she said that she believes that Robert was very insistent on going on this mission and might do so, even if it meant resigning from the company. She is concerned for her company, the welfare of Robert, the views of the regulator and, of course, the people of Abidjan. She is seeking advice and a course of action.

What are the first four things you would do?

Panellist 1: Stephen Flohr

They key theme for me is the risks and opportunities associated with corporate stewardship. The challenge is managing the tensions between protecting the interests of the business and stakeholders and the broader moral and social responsibility agenda of Robert and the mission by Actuaries without Borders.

The Collins English Dictionary (10th edn) defines stewardship as:

> … the position and duties of a steward, a person who acts as the surrogate of another or others, especially by managing property, financial affairs, estate; and the responsible overseeing and protection of something considered worth caring for and preserving …

Let's consider some of the more immediate risks associated with this business dilemma:

- penalties enforced by the regulator;
- the loss of client confidence;
- the temporary loss of Robert and his expertise; and
- the safety of Robert on the mission.

Then we should contemplate the longer-term risks;

- financial damage;
- legal action;
- loss of clients;
- loss of reputation; and
- the resignation of Robert and the loss of intellectual property.

Based upon the relatively common risks identified, let's now look at the current controls and potential treatments in order to find a reasonable and balanced outcome for all parties. This was a difficult case. As you will read, I have taken the liberty to make a few positive assumptions across the four key areas on which I focus my attention.

Protecting the business and its reputation

Based upon Robert's current and firm position, the practical option is to enter into immediate discussions with him to collectively find a way to manage the reporting workload. Discuss the obvious opportunity of working extra hours and weekends to finalise the reporting, or at least to have a strong draft for finalisation by others. Look towards settling on a challenging deadline.

If the extra work cannot be resourced internally, negotiate engaging an outside expert to complete the tasks and have the costs covered by Robert's salary during his planned absence. Use this as an opportunity to renegotiate Robert's contract to formally recognise his executive role in Actuaries without Borders and immediately implement any agreed arrangements moving forward with the business.

Communicate with key stakeholders

I would advise the CEO to develop an urgent communications strategy aimed at critical stakeholders, such as major clients and the regulator. An analysis of those likely to be most impacted by the situation will provide a good basis for a timely and factual liaison. The primary purpose is to seek agreement and authority to part or fully defer the reporting. The objective is to minimise noncompliance, the risk of any pecuniary penalty, and the loss of reputation from clients and the regulator.

It is important to seek support of stakeholders through transparent communications promoting the company's corporate social responsibility charter, the role of not-for-profit and non-government organisations such as Actuaries without Borders, and the significant role that Robert will perform on the mission.

Protecting Robert on the mission

Although it is assumed that Robert will be reasonably supported on the mission by Actuaries without Borders, the business working with Robert should also organise some additional safety nets not covered by the mission. The business needs to investigate the mission security, transport, logistics and medical conditions. It is important to ensure that Robert's health, safety and wellbeing are paramount, starting with assurance that he is provided with appropriate vaccinations and medical advice, along with confirmation that there are emergency evacuation and repatriation arrangements in place if things deteriorate on the mission.

Better governance

I would advise the CEO that this dilemma is also a genuine opportunity to improve governance and policy around the issues being managed. For example, I would recommend that the CEO create a corporate social responsibility charter that promotes the company's official support of Actuaries without Borders. Creating a positive culture through this potential alliance with Actuaries without Borders is essential. The company will promote strong business ethics and add strong reputational value to the business in the marketplace.

Steve Flohr
Manager
Australian Broadcasting Corporation (ABC) Business Continuity Management Program
flohr.stephen@abc.net.au

About the author

Steve Flohr is involved in preparing the ABC to best respond to and recover from any major business disruption event. The Business Continuity Management Program aims at building organisational resilience by integrating best practice in emergency coordination, crisis management and business recovery.

Prior to joining the ABC in 2005, Steve spent 15 years with the Australian Federal Police, where he performed a variety of operational and leadership roles in Sydney and Melbourne. During this period, Steve also undertook multi-jurisdictional assignments in the United States and Hong Kong. In 2001, he served with the United Nations Transitional Administration in East Timor as part of the international peace-keeping mandate. He performed a variety of policing command roles aimed at

maintaining law and order during the country's inaugural democratic election held in August 2001.

Steve holds a Masters in Business Management and postgraduate qualifications in Public Policy and Administration. He is also the Co-Chair of the Communications Sector Group under TISN and a member of the Critical Infrastructure Advisory Council.

Panellist 2: Chris Peace

I remember Abidjan — not because I've visited the place, but because 20 years ago I drank a beer called Mamba brewed there and exported to where I was working in the United States. I hope the brewery survived this earthquake (the beer is still made)!

Assuming that Robert will go to Abidjan, my first four things would be the following.

- Check how much work remains before the annual reports are ready. Is the chief actuary needed to complete that work?
- Confirm that the actuarial team really is capable of operating effectively in the absence of the chief actuary.
- Try to find a temporary actuary who can be hired on a short-term contract for three to six months, or a member of the team who could act as temporary chief actuary.
- Talk to our insurance brokers about the adequacy of our travel insurance for Robert (including medical evacuation cover) and life insurance should he die while away.

These suggest two proactive and two reactive risk treatments, along with an opportunity to review the functioning of the actuarial team.

Starting point

If I were the risk professional, the contingency planning would be based on an assessment of disruption-related risks. I use the definition of risk in AS/NZS ISO 31000 — "the effect of uncertainty on objectives". Combining the definition of disruption-related risk in AS/NZS 5050 — "risk arising from the possibility of disruptive events" — with this we get:

> Disruption-related risk is the "effect of uncertainty on objectives, arising from the possibility of disruptive events".

Uncertainty might be summarised as our imperfect knowledge about events, their consequences and the likelihood of the consequences, while objectives can be operational or strategic.

For me, as a consultant and researcher (and perhaps for many others), uncertainty is *the* big issue in risk management.

A financial services organisation must consider risks associated with its people — their interpersonal qualities, qualifications, reliability and so on — leading to uncertainty about achieving organisational objectives.

In this case, uncertainties abound, including the following.

- Did we know that Robert was a member of Actuaries without Borders?
- If not, why not? Ideally, all staff — especially senior managers — should register such interests to allow planning for such disruptions.
- What is Robert's time commitment to the recovery work?
- Are his vaccinations up to date? Abidjan is close to the equator and tropical diseases are a threat to health.
- What are his family commitments?

I turn now to my first four things and what they should mean, before discussing what to tell the CEO.

The outstanding work

A well-run financial services business (indeed, all businesses) should have timetabled the reporting cycle to allow for staff absences and other disruptions. In one of my jobs, we flowcharted a reporting process to debug it and so make more certain that we would be both accurate and on time. An effective manager should allow some breathing space to allow for report review after completion and before it is due.

Good contingency planning should include absence or loss of key people at such times.

Team functioning

A well-managed team should be able to function together without their leader (if not, how will they get by when he or she is on holiday or ill?). The functioning of such a critical team should be kept under independent review by HR and others. Do they always meet deadlines? Are they obviously cohesive and happy? What are our people-related leading and lagging indicators for the business as a whole and for each team?

Temporary actuary or team leader

The military approach to succession planning is admirable — there is always someone able to act in place of an officer or NCO. However, actuaries are often in short supply. Assuming that we only have one actuary, are we able to find an available actuary who can fill in?

If we have more than one, are they sufficiently experienced and will their temporary promotion cause any problems for the regulator or other stakeholders? Do they have the necessary leadership skills?

Insurance covers

If Robert is insistent on going, it might be reasonable to make sure that he has good travel insurance that will cover medical evacuation or other eventualities. Will the insurer require evidence that his vaccinations are up-to-date? Do we provide life insurance for him and, if so, who is the beneficiary?

In the given scenario, these matters would form part of our contingency plans developed before such an event.

What to tell the CEO

This outline covers what I should know or be able to find out in the next hour or so. Armed with that information, I could then give advice to the CEO.

What might that include?

If we're up-to-date with report preparation, the actuarial team can function for a few months in Robert's absence and the regulator would not be upset. Robert should be allowed to go.

If, however, his team is not functioning well and he could be replaced, this unreliability might be unacceptable, perhaps creating the opportunity to truly "let him go".

Assuming that we do want him back, instruct the insurance broker to ensure that the travel and life covers are okay, and make sure that Robert's vaccinations are up-to-date.

Finally, if he does go, perhaps he could bring back some of that beer. I'd love to drink it again!

Chris Peace
Principal Consultant
Risk Management Ltd
chris.peace@riskmgmt.co.nz

About the author

Chris Peace was born and educated in the United Kingdom. He has a BSc with Honours in Environmental Health and an MSc in Risk Management, both from Aston University, and is currently researching the effectiveness of risk assessments at Victoria University in Wellington.

Chris has gained wide experience as a consultant, risk manager and trainer in New Zealand, the United Kingdom, the United States and other countries. In 2003, he established Risk Management Ltd, an independent risk management consultancy. He taught risk management part-time at Massey University from 2007–2012.

Since 2007, Chris has been a member of the joint standards committee OB007, which wrote the original risk management standard and risk handbooks published by Standards Australia and Standards New Zealand. He now represents the New Zealand Institute of Safety Management on that committee and QR005 (dependability).

Panellist 3: Tony Harb

As the chief risk officer for this medium-sized financial services company (assume a general insurer), there are four things that immediately come to mind. I assume that Robert is passionate about his volunteering cause and that denial of leave would lead to an immediate and sudden resignation — a risk that is outside the organisation's risk appetite.

The CEO is typically a focused and driven individual who will request a four-point plan that can be implemented using available resources and that protects the organisation's "risk and value proposition".

Consider the organisation's succession plan and business continuity plan

An organisation that leaves itself exposed to key person risks is not managing its risks well. An insurance company that leaves itself exposed to key person risks is risking its insurance licence to operate and exist!

An effective succession plan and business continuity plan (BCP) ensures that an organisation is well prepared for the loss of a key employee, and hence is the first point to consider. These documents need to be reviewed and put into the context of the current situation.

Robert is the chief actuary and would be the appointed actuary. The appointed actuary role is not a negotiable or "nice to have" position. It is a key role in an insurance company and it's a legal requirement for all Australian licensed insurers under the Australian Prudential Regulation Authority (APRA) Prudential Standards and the Insurance Act 1973 (Cth).

Not surprisingly, the CEO regards Robert as a key employee of the firm. For this reason, Robert should be included in the organisation's recently completed succession plan and key person insurance policy.

Failure to provide reports to APRA on time could result in financial penalties, interventions by the regulator, and ultimately loss of the company's insurance licence. For this reason, the organisation's BCP should include strategies to respond to loss of key staff.

Implement key elements of the business continuity plan

While the organisation's succession plan should identify the key staff, alternative staff (successors), and draft strategies to retain and develop staff, it may not adequately help respond to the loss of key staff. The succession plan is mainly a "preventative control".

The BCP, on the other hand, is a "corrective control" because it would outline specific strategies to respond to the loss of key staff when it occurs. While Robert may not leave suddenly, the BCP can still be used to manage the transition from Robert to another chief actuary. The BCP response strategy would include:

- immediately notifying APRA, as honest, continuous communication builds trust and creditability — the regulator is an important stakeholder who must be reassured;
- identification and appointment of a new appointed actuary — this could be an internal appointment or a secondment via a specialist actuarial services firm;
- preparing formal documentation for the appointment of a new appointed actuary, including compliance with APRA's fit and proper requirements; and
- reviewing the current schedule of work, status and timeframes (ideally, the BCP would list the priorities of key activities and maximum acceptable outages (MAO) — it is critical that the activities continue to be performed and not reach the MAO levels, as this could result in a breach of APRA's reporting requirements).

Review the regulatory reporting timetable requiring actuarial involvement

I recommend that the CEO approves Robert's leave on the condition that Robert does not leave immediately, but provides two days of "handover" support to the incoming actuary.

If possible, the CEO should request that Robert be contactable in Abidjan for urgent matters and that he check his emails and confirm his welfare.

Robert would help draft a timetable and handover notes covering:

- key activities leading to annual report and regulatory reporting;
- status of activities to date, percentage completed and issues; and
- timeframes and deadlines.

Where timeframes cannot be achieved, it is important to notify the regulator early to seek a formal extension.

Develop a communication strategy to capitalise on the chief actuary's involvement

Most dark clouds have a silver lining. The secret is to be able to recognise the silver lining, which often takes some lateral thinking and out-of-the-box strategies. The trick is to capitalise on these opportunities while adequately addressing the risks. There is a potential for the CEO to turn this potentially risky event of losing a key staff member into an opportunity.

The organisation can work with Robert and Actuaries without Borders to help further promote the relief efforts in Abidjan. The organisation should:

- make a donation to Actuaries without Borders to support the relief effort;
- encourage staff, clients and service providers to donate to the relief efforts;
- consider implementing donation matching for staff and customers;
- establish a web page and social media presence (Twitter) to raise awareness of relief efforts; and
- tweet pictures and progress reports from Robert in Abidjan.

This strategy is a win, win, win:

- Robert would assist in the Abidjan relief efforts;
- Actuaries without Borders would see a benefit from increased financial donations or more volunteers; and
- the CEO and the insurance company would be seen as good corporate citizens for promoting the Abidjan relief efforts and supporting staff while, in addition, receiving regular progress reports from Robert will confirm his welfare and safety as well as provide opportunities for the CEO to contact him should there be any urgent matters that only Robert can help with.

Tony Harb
Managing Director
InConsult
tonyh@inconsult.com.au

About the author

Tony Harb, BBus, FCA, MBA, MIIA (Aust), is a highly respected risk management professional. He is Managing Director of InConsult, a specialist risk management, business continuity and audit firm. Tony is presenter of InConsult's YouTube program, "One Minute Risk Manager", and is Deputy Local Controller at NSW State Emergency Services.

EDITOR: Virginia Ginnane MANAGING EDITOR: Joanne Beckett 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: Virginia.Ginnane@lexisnexis.com.au.
ISSN 1448-3009 Print Post Approved: PP 349181/00244. This publication may be cited as (2014) 24(4) *ARM*.