RISKNZ

The sector body in NZ bringing together people and organisations managing risk.

RISKPOST

WEB
risknz.org.nz

POST
PO Box 5890, Wellington 6140

EMAIL
adminofficer@risknz.org.nz

RISKPOST DISCLAIMER

RiskPost is the newsletter of RiskNZ Incorporated. RiskPost welcomes contributions from members of RiskNZ. Any such contributions do not necessarily represent the views of RiskNZ as a whole, although from time to time RiskPost will publish items setting out the views of RiskNZ on a particular topic.

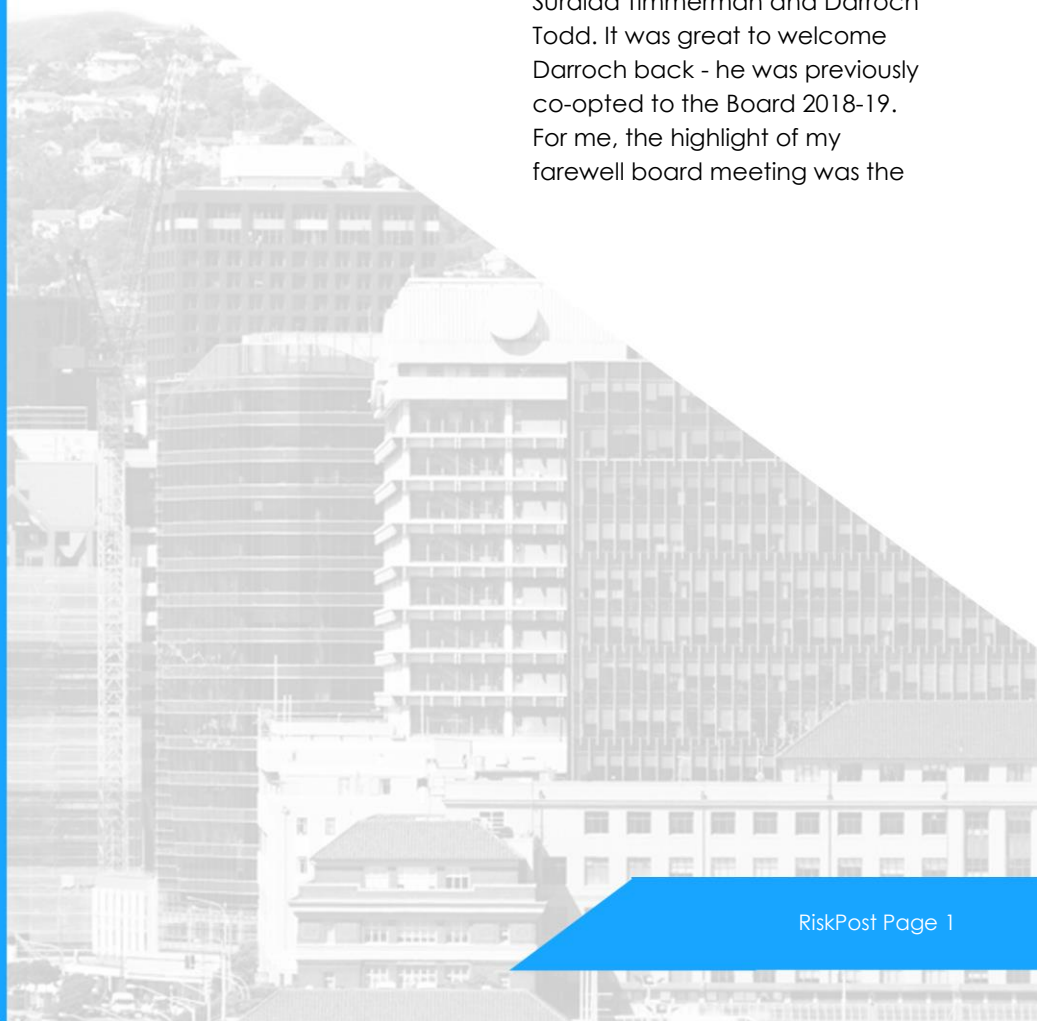
RiskPost gratefully acknowledges the support of our premier sponsor Marsh

A WORD FROM THE CHAIR

STEPHEN HUNT – *Exiting Chair, RiskNZ*

In November last year, I announced that I would not be standing for re-election to the Board in January 2021. After four years on the RiskNZ Board, two as Chair, I have decided to devote my attention to my new role of CEO MetService. On 25th March, at our annual post-election face-to-face board meeting where new board members are appointed, Kristin Hoskins and I left the Board. Kristin has served the Board and the members for RiskNZ over four years and in that position has been outstanding as the member responsible for representing RiskNZ on the Australia/New Zealand Standards Committee. Her work on developing Standard OB007 alongside many other standards projects, workshops and events has made sure our members are represented in this important area and are kept up-to-date over important industry developments. Kristin has kindly offered to continue representing RiskNZ in the Standards role as an ordinary individual member.

At the meeting we greeted the newly-elected board members; Chris Kumeroa, Lorna Hayward, Suralda Timmerman and Darroch Todd. It was great to welcome Darroch back - he was previously co-opted to the Board 2018-19. For me, the highlight of my farewell board meeting was the



A WORD FROM THE CHAIR CONTINUED…

appointment the new Board Officers for RiskNZ. I am absolutely delighted that RiskNZ will be led into 2021 and beyond by a fantastic and talented new team, and offer my warmest congratulation to:

- Jane Rollin, our new Chair
- Suralda Timmerman, our new Deputy Chair
- Lorna Hayward, our new Secretary
- Gary Taylor, our returning Treasurer.

It has certainly been a challenging year for our Society but thanks to the extraordinary work of our Managing Director, David Turner, our Admin Officer, Emily Thorpe, and the whole board, we are starting the year in a strong position of growth. The hard graft of 2021 is starting to deliver with our delayed conference in April, and an exciting rollout of new member products, services and events scheduled for the year ahead. There has never been a better time to join RiskNZ and the new Board is taking the hard work from the last year and are accelerating us into a highly successful future.

I have known Jane Rollin since we worked together in Christchurch in the aftermath of the 2011 earthquake. Jane and I joined the RiskNZ Board together back in 2017 and I know of no better person to be your Chair over the coming years.

STEPHEN HUNT

JANE RÖLLIN – Chair, RiskNZ

Stephen leaves the RiskNZ Board at a time where so much is about to start, it feels a bit mean to slide into the Chair role just as things get exciting! I'm so delighted to be the new Chair of the Board and really proud of what we have planned for this coming financial year, so while Stephen gets to reflect on a challenging year for us all, I get the joy of working with the Board on what comes next.

As you're reading this, we will have just held our RiskNZ "Reflect and Reconnect" Conference and Awards of Excellence. Congratulations to all our Award winners! It was great to see so many people at the conference and to be able to share insights from so many speakers. There was a time earlier this year that we wondered if we dare to plan an in-person conference - but re-connecting as risk professionals is important for us all to be stronger in the future. The challenges of last year have not gone away – so let's keep adapting!

We are really keen to hear from our members so we can check and adjust our plans for the next 12 months, so do feel free to reach out to connect or ask questions. I hope you enjoy this bumper edition of RiskPost, and do remember to check in on the members area of the RiskNZ website if you're looking for additional resources to help you.

JANE RÖLLIN

FROM THE EDITOR AND MANAGING DIRECTOR

DAVID TURNER

Hello everyone,

We have been listening to members' needs and wants across the past year, and we have been doing our best to achieve some of these expectations in 2021.

RiskNZ now have some initiatives coming together such as the launch of the first risk management and leadership courses from Bryan Whitefield and Mark Brewer, the launch of our members forum on the RiskNZ website (which needs your participation so we can get some good conversation and learning opportunities going), a growing membership base and LinkedIn profile which provides us with professionals to learn from and network with, and our RiskNZ conference presented by a range of experts throughout New Zealand and based on knowledge sharing and interactivity.
Please also look out for short workshops and webinars from our sponsors and partners which are planned for the second half of 2021.

We have also rebranded! So please look out for the new logo in future editions of RiskPost.

Now to our RiskPost articles:
A big thank you to all of our authors who have taken the time to contribute to this edition.

I am excited to share these articles with you. We have subjects from pandemic planning to the role of training in risk management so please enjoy!

In this edition:

BACK ISSUES OF RISKPOST

The RiskNZ website risknz.org.nz was updated in 2019, and the back issues of RiskPost are available in the members area of our website.

If you have forgotten your password for the members area then you can enter your email address to reset your password. If you do have problems logging on please email our admin officer at adminofficer@risknz.org.nz

LONG REFERENCE ARTICLES

We can publish reference papers in the members area of the RiskNZ website.

EDITION 2 OF RISKPOST 2021

Work on Edition 2 of RiskPost 2021 will start shortly with the aim to publish end July/August 2021

If you would like to submit an article, or update a historic RiskPost article, please get in touch editor@risknz.org.nz

Thank you!

DAVID TURNER

RISKNZ STANDARDS UPDATE

KRISTIN HOSKIN - *Advisian*

ISO meetings continue to be held online. Starting in March last year the decision was made that all the standards meetings would be held online. This has presented an increased accessibility for attending meetings and an increase in the number of meetings we have taken part in, although these are usually aligned to North American or European business days.

Publication Projects Update:

Comments on ISO DIS 31030 Managing Travel Risks were submitted from NZ and many other countries a few months ago, and the committee developing this for FDIS is currently working through those. If we remain on schedule comments consideration will be completed mid-April. Publication currently scheduled for late 2021.

- ISO WD 31050 Guidance for managing emerging risks to enhance resilience is expected to go out as CD version in a few months with an anticipated timeline extension for this project.
- ISO WD 31050-1 Managing Risk for Youth and School Trips is expected to hold its first meeting in April to begin work on this standard. Publication scheduled for late 2022.
- Previously ISO Guide 73 Vocabulary has been submitted for DIS as ISO WD 31073 Risk Management – Vocabulary.
- The ISO 31000 Guidance Handbook comments review was completed in February and submitted to ISO CS in early March is on track for publication in the second half of this year, possibly August.

Upcoming ISO Committee Meetings:

ISO TC 283 Occupational health and safety management is due to meet 4 May

ISO TC 262 Risk Management is due to meet 26, 28 May

ISO TC 314 Is Aging Societies is due to meet on 8 July

If you have any questions relating to risk standards, please contact me at kristin.hoskin@advisian.com

2021 RISKNZ AGM

Notice is hereby given to all RiskNZ Members that the RiskNZ Annual General Meeting for 2021 will be held on Tuesday 29 June.

All voting members are invited to submit motions for consideration by the Board, to the Secretary - secretary@risknz.org.nz by Monday 31 May.

A finalised agenda and associated documents will be issued at a later date.

Date: Tuesday 29 June
Time: 12:00 – 1:00pm

At this stage, the Annual General Meeting will be delivered by webinar, however, more information will be communicated.

Please feel free to contact:

- **Lorna Hayward, Secretary of RiskNZ - secretary@risknz.org.nz or**
- **Emily Thorn, Administration Officer - adminofficer@risknz.org.nz**

PANDEMIC PLANS – TEN TIPS AND A FREE PLAN TO GET YOU STARTED

NIGEL TOMS – *Watercare Services Limited*

In 2019, if a selection of organisations had been asked about how many of them had pandemic plans, I doubt many would have said yes.

If asked again at the beginning of 2021, even if they did not have a specific pandemic plan yet, most would accept that significant revisions and wider thinking were required in order to maintain business operations when faced with Covid-19.

While Covid-19 challenges continue, it is interesting to note that conversations with counterparts in other utilities confirmed that:

- Significant innovations were identified and implemented to address the challenges that came with Covid-19
- New ways of working are now the "norm"
- The pace at which changes were made was impressive and far beyond expectations.

However, when asked if their pandemic plan (if they had one) has been updated to encapsulate these learnings and innovations, the answers varied from,

- Not yet – no timeframe set
- When normal operations resume
- As soon as resources are available – resources undefined
- It will be a separate project, timescale to be discussed

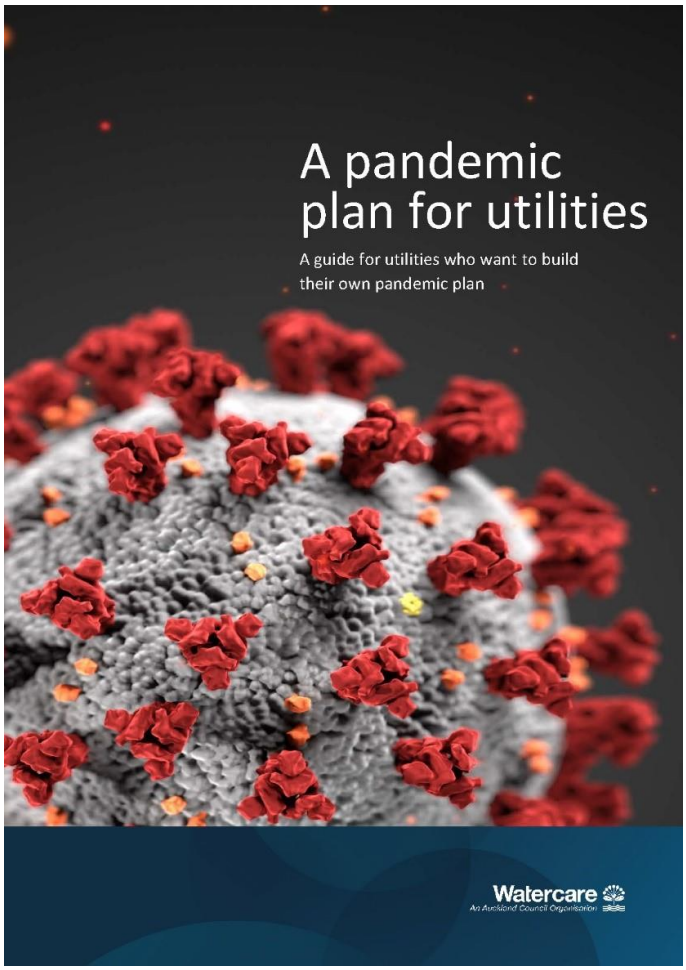
While I sympathise with the challenges faced, the dichotomy between the wide acceptance for the requirement for an update of the pandemic plan and the need to address other competing priorities, should not leave the pandemic plan in second place.

I am the Acting CFO at Watercare Services, which is the primary water and wastewater services utility for the Auckland and Waikato regions in New Zealand. Maintaining 24/7 operations is critical with an expectation from all stakeholders that these services will continue uninterrupted, to the standard required with significant/regulatory consequences for any failures.

With this in mind, Watercare completed a full update of its pandemic plan late in 2020 and I am proud to say we have released a FREE generic version, which can be used by other large organisations and utilities to create or enhance their own plans. Our plan could also be used simply as a matrix for comparison to ensure that nothing critical is missing from other organisations' pandemic plans.

Continued on next page…

We have designed this plan to be easy to roll out, easy to adapt to different contexts, and easy to use when responding to specific challenges from future outbreaks.



© Watercare Services Limited, Auckland, NZ, 2020

We have designed this plan to be easy to roll out, easy to adapt to different contexts, and easy to use when responding to specific challenges from future outbreaks.

Watercare's plan is FREE (yes, really, which is why I mention it twice!), interactive with guidance, videos, samples and templates, and is issued under a Creative Commons license, meaning others can adopt and use any components of, or even the whole plan, as long as they understand that it is at their liability.

Watercare's plan can be found and downloaded here.

With the experience of having just completed an update to our pandemic plan, here are ten tips to get other large organisations and utilities started on creating or updating their own pandemic plans.

1. Identify your core – and protect it

Your pandemic plan, much like your business continuity and disaster recovery plans, has to be clearly focused on the critical or core areas of your business. Not all areas of a utility are critical to maintain services and your plan should ideally be designed to wrap organisational support around the core business. So the first action is to clearly identify the core and make sure everyone understands the areas with these core elements. A good check is that in most cases the critical/core parts of your business are covered in the mission or strategy statement of organisations.

Continued on next page…

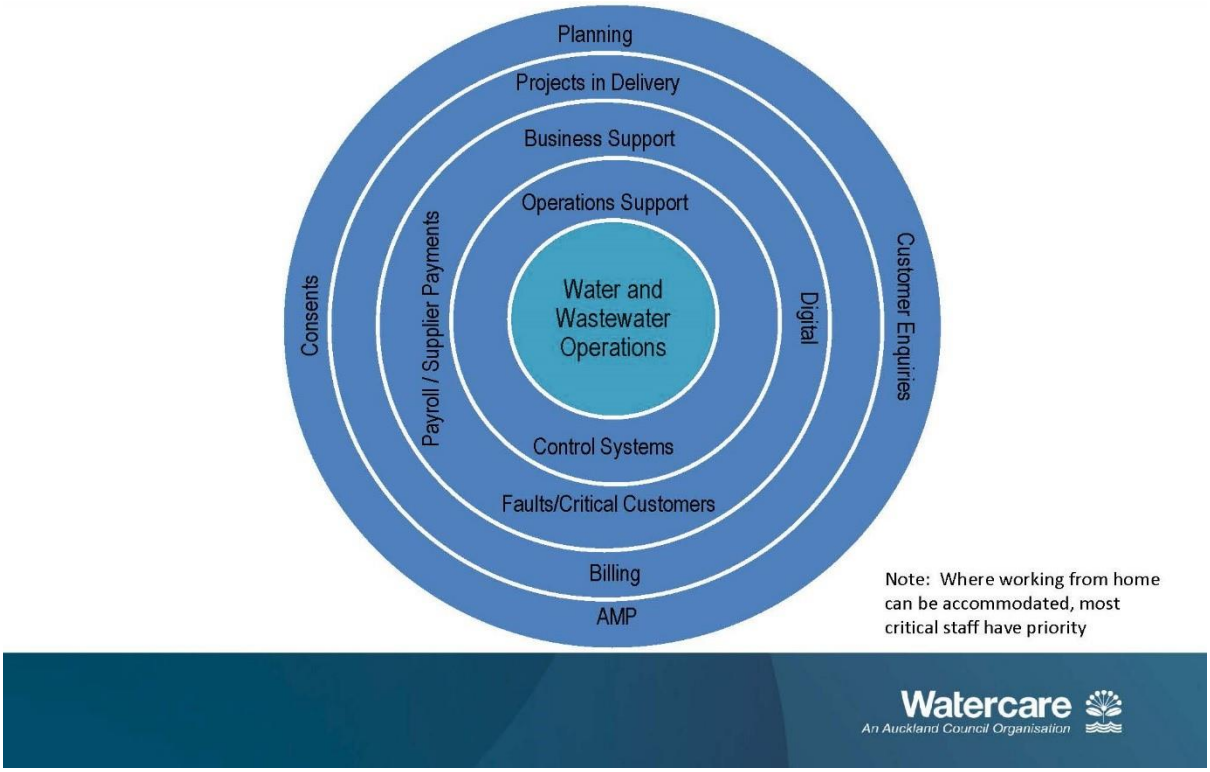


Figure 1: Clearly identify the core of your organisation and your plan should wrap organisational support around the core business.

2. Bring your departments together – it is a team effort

The intrinsic nature of a pandemic demands that all groups within the organisation will use the pandemic plan in some way. Make sure to integrate risk-and-resilience thinking in the plan and develop it to encourage collaboration among the different departments, units and functions to ensure efficient and effective implementation and operation.

3. Structure and process to support the plan

Watercare's plan is drawn from and aligned to the Coordinated Incident Management System (CIMS) to aid organising our response. The CIMS structure provides clear delineation of responsibility across various functions, while demanding coordination from them. The structure also enables us to have as big or as small an incident team as necessary to maintain crucial functions and manage incident response.

Whether you decide to build your plans on CIMS or an alternate system, the important part is to have a clear structure with clear responsibilities that is well understood by your staff. This should be the case, not just for pandemics, but for all incidents.

4. Delineate stages and outline actions to each function

Break the pandemic response into stages that take into account global and national reactions. Customise these stages to closely reflect the realities within your national and local environments. While taking account of what might be happening around you, also use these stages to clearly define what you as an organisation will be doing to protect your core business at that time. For example, you might decide to put in place strict work-from-home and contact tracing measures, even before your country announces any kind of lockdown. Such pre-emptive measures can go a long way to protect from multiple staff infections within your organisation. All of this needs to be delineated in stages and actions, defined in detail for each function.

Continued on next page…

5. Driven top down to build long term thinking

The pandemic plan needs to be driven top-down by the leadership. The executive and the board should be seen to support the plan and encourage the thinking embedded in the plan at every opportunity – not just during a pandemic but before and after. This should be part of a larger effort to build risk-and-resilience thinking within the company's culture.

6. Run incident practices/exercise with varied teams

A plan is only as good as the number of practice runs you put it through. Different teams should be put through practice sessions on a regular basis to ensure that they remain aware and up-to-date on the requirements of the plan, and to ensure that the plan itself is changed regularly to reflect any modifications in organisational functions and processes. A plan is only as strong as the people and process supporting it, so keep testing both regularly to find and address gaps. It is alright to have failings during tests. Failing safely allows improvements to be identified and implemented.

7. Pick inexperienced staff to act as deputies

Make sure that your incident management teams are diverse and include staff from different tiers as deputies during practice sessions. This is essential to making sure that knowledge related to incident management is well-understood across the organisation and is not restricted to a few higher tier staff. Once again, this goes to risk-and-resilience practices that can set the organisation up for the long-term. In addition, using experienced staff as mentors allows knowledge to be passed on.

8. All to participate in lessons learned debrief at incident completion

All team members should participate in a lessons learned debrief at the conclusion of practice sessions. Participation at these sessions leads to a shared understanding of the elements that worked well during an incident response and elements that could have been improved upon. Do it as soon as possible after the incident closes, as memories fade quickly.

9. Include support networks (contractors, suppliers, consultants) in exercises

One of the parts of any plan, which is most often forgotten, is the inclusion of the organisation's support networks in any exercises related to pandemic plans. You have to keep in mind that your support network will also need to continue to function in order for you to continue to provide critical services to your stakeholders. Include them in your exercises. That way they know what your plan and expectations are in case of pandemics (or any incidents) and they can modify their response structure to support your position.

10. Record experiences on staff systems and keep your plan updated

Use training systems to record staff who have gained experience from each incident and exercise. This is a powerful way to identify requirements for learning and training, especially with new staff and support networks. It is also a good way to identify and train future leaders.

Review and modify your plan regularly, and review after every training exercise. This will keep the plan fresh and ultimately easy to roll out when it is needed.

NIGEL TOMS

Nigel Toms is Acting CFO of Watercare Services Limited, the sole provider of water and wastewater 1.7 million Aucklanders. Prior to his appointment as CFO, Nigel was Head of Risk and Resilience at Watercare.

Nigel is the technical author responsible for the drafting and development of PAS 60518:2020 Developing and implementing enterprise risk and resilience management (ERRM) in utilities standard, published by the British Standards Institute (BSI) in July 2020. He was also a member of the Steering Committee.

In his time at Watercare, he has developed and grown the risk function to become a key part of the executive. Nigel championed and developed Watercare's own enterprise risk and resilience framework and the PAS 60518:2020 draws upon his expertise and reflects some of the ERRM work done there. Nigel can be contacted at nigel.toms@water.co.nz

SKILLING UP TO DELIVER ON OUR PROMISE

BRYAN WHITEFIELD

In late February 2021 I ran a poll of around 100 risk professionals while they were attending an event I was hosting. They came from more than 20 countries. I asked them to indicate how risk management is viewed in their organisation. The choices I gave them were:

1. Leadership – Risk management is used to identify where we can and should take more risk and where we should pull back.
2. Insight – Risk management is helping by providing good insights to decision making.
3. Comfort – Risk management is about providing comfort to the board and/or a regulator.
4. Compliance – Risk management is treated as tick and flick.

Pleasantly just over 50% said their organisation was operating "above the line" with just over 20% indicating risk management was providing leadership. Sadly, almost 50% are not treating risk as valuable, with 14% on the bottom rung, treating risk as a compliance activity. Keeping in mind, it is more than 25 years since the first national standard on risk management AS/NZS 4360 was first published in 1995.

While these results are not pure market research, they were in line with my experience of working with risk professionals of all kinds across many, many industries and across the public, private and not-for-profit sectors.

The conclusion? We still have a lot of work to do.

We need to deliver value

It's pretty obvious, however, if you want business leaders to value what you do and adopt your advice you must deliver them something of value. Now value is in the eyes of the beholder. And for some, they value that you keep the regulator and the board happy and only disturb them when you absolutely have to. Unfortunately, that type of value is a dis-service to business leaders and the organisation as a whole.

The type of value you need to deliver is to help them think through their decisions to improve their success rate. McKinsey has published a range of surveys over the years that asked executives to rate the quality of decision making at their organisation. The results have consistently been poor. In one of their more recent surveys (2019) the results were that "only 20 percent of respondents say their organizations excel at decision making" and the "majority say much of the time they devote to decision making is used ineffectively." Perhaps the 20% that excel are using risk as a leadership tool?

Continued on next page…

Decision making is very often a complex task. Multiple unknowns, multiple opinions, the needs and wants of multiple stakeholders to balance. The job of the risk professional is to help work through that complexity. Not perfectly, just better. And better comes from good analysis across a range of disciplines and effective communication which requires a broad and strong skill set.

What skills should a risk professional have?

Figure 2 is a set of 20 skills I have identified, under five key categories. I would like you to treat the skill sets a bit lightly with the logic behind the five categories as follows:

- Structure: Risk departments in organisations are usually responsible for the design and implementation of the risk management program.
- Fundamentals: The core work of a risk professional.
- Specialties: Four key areas that lend themselves to specialisation.
- Essentials: The areas that make the difference between a low impact and a high impact risk professional.
- Influence: The skills required to formulate and deliver your advice so your messages cut through.

I am not going to detail here each of these 20 skill sets. Instead, I am going to highlight the ones under each category which I feel are underdone by many risk professionals, or I feel should be applied differently than what I see as the norm. To find out more, you can download a PDF here that has brief descriptors of each of the three skills that underly each of the 20 shown below.

Figure 2

STRUCTURE CATEGORY

Under the Structure category, documenting and operationalising the organisation's risk appetite is often underdone. Too often I see very bland risk appetite statements that tell me nothing. "We have a very low appetite for cyber risk." "We have a high appetite for innovation." Pretty much who doesn't?

Better practice is to have the discussion with the executive and board about their willingness to accept specific areas of risk when it comes to achieving each corporate objective. And the areas of risk to be avoided. I ask them about "The line in the sand we must cross to achieve the objective and the line in the sand we should not cross." This results in a much deeper conversation about what is at stake and their desire to achieve goals. For a more in-depth look at a strategic objectives approach to risk appetite, see this May 2020 COSO paper.

Continued on next page…

The other issue I constantly see is overly complicated frameworks. Please, please, please apply the KISS principle. No one in the business cares how technically correct you are when it is too long and difficult to comprehend.

FUNDAMENTALS CATEGORY

Anyone can assess risk and devise controls, poorly. Your job is to help others to do it well. And that is where your facilitation skills come in. If you are not being asked to run workshops, or worse still, the business is avoiding your workshops, you might need a change of approach. Start with your mindset. The purpose of a risk workshop is not to collect risks in a risk register or to update an old one. It is to help the team find answers to challenging questions. So that they are better informed and better prepared to work towards achieving their goals. If you think, and talk, like this you will start to shift the mindset of others to value creation and protection. Not dreaming up a collection of risks.

And one quick tip on risk reporting: Integrate it into business-as-usual performance reporting. Risk and strategy go hand in glove. So should their reporting.

SPECIALTIES CATEGORY

If you are in a smaller organisation you may not have internal resources to rely on for these and other areas of specialty. Please recognise there is plenty to learn in these areas and reach out to colleagues or external providers for assistance or consider RiskNZ's training offerings. If you are in a larger organisation, the imperative is to seek alignment of approach. That is, ensure each specialty area is using common language and common risk criteria that are being applied with a common understanding of risk appetite.

ESSENTIALS CATEGORY

You may find it interesting that I call this category "essentials". The reason being, that each of these skills are needed to create a resilient and ultimately higher functioning organisation. You need to be good at critical thinking, be acutely aware of the culture you want and the culture that exists so you can create change and lead the organisation to the creation and protection of more value.

The last skill in this category, quantification of risk, is problematic. In fact, I call what I often see, quantifornication: the plucking of likelihood, consequence and control effectiveness ratings out of thin air in a facilitated risk workshop. We can do so much better. Please start collecting more data.

INFLUENCE CATEGORY

It is one thing to be technically correct across all facets of risk management. It is another thing for business leaders to listen to you and act on your advice. I consistently see risk professionals seeking more and more technical training while ignoring these core skills which collectively provide you the ability to influence with impact.

Being a strong influencer starts with listening. Listening, combined with your critical thinking and analysis skills helps you in understanding the person(s) and their challenges so you can provide valuable advice. Having valuable advice is worthless if you are not communicating it in a compelling way. And lastly, you need to be acutely aware of the level of psychological safety for staff to speak up. If it is not safe, they won't speak up and it can be career limiting for you if you speak up on their behalf. You must learn to influence business leaders on the importance of psychological safety and learn how to foster a psychologically safe culture throughout the organisation. So, it is safe for you and others to speak your minds.

BRYAN WHITEFIELD

Bryan Whitefield helps risk professionals lead through complexity. One thing he knows for sure, is that being technically correct is one thing, to be correct and to be listened to is quite another. Hence his passion for increasing the influence of the profession and why he has written ***Risky Business: How Successful Organisations Embrace Uncertainty*** and **Persuasive Advising: How to Turn Red Tape into Blue Ribbon**.

HOW TO BUILD ORGANISATIONAL RESILIENCE IN 2021 FOUR THINGS RISK MANAGERS CAN DO RIGHT NOW

BEN CROWTHER– *Marsh*

It's been a year of risk. Pandemic, bushfires, flood - all in extremely challenging insurance market conditions. While the pandemic will one day end, risk is here to stay, and risk managers need to change their approach on organisational resilience.
The 2021 Global Risks Report, published by the World Economic Forum in partnership with Marsh McLennan, reveals the top concerns business leaders are most concerned about when leading their organisations into the future.

So what do the responses from over 700 experts and decision-makers specifically mean for risk managers? Risk managers are in the driver's seat. Evidently, the risk conversation has changed. Risk is now informing every decision made. Organisations are looking to risk managers to help rethink short and long-term business strategies, and help build organisational resilience.

So where to start? We believe risk managers should focus on four key things:

1. **The pandemic showed how risks such as infectious diseases bring more than just health threats – they disrupt supply chains**

You're only as resilient as your supply chain is. Risk managers need to consider what it truly means to be 'resilient'. If you're running at peak performance, but there's sudden disruption with your supplier, you might be soon hitting the breaks.

Think of COVID-19 at a time when demand for medical equipment outpaced supply. Risk managers can take inspiration from Dr Nicole Townsend who had the foresight to see that the pandemic was going to create shortages of essential items such as medical gowns. Heroically, she started making and distributing the garments across Victoria!

Look around you. Successful risk managers are those who anticipate risk outside of their own organisation. At Marsh, we've been helping clients understand where their customers and suppliers were located during the recent La Niña weather season, and whether any supplier was exposed to any flooding events.

2. **Shifting from static risk assessments into probability-based insight**

The way in which to define, measure, and manage enterprise risk has evolved to a game of probability.

In our data-based insights article, we called out the need for data to help identify the probability of scenarios. On the back of this, actions can then create a clear path forward for each eventuality. So when data indicates a potential problem, your organisation's pre-planned decision can lead to swift action.

In the thick of COVID-19, organisations suddenly needed to make decisions on a response to a virus the world knew little about – there was no trusted data. Now organisations can identify, access, run and use data from models and even databases that may not exist in-house. Think about how data might work for you as a risk manager.

Continued on next page…

3. The power of debriefing risk events – memories fade

Amongst the chaos, do you ever take the chance to stop, pause and reflect on your decisions in the heat of the moment? Memories of what happened during the early stages of any big event and the context in which you had to make decisions fade quickly. Information and lessons learned may be lost.

As the saying goes, "Identical crises never happen twice", however, this makes it even more important to learn whether your workplace had the skills of adoption, invasion and tolerance for uncertainty.

Events like COVID-19 should not be perceived as a one-off event but rather an indicator of how well your organisation can respond to any test. Business Continuity Debrief workshops can help your business understand questions such as:

- Was there sufficient preparation?
- What level of planning did your organisation have in place before the event?
- Why was the specific level of planning in place?

Workshops can also help avoid costly impacts to your business interruption insurance. Have you, your suppliers' or customers' ways of working changed over the past year? These need to be documented to optimise your business continuity plan. If not, you might be subject to potential increases in business interruption insurance.

4. Avoiding a climate change business disaster with a risk lens

Know what climate change risk means for you, not just the world. Climate change is not just a social problem, it's a business one, with climate related costs only rising.

Start by mapping out what the variables are. For example, what does a single percentage change in temperature mean for your employees and business assets in the real world? For farmers, it might mean destroyed crops and decreased outputs of agriculture. Consider risks like a water and energy crisis.

Secondly, understand what the impacts of rising sea levels might be. Think about locations close to sea level or only accessible via roads close to sea level. For your workplace, distribution networks or suppliers, it might require a relocation. What might intense flooding mean for your business?

Physical assets like buildings close to rivers or areas prone to flooding will only become more vulnerable with climate change. Thirdly, consider the adaptation and intervention needed to avoid a climate change business disaster. Perhaps it's water and energy conservation and finding innovative alternatives to rain water storage.

As we observe changes in natural disaster activity and intensity, insurers are reacting by increasing premiums and enforcing stricter exclusions and lower limits. One step further, they're reducing capacity or withdrawal altogether from industries seen to be contributing significantly to climate change. Risk managers can't afford to sit and wait. Climate change is a 'here and now' business challenge.

Looking forward with confidence

Risk managers are in pole position as the world recovers from a global pandemic and responds to ongoing threats such as cyber-attacks and catastrophic climate change.

Now is the time to rise to the occasion and review your risk management strategies, so you can build resilience for what comes next.

Talk to us

If you would like to better understand how emerging risks might impact your business and how you can be prepared to respond, you can contact us here.

For more insights, you can read The Global Risks Report 2021, published by the World Economic Forum with support from Marsh McLennan.

BEN CROWTHER

Head of Strategic Risk, Marsh

Ben leads the Strategic Risk Practice within Marsh Advisory where his team assists clients in measuring the impact of risk management efforts, optimising risk frameworks, analysing insurable risks and building organisational resilience. Ben also consults in the area of emerging risks including supply chain resilience, cyber, and geo-political risks. He has a Bachelor of Business, Master of Business Administration and Master of International Security.

DID YOU KNOW YOU HAVE AN INTERNAL RISK MANAGEMENT PROCESS?

TONY YUILE

Introduction

As risk managers we're all familiar with risk management and the risk management process. But did you know you also have an internal risk management process? It's part of your natural survival system and enables you to deal with risks to your physical and/or emotional wellbeing.

It's a highly effective and reliable process, after all it's been in development for hundreds of thousands of years. Its effectiveness is demonstrated by the fact the human race has survived where many other species have become extinct.

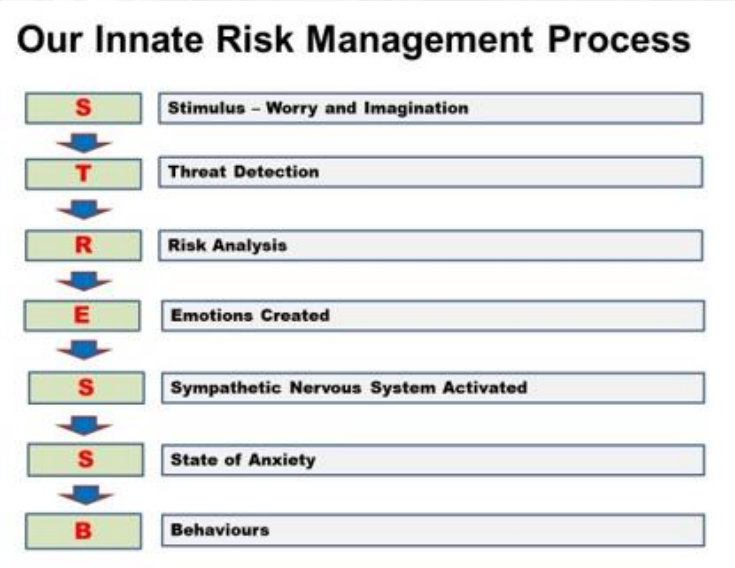
Why an understanding of our innate risk management process is essential

Our innate risk management process produces anxiety. Anxiety is the most common mental health issue in the world today. Its impact on us can range from being a silent thrum under the surface of our daily lives to being totally debilitating.

With an understanding of how your risk management process operates you can begin to explore how well your process is functioning, and can make any necessary adjustments, so you avoid unnecessary, unhelpful anxiety. Your wellbeing will improve, and you will enjoy life more.

Our Innate Risk Management Process

Here are the steps in our innate risk management process.



As you can see the first letters of each step in the process spell the word 'STRESS' which makes remembering the six steps easier!

Let's explore each step in a little more detail.

Continued on next page…

Step 1: Stimulus – Worry and Imagination

The inputs into our risk management process are our thoughts and the imagined future scenarios those thoughts trigger. It's estimated we have some 60,000 plus thoughts every day. Most of these thoughts are 'automatic', they just pop into our heads. Very often we're not even aware we're experiencing them. Many of these thoughts take the form of worries.

Worry

We live in an uncertain world. There's no escape for us from living with uncertainty. Most people have an intolerance of uncertainty. As far as our brain is concerned uncertainty equals risk.

Faced with uncertainty and the unknown, our mind races to fill in the possibilities and worry is our attempt to reduce uncertainty and gain a sense of control over the future by thinking through what could happen and what might be the consequences. Our worries can be consciously generated but as mentioned earlier, for the most part they just pop into our minds automatically.

Worrying essentially involves asking ourselves some variant of the question "What if….".

What if I get COVID and end up in hospital?

What if there's a traffic jam and miss the important team meeting?

What if I forgot to turn off the stove and there is a fire?

What if I apply for that job, and I don't get an interview?

What if my partner leaves me?

There is no end to the "What if …" questions we can ask ourselves. And because our mind loves questions it will happily go off searching our memory for the answers. And because we have a natural negativity bias, we spend more time and energy exploring what might go wrong, than what might go well.

Some people seem to worry about everything. You can probably identify people in your life who are constant worriers. They are always expecting or preparing for the worst. When worry is frequent, intense or both or persistent and uncontrollable it can become problematic, overwhelming and can adversely interfere with our enjoyment of life. People who engage in persistent, pervasive, unhelpful worrying for an extended period, may be diagnosed as experiencing Generalised Anxiety Disorder (GAD).

Catastrophising

A common form of worry at this step in the process is 'catastrophising'. Catastrophising is jumping to the worst possible conclusions, however unlikely, and seeing the consequences replayed in the most gruesome detail in the mind. The reality of the situation might be quite insignificant and small.

It can be helpful for us to consider worst-case scenarios so we can identify and analyse significant risks and actively prevent those risks from materialising. However, when we habitually default to imagining the worst-case scenario this can result in unnecessary anxiety.

For example, you get on an aeroplane and catastrophise about it falling from the sky; you go to a restaurant and catastrophise about being killed by food poisoning; you walk to the shops and catastrophise about having left the cooker on and burning the house to a cinder. While all of these are risks are extremely unlikely to occur, they are possible, and they can feel very real at the time we think about and imagine them.

Our imagination

Our brain can't differentiate between what's real and what's imagined. External and internal stimuli are both treated as just data to be processed.

We use our imagination to project ourselves into the future in an attempt to predict the consequences of a future situation that may never occur. Sometimes our brain gets the prediction right but, most of the time it doesn't, and we waste a lot of energy and time imagining risk scenarios that will never occur.

Continued on next page…

Step 2: Threat Detection

Our brains have been built over our lifetime based on experience. From the 100 billion neurons the brain contains at birth, a unique network of synaptic connections develops capturing each new experience and our emotional response to it. I call this vast network of synaptic connections our 'memory matrix.'

Experiences that harmed our physical and/or emotional wellbeing, or had the potential to, are tagged in our memory matrix as 'threats'. These experiences do not have to have been life threatening. In fact, many threat memories relate to of interpersonal pain, mistakes, near misses, missed opportunities, minor injuries etc.

The purpose of our memory matrix is to serve as a reference source for our brain, enabling it to interpret what incoming data, real or imagined, means.

Incoming data is routed to a brain area called the 'thalamus' (found roughly at the cross-section of lines projected inward from his eyes and ears). The thalamus operates like a telephone exchange sending the data in two directions for processing - to our limbic system (known as our 'emotional brain') and to our neocortex (known as our 'thinking brain').

The limbic system, being closer to the thalamus, receives the data first and compares it to the information held in our memory matrix in order to identify, and give meaning to, it. What the limbic system is looking to detect is real and present danger, or risks, to our psychological and emotional well-being.

I like to think of this matching process as being akin to a mental game of SNAP! When there's a pattern match, i.e., the incoming data is the same as, or closely matches, a known threat, then electrical signals are sent to other parts of the brain to initiate the Threat Response. This matching process takes place in a matter of milliseconds and we react to the perceived threat before we're even consciously aware we are in danger or at risk.

The identification of threats via this lightning-fast subconscious pattern matching process can result in us feeling anxious without consciously knowing why we're feeling anxious.

Threat Detection is a 'better-safe-than-sorry', process.

The threat detection process sacrifices accuracy for speed. When it comes to our survival, time is of the essence. So, the threat detection process adopts a "better safe than sorry" approach. Our brain would rather be wrong a hundred times than be wrong once. We're not descended from early humans who underestimated danger!

As such, like all good alarm systems the Threat Detection process is guilty of making faulty pattern matches. You don't want a smoke alarm that goes off only when the house is engulfed in flames; so you accept that it goes off occasionally when people are making toast or frying food.

For example, if you're out tramping and you think you see, or hear, a wild pig, you don't want your brain to wait until it's absolutely sure it's a wild pig before triggering the Threat Response. You want the Threat Response triggered immediately so you can get the heck out of there fast, before the pig charges you. Your thinking brain will, via the Risk Appraisal, process (see below), establish whether the emotional brain got the threat detection right, but this takes precious seconds, and if the pig comes charging at you, that extra time may mean the difference between a narrow escape and no escape.

Step 3: Risk Appraisal

A moment after the data arrives in the limbic system it arrives at the neocortex. The neocortex, and in particular the pre-frontal cortex – aka our 'thinking brain', has two roles to play in our risk management process.

It's first role is to identify threats and risks not identified by the limbic system perhaps because the experience we're having is new to us, or we've had the experience before, but it wasn't tagged as a threat.

To identify risks the thinking brain performs a risk appraisal. The risk appraisal process has two stages: primary appraisal and secondary appraisal. Our brain completes this analysis process in less than a second.

In primary appraisal, our brain evaluates whether the real or imagined situation is irrelevant, safe or a risk to our physical and/or emotional wellbeing. Our brain operates according to this rule: "Familiar is safe and comfortable. Unfamiliar is dangerous and uncomfortable."

Continued on next page…

If a risk is identified our brain undertakes a secondary appraisal. Secondary appraisal involves asking 'Do I have the resources to mitigate this risk or deal with the consequences should it materialise?
Some of the key things our brain evaluates are, our previous experience dealing with a similar threat/risk, how much control we have over the situation, our level of tolerance with uncertainty, how healthy we are, how much energy we have, our beliefs about ourselves, the world, other people and things, our relevant skillsets, our level of self-esteem, what support we have from family, friends, and the community.

If we appraise that we lack the necessary abilities/resources to deal with the risk, the Threat Response will be activated. Conversely, if we believe we have the necessary abilities/resources, the situation may instead be perceived as a challenge rather than a risk and our Challenge Response will be activated.

The second role of the thinking brain is to check whether the emotional brain got its threat detection right or whether it's guilty of raising a false alarm. When the thinking brain detects a false alarm, it sends a signal back to the limbic region to switch off the Threat Response.

Our thinking brain can, and does, get the risk appraisal process wrong.

Research has shown repeatedly that most people who experience anxiety overestimate the likelihood of the risk materialising and underestimate their ability to cope. In addition, research has shown that:

- people consider events over which they have some control of their own fate to be less likely to have adverse outcomes (e.g., driving to work, solo parachute jumping) than events over which they have no control (e.g., a passenger in an aeroplane, tandem skydiving).
- Dread of consequences leads people to over-estimate the likelihood of an event.
- People over-estimate the likelihood of unusual but high-profile events (e.g., a single plane crash) compared to more usual but less notable ones (e.g., car crashes).
- People's answers to questions about risk can differ enormously according to how those questions are framed (e.g., surgery with a 70% survival rate vs. a 30% chance of death).

Step 4: Emotions created

"Emotions that seem to happen to you, are made by you." ~ Lisa Feldman Barrett (2017). How Emotions Are Made: The Secret Life of the Brain

Psychologist and neuroscientist, Feldman Barrett research suggests emotions are a response to the meaning our brain attributes to a situation. They are complex neurochemical constructions built in the moment, as you need them and are recipes for what response our sympathetic nervous system should activate. For example, fear triggers the Threat Response and excitement triggers the Challenge Response.

When triggered by pattern matching, during the Threat Detection step, fear occurs with no associated thoughts and we can feel it before we are even consciously aware we are under threat or at risk.

The intensity of the emotion determines the intensity of the response. In the case of a risk the level of fear can range from mild apprehension to outright terror.

These chemical signals travel rapidly all over your body and last for about six seconds. The effect of an emotion can, however, have a longer lasting effect.

Step 5: Sympathetic Nervous System Activation

Our autonomic nervous system has two branches the sympathetic nervous system (SNS) and the parasympathetic nervous system (PNS). One way of thinking of these two sub-systems is that the SNS is the accelerator pedal (it gets us moving) and the PNS is the brake pedal (it slows us down and puts us into neutral).

The SNS can trigger many responses, of which the Threat Response (more commonly referred to as the "Stress Response') is just one.

Continued on next page…

The Threat Response unfolds in two stages, a fast initial stage employing electrical impulses, and secondary stage employing hormones.
When the Threat Response is activated our body immediately begins to adapt to be able to either fight off the threat/risk or escape from it. For the first few minutes the adaption is fuelled by adrenaline. During this phase of the response, adrenaline switches on certain responses in the body, such as sweating, quicker breathing, accelerated heart rate and so forth, gearing you up for the action you need to take to fight off or escape from danger. It also shuts down long-term and metabolically expensive functions of the body like digestion and reproduction.

This initial electrical response is lightning fast, and when successful carries us clear of danger. But it is metabolically draining and if exposure to the threat lasts longer than a few minutes, then the adrenaline becomes exhausted and a hormonal response takes over.

Our adrenal glands begin to secrete ever increasing amounts of stress hormones, the most well-known of which is cortisol. Cortisol is crucial in supplying us with energy and supports us in a more sustained effort against the threat/risk and can continue to be released over the course of minutes to hours, even days.

It is the continued release and build-up of cortisol that is the main cause of the feelings we experience as chronic stress.

Step 6: State – Acute Anxiety

"Anxiety is nature's way of telling us that key emotional needs have not been met in our lives." ~ Ezra Hewing, head of mental health education at Suffolk Mind in the UK

Acute anxiety is a red flag from your unconscious that it has noticed or is anticipating trouble ahead and something needs your attention. Consciously you may know what the risk is, or you may have no idea what the risk is, you just sense there's a risk out there.

Acute anxiety is a temporary state of being - once you have satisfactorily mitigated the risk, the anxiety related to that risk will dissipate.

Acute anxiety is experienced as a complex blend of uncomfortable feelings (physiological sensations and emotions). The feeling is intense enough not to be ignored, but not intense enough to be debilitating.

Describing what anxiety is like can be hard since the experience varies for everyone. However, common physiological symptoms include butterflies in the stomach, sweating, heavy, rapid shallow breathing, an elevated heart rate, muscle tension, a tight chest; gastric discomfort; restlessness, headache, nausea.

Anxiety can also cause sleep problems: such as having a hard time falling asleep, waking up frequently during the night, having a restless night and unsatisfying sleep.

Emotional symptoms include a diffuse, unpleasant, vague sense of apprehension, unease, nervousness, being on-edge, dread, fear.

Cognitively anxiety causes our mind to zero-in on the environment around us and we become more vigilant as we seek to find the source of the risk(s). This hyper alertness compromises our ability to see the bigger picture, to concentrate, to make clear, rational decisions, or to plan.

Chronic Anxiety

Anxiety like stress can be acute (short-term) or chronic (long-term). Chronic anxiety is driven by a persistent state of worry. When chronic anxiety has a debilitating impact on a person's daily life they may be medically diagnosed as having an anxiety disorder. Anxiety disorders are the most common mental health problem in the world today with the World Health Organisation suggesting that 1 in 13 people globally suffer from an anxiety disorder.

Continued on next page…

Step 7: Behaviour

"Check out the alarm, but don't mistake it for reality; the smoke alarm is not the fire. Most of the time, it signals caution, not danger." ~ Steven Stosny, Ph.D.

Remember, anxiety is a call to action to mitigate a perceived risk. Its job is to keep bugging you, until you pay attention and start taking action.

The benefits of anxiety are lost when we interpret it as a stop signal - a red light - rather than an amber (caution) light. When that happens, we can be discouraged from taking any action at all, or as is often the case, we may engage in maladaptive behaviours such as avoidance behaviours, escape behaviours and safety behaviours, that only serve to reinforce our perception of the particular risk and gradually disrupt our ability to live normal lives.

Avoidance Behaviours: When we feel anxiety, we have a natural reaction to retreat, find safety and isolate ourselves. We often seek to prevent the feeling by avoiding the situations we believe cause the anxiety. For example, we might just stay in bed, call in sick to work, decline an invitation to a social outing or event.

Escape Behaviours: Although we may start something or attend things, we might not follow through or cut something short if we're feeling anxious. Examples of escape behaviours include: - leaving the party early, getting off the bus/train before your stop as you cannot cope with the crowds, asking a co-worker to finish a task for you, declining a promotion.

Safety Behaviours: When we're anxious we may engage in "safety" behaviours to try and feel safer or to prevent feared outcomes from occurring. Examples of common safety behaviours include only going to places with a trusted companion, sitting near exits, engaging in excessive research prior to taking a trip, repeatedly rechecking things to make sure they were done correctly.

Positive behaviours in response to anxiety include contingency planning, problem solving, building up our resources to withstand risk, and enhancing our skills and knowledge. By taking action such as these we can successfully mitigate the risk as well as reassure ourselves we are sufficiently resilient should the risk materialise.

The risk management process has a built-in feedback loop.

The risk management process has an inbuilt feedback loop such that our anxiety and the consequences of our behaviours are fed back into Step 1: Stimuli – Worry and Imagination. This means it's possible to get trapped in an anxiety cycle. For example, in the case of panic the feelings a person experiences, racing heart, shortness of breath et cetera can cause the person to believe they are having a heart attack. The thought that they are having a heart attack is perceived by their brain is a new threat and so the threat response is activated, heightening the existing feelings, which get interpreted as an even greater threat. In this way anxiety and panic can quickly escalate.

An example of the Risk Management Process in action

Here's a simple example of how our innate risk management process operates in practice.

Continued on next page…

Process Step	**Scenario**
Stimulus – Worry and Imagination	Your boss tells you the company is struggling to survive due to the impact of COVID and there will have to be some redundancies. You think 'what if …' that happens and imagine a future in which you are one of those made redundant.
Threat Detection	Your limbic system ('emotional brain') processes the imagined scenario and, even though you haven't previously experienced redundancy, matches it to a memory that 'redundancy = threat'.
Risk Analysis	Your neocortex (thinking brain) performs its primary risk analysis and identifies redundancy as being a significant threat to the continued satisfaction of one or more of your emotional needs. It performs a secondary appraisal and determines your current resources are inadequate and the impact on your emotional wellbeing, should the risk materialise, will be significant.
Emotions Created	Your brain creates fear at a level commensurate with the perceived risk.
Sympathetic Nervous System Activation – Threat Response	Your Threat Response is activated, and your body instantly begins to adapt to prepare itself to enable you to take physical action to mitigate the risk.
State – Anxiety	You experience the physical sensations and fear as a high degree of acute anxiety. You recognise the feeling as a signal that you need to take action to mitigate the risk.
Behaviours	In response to the acute anxiety, you begin updating your resume and start contacting people in your network about possible openings. You identify which of your skills need updating to facilitate finding a new role and sign up for a night class. You review your household expenditure to see where savings can be made. As you complete more of these actions your risk appraisal changes because your brain appraises you are now able to manage the risk and as a result your anxiety level drops.

Intervening in your risk management process

I mentioned at the start of this article that with an understanding of how our innate risk management process operates we can explore how our own process is functioning and make any necessary enhancements with the aim of avoiding unnecessary, unhelpful anxiety.

In the table below I've provided some examples of possible interventions. Many of these you can make yourself, but some are best undertaken with the help of an anxiety solutions coach or anxiety therapist.

Process Step	What can go wrong	Examples of possible interventions
Stimulus - Worry and Imagination	Worrying becomes obsessive, irrational, chronic. Misuse of the imagination.	Worrying well is a skill anyone can learn. To experience less anxiety, you need to identify, control and/or change your unhelpful thinking habits. There are many techniques available to help you create this habit change. You can train yourself to stop misusing your imagination. You can practice visualising what you want to happen rather than defaulting to imagining unfavourable outcomes.
Threat Detection	Threat memories are no longer relevant.	You can reduce the effect of unhelpful threat memories using neural recoding techniques to 'reprogram' your brain. Through mindfulness practice you can de-sensitise your limbic system to threats (metaphorically turn down your smoke alarm's sensitivity).
Risk Analysis	Overestimating the likelihood or consequences of risks.	Consciously and rationally appraise the risk. Develop more helpful mindsets such as: optimistic mindset, challenge mindset, growth mindset. Learn to become more comfortable with uncertainty. Build your skills, such as: problem solving, time management, delegation, assertiveness. Build your resilience - Take action to meet our physical and emotional needs in balance. Acquire more resources e.g., social support, business networks, savings, disaster emergency kit.
Emotions Created	Inappropriate level of emotional intensity	Emotion is the neon flashing light that says: "look at me". Without the emotional flashing light there's no compulsion to continue to worry about the situation. You can use dissociative techniques to put some space between you and the emotion which has the effect of reducing its intensity.
Sympathetic Nervous System Arousal	Constant activation of the Threat Response	Use breathing exercises to switch on the Parasympathetic Nervous System (Rest and Digest) and switch off the Sympathetic Nervous System.
State – Anxiety	Anxiety impacts on your daily life.	Use coping skills such as exercise, relaxation techniques, mindfulness, self-hypnosis.
Behaviours	Avoidance, escape, safety, behaviours.	Desensitize yourself to the risk through gradual exposure (physical and or imagined).

Final thoughts

My aim in writing this article was to provide an understanding of how and where our experience of anxiety comes from. Anxiety isn't something that's done to us, it's an experience we create ourselves as a product of our incredible, inborn risk management system. The fact that we create our experience of anxiety is significant because it means, we can also stop experiencing unnecessary, unhelpful, and potentially harmful anxiety. The good news is there are plenty of evidence based, proven ways to rapidly create the changes to our risk management system we need to make.

Finally, if you are experiencing anxiety, I recommend you, in the first instance, consult with your medical or health practitioner for advice, diagnosis, and recommendations as to treatment.

TONY YUILE

Tony Yuile is a certified life coach, clinical hypnotherapist, and the author of 7 Ways to Reduce Anxiety in 7 Minutes or Less. He is a coach and instructor with YourlifeLiveit an international coaching and training company. Tony is passionate about helping people develop the life skills they need to minimise the stress and anxiety in their lives and enhance their resilience.

Tony spent 30 years in senior financial and risk management roles across the private and public sectors. He was secure and happy in his career until thrown a curve ball – redundancy, something he was totally unprepared for. Suddenly he found himself in the vicious grip of stress and anxiety. When he finally emerged from beneath the black cloud, he promised himself that he would never feel so dreadful again. He set out to discover as much as he could about stress and anxiety and to share what he learned with others. Based in Wellington, Tony works with clients within New Zealand and globally.

Tony served on the RiskNZ board for seven years and, as was the organisation's Treasurer for 11 years. He is a life member.

ISO 27001 – A TALE OF A SMALL COMPANY'S JOURNEY TO CERTIFICATION

AHMED ELASHMAWY – Consulting Practice Lead and
TERRY CHAPMAN – Managing Director – *Axenic Ltd*

To certify or not to certify, that is the question

International Standard Organisation certifications can be quite an undertaking for organisations. Whether an organisation decides to adopt an ISO standard only, proceed with certification or do nothing in this space could be a difficult call. In this article, we will walk you through our own journey to certification as we have recently experienced it at Axenic.

ISO/IEC 27001 Information technology — Security techniques — Information security management systems — Requirements consists of seven main clauses detailing the requirements for going through a Plan, Do, Check, Act (P-D-C-A) cycle to manage information security risks. The following sections provide a high-level overview of how we approached it.

Leadership and Commitment

Despite being an information security consultancy that have consistently helped clients create and maintain Information Security Management Systems (ISMS) in accordance with the requirements of ISO/IEC 27001:2013 all the way to certification, it took us few years to build and certify our own. The main reason behind that is the resource commitment. Client work has always trumped internal initiatives, so every time we started establishing our own ISMS, it was interrupted by client work. When the business committed capable resources to deliver the ISMS and managed it as it would manage any client work, we started knocking off the requirements one after the other. Formal resource allocation also served as an essential artefact required to evidence clause 5.1 of the standard (Leadership and Commitment) and clause 7.1 (Resources). Having only two policies (Information Security Policy and Acceptable Use Policy) resulted in a more 'digestible' set of principles and in maintainable documentation.

Operation, Planning (a.k.a. Risk Management) and Context

As the standard adopts a risk-based approach to information security, a logical place to start was to conduct a risk assessment and identify risk treatments. Naturally, a standard risk management framework or methodology was required prior to that. Given that standard risk management methodologies require scope and context (Clause 4), those were documented prior to conducting the risk assessment. As per requirement 6.1.3, the selected risk treatments (controls) were compared to Annex A of the standard to verify that no necessary controls have been omitted. A common misunderstanding (even among some security professionals) is that Annex A is the standard, whereas the standard is outlined in the clauses.

You may be interested in learning more about this by reading **From Chaos to Conformance: A Series on implementing an ISMS** by visiting our blog.

As artefacts to demonstrate risk treatment actions are planned and delivered are required, we produced a risk treatment plan, assigned ownership and deadlines, and reviewed those regularly. As risk treatment milestones where achieved, we produced the relevant evidence and ensured they are properly filed against the controls.

Continued on next page…

Performance Evaluation and Improvement

As monitoring and measurement are key to improvement, the standard outlines a set of requirements for these. Identifying performance measures that are linked to the objectives, as well as regular measurement, and management reviews are corner stones to improvement. A formal agenda for management meetings, calendar bookings and formal meeting minutes to document outcomes and decisions, provide sufficient evidence that the organisation is meeting the requirements of this section of the standard. An improvement log to track improvement opportunities, non-conformities and corrective actions helped us track these and ensure the process is effective and evidenced. Finally, the review of a dashboard mapping objectives outlined in the scope and context to specific Key Performance Indicators (KPIs) was always a standard agenda item in any ISMS review meeting.

Once all of the above are in place, conducting an internal audit in accordance with the requirements outlined in 9.2 (Internal Audit) highlighted any gaps we missed and helped us rehearse the external audit. While having a super competent, independent and certified ISO 27001 Lead Auditor was handy, having a capable external party conduct the internal audit on your organisation's behalf should satisfy the standard's internal audit requirement.

The good, the bad and the ugly

We learnt a number of valuable lessons throughout our certification journey. The ISO 27001 certification provides a competitive advantage for most organisations that need to demonstrate secure practices and that would typically be enough motivation to complete the certification itself. However, the implementation of an ISMS in accordance with ISO 27001 requirements provides almost all organisations with significant benefits as it helps mature a number of business processes. It is also important to be realistic about the time required to build and operate an ISMS. Buying templates and forging an ISMS can easily end up being a very expensive failure. When audit time comes, it pays off to be well prepared. We went into audit sessions (both internal and external) with all our evidence open on laptops and ready to show to the auditors without even browsing to the relevant library. Flipping through tabs or windows fluently during an audit definitely inspires confidence.

Even as professionals with track records of getting other organisations to certification, our own experience was not exactly a breeze. Building our own ISMS was more expensive than we expected as we initially tried to perfect every single aspect of it. It was also continually tempting to expand the remit of the ISMS to cover non-security business requirements. As a result, we ended up with an overbaked set of documentation and leadership time commitment was higher than expected. These scars resulted in massive learnings that we could only get by implementing our own ISMS.

The real ugly part of the process was going through two failed attempts at our ISMS before setting up the implementation with a proper governance structure and dedicated resources. Regularly reporting our progress to the board kept us honest and on track.

When we got those things right, we nailed our ISMS implementation.

AHMED ELASHMAWY – Consulting Practice Lead and
TERRY CHAPMAN – Managing Director – *Axenic Ltd*

Visit https://www.axenic.co.nz/about/people/ to see more about Ahmed and Terry

GAME ON – 5 TRENDS IMPACTING THE RISK LANDSCAPE

SUE TREZISE – *Sue-lutions Ltd*

Deloitte's recently published "The future of risk – new game, new rules" report profiles 10 trends that have the potential to significantly alter the risk landscape for companies around the world. The reports highlights new opportunities and new challenges leaders should prepare for and provides insights for risk practitioners to advise and support key decision makers.

This article summarises five of the profiled trends, selected because they most piqued the interest of this author, and also seemed most relevant to the New Zealand context. Not listed in any priority order, they provide a broad spectrum of emerging risk insight, helping to generate diversity and expansion in risk management thinking. Harnessing these trends will enable/support organisations to improve capability and resilience.

Trend #1 Cognitive technologies augment human decision-making

Driven by developments in artificial intelligence (AI) and easy access to huge amounts of data, smart systems will assist, and at times even replace, human-led risk management.

Applications of cognitive technologies include: technology embedded in a product or service to provide end-customer benefits; process applications to automate or improve workflow/operations and insight applications used to inform operational and strategic decisions across an organisation.

A specific example is managing social media risk using tools which scan social networks to discover and track an organisation's footprint; detect fraudulent social media accounts, unauthorised changes, and anomalous behavior on social account profiles; reduce potential liability from inadvertent posting of sensitive data; and demonstrate compliance with standards and industry regulations.

Forces driving this trend:

- Massive growth in the volume of data available to organisations
- Emergence of new and advanced AI-based algorithms
- Expanding pool of data science talent
- Adoption of behavioural analytics in risk management

Opportunities arising:

- Use of visualisation to analyse and communicate information in a human-friendly way to enable rational decision-making
- Upskill employees to enable more effective use of cognitive technologies to extract insights from data

Potential threats and pitfalls:

- Difficulty in implementing complex cognitive tools
- Lack of trust and assurance mechanisms for AI
- Human backlash against automated decision-making
- Unintended consequences of mistaken predictions

Trend #2 Controls become pervasive

In a sensor-enabled, hyper-connected environment, organisations will deploy pervasive controls as part of their products, services, and business models to monitor and manage risk in real time. Smart devices (also known as the Internet of Things (IoT)) equipped with a variety of sensors, communications, and computing capabilities serve as risk monitoring and enforcement points.

Continued on next page…

Examples include:

- ✓ Deployment of sensors into a truck fleet to track maintenance needs, driver safety, fuel usage, and other metrics in real time
- ✓ Wearable tags that can detect whether users have changed location or posture, have fallen down, or are experiencing high heat. Such tags enable real time monitoring of employees' working conditions with the aim of reducing workplace injuries.

Forces driving this trend:

- Declining cost, decreasing size, and increasing connectivity of sensors
- Advancements in sensor technology and analytics
- Growing adoption of workplace wearables

Opportunities arising:

- Automate compliance monitoring and reporting by embedding risk controls into business technologies
- Reduce cyber security and fraud risk by using sensor-enabled devices to implement identity access capabilities
- Improve traceability across the supply chain
- Manage risks introduced by customers by analysing their behaviour through real-time data feeds

Potential threats and pitfalls:

- Heightened exposure to cyber risks as business processes rely more heavily on the IoT
- Greater availability of data revealing risks in areas that were formerly considered safe, resulting in new obligations to manage those risks or increased liability
- Rising privacy concerns from employees, customers, and business partners
- Difficulty filtering relevant information from the noise, given vast amount of data generated

Trend #3 Behavioural science informs risk insights

Advances in behavioural sciences (study of human behaviour) will fuel efforts to understand risk perceptions, influence risk behaviours, and improve risk-related decision-making.

A specific example is the use of psychological profiling tools to ramp up computer security in the workplace. Such tools aim to identify workers who are most vulnerable to cyberattacks, based on their behaviour while checking and sending emails, and browsing the web.

Forces driving this trend:

- Increasing interdisciplinary research across fields such as cognitive science, psychology, economics, and neuroscience
- Growing popularity of behavioural economics to inform decision-making

Opportunities arising:

- "Design interventions" to help executives overcome the influence of cognitive biases in decision-making
- Improved systems for monitoring high-risk individuals in sensitive roles
- More effective risk, forensics, and financial transaction-related business processes

Potential threats and pitfalls:

- Risk of regulatory action in case of perceived misuse of behavioural interventions
- Backlash from employees and executives who see behavioural interventions as an impingement of free will

Continued on next page…

Trend #4 Risk transfer broadens in scope and application

Risk transfer instruments, such as insurance, contracts, and novel financial instruments, will increasingly be used by organisations to protect them from a wider range of risks – cyberattacks, climate change, geopolitical risks, terrorism, business disruptions, and more.

Forces driving this trend:

- Growing instances of "mega-impact" events such as cyberattacks, political unrest, and climate change, and their growing financial and reputational impact
- Increasing globalisation and the rise of a networked economy leading to cascading risks
- Inability of organisations to completely eliminate risks through preventive controls

Opportunities arising:

- Evaluate risk transfer instruments as an option to achieve business continuity and more predictable performance
- Develop clear and stringent risk-sharing clauses in all partner contracts, and consider collective insurance with partners to address shared risks

Potential threats and pitfalls:

- Potential for conflict, litigation, and disputes with customers, partners, and suppliers over risk-sharing agreements
- Inability to determine the appropriate insurance premium for various risks
- Becoming "over-insured" or purchasing insurance in noncritical areas

Trend #5 Reputation risks accelerate and amplify

To survive in a hyper-connected world dominated by mobile devices, social media, and evolving expectations from society, leaders will proactively address accelerated, amplified risks to their organisation's reputation.

Examples include:

- ✓ A media conglomerate which fired its head of communications for an offensive personal social media post (which went viral in a matter of hours) in an effort to prevent further damage to its reputation
- ✓ Food safety incidents which cause significant reputation loss and revenue impact for food and beverage companies. The impact on a company's reputation is often intensified due to the negative attention received through social media channels

Forces driving this trend:

- Social media creating a more connected, networked world where information is rapidly amplified
- Mobile technologies creating hyper-availability in which people are always available and connected
- An upsurge of socially conscious consumers, and growing consumer activism, putting pressure on businesses to be socially responsible and transparent
- Multichannel marketing strategies built on social platforms allow for greater interactivity for consumers and less control for brands

Continued on next page…

Opportunities arising:

- Develop new capabilities for proactive brand-related crisis management
- Initiate targeted campaigns and develop an external ambassador program to nurture external brand advocates
- Foster a more risk-intelligent culture to help employees see the reputation implications of their actions

Potential threats and pitfalls:

- Personal online activity of employees can cause reputational damage to the organisation
- Organisations may be forced to respond to risk events in haste without fully investigating the situation

For more details, and to review Deloitte's other five trends, check out:
https://www2.deloitte.com/us/en/pages/risk/articles/future-of-risk-ten-trends.html

S U E T R E Z I S E – *Sue-lutions Ltd*

Sue Trezise has over 12 years experience providing risk expertise and advice for government and organisations on strategic, enterprise and operational risk management. An experienced facilitator, Sue assists communication between technical experts and non-technical stakeholders and makes managing risk practical and effective.

LEADERSHIP IN THE RISK PROFESSION – ARE YOU BALANCED

MARK BREWER

Leadership is a critical skill for the risk profession. But perhaps not in the way you might think.

Because gaining influence is critical, the practice of effective leadership focuses heavily on our interpersonal behaviour, including the way we interact with others, how we communicate, make them feel and gain their trust. For without trust it will be almost impossible to recruit others to your cause, regardless of how important or pressing it is.

When considering the importance of leadership practice, we frequently place emphasis on those in formal leadership or managerial positions. People in such jobs are assessed and renumerated for their ability to lead, so it is not unexpected to focus our thoughts on them. But these roles have a degree of inherent authority, which can actually make the work of leaders in them easier.

The real challenge of leadership in the risk profession is for those of us expected to lead others in situations where we don't have any formal authority to rely on. As in a number of similar professions throughout the public and private sector, we often work in specialist principal or senior advisor roles. The business's focus is mainly on the expertise we bring, and where we do fulfil a formal managerial or leadership role, this is usually within our specific area.

Yet, as risk professionals, we actually need to practice leadership in everything we do. We are expected to lead the risk function within our organisation, ensuring the conduct of good risk practices, and the attainment of specific achievements or benefits associated with this critical work. We must also guide the risk function throughout the enterprise, across business units, command lines, areas of conflicting authority, arbitrary boundaries, and sometimes organisations and sectors.

We are often called upon to provide advice to senior leaders and encourage then to take specific actions, even where doing so may not be popular. Occasionally, we may even find ourselves actively trying to gain 'facetime' with decision-makers so as to advocate for immediate changes to planned activities. We do these things because they are important, and they highlight the importance of leadership to all roles within our profession.

So, how do you lead when you don't have positional authority? Why should others follow you or your advice?

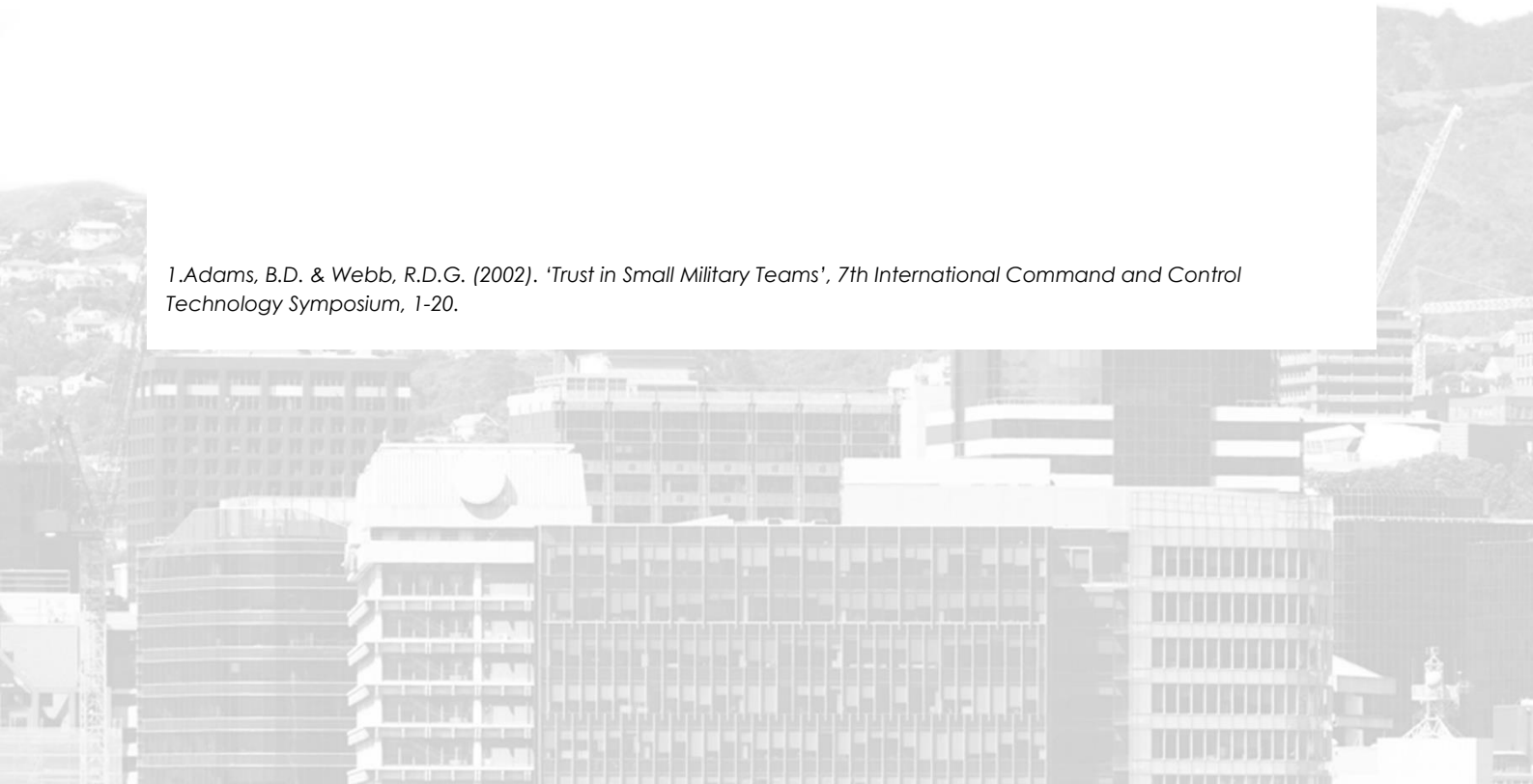
The essence of leadership is influence; the ability to convince others to follow your vision, your example and your directions. Where there is no formal authority available to compel or coerce others to follow, the practice of leadership becomes even more important. For risk professionals this challenge is inherent in just about every role we fill.

Continued on next page…

As professionals, trust is often acquired as a result of our specialist technical expertise. Competence in this area is critical to our employment, and we spend a lot of time acquiring the necessary skills and qualifications to do our jobs effectively. Without technical competence our advice cannot be fully trusted, and a Canadian study has rightly pointed to a lack of competence as one of the fastest ways for a leader to lose the trust of their team.
However, how we make people feel is what gains trust and influence the quickest. The study of trust in small teams in Canada actually highlighted benevolence (kindness, compassion and goodwill) as the most influential element in gaining an individual's trust. How we make others in our workplace feel, is therefore gaining in importance against technical skills as a key determinant of professional effectiveness.

Because risk expertise and competence clearly remain important, the key message here is the need for balance in our practice and professional development. Hard-skills will only get you so far. In addition to technical courses, you also need to consider development opportunities which build greater self-awareness, enhance your interpersonal communication and soft-skills.

So, how balanced is your professional practice? When was the last time you invested time in improving the way you interact and communicate with your workmates, colleagues and senior leaders? What are you going to do this year to give yourself the boost you need to advance the importance of risk practices in your organisation and the direction of your career?



1.Adams, B.D. & Webb, R.D.G. (2002). 'Trust in Small Military Teams', 7th International Command and Control Technology Symposium, 1-20.

MARK BREWER

Mark Brewer has extensive experience as a learning facilitator and leadership coach, having served as the Commander of Leadership Development for the Royal New Zealand Air Force and Research Officer for the New Zealand Defence Force's Institute for Leader Development. Mark now focuses on building leadership capacity in the public sector and improving the performance of not-for-profit organisations. He most recently worked as a principal advisor, designing and delivering leadership development programmes for the United Nations and New Zealand Ministry of Foreign Affairs and Trade in South East Asia and the Pacific Islands. Combining a post-graduate academic research background in human resource development, with deep expertise as a public sector manager, programme manager and organisational excellence advisor, Mark is well positioned to help leaders improve their leadership practice.

BOOK REVIEW by Sally Pulley – Extrinsic Services Ltd

The Precipice: Existential Risk and the Future of Humanity by Toby Ord

"This book is not just a familiar story about the perils of climate change or nuclear war. These risks that first awoke us to the possibilities of destroying ourselves are just the beginning. There are emerging risks, such as those arising from biotechnology and advanced artificial intelligence, that may pose much greater risk to humanity in the coming century".

Toby Ord is a Senior Research Fellow in Philosophy at Oxford University's Future of Humanity Institute. He gives credit to the vast amount of research support that he received from others, and the many experts who gave time to ensure that the book contains state-of-the art knowledge.

What attracted me to the book was the exploration of the science behind the risks that we face, and the discussion about how such risks can be quantified.

Overall, the author thinks that the chance of an existential catastrophe striking humanity in the next hundred years is about one in six. These odds are comparable to playing Russian roulette.

"*Understanding the risks requires delving into physics, biology, earth science, and computer science; situating this in the larger story of humanity requires history and anthropology; discerning just how much is at stake requires moral philosophy and economics; and finding solutions requires international relations and political science*."

The discussion of our history includes examples of nuclear close calls, which are quite chilling, as is the list of the escapes of pathogens from laboratories. These lists of incidents are themselves incomplete, because humanity does not have a full picture of what has happened in countries where the reporting of such incidents is sparse, non-existent, or politically suppressed.

So why is the book relevant to readers of RiskPost?

The book was written before the Covid-19 pandemic. Pre-Covid, a pandemic may not have appeared on many organisation's risk registers, even with the many advance warnings provided by experts and global risk forecasts.

During the Covid pandemic, organisations and professional bodies have reviewed approaches to managing risk, and we can expect this reflection to continue as impacts of the pandemic run into the future. Looking to the longer-term, the unforeseen shocks and impacts of this pandemic may influence the manner in which organisations consider their future risk landscapes.

Rhetorically, how many people have experienced problems when discussing the future, and foreseen risks that have the highest rating of consequence (potentially catastrophic for an organisation) but very low ratings of probability (or likelihood, to use the term adopted in the standards)?

Terminology such as 'improbable', and 'highly unlikely', may lead to the sceptical dismissal of such risks, which may sink to the bottom of an organisation's risk register – if the risks ever appear on the risk register at all. When such a risk becomes reality, an organisation may sink into a morass of recrimination and legal battles and take a long time to recover, if recovery is possible at all.

This book contains approaches and reference materials that support discussion of future risks, and how to quantify them. Importantly, the discussion addresses how risks combine, compare and interact.

The first half of the book contains the main text, which runs to 240 pages. The second half contains another 225 pages of useful reference materials: resources; acknowledgements; appendices; further reading; notes; bibliography; and index.

We as individuals may feel that discussion of existential risk to humanity is not part of our 'day jobs', and that we have no power to effect change. The book's website identifies what you can do, and provides resources for individuals interested in safeguarding humanity's future. This includes a link to the nonprofit 80,000 hours, which provides research and support to help people switch into careers that tackle the world's most pressing problems.

The Precipice: Existential Risk and the Future of Humanity, by Toby Ord

UK Edition, published by Bloomsbury Publishing Plc

Hardback ISBN: HB: 978-1-5266-0021-9

SALLY PULLEY - *Extrinsic Services Ltd*

Sally is a director of Extrinsic Services Ltd. Extrinsic melds the crafts of intelligence with risk management and project disciplines to help organisations explore and own their unique futures. Sally was a member of the RiskNZ Board from 2015 to 2020.

MANAGING RISK IS MORE THAN JUST REGISTERING IT

DR FAHIMEH MCGREGOR (ZAERI) – *DELTA Informed Decisions*

Risk is just an expensive substitute for information.

Adrian Slywotzky

There is a story in your data, but your tools just don't know how to tell it. That story could be the difference between averting risk or ignoring it, but that story must be visually and contextually brought to life. This is storytelling with data and it will change the way you see how risks are interrelated and you can revolutionise problem-solving.

Data visualisation is not a common skill. Those hired into analytical roles typically have quantitative backgrounds that are used to find data, pull it together, analyse it, and build models. They do not usually have skills in design that helps them communicate the analysis to an audience of decision-makers, which is the only part of the analytical process stakeholders will see. More than ever those without technical backgrounds are being asked to interpret data, actually increasing risk not averting it.

The first step in presenting data for accurate interpretation is understanding people. People learn through story and data must tell the story of what risks exist in a way that has a beginning, middle and conclusion so that decisions jump from the page, not confuse and waste time.

Data communication to reduce risk sits at the intersection of science and art and it's time for a revolution in risk management. Too often organisational risk is registered but not resolved. When risks are registered, their interrelationships are not always identified and solutions that could solve multiple problems, are not devised.

As sometimes happens, waiting until the end of the financial year leads to the discovery of unknown risks or worse, known ones that blew out to be much bigger than predicted and budgets collapse.

The leader's Responsibility

Leaders are responsible for creating visibility of risks in projects. Risk registers assist in this process; however, issues are not always listed according to priority and the data used to make key decision is often outdated or poorly presented.

Regular data feeds that provide vital information must be presented visually in a way that all team members can understand and make crucial decisions about the future of projects.

The first step in good data presentation is accurate data gathering. People are complex and do not always present critical information without it being requested. However, that process can fail when the right questions are not asked, and the base data is not presenting the whole picture.

This is why I am an advocate of the LEAN 5 Why's principle to assist in getting to the heart of the problem and having a more accurate assessment of risk.

Managers may think of lean as only process improvement, seeing it prominently as tools and techniques but not a culture of employee engagement. Therefore, they embark on a methods only approach to lean. In this way, they neglect social aspects for sustained change and continuous improvement.

Continued on next page…

As a result, managers taking the easiest path, delegate the implementation to process engineers and consultants, not realising the need for their personal involvement. Because of this, there is a high likelihood of poor decision making, through delegating responsibility without discernment. This, in many cases, results in inappropriate delegations to process engineers and consultants who themselves may or may not take a suitable approach to lean.

Risks Are Always Interrelated

According to Barki et al. (1993), there are causal relationships between risks in any type of project, which makes individual risk management ineffective. Chapman & Ward (2003) suggest that risk analysis without assessing risk interactions results in a superficial and incomplete understanding of risk.

The most effective responses in the treatment of some risks may be to reduce the probability of occurrence of risks that precede them (Aloini et al., 2012; Echeveste et al., 2017). Hence, there is a need for research to collect empirical evidence on the relationship between risks in an organisation. Visualisation of the relationships between risks has been used in software development projects not only to understand such relationships but also to demonstrate the effects of the risks and the factors that originate them (Wallace et al., 2004; Aloini et al., 2007).

The 5 why's Solution

The 5 WHY's approach, a Lean Management tool, is critical in reframing and re-engaging teams to focus on project risks and prioritising their solutions.

In terms of pedigree, '5 whys' traces its roots back to the Toyota Production System (TPS). It also plays a key role in Lean (a generic version of TPS) as well as Six Sigma, another popular quality improvement (QI) methodology.

Father of the Toyota production system, Taiichi Ohno describes '5 whys' as central to the TPS methodology: "The basis of Toyota's scientific approach is to ask why five times whenever we find a problem … By repeating 'why' five times, the nature of the problem, as well as its solution, becomes clear. The solution, or the how-to, is designated as '1H.' Thus, 'Five whys equal one how' (5W's=1How)". (Ohno. T 1988)

This quote also makes the case for the technique's simplicity. Asking 'why' five times allows users to arrive at a single root cause that might not have been obvious at the outset. It may also inspire a single solution to address that root cause.

The pedagogical argument for '5 whys' is that it creates an 'aha moment' by revealing the hidden influence of a distant cause, which illustrates the importance of digging deeper into a causal pathway. This quick and easy learning experience can be a powerful lesson in systems safety.

End at The Beginning

Good stories always have closure and data interpretation is no different. When we only see a partial story, we draw conclusions and make decisions that increase the risk of failure. Worse, when we have all the data, but leaders are not shown it in a meaningful way we overlook critical detail.

Good data visualisation will end where it began, by presenting the story of how you got where you are, highlighting what decisions can be made, and outlining what will be the results of each action. Once the risk is registered it becomes part of the organisational knowledge that informs the next project.

Mischief Managed.

Continued on next page…

References:

Aloini, D., Dulmin, R., & Mininno, V. (2012). Risk assessment in ERP projects. Information Systems, 37(3), 183-199. http://dx.doi.org/10.1016/j.is.2011.10.001.
Barki, H., Rivard, S., & Talbot, J. (1993). Toward an assessment of software development risk. Journal of Management Information Systems, 10(2), 203-225. http://dx.doi.org/10.1080/07421222.1993.11518006.

Chapman, C., & Ward, S. (2003). Project risk management: processes, techniques and insights. USA: John Wiley.

Echeveste, M. E. S., Rozenfeld, H., & Fettermann, D. C. (2017). Customizing practices based on the frequency of problems in new product development process. Concurrent Engineering, Research and Applications, 25(3), 245-261. http://dx.doi.org/10.1177/1063293X16686154

Wallace, L., Keil, M., & Rai, A. (2004). Understanding software project risk: a cluster analysis. Information & Management, 42(1), 115-125. http://dx.doi.org/10.1016/j.im.2003.12.007.

DR FAHIMEH MCGREGOR (ZAERI)

Principal Consultant - DELTA Informed Decisions

Dr Fahimeh Zaeri is a creative lead and people inspirer using data to drive successful business decision making. For more than 15 years she has been leading teams in improving business performance and productivity by developing a data-driven culture and the use of analytical solutions to reduce risk and build success.

THE ROLE OF TRAINING IN RISK MANAGEMENT

DR BOAZ HABIB - *IANZ*

The year 2020 highlighted many realities for us in the wake of Covid-19 pandemic. But the one it put a spotlight on was our ability (or lack of it) to manage our emergent risk blind spot i.e. the pandemic itself. We were made acutely aware of how woefully inadequate our preparation was to deal with the pandemic aftermath, be it in health care, the economy, our business operations or even in our personal lives. We are only just reeling back from its trail of havoc wreaked over the past year however our approach so far still seems to more akin to 'patch up' than preventative.

How did we get here? It would be surprising if the answer had little or nothing to do with risk management. The media is riddled with stories and examples of decisions made by governments, organisations, firms and even individuals that showed a lack of awareness and a lack of planning for the pandemic.

The pandemic has been a global wake up call for organisations shaking them out of their slumber of short-term goal setting strategies and prompting them to open their eyes to long-term planning opportunities and preparing for disruption. Whilst a big shift has come about in how society thinks and operates post-pandemic, it is difficult to expect that it has all the tools and understanding to clearly map out its next steps given how things panned out in 2020 already. This is where the astute application of risk management principles can be a highly effective tool.

Professionals who deal with risk are in a unique position to bring awareness and structure to the process of risk management. Training in risk management can be an influential strategy to help businesses and professionals achieve this. Training helps provide a holistic approach towards addressing risk. It helps us see things we may not otherwise with our short-term priority blinders on. Training can provide a safe environment to discuss big picture risks that we may not have the opportunity to talk about in our work places. Risk management training is about building resilience and flexibility in our risk fibre. It is about providing continuity management for emergent risks such as a pandemic.

The New Zealand Quality College (NZQC) is developing courses that are highly practical in nature and suitable for the practicing risk management professional. As the training arm of the Accreditation Council, NZQC is well placed and qualified in the training domain to address this training need. In collaboration with Risk NZ, NZQC have developed a portfolio of courses for the risk management community that cover a range of skill areas from risk fundamentals through to risk practitioner level based on ISO31000 principles, framework and processes. The highly practical nature of training focuses on the how of risk management through case studies and practical implementation exercises.

1. Risk Management ISO31000 Foundation – Overview of risk management systems and how to apply a risk management methodology in an organisation
2. Implementing a Risk Management System – How to design, develop and implement a risk management systems based on ISO 31000 Risk Management Guidelines, Terminology and Principles
3. Risk Management Practitioner – Provides existing risk management practitioners with the opportunity to demonstrate their knowledge and skills for design, development and implementation of a risk management framework for their organisation and its compliance obligations. Participants get to do an in-course assessment allowing them to practice techniques to be applied post course.
4. Risk based Operational Planning – Provides participants with the knowledge and skills to develop and implement an operational plan and manage the associated risks to achieve required goals and objectives.

The role of training in risk management exists to support integration of risk management into organisations as a more preventative measure than a patch-up after-thought. Any expression of interest or queries can be sent through to the RiskNZ office.

DR BOAZ HABIB

General Manager NZQC

www.ianz.govt.nz

INCIDENT REPORTING SYSTEMS, A COMPARISON OF FOUR CASE STUDIES

SILVIA ZANINI

Incident reporting systems are used to report incidents and near-misses. These systems can have a wide reach, when they are used by several organisations within a sector, or can be limited to a single organisation.
Both types of system are beneficial, as they enable information to be shared across, or within, organisations, which may lead to active learning (ie, becoming aware of an issue and doing something to fix it) and consequently fewer future incidents and near misses. For an incident reporting system to be successful, certain characteristics need to be present.

This article covers these essential characteristics, provides three examples of effective reporting systems, and one example of a system which, despite being created with the best intentions, did not achieve what it was set to do, as it lacked those traits.

Characteristics of effective incident reporting systems

Reporting systems succeed when there is trust, achieved by ensuring that there will not be retribution for reporting accidents or near misses; to enable trust there must be a guarantee of confidentiality, which can be provided by de-identifying the reports or enabling anonymous reporting. It's important to remember that, in environments concerned with attributing culpability, errors still occur, however willingness to report might decline, in which case learning from failure will not occur. The system should also be administered by an independent body, or at least the incident investigations should be carried out by an independent team.

Reporters need to be assured that active learning (ie, becoming aware of an issue and doing something to fix it) will occur, that reporting will result in positive action, as otherwise reporting will be a waste of time. The system needs to be accessible and easy to use. Finally, organisations need to be educated to the benefits of reporting systems, to overcome their need for secrecy or their fear of litigation, and increase the rate of reporting.

Reporting systems are used widely used, some good examples are the ASRS, CROSS, and FINANS reporting systems

The NASA Aviation Safety Reporting System (ASRS) captures confidential reports, analyses the data, and disseminates vital information to the aviation community https://asrs.arc.nasa.gov/. The system was created following the December 1st 1974, Trans World Airlines flight 154 crash, which killed the 92 people on board, and the realization that two near misses (one on the same day) had previously occurred in the same circumstances, but knowledge of this was not widespread, as it was confined to the respective airlines individual reporting systems.

The characteristics of ASRS are very much those of an effective reporting system. An environment of trust is provided, with people feeling safe to report. The identity of reporters is protected and the non-punitive element of the system is respected, with no information submitted used for disciplinary action. Reporting is voluntary, with aviation personnel motivated to report, because reporting highlights issues from which learning occurs. The system is independent, with reports analysed and investigated and data held by NASA and not by aviation organisations, and easy to use. ASRS is effective because the data contained in the reports is rapidly transformed into intelligent and useful safety information and shared with the aviation community. Time-critical information is shared via alert messages, while non time-critical information is published in regular newsletter. All information is stored in the ASRS database, available to the public for further analysis. All this promotes active learning.

Continued on next page…

ASRS has been very successful and contributed to today's high safety standards of the aviation industry and increasingly it is being acknowledged that this model of incident reporting provides an accurate early warning system for the identification of emerging issues. Other industries have acknowledged the benefits of ASRS and have adopted, and adapted, the model to increase their own safety efforts. The most successes have been experienced by the nuclear industry, the maritime and rail sectors, and by the medical community. Other industries, also attracted by the benefits of such reporting systems, started introducing their own versions: the Confidential Reporting On Structural Safety (CROSS) system established in 2005 is an example and so is the FINANS anonymous reporting system created and implemented for a financial trading organisation.

CROSS (https://www.structural-safety.org/) is an internet-based system, with confidential reports submitted via user-friendly web forms. The identity of reporters is protected: the reports are not anonymous, because further information may be needed from reporters, however once all information has been collected the forms are de-identified.

CROSS facilitates active learning: CROSS reports and recommendations have contributed to strengthening regulations and structural requirements, and have highlighted concerns which have been addressed by regulators. The most critical reports, and related analyses, are published in quarterly newsletters and added to the CROSS database. Other reports are added to the CROSS database without further analysis, and may be included in other publications if trends are identified. CROSS reports have contributed to raise risk awareness by providing advice on common industry design issues, and to a reduction in the number of deaths and serious injuries, as industry and regulators have acted on communications issued, resulting in improved safety culture of the UK construction industry. The success of the CROSS system is also reflected by its adoption outside the UK, with CROSS now sharing its database with Southern Africa, Australia, New Zealand, the USA and soon Germany.

Financial organisations also use incident reporting systems, as although these are not safety-critical entities, accidents can be highly damaging for both organisations and economies. In a financial trading organisation, a confidential incident reporting system (FINANS) was implemented to facilitate voluntary reporting via a website. In a two-year period the system recorded 1,042 reports – approximately 10 per working week - a high rate of reporting, possibly due to reporters belonging to the same organisation and having heightened system awareness due to communication and training. Analysis of the incident reports enabled the identification of the causes of errors and accidents, as well as the skills and behaviours that contributed to errors detection and avoidance. The analyses provided many insights that could contribute to active learning. For example, the research found that "teamwork and situation awareness skills are essential to capturing and preventing error" which seems counterintuitive for an industry like financial trading, where performance is highly individualised. This information may be useful when introducing system or organisational changes, or when recruiting, as it increases knowledge of communication and cooperation needs between teams, as well as informing on the operator skills that could lead to error reduction and avoidance. Through the incident reporting system, the researchers were able to highlight causes of incidents and near-misses as well as the skills and actions needed to avoid incidents, enabling the organisation to adopt targeted corrective action to better manage risk.

What happens when an incident management system is not effective?

As part of a research into the Pike River Mine disaster, the Pike River Coal (PRC) incident reporting system was analysed. The system lacked many of the characteristics of an effective incident reporting system.

The PRC incident reporting system was not confidential, which resulted in employees suffering negative consequences for the reporting they had made, while repeated reporters were perceived to be troublemakers, or were made to do additional work to fix the issues they had reported. The system lacked independence, with the incident reports often investigated by the reporter's own manager or colleagues. This lack of independence sometimes resulted in hostility and ostracisation, and in turn decreased the trust in the reporting system.

Rapid and intelligent feedback following reporting of issues helps to ensure that reporters keep reporting. At PRC there was some evidence of reports acted on, but many more were simply not addressed, many repeated issues not actioned. There was no established mechanism to close the feedback loop to reporters, hence workers would not be aware of any action taken as a result of accidents or near misses. The lack of action and feedback had a negative effect on the reporting culture, employees no longer saw value in reporting and doubted that reporting would address the issues raised, deterring them from further reporting. It is unclear how many accidents were reported compared to accidents occurred, quite possibly only a tiny percentage. PRC proved it did not possess a learning culture when it cleared the backlog of accident reports without investigating them, denying itself the opportunity to analyse and learn from the reports, effectively negating the main purpose of reporting.

Continued on next page…

The deficiencies of the reporting system created resentment and anger and ultimately failed the employees, as one of the avenues that should have been available to them to raise concerns was not viable.

Conclusion

Confidential incident reporting systems can promote knowledge sharing by providing and encouraging a culture where it is safe to share information on incidents and near misses. In turn, this information can foster active learning, which occurs when changes are implemented as a result of lessons learnt. Trust in the reporting system is essential for the reporting to happen. Trust in the system is achieved not only by fostering a just culture (where individuals are not punished for actions, omissions or decisions taken by them that are commensurate with their experience or training, but where gross negligence, willful violations and destructive acts are not tolerated) but also by guaranteeing confidentiality, achieved by de-identification of the reports or by enabling anonymous reporting, and ensuring that incidents are investigated by independent teams.

The ASRS, CROSS, FINANS reporting systems support the view that effective reporting systems promote active learning: aviation safety has increased considerably since ASRS was introduced and it is generally acknowledged that without confidential reporting systems the sector would not have reached such safety standards. CROSS and FINANS have also promoted active learning: CROSS in a similar fashion to ASRS, with alerts and regular newsletters sharing knowledge and influencing industry and regulators, while FINANS has shown that by analysing data from reports, causes of errors and near misses can be identified, and subsequently addressed. The last system, that of PRC, shows how, when the described key characteristics are lacking, active learning is inhibited and reporting is rendered meaningless.

Bibliography

Chappell, S. L., Connell, L. & O'Leary, M. J. (1996) Early Warning: Development of Confidential Incident Reporting Systems, Moffett Field: NASA, available online at: https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20020036021.pdf; accessed 2 February 2019.

Connell, L. J. (n.d.) Cross-Industry Applications of a Confidential Reporting Model, available online at: https://asrs.arc.nasa.gov/docs/rs/62_Cross_Industry_Applications_of_Reporting_Model.pdf; accessed 9 January 2019.

Dekker, S. W. A. (2012) (2nd ed.) Just Culture. Balancing safety and accountability. Ashgate Publishing Limited: Aldershot.

Dekker, S. W. A. (2009) 'Just culture: who gets to draw the line?', Cognition, Technology and Work, 11(3), pp. 177–185.

Leaver, M. P. , Griffiths, A. & Reader, T. (2018) 'Near Misses in Financial Trading: Skills for Capturing and Averting Error', Human Factors, 60(5), pp. 640– 657.

Leaver, M. P. (2017) Human Factors in Financial Trading: An investigation of error, non-technical skills and culture. PhD thesis, London School of Economics and Political Science, London, available online at: http://etheses.lse.ac.uk/3625/; accessed 22 January 2019.

Leaver, M. P. & Reader, T. W. (2019) 'Safety Culture in Financial Trading: An Analysis of Trading Misconduct Investigations', Journal of Business Ethics, 154(2), pp. 461–481.

NASA: ASRS (2001) ASRS: The Case for Confidential Incident Reporting Systems. Moffett Field, California: NASA: ASRS.

S I L V I A Z A N I N I – *MSc, CIMA, CGMA, AMBCI*

Silvia is a risk manager currently working in the financial services sector, she recently gained a Risk, Crisis and Disaster manager MSc at the University of Leicester.

Silvia has extensive risk and audit experience gained in Italy, the UK and NZ.

PROFESSIONAL DEVELOPMENT FOR RISKNZ MEMBERS

MARK BREWER

Without question, 2020 was challenging across both the private and public sectors. The year's unique trials were often frame-breaking, and emphasised the growing complexity and unpredictability of the modern globalised World. Changes which also mirror the increased speed of transformation across many societies, driven in large part by rapid technological advancement and increased access to information.
Such turbulence has by necessity hastened changes in the practice of risk management, as well as our expectations of those operating as risk professionals. We are forced to accelerate our capabilities and speed of adaptation, to keep pace with the growing opportunities and threats of our evolving business environment.

For risk professionals this constant churn means it is no longer possible to maintain professional mastery for a long period as was previously the case. Societal and technical changes are occurring so fast, that it would be naïve to think it possible to learn everything you need at the beginning of a professional career, and remain competent throughout.

Practices for identifying and managing risk do not remain static, and as a profession we must drive constantly for improvement and advancement. The same is true for individual risk professionals, who must keep up to date with modern professional expertise. While technological advances will help with this transformation, the 'human in the system' will remain the most important element across our professional risk community.

'Learnability' is consequently becoming the most important skill for modern professionals. Constant focused development can ensure individuals continually have the knowledge, skills, and attitudes necessary to operate effectively and ethically under conditions of increasing uncertainty and complexity. Also, because it is no longer possible to know everything, learning must be constant and occur at the 'speed of need', not infrequently and at the speed of personal comfort.

Central to this concept of 'life-long learning' is the importance of personal ownership, self-awareness and continual critical self-reflection. These practices mirror those methods used by professional athletes to attain peak performance, and are now used extensively throughout the public and private business sectors. Risk professionals need to adopt a similar approach, to ensure they are adequately prepared for what lies ahead.

Professional development in this manner requires intellectual humility. The moral courage to ask ourselves the uncomfortable questions and challenge our own thinking. To advance both individually and as a group, we need to constantly try to find out what we don't know, and identify any assumptions which may no longer hold true. Openness to challenge and diverse thinking must therefore be sought out, encouraged and rewarded.

While specific expertise remains crucial, it is frequently the breakthroughs made from honest introspection and focused adaptation which provide the biggest gains in professional competence and leadership ability. Self-awareness and intellectual humility have now become critical job requirements. Although less tangible, these 'soft skills' are increasingly becoming more important than traditional 'hard skills', especially for managers.

With these challenges in mind, RiskNZ has organised a new suite of development opportunities commencing in 2021, specifically designed to boost the learning and leadership capabilities of risk professionals. These activities are hands-on, immersive learning opportunities which complement our traditional development offerings, so as to improve an individual's interpersonal skills, in addition to their technical proficiency and managerial competence.

Membership education and professional development is one of the five key focus areas critical to the success of RiskNZ. It is clear that the introduction of these unique workshops, will significantly enhance the value RiskNZ provides its members, and ensure they are better positioned for the challenges of the future.

OUR NEW BOARD – WHO ARE WE?

I'm really excited to work alongside such a great board.

We've had four Board Members join us this year – Chris Kumeroa, Managing Director of Global Risk Consulting; Lorna Hayward, Head of Risk and Audit at Christchurch City Council; Darroch Todd, Risk Manager for Auckland Unlimited and Suralda Timmerman, Principal Internal Audit Advisor at Accident Compensation Corporation.

Alongside our existing Board Member team of Gary Taylor (Financial Markets Authority); David Turner (Managing Director RiskNZ); Brent Sutton (Safety Associates); Imogen Perez (Ministry of Business, Innovation and Employment); Lynda McCalman (Hancock Forest) and Vaibhav Bhatnagar (Watercare) and myself at the National Emergency Management Agency, we are committed to providing great opportunities to grow risk capability in New Zealand.

We all look forward to working more closely with our members and to develop tailored solutions to help you, to help others, to grow their confidence and understanding around managing risk.

To learn more about us all, see our website.

JANE RÖLLIN – Chair, RiskNZ

RiskNZ

RISKNZ INFORMATION

THE MANAGEMENT BOARD AND OFFICERS OF RISKNZ

Chair:	Jane Röllin	Deputy Chair:	Suralda Timmerman
Secretary:	Lorna Hayward	Managing Director:	David Turner
Treasurer:	Gary Taylor	Administration Officer:	Emily Thorn

Management Board Members:

Brent Sutton
Chris Kumeroa
Darroch Todd
David Turner
Lorna Hayward
Lynda McCalman
Vaibhav Bhatnagar

Marsh

Risk, Advisory and Insurance Solutions

In an environment where growing challenges require business resiliency, it takes a deft combination of strategic advice and innovative solutions to manage risk.

Rising geopolitical and geo-economic tensions, environmental issues, rapidly evolving cyber and technological advances make anticipating emerging risks business critical.

Marsh can help you look ahead, articulate the relevance of emerging risks to your organisation, and provide the expertise and solutions required for timely decisions.

We are proud to be a Premier Sponsor of RISKNZ and the Risk Professional of the Year Award.

RiskNZ was delighted to host its Annual Conference on 13 April 2021 at the Wellington Club. Our theme for 2021 was Reflect and Reconnect.

Reflection

The conference programme was action-packed with opportunities for delegates to participate in Q&A sessions directly with different panels, plenty of great speakers reflecting on specialist risk topics and the highlight of the day, the 2021 Awards of Excellence.

Reconnect

Delegates at the conference took the opportunity to connect with over 100 other delegates, speakers and sponsors. The room was a buzz with all the korero (conversations), and the delight of being able to meet in person after a year of Zoom and Teams meetings.

Speakers and Panels

Our speakers gave real insights into topics such as:

- A Māori worldview on strategy, governance and risk management;
- Emergency management and disaster recovery;
- Enterprise risk management fulfilling its potential;
- Psychosocial risk management;
- Personal resilience, and
- Payment card industry compliance.

More information can be found on this year's speakers and the programme here.

A special thank you to all our sponsors. We are privileged to have them on board and for helping us bring the RiskNZ Conference to Wellington.

BIT Solutions "Complexity made easy - take control"

Safety Associates

axenic Pure Security

SAI GLOBAL

BW BRYAN WHITEFIELD

MARSH


RISKNZ


RISKNZ
The Wellington Club


RISKNZ
The Wellington Club


RISKNZ

Thank you to our Professional Development Feedback Team

A big thank you to our volunteer team who helped assess the proposed RiskNZ professional Development courses.

This initiative was created from what many members wanted being the opportunity to up skill and learn more about different aspects of risk management. While we have a little bit further to go before we can offer the bulk of these courses, the feedback team provided exceptional input which has made the process quicker and more robust.

We thank:

- Kate McHugh
- Dr Fahimeh Zaeri
- Kerry Boyle
- Imogen Perez
- Stuart Dixon
- Bill Grant
- Raymon Sahib
- Rachelle Miller
- Deborah Fisher
- Tiffany Frans
- Suralda Timmerman

RISK MEMBERS FORUM

The RiskNZ members forum is up and running, we created this for members who wanted the opportunity to chat with other members and share experiences, knowledge, and questions in a secure space.

We hope to see some good discussions going forward and are happy to take any suggestions on topics required.

You can access this through the RiskNZ members website here.

Our Sponsor for the Members Forum is 'Axenic' – Cyber and Information Security Professionals.

Successful Communication during Crisis Situations

The 7 most important differences between a tool for professional crisis management and a collaboration tool for daily business

FACT24
Crisis Management and Emergency Notification

Riding your bike on the highway? It's possible but not the best idea for your safety and won't help you reach your destination as quickly. The same is true for managing critical situations: Emergencies and crises teach us again and again that one thing is essential – communication.

Informing the relevant stakeholders, evacuation from a building to calling the crisis management team and keeping employees in their home office up to date, these are just a few examples. The fact that this communication has special requirements is obvious because emergencies and crises have their own rules.

Rules that often overwhelm common office communication tools and put the whole organisation in danger or exposing it to unnecessary risk. Therefore, a reliable communication tool is so important in a crisis.

In the following table we have summarised what you need to pay attention to in the context of communication in a crisis to reach your goal quickly, safely and above all reach everyone you need to.

Requirements for Communication in Crisis Situations	FACT24 Specialised solution for crisis management and emergency notification.	Standard Enterprise Messenger / Instant Messenger Collaboration in daily business.
Accessibility & Efficiency		
 **Automated multi-channel communication** – for fast, reliable, and targeted contact with the option of redundancy	 Automated via e-mail, SMS, phone call, push – even in parallel and several thousand in a few minutes.	 Only one way via Internet and everything needs to be done manually, which takes significant resources.
 **Usage Independent of App / software installation** – to ease usage and access if own IT is not available	 Recipients don't need any software nor internet connection necessarily Crisis staff does not need any installation or company hardware to work with the tool.	 Most tools require to install an App or Software locally for recipients as well as senders of any information.
 **Automated feedback evaluation** – for an efficient information flow with several hundred or even thousands of people to enable informed decisions	 Real time tracking of alerting status and feedback (e.g. info received or available / not available) independently of number.	 Individual feedback needs to be tracked and documented manually.

Successful Communication during Crisis Situations

The 7 most important differences between a tool for professional crisis management and a collaboration tool for daily business

FACT24
Crisis Management and Emergency Notification

Requirements for Communication in Crisis Situations	FACT24 Specialised solution for crisis management and emergency notification.	Standard Enterprise Messenger / Instant Messenger Collaboration in daily business.
Safety & Reliability		
Contractually guaranteed availability through SLAs – for peace of mind as you know the tool is there if you need it	The availability of services is guaranteed contractually at 99.99% for alerting and 99.50% for all other services.	Most enterprise messengers offer SLAs but those are not guaranteed. This means you might pay less if they don't work but there is no commitment that they work at any time.
High standards of data security and data protection to meet legal requirements (GDPR) and secure sensitive data adequately	Development and operations according to ISO standards ISO22301 and 27001. All data stored in Germany / EU.	Most solutions are end-to-end encrypted. Data storage and GDPR compliance depends on service.
Collaboration & Crisis Management Functionalities		
Structured management of tasks for professional and easy coordination	Possibility to predefine actions specifically for scenarios or depending on severity. Flexibility to manage ad hoc tasks in real time.	Partly offered but not integrated into messenger directly, only with separate app which increases the complexity.
Digital collaboration in real time with automated documentation for authorities, insurances, and your own evaluation	Work on status reports, start spontaneous conference calls – everything is documented, completely automated, audit-proof, and exportable via PDF / Excel.	Most tools offer collaboration on documents and files in real time, but the documentation can only be done manually and thereby is not audit-proof.

MENTORING - UPDATE

RiskNZ is receiving requests for mentorship from young risk practitioners that are stepping into new and demanding risk management roles.

Mentees are asking for:

- A seasoned practitioner that they can connect with on a monthly basis.
- Advice regarding quality of risk management practice.
- A soundboard for their ideas.
- Connecting with fellow practitioners (mentees) that are experiencing similar challenges.

RiskNZ has received **five** requests for mentorship in the past month.

Value proposition:

Young risk practitioners have identified a need in the market and they are bringing this opportunity to RiskNZ. RiskNZ has an experienced board and practitioners that could deliver the programme. This programme has the potential for RiskNZ to demonstrate its value proposition to members and to attract new members to RiskNZ.

Pilot:

The following pilot approach is proposed:

1. Collect the names of senior risk practitioners that are willing to be mentors.
2. Collect the names of risk practitioners seeking mentorship.
3. Run a 3-month pilot in using a group mentorship program. 1 mentor to a ratio of 4 to 5 mentees.
4. The pilot will also be used to set-up the mentorship program guidelines which can be reviewed by the Board and Legal before we decide to run a full programme.

If you require a mentor (or would like to mentor), please get in touch (david@risknz.org.nz) and we can discuss the best approach and match you with other risk professionals to share their experiences and knowledge.

Latest Reads

Find all of our latest reads online

- Scientists set to discover secrets of past earthquakes by digging down deep at Cape Palliser
- Government announces ban for live cattle exports by sea
- Sunscreen safety member's bill passes first reading in Parliament
- Facebook data on 533 million users re-emerges online for free

RiskNZ Lunchtime Seminar – 4 May

Don't risk your decisions - stay informed with accurate visual information.

Too many key business decisions are being made on instinct not data.

When data is introduced, it is often misinterpreted, unclear or simply not useful for the organisation.

It's time to reduce risk by first getting access to the data that is actually useful. And then having it presented in a way that offers clarity and meaning, enabling decision makers to back themselves when critical organisational change needs to be made.

This presentation will first strip back the layers and mystery of data interpretation so that all your team members can have clarity around what is valuable. It will then give you the practical tools you need to use data as the driving force to reduce risk and make key decisions with confidence. It will also show you how to motive people to reconnect with data in a more meaningful way, challenging them to drive change in a facts-based environment.

Date: Tuesday 4 May 2021
Time: 12:00 - 1:00pm
Speaker: Dr Fahimeh Zaeri
Venues: Wellington (KPMG - speaker venue), Auckland, Christchurch and webinar available.

Register now.

RiskNZ Tools and Templates

Please see our latest tools and templates in the Members only area of our website.

If you would like to contribute, please get in contact with David Turner (david@risknz.org.nz).

INFORMATION FOR CONTRIBUTORS

Work on Edition 2 of RiskPost 2021 will start shortly with an aim to publish mid-2021.

Contributions should be sent to editor@risknz.org.nz. Articles are welcome at any time; please contact the editor if you wish to discuss an article.

RiskPost provides a service for the display of notices and advertisements that are aligned with RiskNZ's objectives. Members are welcome to submit notices and advertising material to RiskNZ. Notices may describe an activity or service, or advertise a risk management vacancy.

Advertisements can be included in RiskPost and delivered by email to the RiskNZ membership base. RiskNZ's charges for advertising in RiskPost and by email vary dependent upon membership status, and the nature and scale of the advertisement.

For further details on RiskNZ's submissions of notices, advertising, and relevant changes, please send an email to the Administration Officer: adminofficer@risknz.org.nz, or write to:

RiskNZ, PO Box 5890, Wellington 6140

We regularly post events and other useful information on our *Linkedin company page* - so click through and follow for up to date information!

Membership of RiskNZ is open to any person of good character or an organisation engaged in or with an interest in the practice, study, teaching or application of risk management.

RiskNZ is keen to attract a wide range of Individual and Corporate members representing all the different aspects of risk management knowledge and practice. This includes those with direct involvement in the field and those with a personal or community interest.

Find more information on our website here.

REFER A FRIEND!

We are now offering our members a discount for bringing new members on board.

Share the benefits of a RiskNZ membership with your friends and colleagues, and you will receive a one off 25% discount on your next annual subscription!

Make sure they tell us that you referred them and to enter your name on their application form.

To apply, and to find out more about RiskNZ membership, please click here.

This is a trial and will expire on 1 June 2021. Discount applies to existing members only. Discount is for all members and will be based on referrals having paid their subscription.

STUDENT MEMBERSHIPS

Did you know RiskNZ has student memberships?

Are you studying in the area of risk practice, risk management and risk-oriented decision making?

Or know someone who may benefit from our student membership?

RiskNZ student membership comes with many benefits, such as increased connectivity and networking with the growing risk community across New Zealand.

RISK NZ WELCOMES NEW MEMBERS

Individual Members

Hans Pottstock-Vidal	Principal Adviser	Department of Corrections
Tama Rawhiti	Head of Risk	AIG
Chris Webb	Health Safety and Risk Manager	Network Waitaki
Curtis Morton	Senior Risk Manager	Synlait Milk Limited
Chris Kumeroa	Managing Director	Global Risk Consulting
Kathlyn Cardiff	Consultant	EnviroSafe Consulting Limited
John Creagh	Safety and Risk Manager	Alpine Energy Ltd
Raymon Sahib	Head of Risk - Product & Strategy	AIA NZ
Sonia Chandra	Operational Risk Specialist	Southern Cross Health Society
Andy Wisheart	Resilience Manager	RiskLogic NZ
Adele Hawk	Risk and Assurance Specialist	Callaghan Innovation
Fahimeh Zaeri	Principal Consultant	Delta Informed Decisions
Shelly Fawcett	Internal Audit Advisor	Callaghan Innovation
Peter Fitt	Health, Safety and Emergency Management Advisor	Putarmeen Trust
Anna Taylor	APAC Sales Lead	Resolver Inc
Mark Brewer	Managing Director	Profectiviti Limited
Dave Debney	Project Risk Lead	Auckland Transport
Deepti Nadkarni	Risk and Assurance Advisor	Statistics New Zealand
Janette Osborne	Owner/Director	Briar Patch New Zealand
Syd Gilani	Head Performance & Delivery	University of Otago

Corporate Members

Modica Group Ltd