



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

Issue 2 | Sept 2021

@ adminofficer@risknz.org.nz

risknz.org.nz

Post | PO Box 5890, Wellington 6140

<https://www.linkedin.com/company/risknz/>

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.

Copyright © Risk NZ Incorporated, 2021. All rights reserved



A WORD FROM THE CHAIR

JANE ROLLIN

Welcome to our second bumper edition of RiskPost for 2021.

It's been a busy middle "chunk" of the year with preparations for and holding, our Annual General Meeting. Pulling together our stories for an annual review surprised me by the volume of activities we've managed to deliver over the last 12 months. We also took time as a Board to forecast where we want to be in 12 months' time through preparing our annual business plan for 2021/22. Just to recap, we have three key outward strands to our work:

- Meeting **member needs** and growing our membership base,
- Building our networks and reach through **relationships with partners** that adds value to our members,
- **Enhancing risk management practice** through professional development, quality events, networking and communication.

We've started our regional engagement work in Auckland, Waikato/Bay of Plenty; East Coast; Wellington; Christchurch/ Canterbury and the Lower South Island – so watch for further local events to build your network.

A special thank you to our RiskNZ members (Mark Cubitt and Regan Smith) who have stepped up to lead regional engagement. We recognise that Regional engagement is most successful when it is led and delivered by members within the region who truly understand local need. A huge thank you to all our members who are supporting this work and generally joining in to share experiences.



In this edition

Standards update Kristin Hoskin	Page 5
Italy Cable Car Disaster Silvia Zanini	Page 6
How ERM leads can influence board decision making Dr Fahimeh McGregor-Zaeri	Page 10
Integrity Matters Sue Trezise	Page 14
Fake news and misinformation Cameron Li	Page 17
Climate Related Disclosures Q&A Dr Amelia Sharman	Page 18
The Importance of place in understanding physical security risk Chris Kumeroa	Page 21
Building capability for future growth NZQC	Page 27
Risk management - as easy as 1 to 5 John O'Connell	Page 29
Quelling psychological warfare Bryan Whitefield	Page 30
The cost of keeping risk & strategy separate Beau Murfitt	Page 32
Introducing our new premier sponsor Camms	Page 34
Marsh Global Insurance Markets Report	Page 35

A WORD FROM THE CHAIR CONTINUED...

We've been able to hold a number of local sessions on managing psychosocial risk (Tauranga; Hamilton; Auckland) and several 'drinks and nibbles' sessions in Wellington to help our members build their local support networks. Keep an eye out for events in your region, we'll keep you informed through our weekly emails and via our LinkedIn page.

We are also focusing on building our partnerships with key organisations so that our members can have access to a broader range of support and professional development. Our first formal agreement is with the Chartered Accountants Australia and New Zealand (CAANZ) – We'll share more information on this shortly.

The Board has recently farewell-ed two members – Vaibhav Bhatnagar (Auckland) and Lorna Hayward (Christchurch); both will be sorely missed but we are grateful for their contributions and are glad they will remain connected – Lorna will still be our regional focal point in Christchurch / Canterbury.

There are so many things coming up so let me share a few of them! We are already planning for the 2022 RiskNZ Conference (..shh "*Risk and Resilience Summit*"), which we are aiming to hold in March 2022 in Auckland – a 'save the date' notification is coming. We've partnered with Alex Sidorenko from Risk-Academy to bring our members a 50% discount for Risk Awareness Week (11 -15 October) with many thought provoking international speakers. Our training partners are holding a number of professional development opportunities available in the coming months before Christmas, so do check our website for professional development sessions by Bryan Whitefield, AGLX and NZQC.

As I write this from my Auckland based home office in our current Level 4 lockdown, I just want to remind everyone to stay home, stay safe and be kind. Normal service will resume shortly!



RiskPost gratefully acknowledges the support of our premier sponsor Marsh



Back editions 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

FROM THE EDITOR AND MANAGING DIRECTOR

DAVID TURNER



Hello everyone, the year is passing so quickly, and it seems like just last month since we had our March conference!

The past few months have been exciting for RiskNZ as we welcome new members each week and create wider and stronger networks throughout New Zealand and overseas. Jane mentioned our partnerships and I am happy to say we have been attracting good and valuable attention from organisations who would like to work with RiskNZ, and this will help enable our members to have as much opportunity as possible to access good thought leadership and learning opportunities while broadening their own networks.

I have also noticed a shift in the way risk professionals are coming together and openly discussing and sharing their experiences in social events like our popular drinks and nibbles, and more formal environments such as short workshops and webinars. This is great to see and very timely as I have seen a sharp shift in how people think about risk, how they approach risk, and how they challenge thinking to ensure they choose the best methods possible which are right for them and their organisations future.

We are also planning a series of morning sessions where we can get together and share risk experiences and perspectives, deep dive into current risk methodologies, and share tools and thinking around how we may do things within our own organisations. However, this will be a little delayed due to the recent lockdowns but please watch this space.

Please also remember that you are most welcome to contact myself or Emily our Administration manager anytime if you have any suggestions or ideas on what you would like to see or how we may be able to connect you with the right people within the RiskNZ's membership base and partners and sponsors.

Now onto our Riskpost:

A big thank you for the time and effort our authors have placed into their articles, and a special thank you to Emily Thorn, our Administration Manager who has placed a great deal of effort into putting this edition together.

We have had several submissions for this edition and its great to see the diverse range of content which combines advice, experience, and guidance for members, while also including insights into some partner and sponsor knowledge and services which you may find valuable.

We start with our valuable standards update from past board member Kristin Hoskins and move through our submissions from an analysis of the recent Italian cable car disaster, to ERM, and onto integrity in the public sector, so a valuable read and I hope you enjoy this edition.

We are always on the look out for good content so please do not hesitate to contact me to discuss a subject and content which you would like to add to future RiskPosts or to our website.



RISKNZ STANDARDS UPDATE

KRISTIN HOSKIN - ADVISIAN

Standards activity has continued to focus on the editing, commenting, and approvals of upcoming publications by ISO. OB-007 (the Australia-New Zealand Joint Committee) had some changes made by Standards Australia and with no joint standards currently in development has not met for some time. The last major activity of OB-007 was in July to discuss comments to be submitted on ISO/CD 31050 Risk Management – Guidelines for managing emerging risk to enhance resilience. The NZ Mirror Committee has also made comment and submitted ballots on recent ISO work. The ISO plenary meeting took place in May.

Of note:

- ISO/DIS 31073 Risk Management – Vocabulary was approved this month.
- ISO 31050 Risk Management – Guidelines for managing emerging risk to enhance resilience was approved to progress to CD stage.
- ISO/FDIS 31030 Travel Risk Management – Guidance for Organisations was approved to progress to publication (anticipated late September).
- Public consultation on CWA resilience of transport infrastructures ('Guidelines for the assessment of resilience of transport infrastructure to potentially disruptive events') has just closed. This is an interesting document for those with an interest in emergency management or transport. It describes a methodology for infrastructure managers to properly measure the Level of Service (LoS) provided by, and the resilience of, their transport infrastructure to natural hazards.
- The ISO 31000 guidance handbook project is now complete and should be available for purchase very soon.



ITALY CABLE CAR DISASTER

SILVIA ZANINI

1. The “funivia Stresa – Alpino – Mottarone”

On Sunday 23 May 2021, an aerial cable car crashed to the ground in Mottarone, northern Italy, killing fourteen of the fifteen people on board.

In this particular cable car line, the cabins are suspended from a fixed cable and hauled by a separate traction cable to which they are permanently attached, and move back and forth instead of running in a continuous loop. The line had two separate sections, each with two cabins, and passengers changed cabin at a mid-point station.

The line opened on 1 August 1970, in 1997 both fixed and traction cables were replaced, with the last upgrade of the cabins taking place in 2002. The cables were checked again, to ensure they were sound, between 2014 and 2016. The line had not been operating for a period of time due to Covid-19 imposed restrictions and had only reopened on 24 April after the restrictions were lifted. Cabins could usually hold up to 40 people but passenger capacity was reduced due to coronavirus.

The crash occurred as cabin #3 was approaching the summit of Mottarone. When the traction cable snapped, the cabin reversed, gaining speed, until it collided with a pylon, fell about 54 meters to the ground, and then rolled down the mountain, stopping after impacting trees.

2. The risk theories that might help explain the disaster

This article uses two sociological theories of risk, ‘Man-Made Disasters’ (MMD) and ‘normalisation of deviance’, to carry out an inductive analysis of the disaster.

Barry M. Turner, in *Man-Made Disasters*, investigated accidents and social disasters to seek systematic patterns that might have preceded these events. Turner found that disasters rarely develop instantaneously, rather they have long incubation periods, characterised by a number of events that accumulate, while being overlooked or misinterpreted. It is during these incubation periods that a shift from a normal situation, to a ‘notionally normal’ situation occurs.

continued..

In the normal state, people follow the rules, correct information enables the creation and maintenance of precautionary measures which keep people safe. From this starting point, during the incubation period, at first unnoticed events, at odds with the accepted beliefs about hazards and the norms for their avoidance, occur. With time, these events accumulate, because they are either unknown or their implications are not fully understood: over time what was once unacceptable becomes acceptable, remaining acceptable until a precipitating event occurs, leading to the disaster.

Diane Vaughan described this as the gradual process through which unacceptable practices or standards become acceptable. Because the deviant behaviour is repeated without catastrophic results, it becomes the social norm for the organisation, eventually leading to disaster. Vaughan described this process, coined 'normalisation of deviance' while discussing NASA's tolerance of risk in relation to the Challenger shuttle disaster. At NASA deviations from standard procedures, often occurring over an extended period of time, became normal practice, enabling people to conform, even when personally objecting to a line of action: when deviant behaviour occurs so often that it becomes normal, it effectively creates a new set of rules in which the previously unacceptable behaviour becomes acceptable, catching everyone by surprise when the behaviour causes failure that results in disaster. Vaughan also found that at NASA production pressures permeated the organisation and exercised a powerful influence on decision making, increasing the chance of error.

3. What we know so far (pre inquiry findings)

At the Stresa – Alpino – Mottarone cable car, the traction cable snapped and the safety brakes failed to engage, leading to the cabin crashing.

A few days after the disaster, in late May 2021, it emerged that on the day of the crash, the cable car's safety brakes had been disengaged by using a fork-shaped clamp, because they had been malfunctioning and were impeding the operation of the cable car. Following this finding, a few days later it became clear that there had been recurrent malfunctioning issues, and that on many occasions, possibly over several years, the fork-shaped clamp had been used, meaning that the cable car had been operating without safety brakes on a number of occasions.

Why would anyone knowingly disable the safety mechanism that would ensure people's safety in the event of a cable snapping? This behaviour may be explained by using both MMD and normalisation of deviance risk theories.

4. Applying MMD and normalisation of deviance to the disaster

The normal state comprises of the line's safety features, the regular maintenance, the safety tests carried out on a daily basis. As part of the tests, every night the fork-shaped clamp was used to deactivate the safety brakes, and every morning the system would be tested, to ensure that everything was functioning normally, and the safety brakes reactivated. But the cable car would sometimes malfunction, causing issues and delays.

The incubation period begins when, because of the cable car malfunctioning, a habit of deactivating the brakes – by using the fork-shaped clamp – started to form.

continued..

Newspapers initially reported that at least since 26 April 2021, when the cable car reopened post Covid-29 restrictions, this workaround had been put in place to address the malfunctioning issues. The cable car technician (a long standing employee) reported that disabling the safety brake had become the norm and that everyone at all levels of the organisation was aware of this fact, his belief being that the cable would never break because it was in good conditions.

Additional newspapers reports pointed to the fork-shaped clamp being in place as early as 2014, confirming the technician's statement that disabling the brakes had become the norm. If the reports are correct, it means that the cable car had been at times operating without the safety brakes over a seven-year period. The practice of operating the cabin without safety brakes seem to have extended to the #4 cabin too, demonstrated by a photo published by the 'La Stampa' daily, showing the same workaround being used on that cabin two weeks before the disaster. This may point to new norms having indeed formed, leading to the use of the fork-shaped clamp to disengage the brakes becoming widespread, possibly due to the lack of a true understanding of the implications of this behaviour.

At play there is also the dynamic of economic pressure (a cable car that had just reopened, and that was operating at sub-optimal capacity) compounded by pressure from the top to keep the line open: it was therefore important to keep it open, to minimise losses. The day before the disaster there were reports of the cable car malfunctioning. The technician communicated the issues to the maintenance chief and the company owner (a statement denied by the senior manager, while the owner of the company commented he was not aware of the fork-shaped clamp being used and that safety issues were 'someone else's business') and requested that the line be closed to carry out maintenance. But management's preference was to keep the operation going, delaying maintenance until the seasonal break.

5. Conclusion

Human error is often invoked after a disaster occurs. This is a convenient justification, as it fulfils the need for blame apportionment, and deflects attention from the underlying preconditions to the event. By concentrating on human error we ignore why some decisions are made, we ignore the norms through which people evaluate the risks, the norms that may have the effect to attenuate their perception of risk.

The inquiry into the cable car disaster is just beginning, so far 14 parties are under investigation, including the cable car technician, the maintenance chief, the company owner, and the maintenance company.

continued on next page

It will be interesting to see what direction the inquiry will take, whether it will prefer the human error or the system error approach, and its findings and conclusions. However, Italian inquiries are sometimes known for being quick to point the finger and placing the blame on someone, after all blaming someone for something that has gone wrong is emotionally satisfying: for example in 2012, six Italian scientists, and a government official, were sentenced to six years in prison for failing to definitively predict a 6.3 magnitude earthquake which took more than 300 lives and injured an additional 1,600 in the city of L'Aquila in 2009 (the verdict was overturned two years later).

6. Bibliography

Reason, J. (2000) *Human error: models and management*, BMJ.

Turner, B. A. & Pidgeon, N. F. (1997) *Man-made disasters*. 2nd edn. Oxford: Butterworth-Heinemann.

Vaughan, D. (1996). *The Challenger Launch Decision. Risky Technology, Culture, and Deviance at NASA*. Chicago: The University of Chicago Press.

Vaughan, D. (1999), *The dark side of organizations: Mistake, Misconduct, and Disaster*. *Annual Review of Sociology*, Vol. 25:271-305.

SILVIA ZANINI

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.



HOW ERM LEADS CAN INFLUENCE BOARD DECISION MAKING

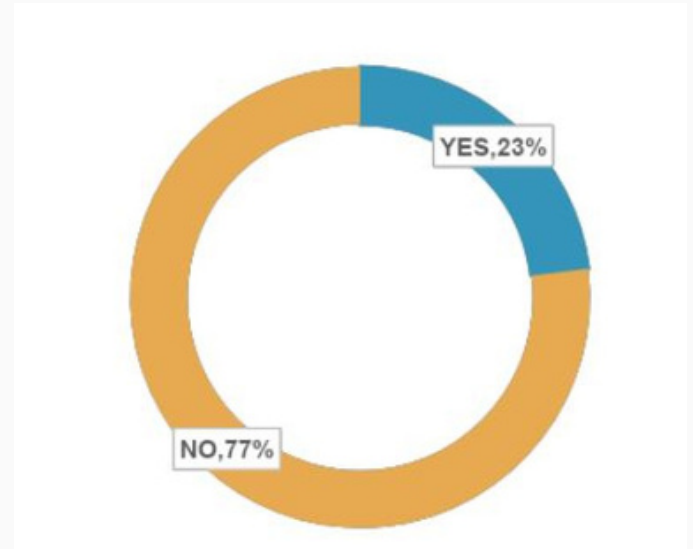
DR FAHIMEH MCGREGOR-ZAERI – DELTA INFORMED DECISIONS

Enterprise Risk Management (ERM) is an essential activity for businesses of all sizes across many industries. A report by Gartner titled 'Risk Reporting That Drives Action - Reducing Executive Effort' highlights some of the barriers ERM leads face when it comes to influencing decisions. It also discovered what successful ERM leads are doing right now to gather, prepare and present data that influences board-level decisions.

The Risk of Ignoring Risk Reporting

According to the Gartner report, risk reporting is considered critically important, with 79% of respondents saying that making risk reporting more impactful is a top goal. Despite this, there is a void between identifying potential business problems and getting executives to act.

77% of respondents don't feel that they regularly achieve decision influence, and so risks and threats are overlooked, potentially causing significant disruption to the organisation.



However, it may not be the threat that's causing a lack of action. Often it's the way the data is presented and how it aligns with the boards' current objectives that can cause decisions to be delayed or, even worse, not made at all. Therefore, ensuring you have the correct data presented in a digestible and impactful way is crucial.

Use Data to Tell Powerful Stories & Prompt Action

An imbalance between qualitative and quantitative data is one factor that significantly influences whether ERM can influence decisions within an organisation. Many board members prefer tangible facts and figures to work with, so they can make data-driven decisions.

continued on next page

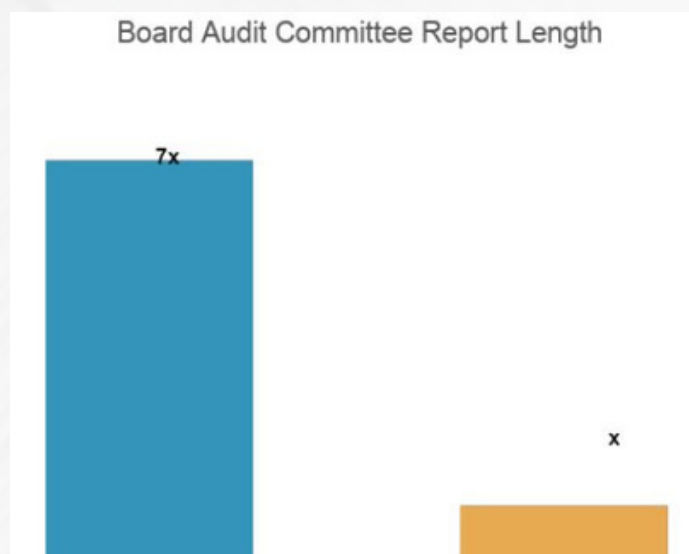
Qualitative data, while still highly valuable, isn't seen as being as credible as quantitative data. So, ERM leads must focus on implementing the right technology and processes to capture data and use it to tell a story that prompts action.

For those already collecting data, a key pain point is the quality and integrity of the data itself. Having confidence in your data collection processes will help you to deliver deeper and higher-quality insights on the factors influencing your market and your organisation.

Quality Reporting Enables Action and Support with Informed Decision-Making

It's clear then senior executives need actionable and relevant information to support their decision making, and ERM leads must ensure they deliver the right-size report.

According to the Gartner review, those reports which dropped pages by 7 times have been more successful in driving actions and influencing decisions than larger reports. This clearly shows the importance of having a concise report with accurate data.



Source: Power Co; Gartner

Discuss The Right Information with the Right People at the Right Time

Not all data and insights need to be reviewed and discussed at every level in your organisation. In the past, ERM was typically siloed, with each department responsible for its risk management and reporting to the relevant senior leader.

ERM is now considered a cross-function process that works holistically across businesses and can be implemented as a top-down and bottom-up approach.

continued on next page

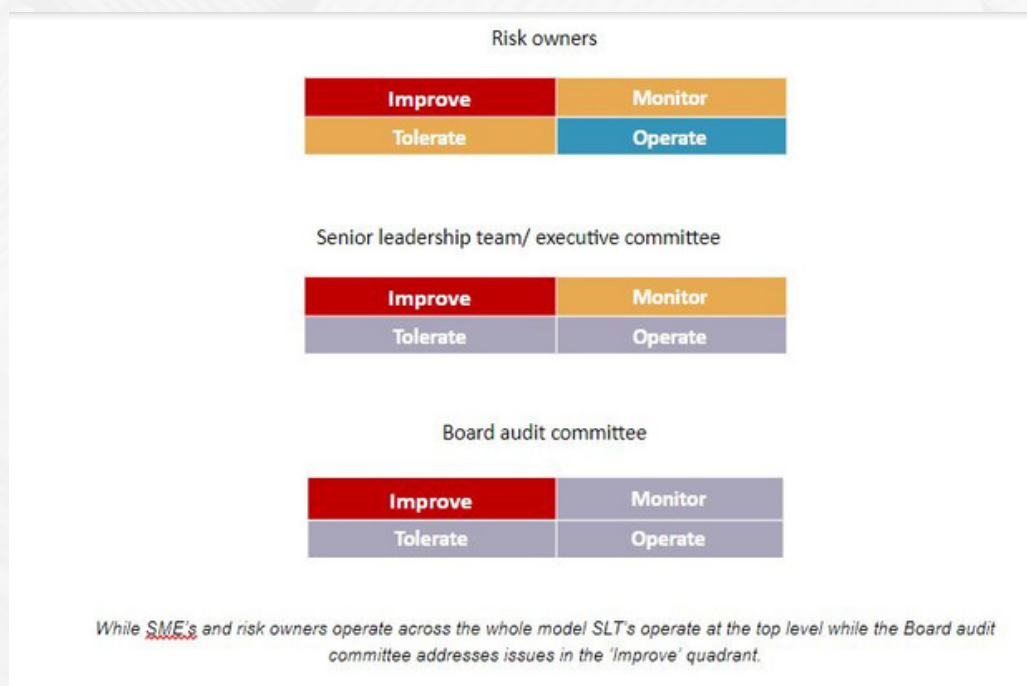
Board	
SLT	
ERM ⁽¹⁾	
Divisional Risk	Domain Risk
GRC ⁽²⁾ Operational Risk teams	
Listening Systems	
Consistent methodology	
Standard Tools	

- (1) ERM works with business units and domain programs throughout the organization, and helps validate senior management's opinion of risk through both top-down and bottom-up approaches
- (2) Governance Risk & Compliance

Another key takeaway from the Gartner report is the recommended use of the 2x2 action-oriented matrix (see images below) to prioritise discussion where the action is needed. The matrix provides clear-cut guidance on activities that must be taken at each stage and gives teams ownership of decision-making at different levels.

While risk owners operate across the whole matrix, they usually deal with and monitor issues on a day-to-day basis that have a low level of risk to the organisation. The SMT, on the other hand, must focus on monitoring issues with high-risk exposure where the current actions being taken are sufficiently mitigating the present risk.

When mitigation actions become inadequate, and there is a high risk of disruption to the organisation, the board must take swift action to improve the issues, ideally based on the data gathered by the SMT in the monitor stage and insights from risk owners who operate across the whole model.



continued..

Structuring your decision-making workflow around this model will alleviate poor or slow decision-making by clearly defining the risk and steps required to progress through the rest of the matrix. Executives can then make fast, informed decisions and reduce the impact of threats on the organisation.

Successful Decision Influence Drives Timely Action

When ERM leads can successfully gather data and present a compelling story to senior executives, the results are significant. 93% of those who achieved decision influence reported that action was taken within the expected timeframe. Conversely, that figure was only 52% for those who did not achieve influence at the board level.

In addition, the report also found that those who achieved decision influence are:

- 3.2x as likely to receive explicit positive feedback on their information from risk committee members
- 3.2x as likely to receive requests for further information/support from risk committee members (or their teams)
- 3.2x as likely to be invited to participate in other management discussions they're usually not a part of

Key Takeaways from The Gartner Risk Reporting Report

To achieve decision influence, it's essential to focus on reducing executive effort. The clearer the picture you paint and the better insights you can deliver through effective and holistic data capture and processing. This will increase your chances of prompting action by as much as 1.8 times.

Ease of information consumption, providing context around the relevance of the decision to your function and across the business, aligning risk information with other executives and adapting the presentation to stakeholder needs are core to implementing effective ERM, and for connecting insights that align with wider organisational objectives (as the matter of concerns by executives from and within different business units).

Reference

Gartner Report: [Risk Reporting That Drives Action - Reducing executive effort](#)

DR FAHIMEH MCGREGOR-ZAERI - PRINCIPAL CONSULTANT - DELTA INFORMED DECISIONS



Dr Fahimeh 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.



INTEGRITY MATTERS

SUE TREZISE – SUE-LUTIONS LTD

Rather than debating the merits of whether an organisation has/needs a risk culture and what that may/should look like, this article suggests it is timely to focus instead on ensuring the organisation has a culture of integrity in the first instance. Embedding a culture of integrity is the key to maintaining trust and confidence in an organisation for staff, stakeholders, customers/clients and the community.

Integrity matters in the public sector especially, given that public funding and support creates and enables government agencies and works. There is an expectation that infrastructure and assets will be appropriately maintained, and that development, resources and services provide maximum value. Public sector employees are expected to perform their duties fairly and honestly. Misconduct, fraud and corruption waste public money and resources and also damage the reputation of the public sector.

Insights for managing integrity risks in relation to fraud and corruption are readily available from government agencies established to ensure accountability. Risk insight from two such agencies is provided for fellow risk practitioners to further inform risk discussions and decision making.

Fraud

Maintaining a culture of integrity, supported by strong internal controls, is the fundamental means by which public organisations prevent and detect fraud.

Each year the Office of the Auditor General (OAG) shares information on fraud incidents to assist public organisations to consider where their risks might lie. The current data set spans the period 2012/13-2019/20 and identifies some key trends which could be useful in identifying risk factors and informing mitigation measures. The data is grouped into broad categories: the type of fraud, the methods and reasons for fraud being committed and how the fraud was identified.

The most commonly reported type of fraud was theft of cash, with the most common reason for committing fraud being that the fraudster didn't think they would get caught (!). As mentioned earlier, internal controls were the key method by which the fraud was detected, followed by internal and external tipoffs.

continued on next page

For each category, the top 3 incidents (where identified) are listed below:

<i>Reporting</i>	<i>Central government</i>	<i>Local government</i>
Types of fraud	1. Theft of cash 2. False invoicing 3. Credit or fuel card fraud	1. Theft of cash 2. Theft of inventory 3. Credit or fuel card fraud
Methods and reasons for fraud	1. Didn't think they'd get caught 2. Policies and procedures not followed 3. Easy access to cash	1. Didn't think they'd get caught 2. Easy access to cash 3. Policies and procedures inadequate

Because the OAG is dependent on information being provided by public organisations the full extent of fraud cannot be reliably known. For further information go to: [OAG/data/fraud](#)

Corruption

In 2020, the independent broad-based anti-corruption commission (IBAC), based in Victoria, published information on building integrity in times of crisis (such as COVID-19). The resources aim to help the public sector (central and local government) review and strengthen integrity responses and improve capacity to prevent corrupt conduct during times of emergency and crisis.

IBAC identified key opportunities for misconduct and corruption arising from changes to the way services are delivered in such circumstances. These are summarised as:

1. Increasing demands and pressure on employees

Crisis-related funding can increase existing fraud and corruption risks. Key risks typically stem from the transfer of funds from the public sector to the private sector for service delivery and other support.

2. Working remotely

Working from home increases security and privacy risks to public sector employees. Risks include inadvertently discussing or exposing information to unauthorised individuals, either in person within shared work spaces, via social media or other electronic means. Cyber threats also pose a risk in remote workforces.

3. Risks to governance processes and oversight

During emergency or crisis situations, employees may come under pressure to take shortcuts to accelerate delivery, such as bypassing proper processes, and reducing or stopping routine consultations with stakeholders and experts.

4. Reduced attention to corruption resistant culture

There is a risk that agencies' integrity-related education and training programs may be postponed or cancelled due to increased service delivery demands or logistical issues associated with remote working.

continued on next page

5. Increased lobbying

Lobbying efforts by groups seeking government support can place undue influence on government decision-making which, if successful, may compromise probity and due diligence measures and decrease transparency.

For each of these 'opportunities', associated warning signs or 'red flags' and suggested prevention/control measures to help minimise risk are set out in the information sheets.

For further information go to: [IBAC publications and resources](#)



SUE TREZISE – 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



FAKE NEWS AND MISINFORMATION

CAMERON LAI

In the past few years, there has been an explosive increase in fake news and misinformation. Various events spring to mind, perhaps the most prominent being the 2020 US General Elections and the congressional hearings where Twitter's Jack Dorsey and Facebook's Mark Zuckerberg were grilled about content moderation and misinformation that occurs on social media platforms. This was not unjustified – suggestions of social media being used to incite violence and unrest ended with riots and the storming of the Capitol, leading to the deaths of 5 people. Closer to home, the gunman in the devastating Christchurch mosque attacks was able to livestream the first attack on Facebook, which quickly spread to other channels.

The filter bubble is also often cited as playing a role in propagating misinformation. Research suggests that when people are exposed to misinformation online, the algorithms that are used by Big Tech companies such as Google continue to recommend such information, trapping people into a kind of feedback loop. This then makes people more susceptible to believing and sharing misinformation.

Many of the examples of misinformation we see tend to occur in the political and social sphere. Examples within New Zealand include the suggestion that the Chinese government attempts to influence Chinese media in New Zealand, and more recently, the Ministry of Health's publications on how to combat misinformation and fake news around COVID and the COVID vaccine. In fact, a recent study by the Office of Film and Literature Classification found that half of New Zealanders surveyed held at least one belief that is linked with misinformation.

Moreover, misinformation can also have damaging outcomes for business. In 2019, a video went viral that allegedly showed a Tesla autonomous driving car failing to brake and crashing into a robot. Whilst Tesla's stock price did fall, it quickly recovered, with a large part of this due to Tesla's immediate response and quickly proving the video to be fake. Other companies have not been so fortunate.

The nature of misinformation and fake news is that it is unpredictable, and therefore difficult to anticipate where it may come from or in what form. But this does not mean that businesses cannot take meaningful steps to plan for and manage misinformation. The first step is to be prepared and have a response plan in place. Secondly, ensure frequent monitoring of news and social media channels. Publicity and media facing roles are frequently tasked with this, and are in an ideal place to find out about and shut down misleading information. Finally, if one does become a victim of misinformation, it is important to respond and take control of the situation. A slow response or no response at all can allow misinformation to quickly spread beyond your control, and have potentially devastating consequences.

CAMERON LAI



Cameron is a risk assurance professional, helping clients manage their technology and cyber risk, using data analytics to analyse and derive insights into their data.

This October, he will be undertaking his PhD at the University of Tokyo's Graduate School of Engineering, exploring the socio-cultural aspects of misinformation. He hopes that his research will help to identify the human root causes behind misinformation and its propagation, and make recommendations from a policy and systems design perspective to manage this growing threat.



CLIMATE-RELATED DISCLOSURES

Q & A WITH THE EXTERNAL REPORTING BOARD'S DIRECTOR CLIMATE STANDARDS - DR AMELIA SHARMAN

Eight weeks into the new role, what has surprised you the most about the Climate – related disclosures project?

The main thing that has been a very welcome surprise is just how willing the rest of the XRB, and the wider accounting world, has been to embrace the challenge of climate-related disclosures. When I worked on the recommendation at the New Zealand Productivity Commission (as part of their Low-emissions economy project), for mandatory climate-related financial disclosures, it was quite a 'hard-sell' to get people to understand their transformative value. Only a few years' later, it feels like we're riding the wave of acceptance that climate change is a very real issue facing us today, not just in the future. I've also been really pleased about the willingness from the early adopters of TCFD disclosures, such as some of New Zealand's energy companies, to share their insights and lessons learned. They have such an important role to play in helping others who are just starting their own reporting journey.

This work is new territory for the XRB – who else is on the Project team?

Sanel Tomlinson, who was previously Interim Director Climate Standards, is now Director Integrated Reporting and Climate Special Projects. Sanel will work alongside the Climate Standards team to ensure that the climate-related disclosure standard is harmonised with other issues, such as biodiversity reporting, and our te ao Māori workstream. Jack Bisset, previously Principal Advisor at Ministry for the Environment, joined the team in August to provide expert advice on scenario analysis and other matters. Judy Ryan, Principal Consultant at Ryan Jones, also recently joined the team on a part-time basis to assist with issues relating to greenhouse gas measurement and reporting. Last but by no means least, Lisa Kelsey is our Senior Project Manager who has the all-important job of actually drafting the standards.

We have established an internal Project Steering Group to provide governance and oversight, chaired by XRB Board member Jacqueline Robertson-Cheyne. We also have an External Advisory Panel which acts as a consultation group on technical climate and sustainability issues, particularly those relating to the practical application and implementation of the standard.

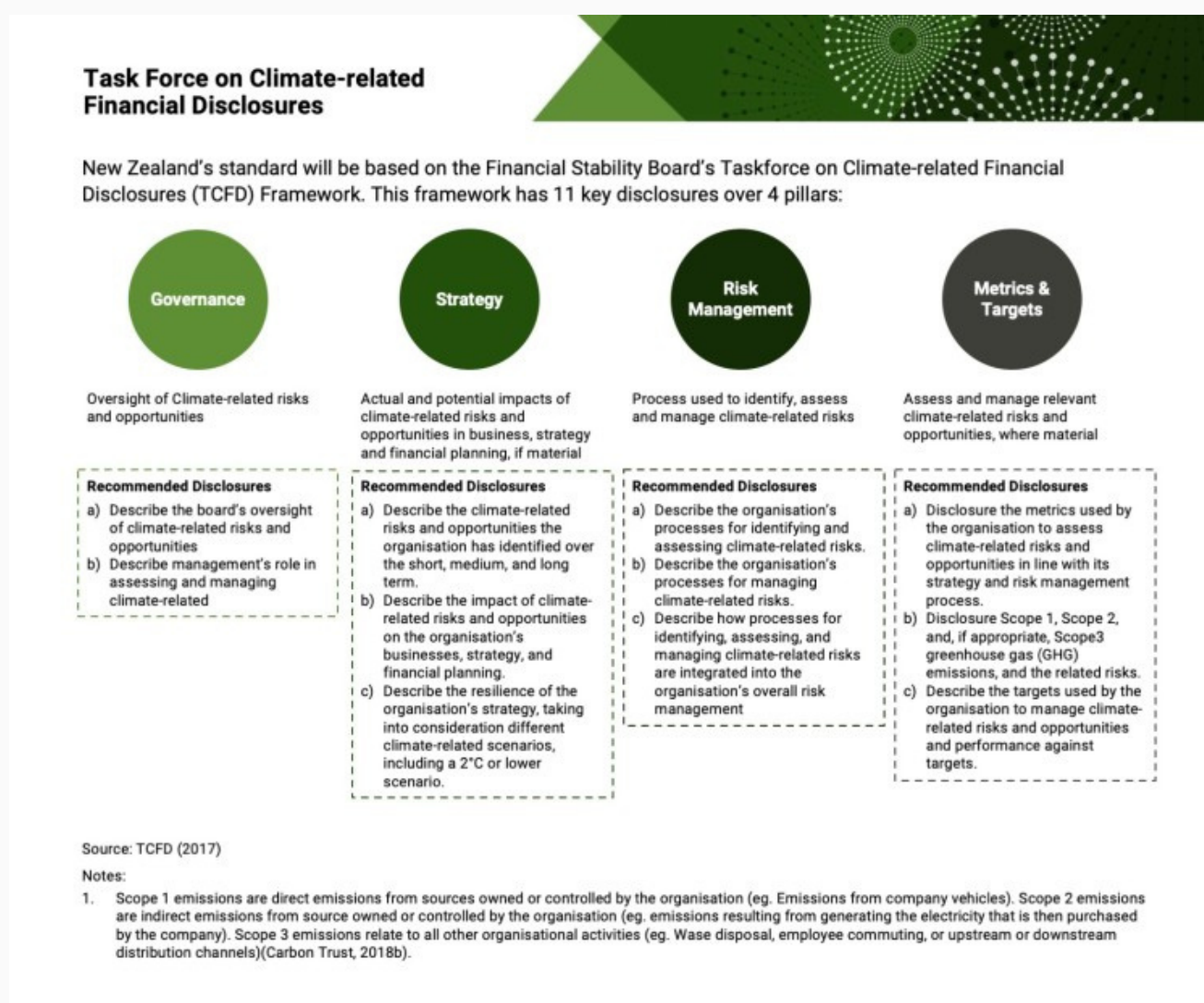
continued on next page

Developing the standards is a huge task –are you basing the work on any design principles?

Yes -the team have developed a set of design principles for the standard. Several of these focus on the need to align closely with the Task Force on Climate-related Financial Disclosures (TCFD) by using their content and terminology unless there is a strong case to make amendments for the New Zealand environment. Others include to ensure that the standard is developed with a user needs focus (with primary identified users being investors), and that the standard is principles based (whilst acknowledging the need for the disclosures (at least in part) to be subject to some form of external assurance).

Another design principle that the standard will be guided by the qualitative characteristics of decision-useful information. The TCFD highlights seven principles for effective disclosures, including that disclosures should be consistent over time, comparable, and provided on a timely basis.

Here's a snapshot providing a bit more detail on the TCFD:

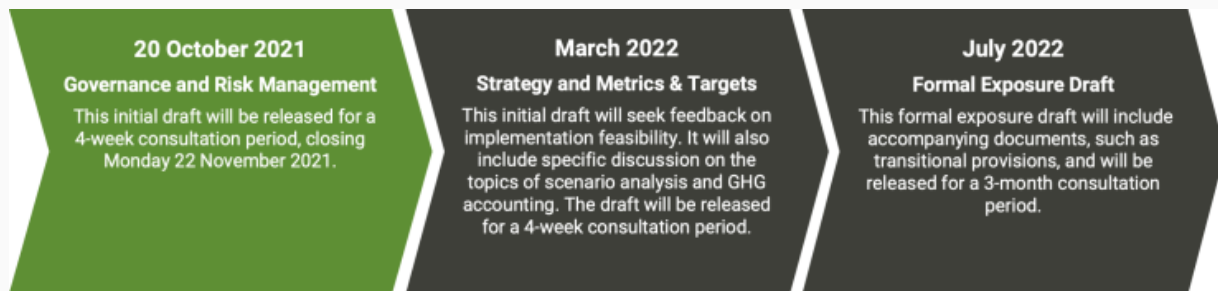


continued on next page

Where are you at right now with the project and what's coming up?

Right now, we've got our heads down getting the first cab of the rank – an initial draft section of the standard ready to be being released 20 October this year. The initial draft will focus on Governance and Risk Management.

The Governance section focuses on oversight by the board of climate-related risks and opportunities and management's role in assessing and managing these. The Risk Management section considers the processes used by an organisation to identify, assess, and manage its climate-related risks. This section emphasises processes used (including how these processes are integrated into existing risk management processes), rather than identification of the risks and their impacts, as these are covered in the Strategy section.



The XRB have been quite active on engagement – what have you been hearing so far?

We're really keen to engage as part of this project – we are very aware that there are a lot of insights held by people who have been working on risk and disclosure inside their own entities that can usefully inform the development of the standard. Several key questions are emerging as part of our engagements, including:

- What data and which scenarios will entities be required to, or could, use to make their disclosures? What about the quality of that data, whether it will be freely available, and how reporting against that data would be assured so that it could be confidently relied upon?
- How will the climate-related disclosure standard relate to other reporting on broader environment, social and governance (ESG) matters, as well as reporting requirements in other sectors and from other agencies such as the Reserve Bank of New Zealand, or local and international stock exchange listing requirements?

We're working on the answers to these, and other, questions as we speak! There are so many issues to consider to move from a formerly voluntary reporting regime, to developing a mandatory regime that provides decision-useful information for investors.

Finally, what advice do you have for anyone wanted to get started on their climate risk journey?

I'll stick to the 'rule of three' to answer that one...

- **Get familiar with the terminology:** The original [TCFD 2017](#) report is a good place to start.
- **Measure your footprint:** One of the key disclosures in the TCFD focuses on measuring greenhouse gas emissions.
- **Create a coalition of the willing:** Start a conversation between senior management and the board about what implementation of climate-related disclosures might look like in your organisation.



THE IMPORTANCE OF PLACE IN UNDERSTANDING PHYSICAL SECURITY RISK

Line of Defence
New Zealand's Defence and National Security Magazine

NZSM
New Zealand Security Magazine

firenz

Magazines of news and analysis
for the sectors protecting
Aotearoa New Zealand
www.defsec.net.nz

According to Chris Kumeroa, Managing Director of Global Risk Consulting, and Nicholas Dynon, Chief Editor of New Zealand Security Magazine, the security world is coming to a greater awareness of the importance of data-driven approaches to assessing risk. But there's some way to go.

Data and national security

Last year we attended the Information Domain Engagement Accelerator Summit (IDEAS) 2020, a virtual event co-hosted by the New Zealand Defence Industry Association (NZDIA), the Ministry of Defence, and the NZDF. It was part of a process of early engagement in relation to Defence's freshly coined 'Information Domain' – a domain of warfare that acknowledges the very 21st century reality that future conflict won't just be fought in the traditional domains of land, sea, and air, but also via data.

The information age and fourth industrial revolution have shifted the locus of geostrategic power from ballistic missiles and aircraft carriers to bits and bytes. Humankind is moving in faster and in ever more connected ways to a future in which data – the building blocks of information – will be the single most important measure of a nation's power.

"In upcoming years and decades, it will be data that determines the superpower," noted Sadegh Riazi, founder and CEO of CipherMode Labs, at the IDEAS event. "The quality of the data, as well as the ability to process large volume of data will be the differentiating factors." Interestingly, Indian government officials have called data a new form of national wealth.

continued on next page

Our everyday lives already scream at us the fact that data is key. Organisations trying to sell us stuff gladly pay for data about each of us and our preferences and spending habits. This is well understood, and it's a contemporary reality that our Defence Force had already acknowledged in both the Defence White Paper 2016 and Defence Capability Plan 2019 (DCP).

"The speed and effectiveness with which the Defence Force is able to respond to events," states the DCP, "is dependent on its ability to collect, analyse, distribute and exploit the immense quantities of information generated by modern information technologies."

But understanding the importance of harnessing data in the identification, assessment and response to geostrategic risks and threat actors is one thing, and actually doing it is another. Militaries, such as the NZDF, have only recently set off on this journey, and intelligence agencies (despite what Hollywood tells us) still have some way to go.

At the domestic security level, developments in machine learning, artificial intelligence and analytics in general have invigorated interest in data among state security and law enforcement agencies. In New Zealand, the relatively recent establishment of the Evidence Based Policing Centre by the NZ Police and the New Zealand Institute for Security and Crime Science by the University of Waikato, are indicative of an acknowledgement that data can enhance public security outcomes. Their appearance is part of a global trend, and they mirror the establishment of similar institutions in other countries.

Data and physical security risk

It's easy to sit back into one's consultant armchair and critique militaries and law enforcement and the rather long data journeys ahead of them. The fact is that the various private sector disciplines that focus on the management of physical security and safety related risks are no better.

When it comes to data-driven approaches to the assessment and management of these types of risk, the private sector is a patchwork of 'haves' and 'have nots', and the distinction between these appears to be drawn along sectoral lines. It could be argued, for example, that the insurance and health & safety sectors are more likely to be evidencing their assessment of physical security and safety risks with data than, say, their consultant peers in the private security sector.

continued on next page

That certain sectors are more advanced in this way than others, however, has probably less to do with any technological edge and more to do with the fact that they're simply more accustomed to taking quantitative approaches to risk.

From our work in the private security consulting space, we know that any respectable consultant bases their work on an appropriate standard, such as ISO31000 Risk Management, HB167 Security Risk Management, and ASIS International's Enterprise Security Risk Management (ESRM) Guideline. A consultant may also have regard for the government's Protective Security Requirements (PSR) guidance, which itself advocates a risk-based approach based on ISO 31000.

Either way, as the below table indicates, given ISO31000's 'gold standard' status, ISO31000, HB167 and ESRM are all quite aligned. But even with the right standards and frameworks in place, there is still the challenge of producing security risk assessments built upon a strong evidence base.

ESRM Cycle Enterprise Security Risk Management	ISO31000 Process Risk Management	HB167 Framework Security Risk Management
Identify and Prioritise Assets	Establishing the Context (5.3)	Establish the Context
		Strategic Context
		Security Risk Management Context
		Organisational Context
Identify and Prioritise Risks	Risk Identification (5.4.2)	Identify the Risks
		Threat Assessment
		Vulnerability Assessment
		Criticality Assessment
	Risk Analysis (5.4.3)	Assess the Risks
		Likelihood
		Consequence
	Risk Evaluation (5.4.4)	Evaluate the Risks
		Tolerance
		Acceptability
Mitigate Prioritised Risks	Risk Treatment (5.5)	Treat the Risks
		Avoid
		Share
		Exploit
		Accept
		Reduce
Continuous Improvement	Monitoring and Review (5.6)	Monitor and Review

continued on next page

Interestingly, when some security consultants talk about quantitative versus qualitative approaches to security risk management and quantitative versus qualitative security assessments, what they are often referring to is – specifically – approaches to scoring risk; a quantitative score referring to a risk rating expressed as a numerical value (e.g. 1 to 10), and a qualitative score referring to a risk rating expressed adjectively (e.g. ‘low’, ‘medium’, ‘high’). That’s great, but it’s certainly not a quantitative approach to identifying risk, and it’s definitely not data-driven.

What security consultants tend to talk less about is the use of quantitative approaches to the identification and assessment of risk through the scientific analysis of historical risk-related data. More often than not, there is a tendency to rely upon anecdotal evidence, assumption, and past wisdom. This can be due to data accessibility or ‘noise’ issues, but more often than it should be it’s due to the lack of adequate engagement with the data.

As a result, the security controls recommended by a consultant as a result of a data-less security risk assessment (or, as can be the case, in the absence of a security risk assessment altogether) are often selected on the basis of what’s worked in the past or – perversely – on the basis of what types and brands of security solutions the consultant has a personal (conscious or unconscious) bias towards.

It’s a tendency noted in a European Safety and Reliability Association (ESRA) research paper *A Study on the Influence of Uncertainties in Physical Security Risk Analysis*:

Security risk assessment is often accompanied by great uncertainties, as there is a lack of evidence of threats, consequences and the abilities of security measures. Thus, qualitative or semi-quantitative models that strongly rely on expert knowledge are often used, although these models can lead to misleading or even wrong results.

In the physical security world, ‘wrong results’ can lead to commercially irresponsible, reputationally risky, wasteful, and potentially life-threatening decisions around security planning, policy, training, and deployment. On the other hand, ‘evidence-based’ security risk assessments can result in security decisions that are well-informed, defensible, and more likely to achieve intended outcomes.

According to a definition we came across in a healthcare sector publication, ‘evidence-based risk assessment’ (EBRA) is the practice of informing risk decisions through the judicious identification, evaluation, and application of the most relevant, quantifiable, and statistically valid risk information.

In the Risk Management Standard (ANSI/ASIS/RIMS RA.1-2015) co-published by ASIS International and RIMS, this is referred to as a ‘fact-based approach’. According to this approach:

Good words for Great Souls

Assessment conclusions should be based on verifiable evidence, where available, gathered through a systematic risk assessment process that ensures reliability and reproducibility. It should be recognized that an assessment is a snapshot in time conducted with finite resources; therefore any sampling techniques should be based on a defined methodology that produces a representative sample... If the evidence falls short of fact because there is insufficient information available, or of a type that limits its ability to be verified, then its credibility should be supported by other reliable information.

Mapped data and physical security risk

As practitioners focused predominantly on the physical security world, much of what we do is in some way related to the idea of ‘place’, whether it’s a shopping mall needing a security assessment, a neighbourhood that’s seen in increase in organised crime, or a senior executive’s travel destination. Understanding the prevalence of hazards (crime, conflict, terrorism, unrest, antisocial behaviour, traffic incidents, natural events, etc) in a particular locality enables us to better manage the risk and to achieve better security outcomes.

It's a simple thesis: an individual's exposure to a hazard (a potential source of harm) is dependent upon the location of the individual relative to the hazard. If an individual remains geographically distant from a hazard, it is less likely the hazard will result in harm to them. Conversely, if an individual and a hazard are located at the same place and at the same time, then the likelihood of harm (i.e. risk) to the individual is heightened.

It's Risk Management 101, and it's a logic that holds true no matter the hazard – earthquake, weather event, crime or traffic incident. COVID-19 clustering, and physical distancing measures, for example, have demonstrated the importance of geographical proximity in the context of virus transmission and exposure to potential harm. Place is a key element in both the spread and the containment of the pandemic.

In the case of crime, law enforcement concepts such as 'environmental criminology theory', 'routine activities theory' and 'place-based policing' demonstrate the importance of location to risk. Environmental criminology theory, for example, posits that crime is a complex event in which four things intersect at one time: a law, an offender, a target, and a place.

Crime has distinct geographical patterns, and the geography of crime can be dynamic over time and space. Many place-based policing theories describe the role of place in shaping how crimes cluster and form 'hotspots', emphasising the role of place as the key element in crime.

Risk Terrain Modelling, for example, uses geospatial analytics to diagnose environmental conditions that lead to crime and other problems. It brings multiple sources of data together by connecting them to geographic places, and then forecasts risk patterns for certain areas. This can assist law enforcement in deploying resources, preventing crime, and reducing risks. According to Melissa Burgess in a NSW Bureau of Crime Statistics and Research brief (April 2011):

The distribution of crime across a region is not random. A number of factors influence where crime occurs, including the physical and social characteristics of the place and the people using the place. Crime mapping can show us where the high crime areas are and help to provide an understanding of the factors that affect the distribution and frequency of crime. This knowledge can help improve crime prevention policies and programs. For example, it can help us to anticipate at-risk places, times and people; direct law enforcement resources; allocate victim services; design the most suitable crime prevention strategies; and so forth.

Place is also important in relation to hazard categories more commonly associated with accident, chance, or 'act of God'. Traffic incidents, for example, can happen anywhere, but the data tells us that certain locations – or hotspots – play host to disproportionately more incidents than others due to conditions at their specific location.

In the case of natural disasters, some extreme weather events, such as severe storms, can appear 'freakish' in terms of being geographically indiscriminate, yet location can play a part in others, such as tsunamis, flooding, landslides, and geological events.

Locality-based data is thus critical to our understanding of individuals' security. Comprehensive historical risk data (such as detailed crime metrics and security incident records) in particular provides an evidence base that avoids the pitfalls associated with guesswork, anecdote, patchy intelligence and conventional wisdom.

continued on next page

This is what's informed our development (along with our colleague, creative technologist Andrew Jackson) of the SecIntel platform, which is a map-based system that uses varied open source crime, incident and hazard data to identify risk 'hot spots' and historical risk patterns at the mesh block, grid-reference and in-premise level. In doing so, it provides an evidence basis upon which to assess security risk.

According to Sir Francis Bacon (or Thomas Hobbes, depending on where you've read it), "knowledge is power". But as our comments at the beginning of this article suggest, in the contemporary world of addressing risks and threats – geostrategic, domestic or otherwise – it is now acknowledged that "data is power". For security consultants not accustomed to data-driven evidence-based approaches to assessing risk, there is much to be done to power-up to this new reality. Understanding the importance of place-based data is a good 'place' to start.

Line of Defence
New Zealand's Defence and National Security Magazine

NZSM
New Zealand Security Magazine

firenz

Magazines of news and analysis
for the sectors protecting
Aotearoa New Zealand
www.defsec.net.nz



BUILDING CAPABILITY FOR FUTURE GROWTH

NEW ZEALAND QUALITY COLLEGE

It's all to do with the training: you can do a lot if you're properly trained. Queen Elizabeth II

Training increases employee engagement leading to higher productivity, higher job satisfaction, more sales and higher revenue. To put some perspective on that, companies that invest in training have 21% higher profit margins than companies which don't. They also have 17% higher productivity. On the flipside, a disengaged workforce can cost companies dearly. In Australia and New Zealand alone, the cost of disengaged employees is estimated at NZ\$74 billion dollars annually. According to LinkedIn's 2019 Workforce Learning Report, 94 percent of employees say that they would stay at a company longer if it simply invested in helping them learn. This is true for all generations, but it's particularly true for millennials. Nearly 90% of millennials say that professional development and career growth are significant to them

Engaged teams are the lifeblood of any organisation and one of the most important keys to engaging them is investing in their personal growth. Nearly 70% of workers rate training and development as the company's most important policy, yet 74% of them don't feel they are reaching their full potential.

Building their capability through training will not only boost their skills but also their engagement and ultimately output.

Building capability also holds value for an individual, not just the organisation. The pandemic is a stark reminder of the need to continue investing in building personal capability. Many excellent workers found themselves unemployed during the pandemic however those who were open to new possibilities and new training i.e. had a learning mindset, were able to find new ground and ended up building their capability and ultimately growing their skillsets. Individuals with a learning mindset are much more likely to remain employed, grow in their career and seek diverse career opportunities not to mention growing their skillset as well. Upskilling is a critical component of becoming promotion-ready as well. If you feel like this doesn't ring true for you, rest assured, a learning mindset can be developed. This in itself is part of building personal capability. That is where it starts.

Engagement and a learning mindset are key to building capability and growth. At NZQC, we promote both. Some of the more important skills in today's work environment have to do with people i.e. communication, behaviour and understanding social context. Even though NZQC courses are geared towards technical knowledge and understanding of ISO standards, they are embedded in the context of social interactions at work. Our courses focus on enabling you to think about standards and risk from different perspectives and provide opportunities for you to develop your understanding with regard to your own skillset and that of the organisation. How should you best respond to and prepare for failure? How should you address risk with people during auditing? Risk is the bedrock on which you build systems thinking stemming from standards which in turn will contribute towards a resilient and capable organisational culture.

continued on next page

Building capability also requires frequent reviewing. Even if you have done the necessary training already it helps to review the basics every once in a while to ensure standards are being consistently met and even improved upon. This is essentially the basis for the auditing profession. Many attendees on our internal audits course have come back after some years of auditing to review their skillset. Because of the practical and applied focus in our courses, their relevance to industry never fades. In fact they are constantly updated with changes to standards and suitably enriched with real world examples of application.

In the bigger picture, what we are really accomplishing through training is empowering the next generation to take the reins in an as informed and prepared way as possible. Training ensures that happens. Through training, we are not just looking after ourselves and our own businesses, but also the wider economy and investing into the future now. It is addressing the social responsibility of embedding a learning culture and a community of learners.

Training will build capability, drive revenue growth, increase resilience as well as risk appetite, and contribute positively towards culture but most importantly it will build the future. As Her Majesty says, it's all to do with the training, you can do a lot if properly trained.

References:

HR Cloud, (2021), [8 employee engagement statistics you need to know in 2021](#),

Bullen, S., (2018), [The cost of employee disengagement](#), LinkedIn,

Hess, A.J., (2019), LinkedIn: [94% of employees say they would stay at a company longer for this reason—and it's not a raise](#), CNBC,

Gutierrez, K., (2017). [Mind-blowing statistics that prove the value of employee training and development](#), Shift disruptive elearning,

Stevenson, M., (2019), [7 stats that prove training value](#), HR exchange network



NEW ZEALAND QUALITY COLLEGE

<https://www.nzqc.co.nz/>





RISK MANAGEMENT – AS EASY AS 1 TO 5

JOHN O'CONNELL- PRINCIPAL RISK & ASSURANCE ADVISOR
MINISTRY FOR THE ENVIRONMENT – MANATŪ MŌ TE TAIAO

Tired of slaving over a hot (or probably lukewarm at best) risk register? Had enough of arguing whether something is a risk, a source of risk, or a consequence of a risk?

Sick of listening to people arguing whether a risk is 'moderate' or 'medium' and hence orange or red on a 5x5 matrix?

Well, throw away those tired old registers (or at least file them away for a while) – here's a different way you might want to try to get a discussion about risk going. It focuses on achieving objectives while protecting what your organisation values. Best of all, it's simple and doesn't involve any unnecessary 'risk-speak'.

How will you do it? Via a workshop with four easy steps. To plan it, you'll just need to identify the objectives you will discuss and work out who you will include in the discussion. It should of course be the people or team responsible for achieving them. 'Sell' the value of this work to them by saying you will run a quick and simple workshop that will help them be successful. I've done it recently with my organisation's leadership team and our strategic (long term) objectives, but you can do it with any objectives (such as those relating to a team, programme, project, or process).

Righto, to the workshop itself. Firstly, ask attendees to **individually** think about how **difficult** it will be to achieve each objective while protecting what your organisation values. Get them to do this by 'scoring' how hard they think each one will be to achieve, from 1 (*"It will be a piece of cake to achieve this, with no real risk of damage to our organisation"*) through to 5 (*"Whoa, that one will be really tough to crack, and we could really suffer while trying"*). Don't have any discussion at this stage, just get people thinking and scoring on their own. Get them to write their scores down.

Don't spend too much time on this step – tell people to use their gut feel and first thoughts.

Secondly, get everyone to read out their scores for each objective (or if you have someone to help you, get them to collect the scores) and add them up. Work out the average score for each objective (you know it – add up each objective's scores and divide by the number of people. I told you this was simple).

Thirdly, starting with the objective with the highest average 'difficulty score', lead a discussion with the group by asking some probing questions: **Why** did people rank it so highly? **What** will make it so hard to achieve? What aspects of **value** could be damaged while we try to achieve it, and **how**? Take a note of the key points and factors people raise.

Do this for each objective or, depending on time available and the number of objectives, focus on the top three for a start. This discussion will tease out the risks (or sources of risk?) associated with each objective, without people even thinking they are talking about risks.

Lastly for now, discuss what they can or need to do to make achieving each objective less difficult, while protecting what you value. There might be a plan or strategy in place to do this already – if so, great. Record it. If not, get them think about what else is needed, by whom and when – and record this too.

Before they know it, you'll have the makings of a risk profile, prioritised to address the most difficult (or risky) objectives. And you won't even have had to talk about risk levels, definitions, controls, matrices, or any of that other risk management stuff!



QUELLING PSYCHOLOGICAL WARFARE

BRYAN WHITEFIELD

Whether it's bullying, authoritarianism or simply a lack of caring for how one responds to a subordinate, psychological warfare is what you have in the complete absence of psychological safety. That is, an environment in which no one dares speak up. And when no one is willing to speak up, while the boss's ego may grow, hand grenades are being left all over the place. Just waiting for someone to pull the pin.

As a risk professional you have a responsibility to identify psychological safety, or a lack thereof, to call it out and to help quell it. If you don't, explosions will happen, and you may very well get the blame.

Spotting the Issue

While there are obvious signs of psychological warfare such as loud voices and poor language, some are more nuanced.

Late last year I was speaking with an old client about her experience in a toxic environment as the head of risk in a large organisation. Let's call her Kate. What Kate experienced was a culture of finger pointing, the blame game and "don't you dare come to me with anything that might make us look bad".

Kate's warfare story played out over an 18-month period. Soon after starting it became evident that her job was to take care of things so that her boss and the rest of the executive did not need to worry about such things. Just tick the box, please!

It took two weeks for Kate to get her first one-on-one meeting with her executive manager. Over the following months her one-on-ones were cancelled or curtailed with great regularity. By the time her tenure came to an unexpected and abrupt end, she had managed just two hours of face-to-face time with her boss in 18 months.

During that time Kate had done her best to create value in the role that was decidedly not evident when she arrived. While doing so, she soon realised the toxic environment that staff were operating in. So she set about creating psychological safety for her team so they could be more effective in supporting the rest of the organisation. Encouraging them to speak up, to try new approaches and to feel safe in failing.

She then reflected that while she had done the right thing for her team, she had not done the right thing for herself. When she spoke up, her boss and others on the executive felt threatened and reacted with an array of avoidance, delay and blame-shifting strategies.

continued on next page

Raising the Issue

Kate and I spoke about how she could have done things differently. In hindsight, she realised she needed to confront the situation much earlier and in a very tactful way.

Kate was familiar with my work with risk professionals in creating persuasive conversations so we discussed how she might have constructed the conversation with her boss. We agreed that her boss was not aware of the damage that was being caused and how that impacted on her ability to shine. So we focused on a diagram to help explain the situation. **Figure 1** is the diagram we came up with.

It shows that staff react to the actions of management based on the emotions stirred in them. And that wrongful actions have impact that fracture the fabric of an organisation’s culture. And in seeking safety, staff put up barriers. They don’t speak up. They hold on to, even hide, bad news.

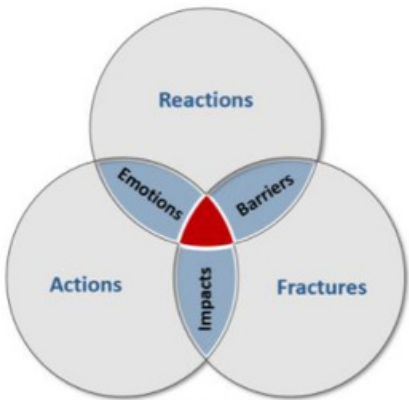


Figure 1

Diagrams like this work very well as a conversation starter. Something to interest the other person and to explain what is actually a complex situation. In fact, if you were to draw this in a notebook or on a piece of paper or on a whiteboard for someone, they would be even more interested. It is because they feel part of its creation rather than feel it is being thrust upon them. One of my key tips for anyone needing to influence someone in a tricky situation.

What you can do

The impact you can have on combating psychological warfare will depend on circumstance of course. For example, if you have developed a trusting relationship with key influencers on the executive, you can simply talk about the issues of how people react emotionally to the actions of their managers and how people put up barriers to protect themselves. However, if you don't know how to broach the subject with the executive, grab a notebook, have a coffee with your manager and draw three circles and start filling in the blanks. You may well be surprised at how much they sit up and listen to what you have to say.

BRYAN WHITEFIELD



Brian mentors risk professionals in organisations to increase their influence and improve decisions across their organisation. He is author of *Persuasive Advising: How to Turn Red Tape into Blue Ribbon* and delivers his Persuasive Adviser Program across all sectors of the economy.



THE COST OF KEEPING RISK AND STRATEGY SEPARATE IS OFTEN SUCCESS

BEAU MURFITT - CHIEF STRATEGY OFFICER, CAMMS

It might sound extreme, but the cost of keeping risk management and corporate strategy separate can be the success of your organisation.

All too often the senior team focus on setting the big picture strategy, with risk and compliance working at a purely operational level.

Here at Camms we have been working over the last 20 years to eradicate this disconnect, and give organisations the right tools for success.

In our recent webinar, *The Journey to Success Starts with Risk & Strategy Integration*, which our Vice President of EMEA, Daniel Kandola, co-hosted alongside our guest speaker Norman Marks, where he shared his views about improving business outcomes and success by bringing risk and strategy together.

One organisation, one view of success

Particularly in larger organisations or those spread across multiple sites or regions, one of the biggest challenges is simply having a vision of the one strategy and operational plan.

Camms risk and strategy solutions break down those siloes through real-time, cloud-based software. But more importantly it connects together the high-level strategy of the business with operational activity and risk management.

According to Norman Marks, a highly experienced risk expert and author, breaking down barriers between teams is important, especially given the prevailing sentiment towards the risk department.

"Too often the risk team is seen as the department of no. The department that quite literally stops people from doing what they want to do and diverts them from what they see as running the business," said Norman.

He says it would be similar to someone presenting you with a list of potential issues when you left your house to go to work or shopping – all it would do is annoy you.

"We all know that life is risky, so if we wanted to avoid all risks in life, we'd never leave the house. Likewise in business, if we avoided all risks, we'd have to close the business down," Norman said.

"The risk managers who simply create a long list of possible risks are both doing themselves and their organisations a disservice, and it's time to set aside this old way of managing risk."

The value of sound strategy and management

There hasn't been a year like 2020 or the start of 2021 for bringing risk right to the forefront of all our thinking. But it's also reiterated that good management decisions are based on knowing your game plan, the right data on risks, and the agility to weigh up all the factors and move on.

The power of a software solution like Camms is that it not only gives complete oversight to all actions at a senior level, by its nature it changes the way people work and how business performance is measured and monitored.

continued on next page

According to Norman, leaders and Boards need to see the value of risk management and how it adds value to the overarching performance.

He cites a [NC State University 2020 State of Risk Oversight report](#), created in partnership with the AICPA, that asked executives and Board members if they saw risk management as vitally important as setting strategy.

"The results found only 3% said absolutely yes, which is a really low result and shows they are not seeing the value of risk being part of the setting of strategy."

Solutions that bring the risk elements into the strategic decisions that need to be made very quickly show the value they can generate, both in opportunity and in avoiding costly issues.

A more mature approach going forward

At its very heart, good risk management, according to Norman, is all about what might happen. That means a mature outlook that explores the "good" opportunities along with the "bad" threats, with an understanding that many decisions will deliver both.

"The key question to always ask is – what is the right thing to do for the business?" Norman said.

"The risk management team has a great range of tools and ways to model risks and opportunities and project the outcomes of different scenarios.

"My proposition is that the term risk itself is unhelpful in bringing risk and strategy together. I know one organisation that changed their risk team to decision support. I also like to think of risk as the department of how. It completely reframes the kind of support the business needs and the kind of intelligence that can be delivered." A view passionately shared by myself and the team at Camms.

With integrated solutions in risk, strategy, projects and people, it's not about being adverse to all risk, it's about focusing on how that risk can blossom into opportunity, which will not only serve your business through turbulent times but it will ensure Camms business software is all about making the right decisions, managing risk, aligning talents and focusing on what matters. It sets the right foundations for success.

Watch [The Journey to Success Starts with Risk & Strategy Integration on-demand](#).

Find out more about how Camms' software can help your organisation bridge the gap between risk and strategy by [requesting a demo today!](#)

BEAU MURFITT - CHIEF STRATEGY OFFICER, CAMMS



Beau has more than 20 years of experience at Camms and oversees the company's global strategy. He possesses widespread experience in the entire spectrum of the development and sales of our business software solutions. Beau has extensive professional development through 4 years of The Executive Connection (TEC) membership. He possesses a Bachelor of Economics and an MBA and is a member of the AICD.



Camms.

It is with great pleasure that we welcome Camms as a new premier sponsor!

Camms have a great deal to offer and we look forward to working together to provide a high level of support for our members.

Thank you,
David Turner

Camms is proud to be helping RiskNZ to enhance risk practices in NZ. The partnership will provide members with timely and valuable thought leadership and services, contributing to the upskilling of RiskNZ members through webinars, events, and lunchtime seminars.

A key focus of the partnership will be the roll-out of regional engagement plans to support organisations across New Zealand. In addition to this, the partnership will enable RiskNZ and Camms to broaden their networks and create extra value to key member events.

Global Insurance Markets: Pricing Increases Moderate in Second Quarter

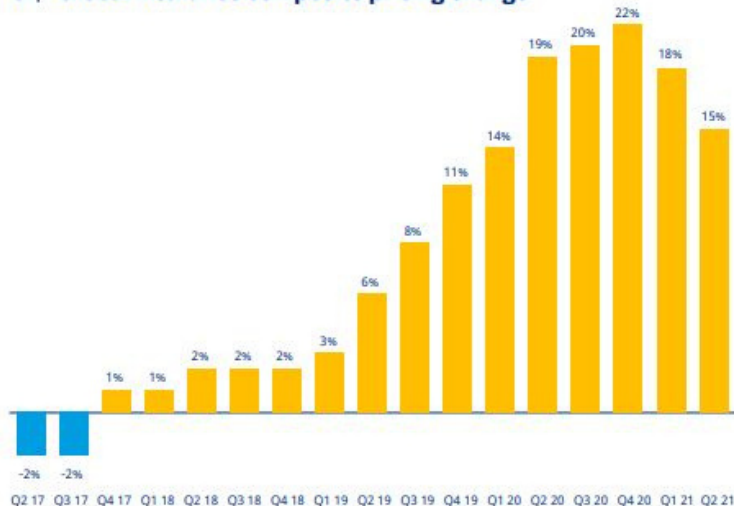
July 2021

2

Global Insurance Market Index Q2 2021

Global commercial insurance prices rose 15% in the second quarter of 2021, the fifteenth consecutive quarter of price increases, continuing the longest stretch of increases since the inception of the Marsh *Global Insurance Market Index* in 2012 (see Figure 1).^{*} It appears, barring unforeseen changes in conditions, that pricing increases peaked in the fourth quarter of 2020, at 22%.

01| Global insurance composite pricing change



Pricing increases across most regions moderated due to a generally slower rate of increase in property insurance and directors and officers liability (D&O) insurance. However, property insurance pricing climbed back up in Europe, and both Asia and Latin America and the Caribbean (LAC) saw moderate acceleration in financial and professional lines rate increases.

Cyber insurance pricing again went against the moderation trend — increasing 56% in the US and 35% in the UK (though accelerating towards 50% during the latter part of the quarter) — driven by increased frequency and severity of losses.

Regionally, composite pricing increases for the second quarter were as follows (see Figure 2):

- US: 12%.
- UK: 28%.
- Continental Europe: 13%.
- Latin America and the Caribbean: 4%.
- Asia: 6%.
- Pacific: 23%.

^{*}Note: All references to pricing and pricing movements in this report are averages, unless otherwise noted. For ease of reporting, we have rounded all percentages regarding pricing movements to the nearest whole number.



RISKNZ WELCOMES OUR NEW MEMBERS!

Individual Members:

Matthias Zuschlag - Treasury Management Accountant, Wellington Regional Council
Kerry Boyle - Director, Solifirst Ltd
Paul O'Byrne - Kaitohutohu Tūraru - National Risk Advisor, Te Wānanga o Aotearoa
Kim Wright - Principal Advisor Risk Management, Wellington City Council
Louisa Homersham - Director of Business Services, Otago Polytechnic
Loata Stewart - Senior Risk Advisor, Stats NZ
David Fox - Senior Consultant, Resilient Organisations Ltd
Stuart Martin - Group Risk & Assurance Manager, Kiwirail
Andy Dingfelder - CTO / CISO, iPayroll
Sharon Foss - Business Improvement Manager, Kapiti Coast District Council
Andrew Gillespie - Risk Advisor, Kapiti Coast District Council
Crespo Gao - Chief Risk Officer, Momentum Life
Mark Cubitt - Chief Risk Officer, Nomos One
Romina Alcatraz - Internal Auditor and Risk Advisor, Whanganui District Council
Nienke Itjeshorst - Sustainability & Resilience Manager, Kapiti Coast District Council
Richard Donnelly - Director
Alecia Cole-Bowen - Risk Business Partner, Ministry of Transport
Peter Moore - Senior Risk Advisor, Massey University
Stephen Dunn - Director of Investigations, Sanofi
Ruth Millhouse - Contracts Manager, Otago Polytechnic
Daria Li - Compliance Officer, FANZ
Sarah Bond - Principal Consultant, Be Safe Now!
Stephen Hookway - GM Risk and Compliance, Equipment, Leasing & Finance Holdings Ltd
Wilbert Goossens - Principal Advisor Risk and Assurance (ICT), MBIE
Brian Berquist - Director, CDPS Services Ltd
Nina Fountain - Founder/Workplace Strategist, Transformed Teams Ltd
Tamara McDonagh - Director, PwC
Shane Bidois - Risk & Opportunities Lead, Waka Kotahi
Bapon Fakhruddin - Technical Director- Disaster Risk and Climate Resilience, Tonkin and Taylor
Bridgette Sullivan-Taylor - Senior Lecturer, University of Auckland

Corporate Members:

Wellington Water
National Emergency Management Agency (NEMA)
NZQA
MetService NZ
TSB Bank Ltd
Aon New Zealand

GROWING POTENTIAL FOR AUSTRALIA AND NEW ZEALAND

It has been a challenging risk landscape during the past year; however, this has also helped to reinvigorate the interest and need for risk management from varied industries which is also great to see. This in turn has enabled increased growth and sharing of relevant and timely risk thinking and materials, and the future looks very bright in terms of organisational risk learning opportunities, alliances, and partnerships across New Zealand during the coming months.

At RiskNZ, we are keeping up with the need for better and more available risk information and practices, and we are excited to say that RiskNZ now provides more opportunities for organisations and individuals to learn about risk management through networking events; training and knowledge sharing; risk tools and templates, and a wealth of articles and case studies available through our website.

Recently we have added peer support networks, a member's chat forum, and a risk speakers' team to our member offerings to give a wider reach and add more value to our membership base.

We see a partnership with RMIA as a natural and logical step in growing our risk knowledge and experience and providing an additional opportunity for our members to utilise RMIA's specific training and resources and vice versa.

This valuable partnership would strengthen our collective risk management knowledge and methods through our combined collection of resources, and help us to collaboratively plan broader risk learning and career pathways between the both RMIA and RiskNZ to give members on both sides of the Tasman the most value.

Additionally, the connection between RiskNZ and RMIA will give members the opportunity to share knowledgeable risk related speakers; hold combined workshops and conferences, and hold shared online, and where possible, in-person networking and learning opportunities throughout NZ and Australia.


While we are in the early stages of our partnership, this is an opportune time for our collective members to tell us what you may need and how we may be able to help. We will collect all comments and feedback to determine the best way to meet those needs as we move forward.



RiskNZ's David Turner recently contributed to the 9th edition of the [RMIA - Risk Management Institute of Australasia](#)'s risk magazine.

Thank you RMIA - Risk Management Institute of Australasia. We look forward to future collaborations.

Another exciting risk awareness week and a big thank you to Alex for supporting RiskNZ to bring great value to our members



RISK AWARENESS WEEK 2021



5 DAYS
11-15 OCTOBER 2021
ONLINE CONFERENCE
30+ SPEAKERS

50+ interactive workshops on decision making under uncertainty and quantifying complex issues from climate change to pollution to cyber to planning

2021.RISKWARENESSWEEK.COM

50% discount on all tickets for RiskNZ members

UPCOMING EVENTS

How Risk Management Enables Success

David Turner will chat to the University of Canterbury MBA students about how our true success in any venture lies in how we approach and manage risk.

He will share some relevant examples of how we can use a higher level of risk based thinking as we move toward an uncertain future.

RiskNZ members are welcome to join the session and watch the Risk Chat online.



Tuesday 14 Sept
5:00 - 5:45 pm



Online only



The recording for this event will be available in the members area shortly.

Improving economic development of NZ through risk and opportunity management

COVID-19 illustrated that crisis can be unexpected and requires smart thinking and smart learning, and that traditionally risk approaches require a fresher and wider lens, as well as education and being open for change.

The use of technology can certainly help with risk management and opportunity management to improve such areas from waste management to domestic and international tourism.



Tuesday 5 October
12:00 - 1:00pm



Multiple venues & online



[REGISTER NOW](#)





Eliminating Chaos in a Cyber-Crisis in Your Organisation

Defeat the next Cyber Attack

Do you feel the need to be better prepared for a whole raft of crises that seem to be hitting organisations currently?

If so, this workshop is a must for you.

You and your colleagues will be fully immersed in two crisis simulations; the first a very realistic cyber-attack that could severely hit the ability of your organisation to function. The second, well, you will find out during the workshop.

Attendees will leave the session with

At a location and date that suits your organisation

- The confidence that your organisation will be able to respond well to a major crisis
- An understanding of what works and what does not in crisis management
- Strengthened incident and crisis management skills
- What tools to use and how to be more effective in crisis management
- The recognition of the importance of collaboration and communication in crisis management
- How to operate and manage in a calm, clear and structured way during a crisis.

Our Speakers:



Martin Petts

Head of Operations - F24
Crisis Management
Software | F24 AG



Ahmed ElAshmawy

Consulting Practice Lead -
Cyber and Information Security
| Axenic Ltd

Hurry! Secure your organisation's spot!

Visit www.risknz.org.nz to find out more



Bryan Whitefield

Bryan Whitefield is a management consultant operating since 2001, specialising in risk-based decision making and influencing decision makers, born from his more than twenty years of facilitating executive and board workshops.

He is a certified Visual Presenter and highly respected trainer known for his relaxed, humorous, 'says it how it is' approach resulting in a fun experience for his students.

Bryan is currently running 5 development courses in partnership with RiskNZ:

 Online

Essentials of Effective Risk Management



6 October

Project Risk Management - An essential skill



Expressions of interest

Mastering Risk Workshop Facilitation



28 & 29 October

Persuasive Adviser Program

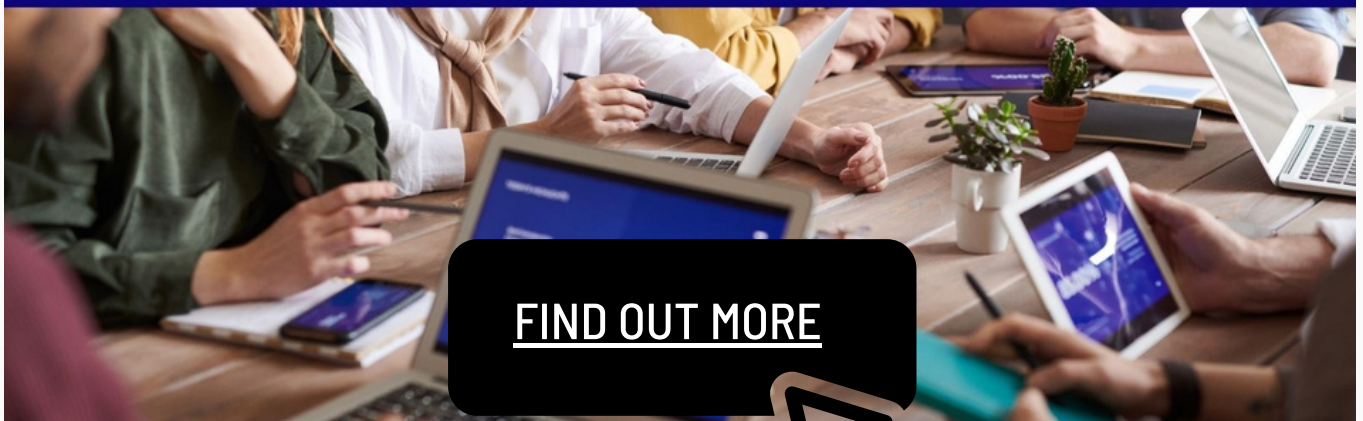


29 & 30 November

Control testing - Applying science to assessing control effectiveness



Expressions of interest



[FIND OUT MORE](#)



Check out this recent interview with RiskNZ's Managing Director, David Turner with [Insurance Business Australia](#).

David was asked three key questions:

- How has risk management changed from the first Covid lockdown to now?
- What is the expectation of risk management today? and
- What is needed to meet future risk expectations and demands?

David's takeaways are that NZ Businesses now have a higher appreciation of the value of risk management; that there is a growing focus on wanting to be better at managing risk, and that increasing overall organisational risk literacy is one strategy to make significant gains.

How's your organisational risk literacy?



Insurance BUSINESS TV

David Turner
Managing Director, RiskNZ

BUSINESS ASSOCIATION

RiskNZ

Watch it now

Effective risk management in challenging times

David Turner, managing director at Risk NZ, describes his organisation's role in promoting risk management in New Zealand. He explains how companies can effectively apply risk management principles to their operations as well as understand and mitigate potential risks.

Read More: [How have attitudes to risk management changed throughout COVID-19?](#)



LATEST READS

Find all of our latest news and articles [online](#)

- [FMA releases updated guidance on customer vulnerability](#)
- [Lloyd's releases new study on geopolitical risk](#)
- [Fall of Afghanistan: Inside the extraordinary New Zealand Defence Force evacuation mission to Kabul](#)
- [Remote working putting organisations at risk of ransomware](#)

RISKNZ 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.

RiskNZ Regions



*Bringing together people and organisations
managing risk*



find out more at risknz.org.nz



<https://www.linkedin.com/company/risknz>



RiskNZ

MANAGEMENT BOARD AND OFFICERS

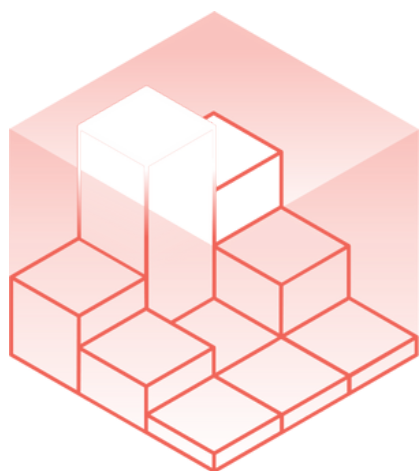
Chair:	Jane Rollin	Secretary:	Vacant
Deputy Chair:	Suralda Timmerman	Managing Director:	David Turner
Treasurer:	Gary Taylor	Administration:	Emily Thorn

Brent Sutton	David Turner
Chris Kumeroa	Imogen Perez
Darroch Todd	Lynda McCalman

COVID-19

Contact tracing locations of interest

New Zealand



SecIntel

Secintel is sharing this innovative technology to help you stay informed about Covid19 contract tracing locations of interest in New Zealand. This is technology which can help shape the future of risk management.

Thank you Chris Kumeroa (RiskNZ Board member) for sharing and Andrew Jackson for designing the CovidMap.

FIND OUT MORE NOW



We have worked with VA for a number of years and RiskNZ are proud to be partners as we move forward to 2022

VIRTUAL ASSISTANTS



Virtual Assistants is a premium virtual assistant company with team members all across New Zealand, who help founders and executives move their business forward by providing highly skilled assistants they can trust to take on responsible tasks.

Virtual Assistants provide personalised and customised virtual assistance. They get to know your business and recommend qualified team members to support you.

Identifying reliable, trustworthy, and competent help has always been one of the foremost challenges of running a successful business or project - and it's even more relevant when using remote resources. Virtual Assistant's team of experienced, reliable, and vetted professionals can provide your business with support you can bank on.

Contact Jess Larsen (Business Manager) today to have a chat about how their business support specialists can assist you.

Outsource to Virtual Assistants today!



Info@va.nz





ADVERTISE WITH RISKNZ!

Would you like to advertise with us and reach a wide network of members which include: risk leaders, government departments and corporates, regional councils, entrepreneurs, consultants and training organisations within New Zealand?



**GET IN TOUCH WITH US NOW
TO DISCUSS OPTIONS**

adminofficer@risknz.org.nz