RISK NZ

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 and crisis management partner F24

MARSH

F24

A WORD FROM THE CHAIR

STEPHEN HUNT – *Chair, RiskNZ*

Welcome to RiskPost

This edition of RiskPost is published during what may be the greatest destabilising event of our lifetimes. From the perspective of a risk professional, this global challenge goes well beyond accustomed topics, such as resilience, response, and continuity.

It might feel incongruous to publish articles that were written over the last year, before the pandemic emerged. What these RiskPost articles represent, however, are examples of the unbiased disciplined approach and quality of thinking that will be needed from risk professionals in the months and years ahead.

What has served as common language and practice in the past now seems inadequate to describe and manage the ongoing waves of events, impacts and consequences that undermine the cornerstones of global stability. The equilibrium of our society has been severely disrupted and across the world there have been profound impacts to our collective social contract – the authority of the state over the individual.

Continued on next page…

IN THIS EDITION…

A WORD FROM THE CHAIR CONTINUED...

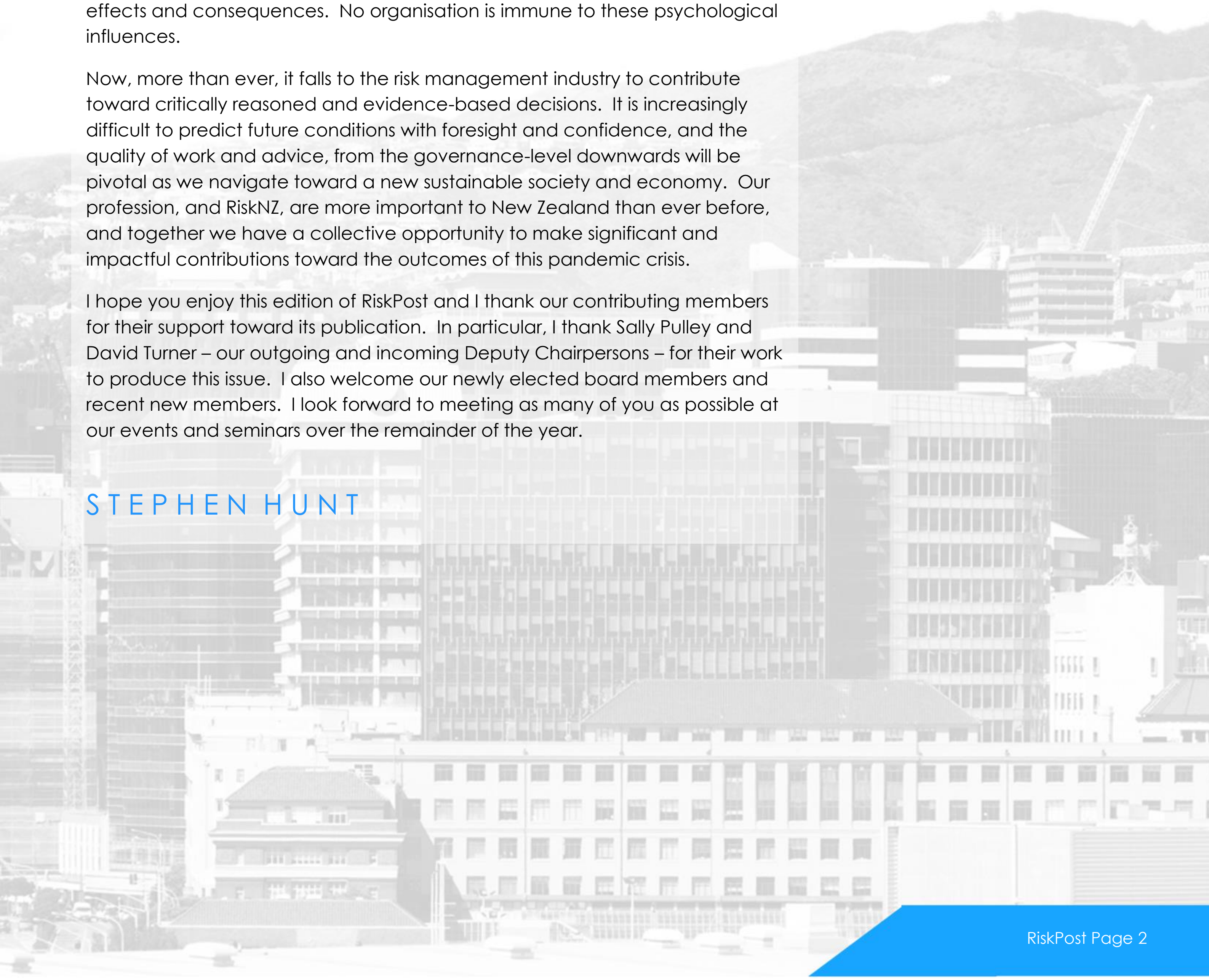
Each nation has responded to this pandemic differently and in doing so has laid open the strengths and vulnerabilities of their societies. As nations and populations come under increasing stress, growing inequality and social deprivation will influence views on fairness, wellbeing and our futures. These changes to society could destabilise governments and the global network of partnerships and alliances that until now have sustained a degree of stability and security.

This crisis is revealing that Human Factors – the principles and biases behind psychological behaviours – are influencing heavily the decisions and actions at all levels of state and society. Despite unparalleled access to high-quality scientific advice and rich data, Human Factors are shaping pandemic responses and decision-making around the world, with a broad variety of effects and consequences. No organisation is immune to these psychological influences.

Now, more than ever, it falls to the risk management industry to contribute toward critically reasoned and evidence-based decisions. It is increasingly difficult to predict future conditions with foresight and confidence, and the quality of work and advice, from the governance-level downwards will be pivotal as we navigate toward a new sustainable society and economy. Our profession, and RiskNZ, are more important to New Zealand than ever before, and together we have a collective opportunity to make significant and impactful contributions toward the outcomes of this pandemic crisis.

I hope you enjoy this edition of RiskPost and I thank our contributing members for their support toward its publication. In particular, I thank Sally Pulley and David Turner – our outgoing and incoming Deputy Chairpersons – for their work to produce this issue. I also welcome our newly elected board members and recent new members. I look forward to meeting as many of you as possible at our events and seminars over the remainder of the year.

STEPHEN HUNT



FROM THE EDITOR

SALLY PULLEY

Our Chair and Deputy-Chair provide a forward view to the AGM and beyond whilst I cast a retrospective eye over the last 12 months or so.

2019 was a year of change for RiskNZ with the implementation of the new Constitution, the appointment of a new Secretary, and the introduction of electronic voting for Board positions. The new Management Board took up their roles on 1 April. See page 29 for the 2020 election results, and page 30 for the new board line-up.

Looking back over 2019-20 a number of events were experienced as shocks to systems and society.

All of us at RiskNZ were deeply saddened and shocked by the tragic attack on the two mosques in Christchurch on March 15th 2019, and by the eruption of Whakaari / White Island on 9th December. The mosque attacks triggered rapid societal reactions and led to changes in gun laws. The Whakaari / White Island eruption led to searching questions about why tourists were allowed on the island; what could have prevented the tragedy; and what official enquiries may be necessary.

Because they happen so frequently we expect and can make plans for natural hazard events. Floods were experienced in Coromandel in September 2019, Canterbury in December 2019, Southland and Otago in February 2020. Fires and drought conditions were experienced in other areas of NZ.

The 5.8 quake north-west of Levin on 25 May 2020, and its aftershock sequence, reminds us that NZ is tectonically active and sits on a subduction zone.

Looking at the list of declared States of Emergency on the NEMA (National Emergency Management Agency) website, since 2002 the emergencies have included: flooding (36), severe weather conditions (14), earthquakes (10), landslides (3), fires (3), cyclone (1), tornado (1), with the latest emergency being a pandemic (Covid-19).

The NEMA website notes that not all emergencies result in the declaration of a state of emergency - so the full gamut of local and national disruption over the years is bigger than this.

A pandemic has been on many risk forecasts and predictions over the years, but has still been experienced as an international shock.

So - should we expect Covid-19 to introduce changes to the way society thinks about risk? Will this provide sufficient disruption to make people think deeply about the possible ramifications of risks that have been forecast in risk predictions for years, but often lurk at the bottom of risk registers (if they are recorded at all).

How many of you have sat in meetings and heard the words "*we only want to see the top ten risks*", or the top 15, or the top 20? Did any of those meetings include discussion about how to recognize and manage disruptive challenges that come at you out of the blue? Did any of those discussions evaluate what might eventuate if Borders were closed?

Continued on next page…

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. See page 5 for more details.

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 2020

Work on Edition 2 of RiskPost 2020 will start after the AGM, which is scheduled for 30 June.

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

In my experience, truth is often stranger than fiction and scenario planning for challenges ahead is too often constrained by '*that will never happen*'.

To quote Dwight D. Eisenhower "*When it comes to the point, plans are worthless but the act of planning is priceless*".

Few challenges will be bigger than those presented by the Covid-19 pandemic. In five years time, it will be interesting to look back and look for step-changes in how we discuss and prepare for disruptive events, or if memories have faded over time, with organisations moving quickly towards a comfortable state of normalcy bias.

Covid-19, and pandemics, are discussed in some of the articles in this edition, but are not the primary focus.

- Kristin Hoskin keeps you up to date on standards development, see page 6.

- Nick Lewis is an experienced director, he joined RiskNZ's Network Forum meeting on 20 February at NZTA's office in Wellington to share a few thoughts on how boards can best work with risk managers. Nick provides the key points of that discussion.
  THE BUCK STOPS HERE: GOVERNANCE OWNS ALL THE RISKS, page 9.

- Silvia Zanini graduated from Leicester University in January 2020. She provides a look back over her MSC course, and some thoughts on her learning journey.
  A MSC IN MY BACK POCKET, page 7.

- Cybele Souza provides a summary of her research on electronic voting risks and vulnerabilities. Cybele's research was carried out in a pre-Covid world, she has updated her summary to provide comment on Covid-19.
  ELECTRONIC VOTING RISKS AND VULNERABILITIES: AN INFORMATION SYSTEMS SECURITY APPROACH, page 24.

- Dr Margaret (Maggie) Trotter provides a paper on the use of work domain analysis in safety case development, the context being the production of a Foundation Safety Case for the integration of unmanned aircraft into the New Zealand Airspace.
  USING WORK DOMAIN ANALYSIS IN SAFETY CASE DEVELOPMENT, PAGE 11.

- Ross Liston discusses Covid-19, inevitable changes that will flow from the pandemic, and the core objective of getting back to business. Ross provides an introduction to bowtie analysis, and discusses how bowtie methodology provides a systematic analysis of how risks are, or should be, managed in our ever increasingly connected world.
  MAKING A CASE FOR BOWTIES IN THE BOARDROOM, page 20.

- At this time of year our regular contributor Sue Trezise usually provides a summary of reports such as the Allianz risk barometer. In this edition Sue comments on how 2020 is different with the COVID-19 pandemic creating a completely different context for risk practitioners, given the depth and breadth of unknowns and the velocity with which change has happened.
  You may have seen the recent warning from the UN that cybercrime is on the rise. The coronavirus crisis is moving the world towards increased technological innovation and online collaboration. The UN's high representative for disarmament affairs said growing digital dependency has increased the vulnerability to cyberattacks, and it is estimated that one such attack takes place every 39 seconds.
  Sue provides a commentary on cyber crime in a pandemic environment.
  THIS YEAR IS DIFFERENT, page 17.

In addition, our sponsors SAI Global have provided online reference materials via the SAI Global Pandemic Information Center. See page 27 for more details.

On a personal note. I left the RiskNZ Management Board in March this year after having served 3 consecutive terms. In addition to editing the 2019 and 2018 editions of RiskPost, I have been honoured to act as Deputy Chair for 2 years, and to fill-in as Secretary after the 2019 AGM and before Katie Phillips took up the role.

Many thanks to all of you who have supported me in the various roles over the last 6 years; and my very best wishes to the new Board.

SALLY PULLEY

BACK ISSUES OF RISKPOST

The back issues of RiskPost are available on the members area of the RiskNZ website - select the menu option Member Resources | RiskPost.

The following articles from RiskNZ members can be found in the back editions in addition to the regular series of topical articles and updates from Kristin Hoskin, Sue Trezise, our Chair, our Sponsors, and members of the Board.

The articles provide enduring knowledge - just remember that the articles were written to be current at the point of publication. If in doubt about the currency of the content - contact the Editor@risknz.org.nz and we will pass your queries onto the author.

March 2019

- Leicester University Distance Learning - Risk Crisis and Disaster Management. Author: Silvia Zanini
- Risk Homeostasis Explained. Author: Grant Avery

December 2018

- How Effective is Managing the Risks of Uncertainty with people. Author: Brent Sutton
- Turning the Induction into a Powerful Risk Management Tool. Author: David Turner
- Building our Disaster Resilience. Authors: Jo Horrocks and Jane Rollin

September 2018

- Practice Note: Quantitative Risk Analysis as an input to Options Decision Making. Author: Mike Wood
- How an Informed Culture can help Project Success. Author: Silvia Zanini
- Post Implementation of Anti-money Laudering Compliance. Author: Kerry Grass
- What's in a Business Model? Author: Ben Stephens

May 2018

- From Risk Management to Resilience. Author: Nigel Toms
- New Zealand Spreads a Wider Net to Detect Money laundering. Author: Kerry Grass
- Abstract: Informing Decision-Making in the Face of Adversity. Author: Miles Crawford

February 2018

- Research Excerpt - Risk Modelling. Author: Miles Crawford
- Paper - Considering the Human Factor. Author: Cathy Hua
- My Thoughts - Remote Worker Risk. Author: Cameron Smith

April 2017

- Lessons from a lifetime of risk and its management. Author: Robin Gunston

2016 and **2015** editions of RiskPost are also available on the website for your reference.

RISKNZ STANDARDS UPDATE

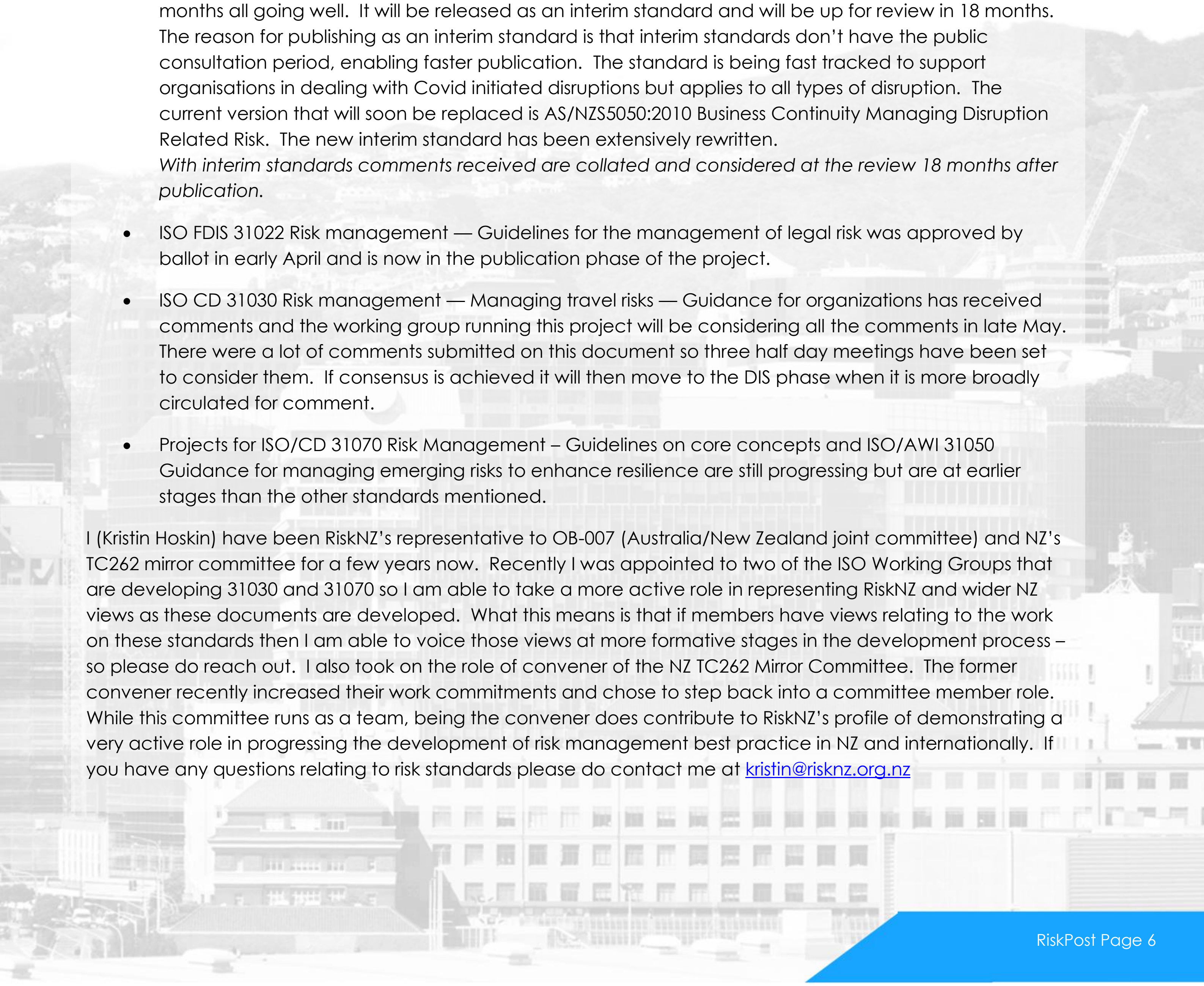
KRISTIN HOSKIN - *RiskNZ Management Board Member*

While COVID has caused many pieces of work to slow down; not so for standards. Most recent activity has revolved around standards that were to have working group meetings adjunct to the May plenary meeting of ISO TC262. Originally this was planned as a series of face to face meetings towards the end of May but has now been morphed into a number of online meetings. While the time zones are a little more difficult to manage the online format has increased the accessibility to take part as there is no travel required in order to participate.

Documents that have been very topical in the last couple of months are:

- AS/NZS 5050 – content has been rewritten and the new version is to be released within a couple of months all going well. It will be released as an interim standard and will be up for review in 18 months. The reason for publishing as an interim standard is that interim standards don't have the public consultation period, enabling faster publication. The standard is being fast tracked to support organisations in dealing with Covid initiated disruptions but applies to all types of disruption. The current version that will soon be replaced is AS/NZS5050:2010 Business Continuity Managing Disruption Related Risk. The new interim standard has been extensively rewritten.
  With interim standards comments received are collated and considered at the review 18 months after publication.
- ISO FDIS 31022 Risk management — Guidelines for the management of legal risk was approved by ballot in early April and is now in the publication phase of the project.
- ISO CD 31030 Risk management — Managing travel risks — Guidance for organizations has received comments and the working group running this project will be considering all the comments in late May. There were a lot of comments submitted on this document so three half day meetings have been set to consider them. If consensus is achieved it will then move to the DIS phase when it is more broadly circulated for comment.
- Projects for ISO/CD 31070 Risk Management – Guidelines on core concepts and ISO/AWI 31050 Guidance for managing emerging risks to enhance resilience are still progressing but are at earlier stages than the other standards mentioned.

I (Kristin Hoskin) have been RiskNZ's representative to OB-007 (Australia/New Zealand joint committee) and NZ's TC262 mirror committee for a few years now. Recently I was appointed to two of the ISO Working Groups that are developing 31030 and 31070 so I am able to take a more active role in representing RiskNZ and wider NZ views as these documents are developed. What this means is that if members have views relating to the work on these standards then I am able to voice those views at more formative stages in the development process – so please do reach out. I also took on the role of convener of the NZ TC262 Mirror Committee. The former convener recently increased their work commitments and chose to step back into a committee member role. While this committee runs as a team, being the convener does contribute to RiskNZ's profile of demonstrating a very active role in progressing the development of risk management best practice in NZ and internationally. If you have any questions relating to risk standards please do contact me at kristin@risknz.org.nz



A MSC IN MY BACK POCKET

SILVIA ZANINI

January 17 2020 was my graduation day at Leicester University – I'm guessing it will be the last graduation ceremony they will have for quite some time.

I'm really glad I went, as no one does pomp like the British. The ceremony was fantastic, my mum said I looked like a diva when walking on stage – she was so proud she kept showing the video clip to anyone with eyes and ears. My best friend and my daughter shared the experience with me, helping to create great memories.

The journey and the collaboration

Just over two years prior I received the study material, and to celebrate I treated myself to fancy pencils, a ton of post-it notes, and a new notebook, to carry with me every day, in case inspiration struck (it never quite happened). I was ready to learn. So was my student cohort, a group of like-minded people that jumped at the opportunity to collaborate online and share ideas, thoughts, and the odd research article. Sometimes I wondered if we were all studying the same course, as our interests took us in different directions and we discovered different authors and different ways to think about risk. Our collaboration is what made us so successful – we were different people, with different experiences, from different parts of the world, with one common interest: risk management.

What a weird thing to be interested in! My daughter sarcastically named the course 'happy studies', and wondered why I read about so many disasters, incidents, mismanagements, mishaps.

It is important to learn from past incidents and disasters, to know why they happened, so that we may lessen the risk of future disasters happening. Past events tell a story, they are authentic, it is easier to learn from them than to believe a model, or a simulation.

This sounds pretty straightforward, but of course nothing is that simple, and we often fail to learn. There are multiple reasons why: we may think that what happened to others may never happen to us; we may argue that no two incidents or disasters are ever the same; we may lack time to read and analyse what happened; also we generally don't enjoy learning from negative events.

Other reasons include the unwillingness of organisations to exchange information about near misses; the adversarial nature of public enquiries; and the passing of time which, combined with people leaving organisations, results in organisations forgetting the lessons of the past.

The act of learning is itself complex, with two types of learning existing: passive learning, which is simply knowing that an event happened, and active learning which is knowing that something happened and then acting to implement change. Unless remedial action is taken, no active learning occurs: there is not much point in knowing about a disaster, if steps are not implemented to prevent it.

The course content

The course covers a great deal of content; the most important for me are the systems and cultural theories of risk. Systems theory looks at socio-technical systems within an organisation. Some authors examined the level of complexity and interconnectedness between systems and the people that use those systems, suggesting that in certain circumstances accidents are inevitable, and those systems should be abandoned, while in other instances active learning may occur, resulting in safer systems.

Cultural theory is about recognising the human element to organisations, and that organisations over time develop their own culture. Safety culture, a subset of organisational culture concerned with minimising people's exposure to dangerous conditions, is also covered extensively.

It was a revelation learning that culture is vital in risk management. The right culture enables active learning, ensures that there is no pointing of fingers to find out 'who's done it wrong', promotes and rewards the reporting of incidents and near misses. Unfortunately the right culture is not achieved overnight, and it is certainly not enacted by management decree; it takes time, senior management commitment, and support from the top, not only in words but in actions.

Continued on next page…

That is why it is so difficult to achieve and also why many cultural change programmes fail.

I valued learning about Beck's Risk society, which is the idea that modern society has evolved into a risk society, in which risks display new qualities: they are not visible; not easily understood without extensive scientific and technical knowledge; they are no longer localised, crossing national boundaries, becoming global, they also no longer discriminate by social class or social wealth (radioactive pollution crosses national boundaries and affects the rich and the poor); the new risks are irreversible, the clock cannot turn back to a pre-risk situation, they are no longer limited in time, with future generations being affected; it is difficult to make anyone accountable for these risks and they are incalculable, resulting in inability to be compensated.

It was interesting learning about risk communication, and the two main risk communication models, deficit and sociological, sitting at opposite ends of the spectrum in how they view and communicate risk. The deficit model views the public simply as the recipient of knowledge from the experts, the scientists, pretty much a top-down approach to communication (just like the Italian Government did during the nuclear free debates of the late eighties); while the sociological model recognises that a single view of risk does not exist, different people have different views, with no view more important or valid than others and therefore proposing a more collaborative approach to communication (this is the stance taken by NZ in the early 2000s, when consulting extensively during the Genetic Engineering debates).

Other topics I enjoyed included episodes of internal fraud which, coupled with lack of internal controls and poor culture, caused organisational failures (like in the Barings Bank case, with Nick Leeson's fraud enabled by the totally inadequate systems for monitoring trading, and protected by a culture of greed); and the principles and practices of insurance risk.

In fact I enjoyed most of the course, with my favourite parts being writing the essays, the dissertation, not to mention the interactions with both my student cohort and my supervisor. My student cohort were always there when I had a question, when I could not find a journal article or a book, when I wanted to know if the direction I was taking was a good one – just like I was there for them. My supervisor was great: he explained topics, offered help, pointed me in the right direction; more importantly he pushed me when he felt that I could give more, he told me that my dissertation proposal was fine and would get me a pass – but was I happy with a pass, when I was able to do more and could contribute to the existing knowledge by doing primary research. I am glad I followed his advice, as although at time painful and emotionally draining, I learnt so much from the research process and I will forever be grateful to all the people that touched my life during this time.

What's next?

I have a list of books I want to read, and disaster movies to catch up on. The interest in risk management is kept alive by what happens worldwide on a daily basis. I keep in touch with my supervisor, we recently collaborated on a journal article, and I am an affiliate of the Avoidable Death Network, a global membership network dedicated to avoiding human deaths from natural hazards, naturally triggered technological hazards and human-made disasters in low- and middle-income countries. I'm done with formal studying for now, but you never know, I might pick up the books again in future.

Course details

If you want to know more about the course, have a look at the University's website (https://le.ac.uk/courses/risk-crisis-and-disaster-management-msc-dl/2020), or drop me a line.

SILVIA ZANINI

(CIMA, CGMA, AMBCI)

This is the second article that Silvia Zanini has contributed about her MSC course. See the March 2019 Edition of RiskPost for Silvia's article about selecting her course. The back-editions of RiskPost are available on the members area of the RiskNZ website risknz.org.nz (search for RiskPost).
Silvia has extensive risk and audit experience gained in Italy, the UK and NZ. She is modest about her achievements, she graduated from the MSC course with Distinction.

THE BUCK STOPS HERE: GOVERNANCE OWNS ALL THE RISKS

NICK LEWIS – *CFA*

Ray Willows kindly invited me to join RiskNZ's Network Forum meeting on 20 February at NZTA's office in Wellington to share a few thoughts on how boards can best work with risk managers. I am not a risk management expert but I am a professional director who regularly 'consumes' the output of great risk managers and their thorough risk management processes. Here are the key points of our discussion.

Every board must have access to effective risk management. Over the past decade, risk management has been elevated from being just another line item on the board meeting agenda to a core expertise that every board and management team must have. Good governance makes full use of effective risk management, and boards, and each director, are being held to a higher standard - a good thing. The old boys network, I'm pleased to report, while not entirely gone, is disappearing.

Directors wear more personal financial and reputation risk if things go wrong than ever before. "But we didn't know!" is no longer an adequate defence if a problem occurs and a lawsuit ensues. The courts are more likely to decide that whether or not the directors knew about a risk, they should have known.

New risks are always emerging that boards need to manage such as climate change, cyber attack, social responsibility, and technological disruption. And of course pandemics. Risk managers need direct access to their boards, and developing a good rapport with the Chair is an excellent starting point. The board should also establish a Risk Committee where the Committee Chair is one of the independent directors but not the board's Chair.

For high-growth companies, the biggest risk is often ensuring on-going access to new capital to fund growth. But risks can emerge from any quarter; I was recently brought in to a situation where the board's own dysfunctionality had became the company's biggest risk.

Could a more effective risk management process have identified and mitigated that risk sooner? And as the company's risk manager, how would you tell your board they have become dysfunctional?

Different industries require different risk management processes fit for purpose. The board of an energy company where staff and contractors work with high voltage, high pressure, high temperatures, and in high places have adopted ISO 45000 (Occupational Safety & Health) and 55000 (asset management). This in turn has prompted them to develop in-depth processes, procedures, training, and internal and external audits around risk identification and mitigation. That Board spends a lot of time discussing on-going risks and what they are doing to mitigate them, looking at both existing controls and how they are treating them to reduce any intolerable risks. Interestingly, after a thorough analysis, the single highest risk facing our staff in that company turned out to be driving.

But how do boards know whether a management team is effectively identifying and managing risk? In some cases, in addition to audits, each director also visits the companies' work sites to complete safety checklists, chat informally with staff and contractors, and report back to the full board on what they have learned.

Continued on next page…

In the financial services sector, a large part of their governance responsibilities are regulatory compliance. Non-compliance with the Financial Markets Authority's (FMA) requirements is among the highest risks those boards face, and the penalties are serious and borne personally by each director. That said, the finance sector considers upside risk, the potential for a positive outcome from a perceived risk.

The boards of listed companies also have much on their plates. Not only must they achieve business growth, access capital and attract top talent, they must do so whilst maintaining full compliance with the NZX Stock Exchange's Listing Rules, the Companies Act 1993, and the Financial Reporting Act 2013.

Risk management as a discipline has never been more required or recognised by boards. In other words, it's a great time to be professional risk manager.

NICK LEWIS

(CFA)

Nick has 15 years of governance experience in the fintech, financial services, energy, hospitality and education sectors. He is an investor in early-stage companies and previously had a Wall Street finance career in M&A, equity, bank, bond, and derivatives capital markets at JP Morgan in New York. He is currently the Chair of NZX-listed payroll company, PaySauce Limited; the Chair of Kiwi Insurance (an affiliate of Kiwibank); a director of renewable electricity generator Pioneer Energy; and a director of CarboNZero-certified electricity retailer Ecotricity. Nick was also formerly the Chair of Mojo Coffee and the crowdfunding site PledgeMe. He is a Chartered Financial Analyst (CFA).

USING WORK DOMAIN ANALYSIS IN A SAFETY CASE DEVELOPMENT

MARGARET J. TROTTER – *Navigatus Consulting*

1. Introduction

1.1. The Safety Case context

Navigatus was contracted by the Ministry of Business, Innovation and Employment (MBIE) to produce a Foundation Safety Case (FSC) for the integration of unmanned aircraft (UA) into the New Zealand Airspace. The operational scope was non-passenger carrying, extended visual line of sight (EVLOS) and beyond visual line of sight (BVLOS) flights in Class G airspace. The FSC is to form the basis for the submission of subsequent Operator Safety Cases (OSC) to the New Zealand Civil Aviation Authority (CAA).

The purpose of a FSC is to set out the processes that must be delivered and the criteria that must be met by a UA operator to ensure the risk associated with airspace integration of that particular UA operation meets an acceptable level of safety. Developing the FSC required identifying these criteria and establishing what constitutes an overall acceptable level of safety. For each subsequent OSC, the calculated level of risk can be compared to the FSC target levels for each of the criteria and the overall safety level.

Identifying the risk criteria necessitates determining the key functions and processes that are necessary for operators to integrate into the airspace with minimal risk. In an emerging area where technology is advancing rapidly, it is important to define these functions without prescribing the specific technologies that an operator requires to perform them, leaving room for innovation and continuous improvement, in other words, a formative approach.

1.2. Cognitive Work Analysis & Work Domain Analysis

Cognitive Work Analysis (CWA) is a structured, formative Human Factors approach to analysing, modelling, designing and evaluating complex socio-technical systems (Vicente, 1999). It considers flexibility and adaptive capacity by describing system constraints and ways in which a system can operate within those constraints (Vicente 1999). CWA can be used as both a design tool (Read, Salmon, Lenné and Stanton, 2015) and as a means of evaluation (Stanton, Salmon, Walker, & Jenkins, 2017) by developing representations of the socio-technical system constituent elements, including technology, operator skills, artefacts, and organizational and environmental factors (Millen, Edwards, Golightly, Sharples, Wilson & Kirwan, 2011).

The WDA framework constitutes five phases, each modelling a different constraint set (Vicente, 1999:

1. **Work domain analysis:** Models the system constraints by describing what the system is trying to achieve, and how it tries to achieve its purpose.
2. **Control task analysis:** Models situational constraints and decision-making requirements.
3. **Strategies analysis:** Models different ways in which activities can be carried out within the system constraints.
4. **Social organisation and cooperation analysis:** Describe communication and coordination demands based on organisational constraints.
5. **Worker competencies analysis:** Describes skills, rules and knowledge required by actors within the system.

Work Domain Analysis (WDA) is the first stage of CWA. WDA identifies and models the properties of the work domain (in this case flight operations in the NZ airspace) that constrain the possibilities for action without explicitly identifying specific sequences of actions. It is thus a formative rather than a prescriptive model and is context independent, making it particularly useful for analysing the introduction new or developing technologies such as UA.

Continued on next page…

WDA identifies the functional purposes, values and priority measures, purpose-related functions, object-related processes, and physical objects and artefacts within the system and how they relate to one another within the system (see Table 1 for descriptions of the WDA levels). Each element in a WDA level is connected to other elements in the levels above and below via means-ends links; for example, the means for a specified function is provided by processes in the level below to support the value measures in the level above. It is therefore possible to see how changes to artefacts affect the system as a whole and impact on its overall purpose. These analyses are used in the design stage to determine what system objects need to be in place to afford the process need to carry out the system's key functions. These key purpose-related functions were of most relevance for the development of the safety case as they define the functions that need to take place to allow safe, effective airspace integration.

In this piece of work, we used the WDA in order to inform the structure of the FSC and subsequent OSCs.

Table 1. Description of Work Domain Analysis levels

Row	WDA level	Key Questions	Key words
5 Top	**Functional Purposes**	• For what reasons does the system exist? • What are the ultimate purposes or highest-level objectives of the system? • What has the work system been designed to achieve?	Purposes, reasons, objectives, aims, mission, ambitions
4	**Values and Priority Measures**	• What criteria can be used to judge whether the system is achieving its purposes? • What laws and regulations does the environment impose on the system? • What performance criteria are used to compare the results of system functions?	Regulations, standards, values, measures of effectiveness/ efficiency/ quality
3	**Purpose-related Functions**	• What functions are required to achieve to purposes of the system? • What are the functions performed with the physical resources within the system? • What functions coordinate use of resources within the system?	Functions, tasks, roles, activities, operations, jobs
2	**Object-related Processes**	• What can the physical objects in the system do or afford? • What are the physical objects in the system used for? • What are the functional capabilities and limitations of physical objects in the system?	Processes, uses, functionality, capabilities, applications
1 Bottom	**Physical Objects**	• What are the physical objects/ resources in the system – manmade and natural? • What are the material characteristics of physical objects /resources in the system? • What is the topography or organisation of the system?	Objects, tools, equipment, dimensions, attributes, locations, orientations design

Continued on next page…

2. Method

The development of a WDA is an iterative process. In this case, the WDA was developed through a series of workshops, meetings and online interactions with key stakeholders and refined through its integration into the save case proper.

2.1 Participants

Representatives from MBIE, CAA, the Ministry of Transport (MoT), Airways, and a UA Operator were involved in the development of the WDA. Depending on time available, different stakeholders engaged at different times and stages of its iterative development. All representatives from each of these agencies joined in an initial presentation and discussion in a workshop, while MBIE, CAA and Operator representatives engaged further via small meetings and through online feedback.

2.2 Equipment

Each version of the WDA was produced using the 'CWA Tool', a computer programme developed originally by the University of Southampton to produce each stage of CWA analysis. This project used the WDA stage, and specifically the 'Abstraction Hierarchy' function of this programme.

2.3 Procedure

The first iteration of the WDA was produced by Navigatus' lead Human Factors (HF) consultant based on the first all-stakeholder workshop conducted for the project. This was then assessed by two Navigatus directors with in-depth aviation knowledge and experience to produce a second iteration. Iteration 2 was then presented to the Operator, CAA and MBIE representatives at two meetings and their feedback was incorporated during these meetings. Each entry in each level of the WDA was scrutinized along with associated links. Additional entries were added at each level, wording was updated and further links established. The updated iteration (iteration 3) was sent out via email and further updates made based on comments received.

The identified functions were then mapped against the International Civil Aviation Organization (ICAO) safety regulations in order to identify any functions not yet covered in the WDA. This mapping process identified two further functions, which were added to the WDA and linked appropriately to processes and measures, becoming iteration 4. This iteration was used for integration into the safety case.

3. Results

The size and complexity final version of the WDA make it difficult to present in print format, so for clarity the functions and associated processes are given in Table 2. A total of 18 functions were identified. These were linked to 26 processes, with processes able to link to multiple functions and functions to multiple processes. The most highly linked function was "Execute responsibilities of pilot in command", which was linked to ten processes (see Table 2)

For the purposes of this safety case, the CAA are interested in the safety of the aircraft and operation, rather than the organisational factors related to the Operator (although the latter are important to overall system safety and so are included in the WDA). Therefore, only functions 1 to 12 as shown in Table 2 were integrated into the safety case.

Continued on next page…

Table 2. Functions and linked processes from Work Domain Analysis for integration of UA into New Zealand airspace.

Purpose-related Functions	Function-related Processes
1. Positional awareness and navigation	• Allows IFR & VFR navigation
2. Maintain airspace domain situational awareness	• Detects position of other air craft • Provides knowledge of fixed hazards • Provides terrain awareness
3. Maintain obstacle and terrain awareness and separation	• Provides knowledge of fixed hazards • Provides terrain awareness • Allows aircraft manoeuvrability and response
4. Identify other traffic	• Detects position of other air craft • Allows traffic avoidance • Allows awareness of dynamic hazards • Allows 2-way communications and info flow
5. Comms capability with other system users	• Allows 2-way communications and info flow • Allows traffic avoidance
6. Detect other aircraft	• Detects position of other air craft • Allows awareness of dynamic hazards
7. Be detectable by other traffic	• Allows 2-way communications and info flow
8. Avoid other traffic	• Allows traffic avoidance • Allows awareness of dynamic hazards • Allows aircraft manoeuvrability and response
9. Respond to changing operational conditions	• Allows 2-way communications and info flow • Allows aircraft manoeuvrability and response • Execute mission and respond to amendments • Allows decisions/ responses to new information • Allows awareness of aircraft status and capabilities • Allows air traffic management • Impacts flight requirements
10. Execute responsibilities of pilot in commend	• Allows take-off, landing and ground handling of UA • Allows awareness of dynamic hazards • Allows 2-way communications and info flow • Allows aircraft manoeuvrability and response • Execute mission and respond to amendments • Allows decisions/ responses to new information • Allows awareness of aircraft status and capabilities • Defines operating procedures and instructions • Impacts flight requirements • Identifies applicable rules of the air
11. Execute command and control	• Allows 2-way communications and info flow • Allows aircraft manoeuvrability and response • Execute mission and respond to amendments • Allows air traffic management
12. Respond to UAS faults and failures	• Allows awareness of dynamic hazards • Allows 2-way communications and info flow • Allows aircraft manoeuvrability and response • Execute mission and respond to amendments • Allows decisions/ responses to new information • Allows awareness of aircraft status and capabilities • Allows data and information recording

Continued on next page…

Purpose-related Functions	Function-related Processes
13. Meet passenger needs	• Allows 2-way communications and info flow • Allows aircraft manoeuvrability and response • Enables passenger and load handling • Carries passengers and cargo • Allows protection of passengers and cargo
14. Maintain training & qualifications of operators and personnel	• Defines operating procedures and instructions • Defines licencing requirements • Develops and maintains operator skills • Approves operation of UA within aviation system by operator
15. Maintain quality of cargo being transported	• Allows aircraft manoeuvrability and response • Execute mission and respond to amendments • Allows protection of passengers and cargo • Impacts flight requirements • Enables passenger and load handling
16. Deliver intended service (e.g. air works, deliveries etc)	• Execute mission and respond to amendments • Allows decisions/ responses to new information • Carries passengers and cargo • Allows conduct of air work tasks • Allows protection of passengers and cargo • Enables passenger and load handling • Develops and maintains operator skills
17. Continued airworthiness management	• Determines airworthiness requirements • Approves operation of UA within aviation system by operator
18. Maintain approved SMS	• Defines licencing requirements • Allows data and information recording • Approves operation of UA within aviation system by operator

4. Discussion

The safety case framework was structured around the 12 functions and their associated processes as identified by the WDA. Each process was further divided into on the UA itself, within the UA system (i.e. the ground station and command and control links between the ground station and the UA), and external to the UA system (e.g. telecommunications networks) to ensure consideration was given to each of these aspects in turn when considering potential failures and mitigations.

Failures of each process are then considered as the key events in bowtie analyses, prompting the identification of event and consequence mitigations. The likelihood of events and the effectiveness of mitigations are then calculated and combined to give an overall risk level for the Operator. Should the risk level fall below a specified level (currently 1 x 10^{-7} in this case), the individual risk scores for the functions and processes can be examined to determine where stronger mitigations are required.

Continued on next page…

WDA was a useful tool for the development of a safety case because it:

- Takes a system wide approach rather than focusing on changes at the "pointy end" the system;
- Integrates research and information from varied sources into a unified framework;
- Aids communication with key stakeholders. For example, the breakdown of physical functions can map directly onto the underlying technical infrastructure of a system, so the impact of minor system changes can be seen and understood (Millen et al, 2011); and,
- Supports the identification of design solutions that can help operators manage unanticipated events (Jenkins et al., 2007; Naikar, 2006; Sanderson, 1998).

5. References

Jenkins, D.P., Stanton, N.A., Salmon, P.M., Walker, G.H., Young, M.S., Whitworth, I., Farmilo, A., & Hone, G. (2007). The Development of a Cognitive Work Analysis Tool. *International Conference on Engineering Psychology and Cognitive Ergonomics*, 04-511.

Millen, L., Edwards, T.E., Golightly, D., Sharples, S., Wilson, J.R., & Kirwan, B. (2011). Systems change in transport control: applications of cognitive work analysis. *The International Journal of Aviation Psychology, 21(*1), 62-84.

Naikar, N. (2006). Beyond interface design: Further applications of cognitive work analysis. International. *Journal of Industrial Ergonomics, 36*, 423–438.

Read, G.J.M., Salmon, P.M., Lenné, M.G., Stanton, N.A. (2015). Designing sociotechnical systems with cognitive work analysis: Putting theory back into practice. *Ergonomics, 58*(5), 822-851.

Stanton, N.A., Salmon, P.M., Walker, G.H., & Jenkins, D.P. (2017). *Cognitive Work Analysis: Applications, Extensions and Future Directions.* Boca Raton, FL: CRC Press.

Sanderson, P.M. (1998). Cognitive work analysis and the analysis, design, and evaluation of human-computer interactive systems. *Proceedings Australasian IEEE Xplore Conference: Computer Human Interaction Conference*. DOI: 10.1109/OZCHI.1998.732218

Vicente, K.J. (1999). *Cognitive work analysis: Toward safe, productive, and healthy computer-based work*. Mahwah, NJ: Lawrence Erlbaum Associates.

MARGARET TROTTER

(PHD)

Dr Maggie Trotter gained her PhD in Human Factors Psychology from Monash University.

Since this article was written Maggie has moved to the NZ Transport Agency in the role of Senior Advisor - Behavioural Insights.

Her LinkedIn profile is available here.

ONLINE READING - THIS YEAR IS DIFFERENT

SUE TREZISE – *Sue-lutions Ltd*

Looking beyond the Top 10 and doing the 'Pivot'

By this time any other year I would be providing a summary of reports such as the Allianz Risk Barometer or the AON Global Risk Survey, using the insights to benchmark risk activities and awareness in the New Zealand context.

2020 is one out of the box (as they say) with the COVID-19 pandemic creating a completely different context for risk practitioners, given the depth and breadth of unknowns and the velocity with which change has happened.

What's different this time?

It is as if the Top 10 risks have all been realised in the same event, rather than as independent developments as might normally be anticipated. It's the earthquake risk (low likelihood, high consequence risk) realised in all places at once – no one and no place is unaffected. It's a collection of threats that has become a super-issue situation: mass business closures; supply chain breakdown; loss of resources through lockdown or quarantine; a substantial decline or significant increase in customers depending on the face-to-face or online presence; sudden change in business regulations/requirements (eg social distancing constraints in work and retail space); and the malevolent presence of IT cyber attacks, security breaches and internet failures.

From the same setting, new thinking has been triggered. For example, opportunities created by the acceleration of telework (increased use of virtual meetings, confidence in online productivity), working from home flexibility, sharing of strategies for coping with isolation (cooking, exercise and mindfulness videos), and big wins for those industries well positioned to respond to demand for online products and services.

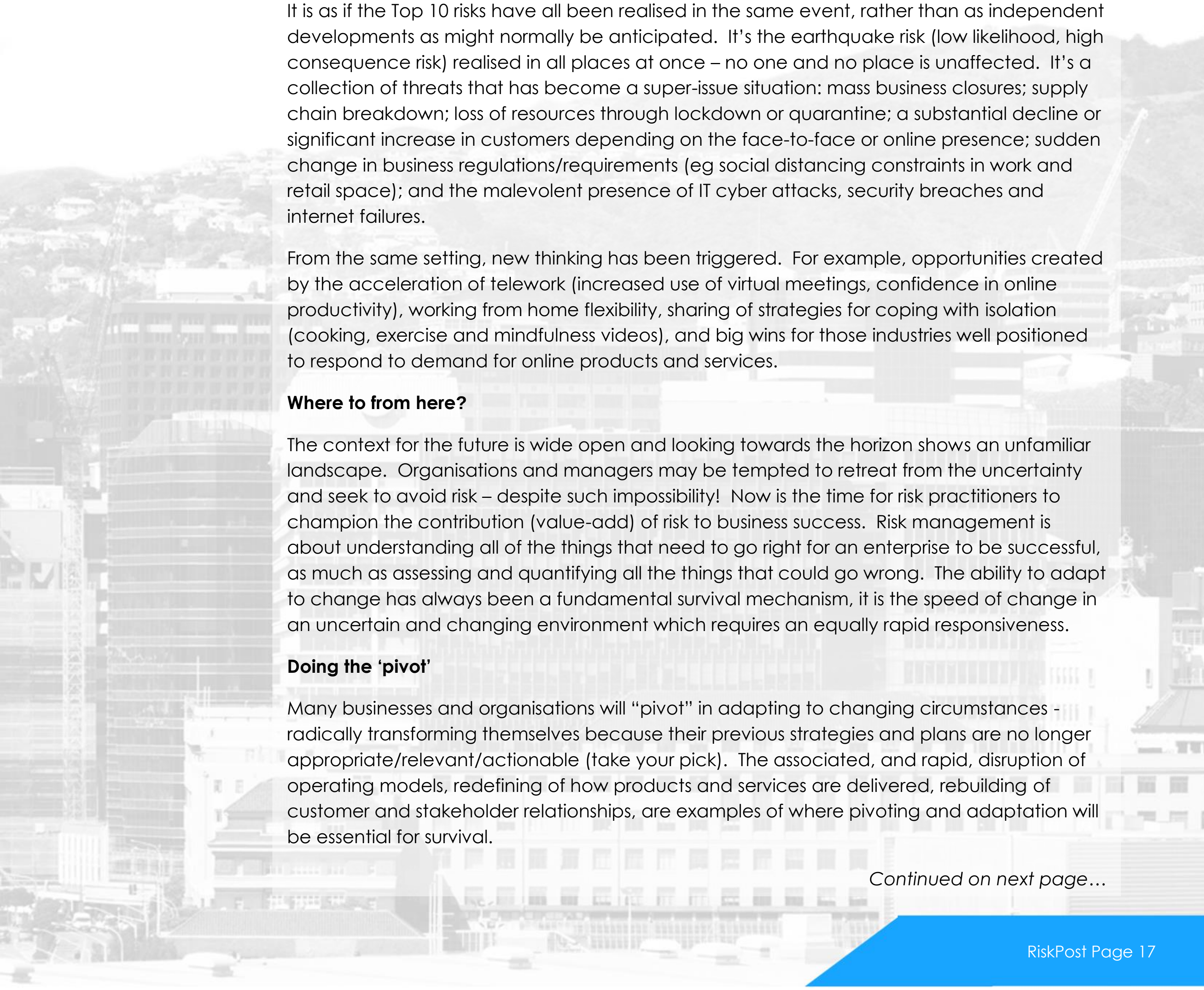
Where to from here?

The context for the future is wide open and looking towards the horizon shows an unfamiliar landscape. Organisations and managers may be tempted to retreat from the uncertainty and seek to avoid risk – despite such impossibility! Now is the time for risk practitioners to champion the contribution (value-add) of risk to business success. Risk management is about understanding all of the things that need to go right for an enterprise to be successful, as much as assessing and quantifying all the things that could go wrong. The ability to adapt to change has always been a fundamental survival mechanism, it is the speed of change in an uncertain and changing environment which requires an equally rapid responsiveness.

Doing the 'pivot'

Many businesses and organisations will "pivot" in adapting to changing circumstances - radically transforming themselves because their previous strategies and plans are no longer appropriate/relevant/actionable (take your pick). The associated, and rapid, disruption of operating models, redefining of how products and services are delivered, rebuilding of customer and stakeholder relationships, are examples of where pivoting and adaptation will be essential for survival.

Continued on next page…

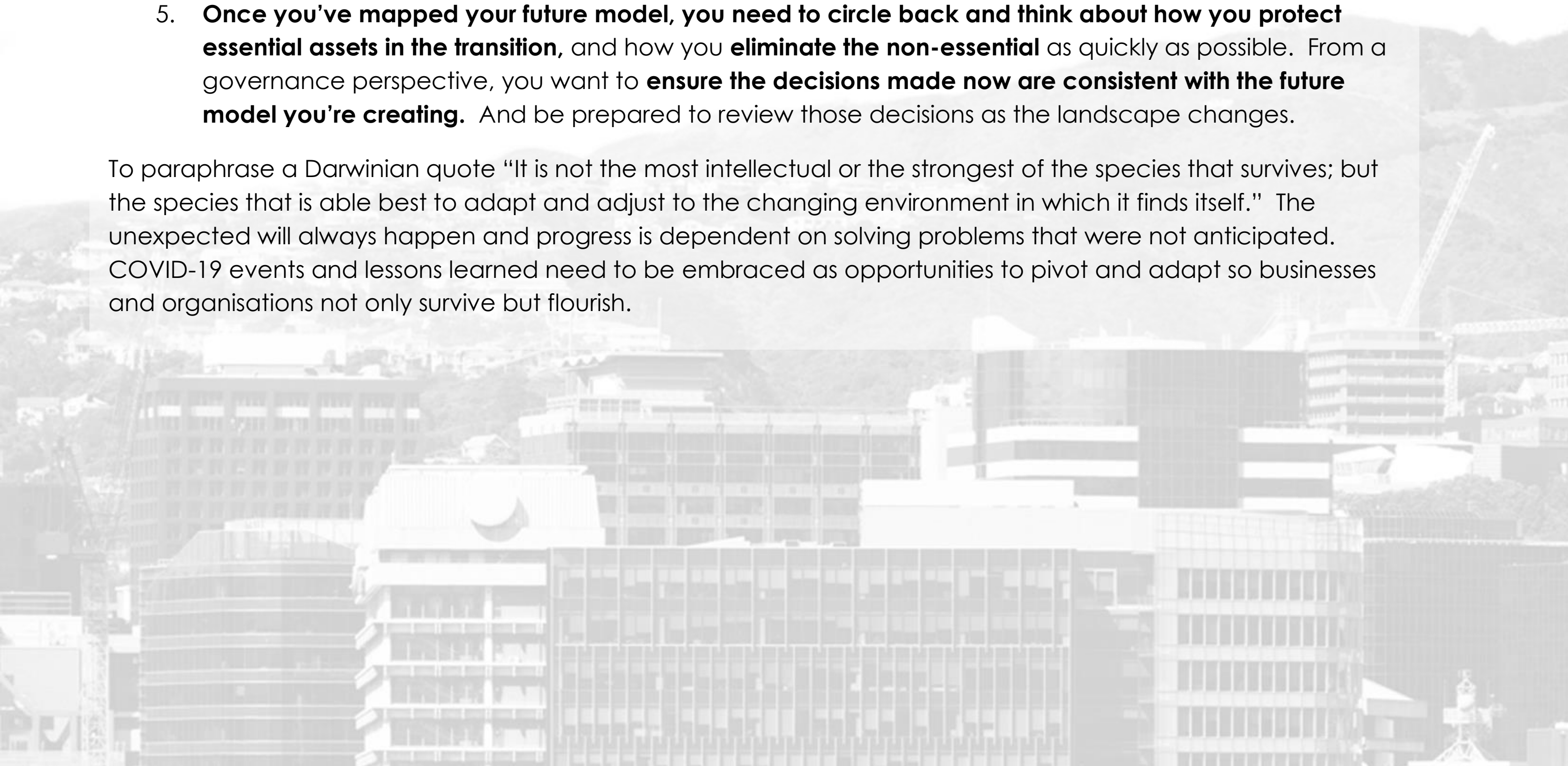


Some relevant insights can be gained from a study co-authored by Paul Tracey of Cambridge Judge Business School which focused on the prevalence and pitfalls of pivoting for new ventures. While not necessarily embarking in a truly entrepreneurial way, for many organisations the pivot required in COVID-19 times has similar concerns. A key approach is creating a bond with 'user communities' by shared experience of the difficult transition journey, to rebuild their connection with the organisation's products/services/values. The study noted that while entrepreneurs (or businesses) can rebuild relationships with customers and suppliers, there is a flip side – that building these kinds of relationship creates a sense of obligation and a sense of expectation for continued engagement. As needs change or new opportunities for the business are discovered, further pivoting will continue. Applying a risk-lens will minimise the chance of a poorly planned or managed pivot alienating those relied-on supporters.

In her Icehouse webinar, Melissa Wragge presented the following Pivoting Tips and Traps

1. **Being adaptable is your biggest asset.** Things are changing daily so stay open and move where the market is.
2. You might think you need clarity first when actually **you get clarity from the doing**. Test and learn.
3. You can **move quickly in short sharp sprints**.
4. **Before you go on the journey, it's really important to know where you stand.**
5. **Once you've mapped your future model, you need to circle back and think about how you protect essential assets in the transition,** and how you **eliminate the non-essential** as quickly as possible. From a governance perspective, you want to **ensure the decisions made now are consistent with the future model you're creating.** And be prepared to review those decisions as the landscape changes.

To paraphrase a Darwinian quote "It is not the most intellectual or the strongest of the species that survives; but the species that is able best to adapt and adjust to the changing environment in which it finds itself." The unexpected will always happen and progress is dependent on solving problems that were not anticipated. COVID-19 events and lessons learned need to be embraced as opportunities to pivot and adapt so businesses and organisations not only survive but flourish.



REFERENCES

The Art of the Pivot: *How New Ventures Manage Identification Relationships with Stakeholders as they Change* Direction Sources: https://insight.jbs.cam.ac.uk/2019/pivoting-successfully/ and https://journals.aom.org/doi/10.5465/amj.2017.0460

Icehouse Webinar:

Source: https://info.theicehouse.co.nz/webinars

ONLINE READING - THIS YEAR IS DIFFERENT…*continued*

Cyber crime in a pandemic environment

Cyber incidents remain the #1 business risk according to the Allianz Risk Barometer 2020. The annual survey (responses by 2,718 risk experts in 102 countries, across 22 industry sectors) predates Covid-19 chaos, however its relevance should not be overlooked.

While we are focused on the multiple and more obvious impacts of the global shutdown – business closures, home isolation, staff layoffs, remote working, social distancing requirements, etc – it is a timely reminder to maintain vigilance for the less visible risk of IT failure/outages and cyber crime in particular.

Organised criminals seize on topical issues like Covid-19 to lure people to bogus websites with malware on them or harvesting credit cards through fake charity donation pages. Organisations can be more vulnerable in times of crisis if staff are distracted by the urgency of response work from watchfulness for phishing emails (for example). Working from home also increases the likelihood of clicking malware through into business systems as people operate in a more relaxed 'office' environment which crosses into their personal space.

Some close to home examples of cyber incidents include:

- IT system attacks on freight company Toll Group. In the most recent of two incidents already this year, Toll had its IT system attacked and a ransom demanded by hackers. The system had to be shutdown (and customers notified) and was offline for 36 hours leaving staff to process bookings manually and using the external gmail accounts to communicate. Toll has a clear policy of not paying any ransom. https://www.newsroom.co.nz/2020/05/05/1158942/freight-firm-toll-struck-again-by-cyber-threat
- A news report of computer issues at meat processing company AFFCO described a disruption to supply deliveries of meat for at least three nights in a row and interruption to its ordering system. Staff were also reported to have had their pay affected. The company did not contribute to the article[1]. https://www.newsroom.co.nz/2020/05/05/1157253/affco-meat-supply-affected-by-it-issue
- From across the Tasman - A sophisticated form of malware was detected in an email sent to the Western Australian Premier's office by the Indonesian Embassy in Canberra. It is claimed hackers infiltrated the computer of a diplomat, found a draft email, completed it and concealed the malware within an attached document before sending it. The malware involved was designed to give the hacker administrative access, basically near total control over their victim's computer system with access to copy, delete or create files, carry out extensive searches of the device's data, and send emails on behalf (ie allow a hacker to digitally impersonate their victim). https://www.nytimes.com/2020/05/07/world/asia/china-hacking-military-aria.html

The impact of COVID-19 has increased our already high dependence on technology and with it the magnitude of the threat posed by cyber crime. While money is at the heart of some if not most cyber crime, collateral damage includes further business interruption/failure/loss through system shutdowns, operational rework, IP/data theft, reputation damage, loss of business custom and customers.

Cyber crime is not an 'earthquake' risk (the standard low likelihood, high consequence risk), it is an 'elephant' risk (the risk no-one wants to mention). The increasing likelihood of high to extreme consequence at any level (local, global, all sectors) makes this a red flag topic for risk practitioners to continually raise. We have seen how bad it can be with a contagious people virus, where might a computer virus take us?

[1] It is noted that this is not uncommon, with companies attacked in this way being typically quiet about it. The Government's Computer Emergency Response Team (CERT) to whom such incidents are generally referred also respects the sensitive nature of any reports and does not confirm or deny involvement.

SUE TREZISE

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.

UNDERSTANDING AND MANAGING INTERCONNECTED RISK WITH BOWTIE ANALYSIS

ROSS LISTON – *Risk Advisory, KPMG*

'The New Normal' / 'The Next Normal' / 'The Now Normal'

Since the outbreak of COVID-19 and the subsequent global lockdown, risk management as a discipline, has come under a lot of criticism. Boards and executives have asked why a pandemic was not on the list of top risks for the organisations they look after, and when it was, why the assessment was so woefully inadequate. Forecasting modellers of every sort have been poles apart in their predictions; made worse by the political agendas they support or challenge. Everybody is arguing over whether covid-19 is a 'black swan', a 'black elephant' or a 'gray (sic) rhino' – like giving it the right label will make a difference. We're even falling all over ourselves to coin the most appealing phrase for what things will be like when we emerge from this (refer to the paragraph heading above).

While there are some very smart assessments and beneficial recommendations of how to manage businesses as we transition out of lockdown, it is fair to say there is far more noise than there is signal. What is not a moot point is how interconnected we all are and that risk contagion is very real phenomena.

However, once we've decided on a regime for face masks; demarcating where people can stand relative to one another; and have dispensed copious amounts of hand sanitiser, we still need to get back to the core objective of getting back to business.

Changes to how we think about risk are inevitable, but I would argue that the fundamental risk principals of 'cause' and 'consequence', and how we understand and manage them will remain largely unaltered. Until sophisticated models become more accurate and common place, we have tools such as bowtie analysis that allow us to simplify and adequately map connections between risks and where to intervene to 'get things right' and/or 'stop them going wrong'.

What is Bowtie Analysis?

Let's assume that the majority of people who read this article will have sufficient knowledge of risk management to know what bowtie analysis is. However, since there is no single way of doing bowtie analysis, and it is not yet common place, there is merit in clarifying this to begin.

In its most rudimentary form bowtie analysis refers to a wording convention adopted by certain organisations for naming risks – i.e. the risk name should align to "The risk of an event as a result of a certain cause/s leading to certain consequence/s" (refer to Figure 1a).

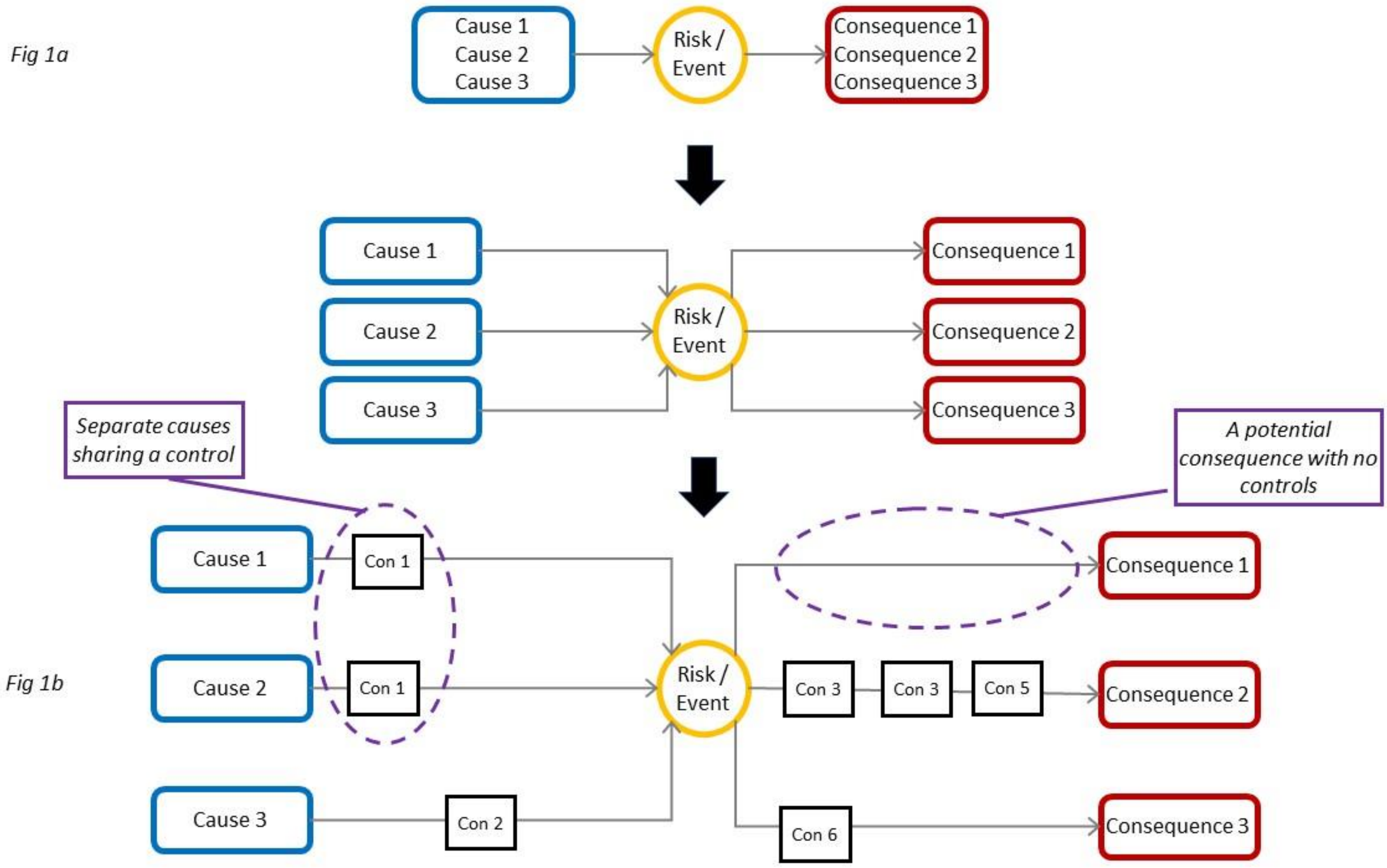
While this practice helps to communicate how a risk is caused, and its consequences, the most valuable characteristic of true bowtie analysis focuses on how the source of risk is controlled (refer to Figure 1b).

The bowtie is basically a barrier-based risk assessment, representing the 'layers of protection' to manage a risk (hence its use in Layers of Protection Analysis (LOPA)). Since its initial applications in high hazard industries, for the assessment and/or investigation of major industrial accidents, the application of bowtie analysis has become more prevalent in a range of industries particularly to create an effective connection between internal controls and the management system.

Based on the conceptual example shown in Figure 1b, we could immediately see the likes of: what controls we have in place (or not); which controls address multiples causes and consequences; and whether we have a stronger focus on preventing or responding to the risk event.

Continued on next page…

Figure 1: Bowtie Analysis: From risk naming to control mapping



Risk Trajectories and Risk Contagion

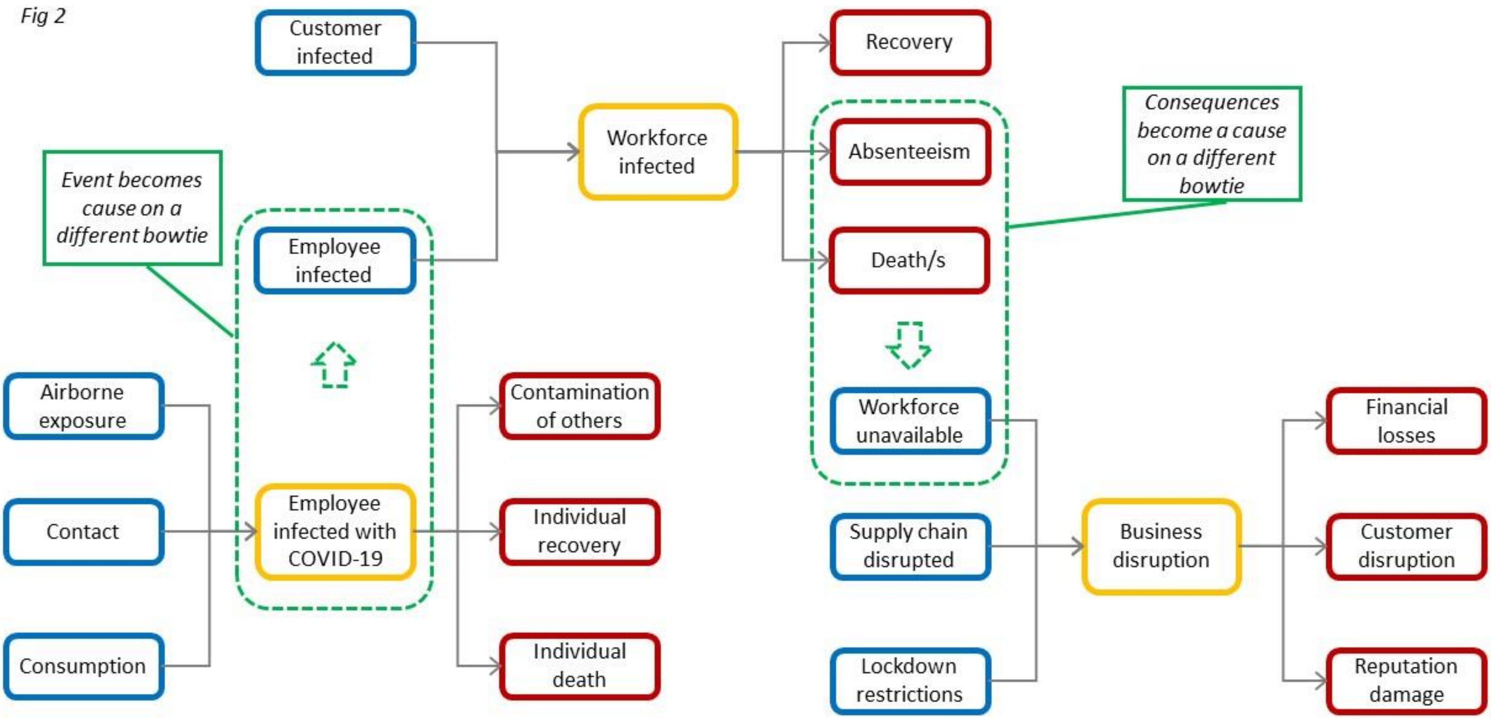
Whether it's the basic risk naming convention or the more detailed exploded view for control mapping, a common characteristic of bowties is the representation of the risk developing over a period of time – from the cause, to the event, and to the consequence. In essence, this is the trajectory of the risk. Our view and understanding of risk is determined by our position on this trajectory – which typically aligns to our span of control and functional responsibility.

However, if we consider how the contagion effects of COVID-19 rapidly evolved from concern for our personal health to concerns for the global economy, it becomes very apparent that understanding and managing interconnected risk has to consider a wider arc of the risk trajectory and stepping outside of siloed functional responsibilities to look at the system.

Figure 2 below shows a chain of bowties to illustrate the concepts of risk trajectory and risk contagion. The basic format of bowtie analysis means that risk events on one bowtie can be represented as the cause of a downstream bowtie, and the consequence of that bowtie can be represented as the upstream causes of another bowtie.

Continued on next page…

Figure 2: COVID-19 – from viral exposure to financial loss



To make it understandable and suitable for this article, the above representation has been significantly simplified, which has meant the fundamental element of controls has been excluded. Nevertheless, the reader should appreciate that with the controls incorporated into this diagram, the risk management requirement becomes very apparent for the organisation (from Board to frontline employee) and the stakeholders (vendors, customers, civil society, etc.) it is influenced by or has influence on.

For Bowtie Analysis It's Business As Usual

In summary, bowties encompass the following characteristics:

- They provide **visual representation** of the risk and how it might manifest, it can better facilitate communication of how the risk is being managed beyond what a narrative representation can do.
- Although they are predominantly used for safety risks, their capability of representing the 'wider system' allows them to be **agnostic of risk type.**
- The methodology allows one to **'zoom in and zoom out'** from very precise risk management detail to more high-level perspectives; it can be used from hands-on operational application to boardroom discussions.

Continued on next page…

- They show **risk trajectory from causes through to consequences (i.e. shift focus 'upstream' or 'downstream')**.
- They highlight **risk and control interconnectivity** across the organisation (and beyond the organisation's boundaries).
- Taken in combination, the aforementioned characteristics enable **multifaceted understanding of how the risk is managed**, such as through:
  - Associating controls with **varying consequence types** (viz. not restricting understanding to just a single consequence type);
  - **Assigning ownership** and **collaborative management efforts** to risks and controls;
  - Identifying **absent and inadequate controls** (in terms of design or execution) and where to pinpoint attention;
  - Identifying **superfluous, over-complicated and contradictory controls** and thereby streamline the number and type of controls;
  - Identifying key/**critical controls** to be given greater attention, and highlight the correct key risk indicators (KRIs) and key control indicators (KCIs) to monitor and be reported on.
- It guides the design of a **more effective assurance programme**, shifting assurance from just being 'forensically-minded' to more 'predictively-minded'.
- It is useful to **communicate to stakeholders** (such as shareholders, vendors, clients, regulators, even the public, etc.) that the risks that have been identified, are understood and are being effectively managed.
- In addition to assessment and assurance, the bowtie methodology is also useful for the **analysis of incidents**.

In conclusion, the bowtie methodology provides a systematic analysis of how risks are or should be managed; particularly in our ever increasingly connected world - irrespective of what you want to call it.

ROSS LISTON

Ross Liston is an Associate Director in KPMG's Risk Advisory practice in New Zealand. He has over twenty years consulting and industry experience in enterprise, operational and project risk management. Ross has experience from around the globe, across a wide-range of sectors and risk profiles. He assists organisations to strategise, integrate and enhance risk and assurance practices within their business.

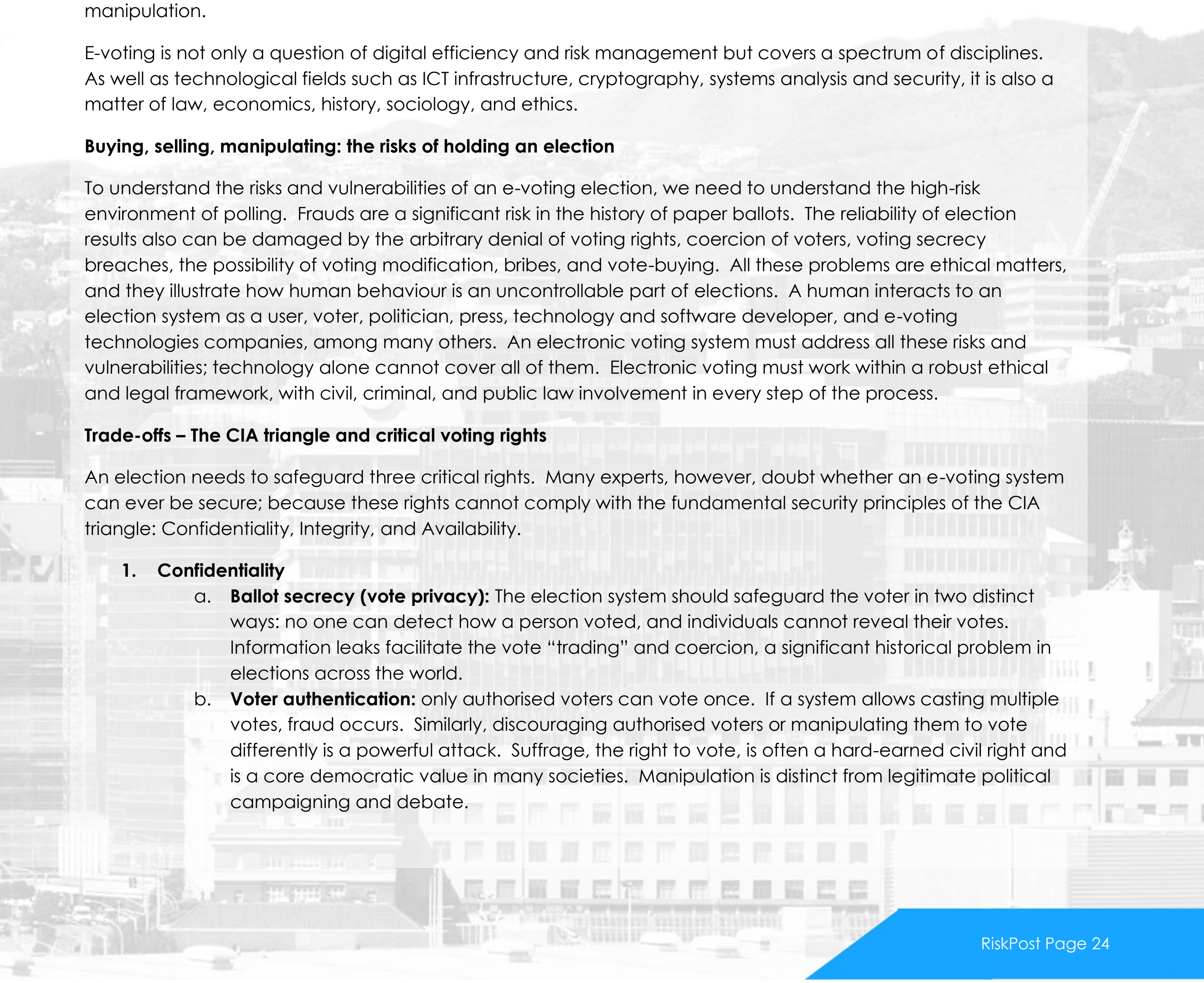
RiskNZ would like to acknowledge the support we have received from KPMG Wellington and pass on our thanks.

ELECTRONIC VOTING RISKS AND VULNERABILITIES – AN INFORMATONI SYSTEMS SECURITY APPROACH

CYBELE SOUZA

Digital technology facilitates our lives. In times of COVID-19, society has become even more dependent on e-commerce, e-banking, and video conferences while staying at home. Likewise, the daily business of governing countries has also become digitised. So why do most democratic countries not use technology to facilitate elections? There is high resistance to adopting the digital option, although there have not been any well-known attacks against e-voting systems.

Only 26 countries have electronic national elections, while 80% of the world do not have e-voting in place. Britain, Germany, the Netherlands, Ireland, and Switzerland attempted use e-elections. However, many of them later gave up, after detecting process deficiencies that could affect the integrity of the votes and the election results. According to security experts, reasons for not adopting e-voting include lack of specialists; lack of trust in the system security, such as data collection, analysis, and storage in a complex information system; lack of transparency; and legal compliance difficulties. Most dangerous of all, however, is the risk of vote manipulation.



E-voting is not only a question of digital efficiency and risk management but covers a spectrum of disciplines. As well as technological fields such as ICT infrastructure, cryptography, systems analysis and security, it is also a matter of law, economics, history, sociology, and ethics.

Buying, selling, manipulating: the risks of holding an election

To understand the risks and vulnerabilities of an e-voting election, we need to understand the high-risk environment of polling. Frauds are a significant risk in the history of paper ballots. The reliability of election results also can be damaged by the arbitrary denial of voting rights, coercion of voters, voting secrecy breaches, the possibility of voting modification, bribes, and vote-buying. All these problems are ethical matters, and they illustrate how human behaviour is an uncontrollable part of elections. A human interacts to an election system as a user, voter, politician, press, technology and software developer, and e-voting technologies companies, among many others. An electronic voting system must address all these risks and vulnerabilities; technology alone cannot cover all of them. Electronic voting must work within a robust ethical and legal framework, with civil, criminal, and public law involvement in every step of the process.

Trade-offs – The CIA triangle and critical voting rights

An election needs to safeguard three critical rights. Many experts, however, doubt whether an e-voting system can ever be secure; because these rights cannot comply with the fundamental security principles of the CIA triangle: Confidentiality, Integrity, and Availability.

1. **Confidentiality**
   a. **Ballot secrecy (vote privacy):** The election system should safeguard the voter in two distinct ways: no one can detect how a person voted, and individuals cannot reveal their votes. Information leaks facilitate the vote "trading" and coercion, a significant historical problem in elections across the world.
   b. **Voter authentication:** only authorised voters can vote once. If a system allows casting multiple votes, fraud occurs. Similarly, discouraging authorised voters or manipulating them to vote differently is a powerful attack. Suffrage, the right to vote, is often a hard-earned civil right and is a core democratic value in many societies. Manipulation is distinct from legitimate political campaigning and debate.

2. **Integrity:** the winner is the candidate with the most votes. An election system should avoid frauds in two areas: votes being cast as voters intend, and all votes cast being accurately counted.

3. **Availability:** the system must accept votes on schedule during Election Day and produce results on time. Attacks on availability can occur when a threat attempts to stop the system.

Most concerns with an e-election focus on protecting its integrity and confidentiality (privacy or ballot secrecy) against systems attacks. There is no one way to balance all voter rights and security principles. Although e-voting probably never will be completely safe from manipulation or unlawful action, many e-voting systems have a unique combination of security and privacy challenges to face the inevitable trade-offs.

Rather than considering the security of individual parts of the system, the only way to secure an election system is to consider security requirements in a holistic, end-to-end manner. Failing in breaking it down into individual pieces can result in missing attacks. Standards and procedures should address more than security. Security, accuracy, accessibility, usability and transparency are all critically essential features to address.

Brazil – a study of an e-voting pioneer

In 2000, Brazil became the first country in the world to hold fully electronic elections. Its pioneering elections are a worldwide reference due to its importance as one of the largest countries, economies and democracies in the world. The Brazilian electronic system is considered state-of-the-art, with results announced in a few hours.

Several risk management and measures are in place to reduce the risks of its complex e-voting system. Brazil applies more than 30 barriers of defence to minimise the attacks to the software, hardware, networks, and data. Technological mechanisms are applied. Information protection utilises cryptography, hashing and PKI; access control mechanism uses biometrics, while a VPN protects networks. These techniques are minimum requirements for a safe e-voting system because they minimise vulnerabilities on the data confidentiality, integrity, and availability. Well-defined processes and an extensive risk management plans are in place to manage people and processes. To minimise vulnerabilities, the system has constant updates with new technologies and information security plans. However, after 24 years of e-voting, many questions are raised about the system security and vulnerabilities which may not comply with the risks management and information security framework.

Considerations and my contribution to the research field

I presented an extended e-voting research case while studying towards a Master's Degree in Information Systems at the University of Canterbury. It was one assessment for Information Systems Security and Risk Management course (2018). At the time, Brazil was holding its general elections. People were discussing their votes and debating their preferred politicians. Observing social media, I had the idea of applying the knowledge gained in my classes to the reality unfolding before my eyes. I was concerned about people of my circle sharing "fake news" and destroying personal relationships because of the elections. I realised that some "fake news" manipulated its audience by raising doubts about e-voting security, contributing to misinformation and political instability.

An unprecedented ethical and data privacy scandal occurred when social media giants Facebook and WhatsApp were accused of commercialising and mass delivering fake news packages with false rumours, manipulated photos, decontextualised videos, and audio hoaxes. These revelations became campaign ammunition, going viral on the platform with no possibility of monitoring their origin or reach because of WhatsApp's end-to-end encryption. The justice system asked the companies' executives to inform who paid for the information misuse. The Election Court, however, was confused about the new attack methods and took a long time to react towards minimising the damage to the e-voting system credibility. There was no legislation in place to regulate this new environment – analogue laws were attempting to regulate a digital world.

Continued on next page…

Novel ways of attacking the historic elections vulnerabilities

I conclude that what happened is a new way of interference on the elections because:

a. "Fake news" manipulated and affected the ballot integrity and authentication.
b. We can assume that new methods for manipulating voters and buying votes have emerged. Digital technologies mean that voter fraud and manipulation can reach far more voters at once.
c. Social media has hurt the authentication and ballot secrecy principles, with the broad public publishing their vote intention or whom they voted.

After almost two years, the international community still talks about the latest Brazilian elections. In this discourse, unprecedented social media contribution to election "attacks", suggesting that the outcomes put the country's democracy at risk.

Ethics precedes technology in importance, and they seem to hold back the development of e-voting systems because elections are social phenomena that replicate human behaviour. Political power and democracy depend on the trust of voters to achieve electoral legitimacy. The election system must therefore avoid the risks of antisocial conduct and threats that corrupt the process, instead promoting the full exercise of citizenship. This only can be achieved with widespread education and awareness on voting risks and vulnerabilities.

References

- Boadle, A. (2018, October 20). Facebook's WhatsApp flooded with fake news in Brazil election. https://www.reuters.com/article/us-brazil-election-whatsapp-explainer/facebooks-whatsapp-flooded-with-fake-news-in-brazil-election-idUSKCN1MU0UP

- Gerlach, J., & Gasser, U. (2009). Three Case Studies from Switzerland: E-Voting [PDF]. The Berkman Center of Internet & Society at Harvard University.

- Halderman, JA., et al. (2008) "You Go to Elections with the Voting System You Have: Stop-Gap Mitigations for Deployed Voting Systems."

- LAUDON, KENNETH C., & LAUDON, JANE P. (2019). MANAGEMENT INFORMATION SYSTEMS: Managing the digital firm. S.l.: PEARSON.

- Magenta, M., Gragnani, J., & Souza, F. (2018). How WhatsApp is being abused in Brazil's elections. https://www.bbc.com/news/technology-45956557

- Pfaffenberger, B. (2013). Broken Ballots: Will your votes count? By Douglas W. Jones and Barbara Simons (review). Technology and Culture, 54(4), 1001-1003. DOI:10.1353/tech.2013.0132

- The Economist (2018). Brazil's voters worry about the integrity of their elections https://www.economist.com/the-americas/2018/10/05/brazils-voters-worry-about-the-integrity-of-their-elections

- Whitman, M. E., & Mattord, H. J. (2016). Principles of information security (5th ed.). Australia: Delmar.

- World International IDEA (2020). Is e-voting currently used in any elections with EMB participation? https://www.idea.int/data-tools/world-view/61

CYBELE SOUZA

Cybele Souza is an economist, accountant, and senior business analyst with over 15 years' experience in the financial and business field. She brings a unique blend of expertise across diverse areas, with experience in auditing and consulting projects in the USA, New Zealand, and Brazil. During her career, she has worked in a variety of industries and organisations, including PwC, Richemont International, Kathmandu, Broadspectrum, and the New Zealand Government.

Cybele lives permanently in New Zealand, and it is about to complete her Master's Degree in Information Systems. She has researched systems' post-implementation issues, digital business, e-commerce and e-government, end-to-end processes, and Lean Six Sigma wastes, with an emphasis on the public sector systems.

She likes to say that technology and human factor walk together hand in hand, because people are the main component of any information system - although it is often overlooked.

Cybele's LinkedIn profile is available here. Her email address is available via the member's area of the RiskNZ website (select Members Area | Member Profiles and search for Cybele)

SAI GLOBAL - RESOURCES

To quote our sponsor SAI Global *"We are all facing new and unprecedented challenges with the rapidly evolving COVID-19 Coronavirus pandemic making its impact around the world"*.

SAI Global provides resources that are available on its website.

SAI Global's Pandemic Information Center provides resources, tools and expert business resilience strategies: https://www.saiglobal.com/risk/insights/pandemic-information-center

Paul John's of SAI Global notes that *"This is a challenging time for leaders. We're faced with a global pandemic on a scale rarely seen before, with far-reaching impact on our modern digital economy.*

We don't know how to accurately model this COVID-19 health crisis and we don't know how and when the world will spring back from it. The Risk Arc serves as a blueprint in a world where there are so many unknowns".

"Companies that lay out a robust path forward will transform the culture of their business from a state of anxious paralysis to one that allows for informed and engaged employees to help propel the business forward. It's the rigor of the Risk Arc and the strategy of the journey that gives leaders the space to be human and companies the time to implement changes that will make them truly more resilient."

Read Paul's commentary on the SAI Global Covid-19 Risk Arc here:

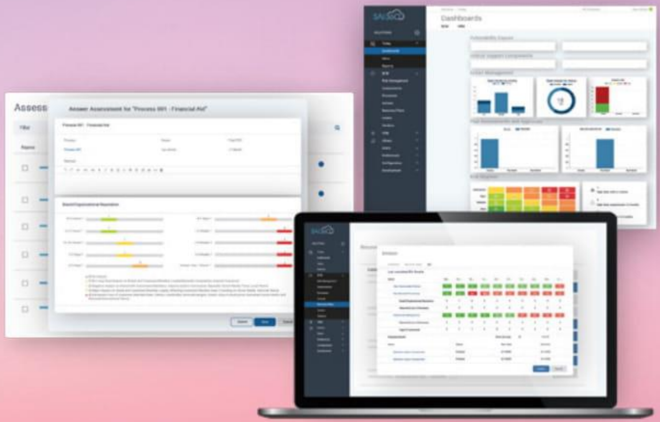
https://www.saiglobal.com/hub/covid-19-business-resilience-blog/the-risk-arc-a-pathway-to-recovery

A CONFERENCE IN 2020?

The business uncertainties surrounding Covid-19 have affected our plans for a 2020 Conference, and the 2020 Awards of Excellence. When the situation becomes clearer, a decision can be made whether to re-schedule the conference later in the year, or postpone it to 2021.

The Board will follow Government guidance on meetings and gatherings and consider the willingness of members and speakers to travel.

In the meantime, lunchtime seminars are being delivered by Zoom webinar and we have had excellent feedback from this initiative. Webinar recordings and key resources can be found on the members area of the RiskNZ website. Learning Group materials can be found under the menu option Member Resources | Presentations and Lunchtime seminars under Member Resources | Lunchtime Seminars.


Assess
Answer Assessment for "Process 001 - Financial Aid"
Dashboards
SAI360

THE 2020 RISKNZ BOARD ELECTIONS

RISKNZ's new Constitution was adopted at the 2019 Annual General Meeting. The new Constitution supports electronic voting and the 2020 elections procedure was radically re-designed to support both candidate nomination and electronic voting.

Of the 199 members eligible to vote in the 2020 RiskNZ Board Elections around 38% cast their votes.

The RiskNZ team would like to congratulate the successful candidates of the election process and the incoming members of the RiskNZ Board:

- Lynda McCalman
- Imogen Perez
- Katie Phillips
- Duncan Stuart
- Brent Sutton
- Gary Taylor

They join RiskNZ's returning board members:

- Kristin Hoskin
- Stephen Hunt
- David Turner
- Jane Rollin

RiskNZ would like to thank all of the voting members who cast their votes during this election.

In April 2020 Vaibhav Bhatnagar became a co-opted member of the RiskNZ Board.

Information about the RiskNZ Board members, including brief biographies, is available on the RiskNZ website under the menu option **About | RiskNZ Team and Board**

The new Constitution can be found under the website menu option **About | Key Documents**

For any specific questions related to the RiskNZ Board, please get in touch with RiskNZ Board Secretary Katie Phillips at secretary@risknz.org.nz

RISKNZ

THE 2020 AGM – Tuesday 30 June

The RiskNZ Annual General Meeting for 2020 will be held on Tuesday 30 June.

At this stage, in light of the Covid-19 situation, the Annual General Meeting will be delivered by webinar.

We will of course continue to review this approach in line with changing Government guidelines, and will confirm details closer to the time.

The Annual report for 2019-20, and the Business plan for 2020-21 will be distributed with the AGM documents.

FROM THE DEPUTY CHAIR – DAVID TURNER

Firstly, I would like to thank Sally for her tireless efforts as Deputy Chair and acting Board Secretary during the past 15 months, and her guidance when I first joined RiskNZ around how RiskNZ worked, its history, and the potential for RiskNZ to create value for our members into the future.

Sally has always provided a very high level of structure and thought leadership for RISKNZ, and this has been reflected in the many positive decisions we have been able to reach, which keep driving RiskNZ forward.

This edition of RiskPost has required a great deal of effort because of the turbulent time we have all experienced over the past few months. However, the Risk Post team led by Sally has produced a great edition which has a focus on the future. As Risk Post evolves we would like to build on the valuable content from our contributors, and continue to provide a high level of thought leadership for members.

A big thank you to Sally and we all wish her the very best for her future endeavours. I hope she is always around for a catch up!

Moving forward:

We anticipate a productive year ahead with our new Board members now in place; they bring a high level of skill and talent to really help us move positively toward 2021.

The Board has taken time to reflect on what has worked well, and what we can do better, to achieve our goals. This included looking closely at the annual plan to see how we can consistently reach needed objectives and outcomes.

To reflect this thinking, two new work streams that provide further focus on risk management and project management have been included within our 2020/2021 annual plan.

These new workstreams will assist the RiskNZ Board to better manage and monitor the work we have underway, and help to grow the footprint of RiskNZ as we move forward. This will enable the Board to focus more time and attention on providing value to our member base, become more of a thought leader in risk management, and capture greater interest and support from sponsors and various Government and private platforms within NZ.

All in all, it looks like an exciting and interesting time ahead, and I wish you all the best for the second half of the year.

Thank you!

DAVID TURNER

RISKNZ

RISKNZ INFORMATION

THE MANAGEMENT BOARD AND OFFICERS OF RISKNZ

Chair:	Stephen Hunt	Deputy Chair:	David Turner
Secretary:	Katie Phillips	Executive Officer:	Sathya Ashok
Treasurer:	Gary Taylor	Administration Officer:	Virtual Assistants Ltd

Management Board Members:

Brent Sutton
Duncan Stuart
Imogen Perez
Jane Rollin
Kristin Hoskin
Lynda McCalman
Vaibhav Bhatnagar

INFORMATION FOR CONTRIBUTORS

Work on Edition 2 of RiskPost 2020 will start after the AGM, which is scheduled for 30 June.

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. A reminder will be issued in early July.

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.

RISKNZ WELCOMES NEW MEMBERS

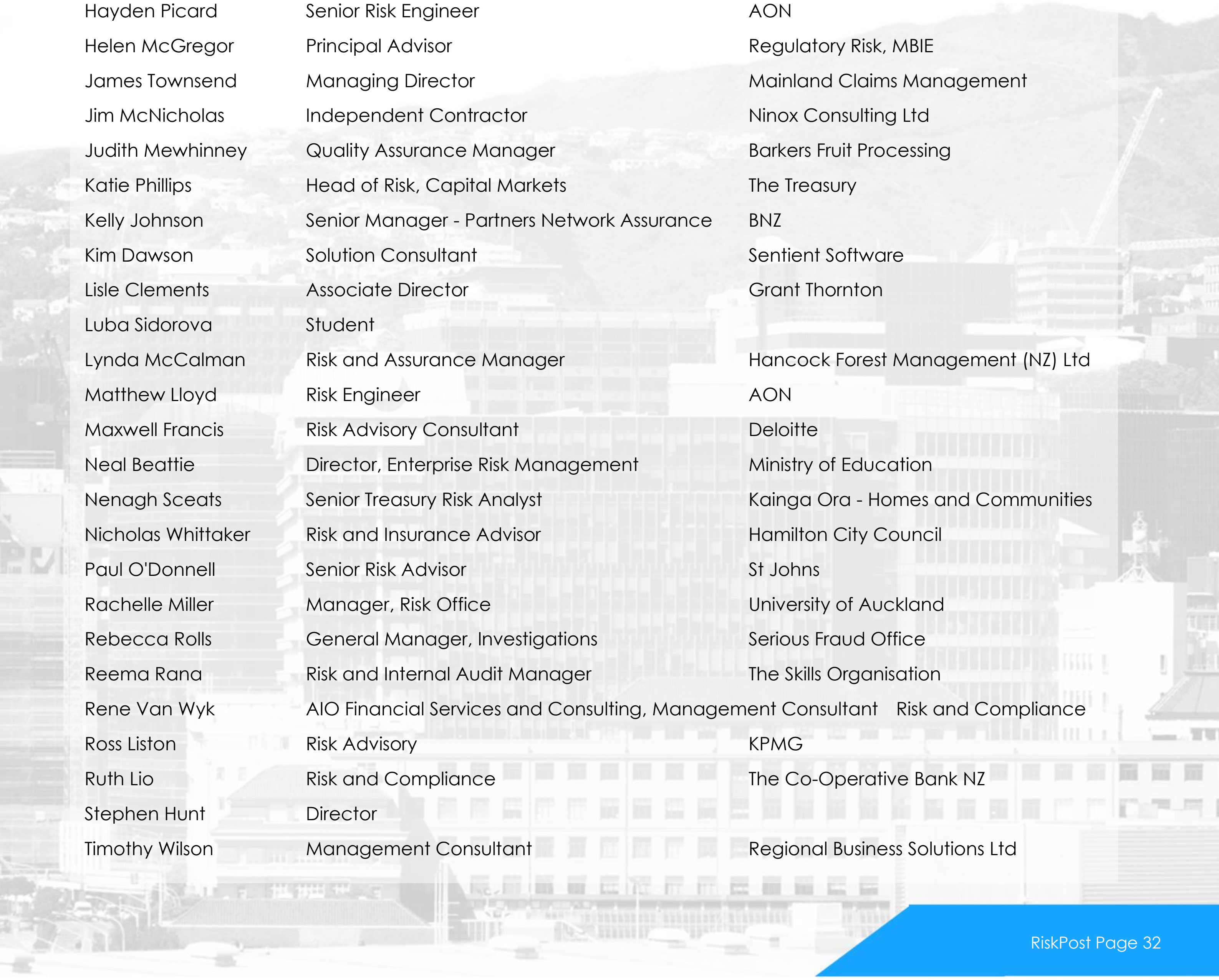
RiskNZ welcomes the following new Members

Corporate Members:

- Medical Council
- Partners Life
- Gisborne District Council
- Te Puni Kokiri
- Datacom
- Department of Conservation
- Avanti Finance

Due to the large numbers of new members please find these on the following page.

RISK NZ WELCOMES NEW INDIVIDUAL MEMBERS



Adam Hampson	Senior Risk Advisor	Ports of Auckland
Andrew Scuffham	Senior Advisor Planning and Risk	Maritime New Zealand
Balajee Narasimhan	Operational and Compliance Risk Manager	Westpac
Cameron Winsor	Operations Manager	Plumbcraft Ltd
Dan Mettham	Country Manager	Oncore Services
David Schoeman	Risk Advisor	Regional Facilities Auckland
Deidre Hemera	Chief Risk Officer	Northland Polytechnic
Duncan Stuart	Manager Risk Reporting and Operations	MBIE
Ed Rafferty	Principal Consultant	Inception Consulting Ltd
Elaine Lorive	Risk and Compliance Manager	Worldfront Inc
Erica Miles	Director	Rutherford Rede
Fallon Howe	Paraplanneer	Rutherford Rede
Fiona Watts	Risk and Compliance Manager	Cigna
Hayden Picard	Senior Risk Engineer	AON
Helen McGregor	Principal Advisor	Regulatory Risk, MBIE
James Townsend	Managing Director	Mainland Claims Management
Jim McNicholas	Independent Contractor	Ninox Consulting Ltd
Judith Mewhinney	Quality Assurance Manager	Barkers Fruit Processing
Katie Phillips	Head of Risk, Capital Markets	The Treasury
Kelly Johnson	Senior Manager - Partners Network Assurance	BNZ
Kim Dawson	Solution Consultant	Sentient Software
Lisle Clements	Associate Director	Grant Thornton
Luba Sidorova	Student	
Lynda McCalman	Risk and Assurance Manager	Hancock Forest Management (NZ) Ltd
Matthew Lloyd	Risk Engineer	AON
Maxwell Francis	Risk Advisory Consultant	Deloitte
Neal Beattie	Director, Enterprise Risk Management	Ministry of Education
Nenagh Sceats	Senior Treasury Risk Analyst	Kainga Ora - Homes and Communities
Nicholas Whittaker	Risk and Insurance Advisor	Hamilton City Council
Paul O'Donnell	Senior Risk Advisor	St Johns
Rachelle Miller	Manager, Risk Office	University of Auckland
Rebecca Rolls	General Manager, Investigations	Serious Fraud Office
Reema Rana	Risk and Internal Audit Manager	The Skills Organisation
Rene Van Wyk	AIO Financial Services and Consulting, Management Consultant	Risk and Compliance
Ross Liston	Risk Advisory	KPMG
Ruth Lio	Risk and Compliance	The Co-Operative Bank NZ
Stephen Hunt	Director	
Timothy Wilson	Management Consultant	Regional Business Solutions Ltd