Risk Management

In pursuit of value

Repeat after me: 'Risk is not about compliance!'

July 2019

Written by
Bryan Whitefield

BRYAN WHITEFIELD

Introduction

Every function within an organisation is expected to deliver value, including the risk function.

You will know the risk function is delivering value when the bad surprises in your organisation are poor luck, not poor judgement. The result will be your organisation achieving its goals 20% faster due to 80% less rework.

This paper is part exposé of the failings of the risk management function, part unveiling the elephant in the room that has caused risk management functions to fail to deliver and part crystal ball with a description of how risk management will add value for organisations through increasingly complex times. Complexity in an era that will take human progress on a trajectory never seen before (see image below).

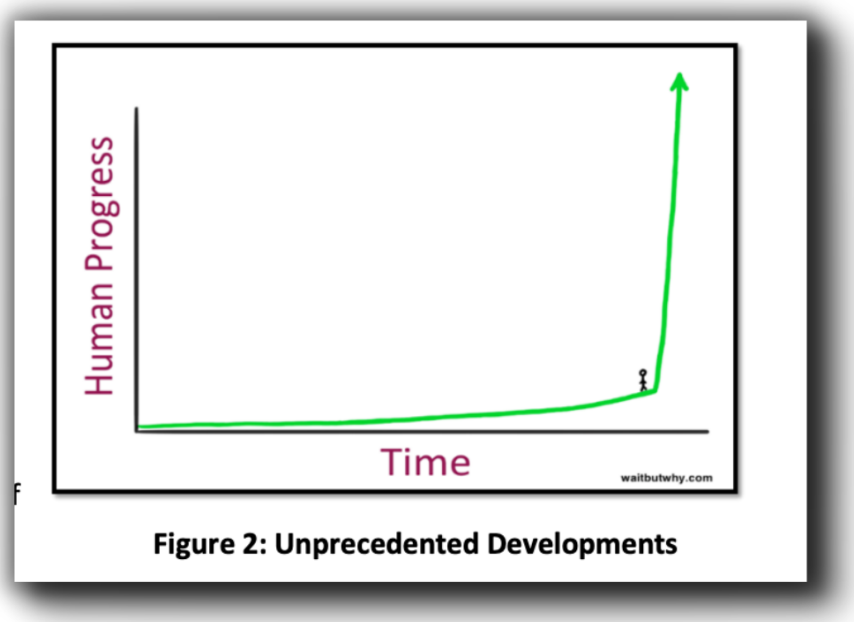


Figure 2: Unprecedented Developments

If you are a senior leader in your organisation who cares about extracting real value from every function in your organisation, read on. Get ready to help the risk function to shift and build on the foundations already in place.

If you are a risk leader in your organisation, read on. I assure you I will help you look at some of your challenges and opportunities in a new light.

If you are a team member in a risk team, read on. Then please share this with your team so we can all get on with delivering more value!

What value has the risk function delivered?

Risk functions the world over have delivered value by helping decision makers to make sense of and manage uncertainty. In some organisations I have had the pleasure to work with, the risk function has delivered value far, far exceeding the investment. However, unfortunately that is not the norm. I can easily conjure a picture in my mind of a few higher profile risk professionals in large corporates who talked a good risk game, yet their organisations unravelled in whole or in part.

The most striking example of the failure of the risk management function to influence the decision making of key leaders is in the finance sector, globally.

Now remember, the first national standard on risk management was jointly published by Australia and New Zealand in 1995 and the first international version of the standard was published in 2009. Over the past decade or so we have had the GFC (Global Financial Crisis) with US$342 billion in fines of global banks that helped wipe out US$850 billion in profits. Many blamed the "risk management models", by inference the risk function. You and I know the risk function was not to blame. Nevertheless, the risk function was not effective.

And the fines continue. Quinlan and Associates estimate fines will top US$400 billion by 2020[1]. These are new fines unrelated to the GFC for abhorrent behaviour such as prejudicial treatment of small customers.

But it gets worse.

In part because of the GFC the banking sector has this type of "investment" in risk and compliance going on. The ANZ Bank reached in excess of $60M FTE on risk and compliance staff. The CBA reached numbers in excess of 3,000 risk and compliance staff globally.

Most recently in Australia we have the APRA report into the governance, culture and accountability at the CBA and the Financial Services Royal Commission.

The Royal Commission was compelling viewing. Counsel Assisting, Rowena Orr, was brilliant in the way she had witnesses squirming as they confirmed criminal breach after criminal breach. She extracted stories of the treatment of customers that looked to many observers as nothing short of contempt.

Some real insight into the state of risk management comes from the report into the CBA. Try these quotes from the report on for size:

"The risk function has had an uneven (that is, an inconsistent and sometimes weak) influence across CBA. This has been partly driven by the natural organisational divide between business units that generate revenues and support functions."

"In some areas, the risk function was perceived more as an inhibitor than a necessary partner."

"The risk function was also described as focusing on policy writing and correctness of frameworks over implementation and engagement with the business."

1 Quinlan and Associates "Value at Risk"
- https://www.quinlanandassociates.com/wp-content/uploads/2017/09/Quinlan_Associates-Value-At-Risk.pdf

Ouch!

There we have it. The risk function of several thousand people in the CBA – "A toothless tiger". And the result? At the time of writing the CBA had made provisions in excess of $1.4bn for fines and compliance costs related to pre and post Royal Commission revelations.[2]

Enough of picking on the finance sector, the Royal Commission and the APRA report are enough, what about outside the finance sector?

Let's start with Ardent Leisure and the Dreamworld amusement park accident that killed four tourists. While the coroner's report was pending at the time of writing, the press acting as jury had already reached their verdict with commentary like "Dreamworld staff admitted there had been a 'total failure' to identify risks with the ride and a series of equipment failures before the accident should have raised red flags.[3]" Since the accident in October 2016, the share price has fallen 57%. While there will be many factors contributing to this fall, don't underestimate the impact of a coronial inquiry on a management team's ability to perform.

Then there is BHP Billiton. The 2015 Mariana dam collapse in Brazil killed 19, caused severe environmental damage along the Rio Doce River all the way to the Atlantic Ocean 650km away and affected drinking water for hundreds of thousands of people.[4] The share price dropped 44% in less than three months. Interestingly, BHP's share price has bounced back and is higher now than before the event. More on that later.

Why risk management is failing in organisations

There are many reasons that risk management is not strong and prevalent across the business landscape. The oldest and most entrenched reason is because of the perceptions of risk management as something negative. That risk management is a handbrake on business, or a wet blanket taking any of the fun out of it. In fact, in my early days in risk in the late 1990s and early 2000s, I felt that when I walked into a room for a risk workshop for a new client, most in the room stared at me as if I was Dracula "Coming to suck your blood".

Many risk functions have failed to convince senior leaders that we can add value beyond compliance

2 https://www.abc.net.au/news/2018-12-12/cba-costs-rise-by-another-335-million/10608818
3 https://www.theguardian.com/australia-news/2018/dec/07/dreamworld-reputation-in-tatters-as-inquest-wraps-up
4 BHP Billiton 'woefully negligent' over Brazil dam collapse: BBC News 2019 05 07

We now have nicknames across the profession like the “Fun Police” and “Business Prevention Officers”.

Why has this perception persisted?

In part it is because of the professional disciplines that picked up the risk management mantra. In the industrial space it was the engineers who are traditionally both technical and have a need for accuracy. This can lead to confusing technical terms and even more confusing equations. The need for accuracy can slow things down. The result – staff and entrepreneurial managers could not relate. All they saw and heard was complexity and gobbledygook. On reflection, being an engineer, I was part of this problem.

In the finance and many other sectors, it has been the audit firms who have led the way. The urge for improved governance, including risk management, came through audit committees. The result has been, to a large extent, an audit mindset about risk. That risk management is about mitigating risk rather than harnessing uncertainty to take calculated risks. The result – staff and pretty much every other manager outside of audit and finance thought risk is about compliance and that audit need to hassle you to assure others that risk was being managed. The mindset – tick the box!

Combined we now have this situation

Recently I was working with the CFO of a 10,000-person organisation who had finance, strategy, performance management and risk all reporting to him. He commented: “Of all the different disciplines that have reported to me over the years, risk is the most difficult. It seems so complicated and inflexible all at once.”

That’s right, we once had a simple process used through evolution for challenges as simple as whether to “fight or flight”. As we evolved, we used it for decisions like when to cross the road safely and finally when to invest or divest, hire or fire, insource or outsource. A process that is designed to help us handle the uncertainty created by complexity. And made it complex. The result - boards the world over had risk registers reported to them containing 400 risks. The reporters were looking for a pat on the back. Board members looked at the list and asked, “So what does it all mean?”

Not only did the profession make risk complex, we created our own language. Risk Speak. We even put “risk” in front of or after perfectly normal words like conduct, appetite and reputation.

We are victims of our own expertise. We haven’t managed our own risk and we have failed to be relevant and valuable.

We then set about creating a whole new world around it and separated it out from the world of business.

Hilariously (NOT) we are victims of the irony of our own expertise. We have been busy telling people how to manage their risk while not managing our own. We are not sufficiently relevant to the businesses we serve to be truly valuable.

In which decade is your organisation operating?

As I mentioned, the first national standard on risk management was published in 1995. In it was a diagram showing the risk management process. Interestingly the only significant difference between that diagram and the one in the current ISO standard was that it did not have the Communicate and Consult box. That's right. The risk profession knew the beauty of risk management. All that was needed was to put it into a standard, publish it, and the rest of the world would applaud and get on with following the process.

Due to our aforementioned mistakes, risk management did not catch on like it was hoped. Since 1995, each decade has ended with a different risk theme (see Figure 1). Let me help you relive them or perhaps describe your organisation right now!

Figure 1
Risk Leadership through the Decades

1990s - The decade of training

In the 1990s as we introduced the risk management standard to organisations across Australia and New Zealand in a nicely complicated way, the most common response from non-risk people was, "Managing risk is something I do every day. Why do I need to go through this process?" The result, the risk process became a compliance activity and the culture of tick and flick was born.

Worse still, a serious injury to organisations was imposed. One that most organisations have never recovered from. The responsibility for the risk function was pushed well down in organisations. Rather than a senior executive taking full ownership, someone was found with time on their hands or who had an interest in the topic.

So, what did organisations do to be seen to be doing something? Training of course. The attitude that prevailed from senior management was "Well of course our people should be trained to manage risk. After all that is what I do every day and it is how I got where I am. But please don't bother me with the training and keep all your risk registers to yourself, thanks very much."

While the training worked for some, for most it failed to shift attitudes.

2000s - The decade of assuring

Following major corporate debacles like Barings Bank in the UK, in the 1990s came Enron and Worldcom in the US, FlowTex in Germany, Parmalat in France and HIH Insurance and OneTel in Australia early in the 2000s. Then we had the GFC around 2008. As the “naughties” grew to a close, boards and their stakeholders were demanding better management of risk. Better all-round governance in fact.

The hope of the risk profession was that now organisations would take risk and its related governance disciplines seriously as it was an obvious antidote to the problems that marked the decade.

Not to be. The interpretation of business was that risk was important because the board, and specifically the board Audit Committee wanted assurance that risk was being managed well. That is, "we have to do this risk stuff for the comfort of others. Not because it adds value to what I do."

Because the Head of Audit was the most trusted adviser to the Audit Committee, more often than not the Audit team were given the risk management function as their responsibility and the Audit Committee became the Audit and Risk Committee. Despite cries from others that it created a conflict. And their go-to for ideas and resources were of course audit firms. Yet more potential conflict of interest to be managed.

As the 2000s closed the assurance industry boomed. That’s right. The assurance industry. The industry of getting an audit firm to have a look at the risk process and various areas of compliance to provide assurance to the board that all was well.

The result was a culture of “be prepared” as the auditors are coming. The attitude that the only reason this “stuff” needs to be done is to placate the auditors who need to placate the Audit and Risk Committee. The whole shebang resulted in a lot more red tape.

2020s - The decade of influence

What of the next decade? We will need the kind of leadership that will ensure organisations are led through the complex maze of the 2020s. And that means a culture where everyone leans in and takes accountability for risk. Not hold up their hands in surrender and say, “It is complex, it is hard. Same for our competitors.”

We will need leaders aware of unconscious bias in their decision making and that of others. Leaders who will put in place the mechanisms to manage their own bias and to challenge those leaders that don’t.

We will need leaders who instil a strong values-based culture in organisations. Those who refuse to put short-term profit over sustainable outcomes. And who are willing to challenge those leaders that do. Those same leaders will need to stand up to financial analysts that drive this type of behaviour from leaders in publicly traded companies. And they will need to learn to do so in very compelling ways.

We will need leaders who will take on the challenge of leading through complexity and look to blend their business acumen with scientific method and creative thinking to deliver the future they wish to create.

And that means we in the risk profession need to convince leaders of organisations to hold themselves accountable to the values of the organisation, to recognise and manage their unconscious bias, to think long-term as well as short and to add to their already considerable business acumen. And we need to convince them we can help.

We need to ensure organisations are led through the complex maze of the 2020s. For the risk function it means the decade of influence.

How are we going to achieve Risk Leadership 2020s style?

By changing the risk profession so it becomes markedly more valuable and hence influential at board and executive level. So it becomes desirable. So we are sought after, not avoided.

It is what the profession has wanted for decades. It won't happen if the profession does not change. As Barrack Obama said about the US Policy on Cuba, "We can do what we have been doing for decades and achieve the same result. Or we can try a new approach."

And the time is now! Opportunities abound. Every time a major catastrophe occurs in an organisation, risk management gets some airplay. Following the Financial Sector Royal Commission here in Australia, the Boards and Executives of APRA regulated entities are sitting up and taking notice. Most, if not all the major banks have risk transformation or risk optimisation projects in play.

The same with non-finance sector organisations who have faced catastrophe. Take BHP Billiton. After the 2015 Mariana dam collapse a risk transformation project was born. And as I pointed out earlier, while there will be many, many factors attributable to BHP's success in recent years, one must consider the value that the risk function delivered over that period. While industry awards don't provide certainty, they certainly should provide sound indications. And which company did the RMIA Risk Manager of the Year 2018 come from? BHP Billiton.

There should be no doubt in anyone's mind that risk management as a discipline has an excellent opportunity right now to make its mark. Boards and senior executives across industry are genuinely wanting risk to be managed better than it has in the past.

What needs to change?

The international standard on risk management, ISO 31000, tells us what risk should look like in an organisation and includes some nice words on how it should be implemented. Including the need for engagement and awareness.

Unfortunately for us risk professionals, the damage has been done and the challenge of engaging management and staff is as difficult as ever. The risk profession must provide a better product for the businesses served and must convince them that "This time, it's different." That is, it's time to cut the crap and get to the essence of improving decision making across organisations. Time to move from red tape to blue ribbon.

It is up to the risk profession. Not business leaders. It is time for the risk profession to break out of the mire where risk is seen as a compliance function. And that means the Three Lines of Defence model of risk management either needs to be replaced OR needs to be changed to address its key deficiencies.

Why the Three Lines of Defense model gained favour?

In the Three Lines of Defence (3LoD) risk management model, the business are the owners of risk and are the first line of defence. That is, they are responsible for getting their decisions right. The risk and compliance functions are the 2nd line of defence. Their job is to support, challenge and provide a level of oversight of decision making by the business. And the third line is audit with the role of assuring senior management and, more importantly, the board that risk is being managed well.

At the surface, the 3LoD model makes sense. It is sort of like the thinking you do when you decide to have a Plan B, a back-up plan. People will often naturally choose to have a back-up plan in case Plan A falls through.

By having a "2nd line" of defence, you have a back-up when it comes to helping business leaders make decisions. We all have blind spots to clear thinking and

having the second line question your thinking should, if done well, lead to better decisions. The "3rd line" assurance function is more than a Plan C. While the 2nd line should be involved proactively at the time of decision making, the role of the 3rd line is to assess the results. That is, did the combined efforts of the business and their risk advisers result in a good or at least a satisfactory outcome? And if not, why not? After all, it is not necessarily the fault of a failed risk process. Some things are much more difficult to foresee. While risk management may reduce the likelihood of something adverse happening, it seldom eliminates it. Risk management makes the achievement of objectives more likely, not certain.

On the surface the 3LoD makes sense. Looking at the finance sector, it is no wonder regulators such as APRA grabbed 3LoD with both hands and essentially mandated it for the organisations they regulate.

The problems associated with 3LoD

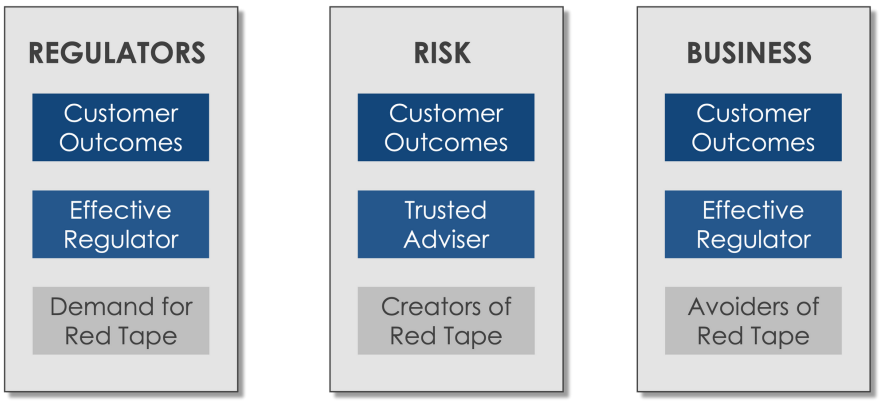
Problem 1

The 3LoD model creates red tape. Look at the Industry Dynamics diagram (see Figure 2). You can see that for all three players, the regulators, the risk function and the business itself, they all want the same thing. They want good customer outcomes.[5] That is where the similarities end.

What do regulators want? They want to be an effective regulator. They don't want organisations failing on their watch (APRA) and they don't want poor behaviour by organisations they regulate resulting in a Royal Commission (ASIC and APRA).

What does the risk function want? It wants to be heard and to become a trusted adviser to the business. My message to senior risk professionals is that unless you are one of the first people the boss calls when contemplating a big decision, you have plenty of room for improvement in your role.

Figure 2: Industry Dynamics



And the business? The leaders of the business want the organisation to be an industry leader. In the for-profit sector, that means great returns for shareholders in a financially and environmentally sustainable fashion while being socially responsible. In the not-for-profit and public sectors, it means impact while maintaining integrity with all key stakeholders. Whether that be through sound fiscal, ethical or any other area of management.

In order to achieve their goals, the regulator demands red tape. The risk and compliance functions duly answer the call and create red tape. And the business? Well they spend the rest of the time trying to avoid red tape. That is, to avoid processes they see as non-value adding.

The result? Refer to the section above on the extent of value creation by the risk function. Not good.

5 Albeit some business leaders allow short-term profit making to take precedence over customer outcomes as evidenced from enquiries into the financial sector.

Problem 2

The implementation of the 3LoD model in many organisations has resulted in the outsourcing of responsibility for managing risk from the business to the risk and compliance functions. Much the same way as organisations did with safety, environmental, IT security, business continuity, security and so many other related fields. Hire a specialist and tell them to make it all go away while the business gets on with business.

While the 3LoD model states that the 1st line (the business) owns the risk, 1st line risk positions were created. Why? To get all the red tape sorted so the business could get on with the business of business.

Sorry, but managing the uncertainty in your business is the business of business. It is why we have policies, processes and systems.

The challenge is to have blue ribbon approaches to risk and compliance that business leaders value and take ownership of.

Problem 3

The 3LoD model has a fundamental flaw that risk and compliance functions battle with every day. The language that surrounds it creates barriers between the business (first line) and both the risk and compliance functions (second line) and internal audit (third line).

While the business should be looking to risk, compliance and audit functions to support them to achieve their goals, their first introduction to the three lines of defence is through language that has negative connotations like defence, oversight, challenge, monitor and independent assurance.

No one goes looking for oversight. People only want to be challenged when they are proved right. People are happy to monitor what they want to monitor, not what is imposed on them. And, the business is traditionally wary of auditors and their role as assurers to audit and risk committees.

In short, the language and the way 3LoD has been implemented in most organisations makes it harder to be influential. It makes the risk function good cop and bad cop. It is a tough ask to be both and be a trusted adviser to the business.

The future of 3LoD

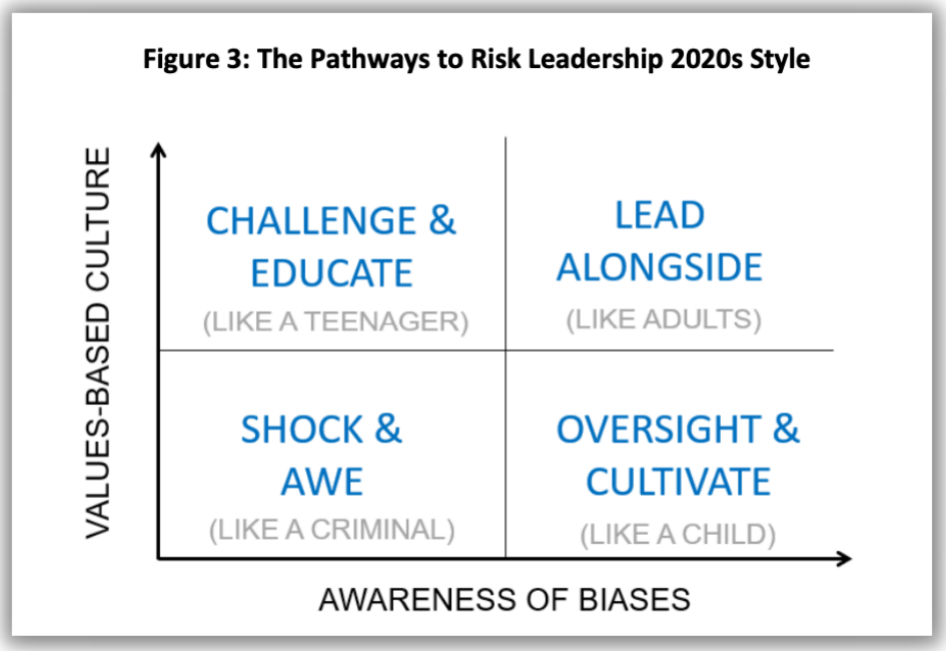
We must try something new. It is time to either ditch the Three Lines of Defence risk management model or change how we implement it. Plenty of successful organisations don't use 3LoD and get the job done with a small centre. A small group of trusted advisers.

Above all, the focus of whatever framework you implement needs to add value to the business. And that means a combination of strong analytical skills and the ability to cut through with your message. To cut through with your message to open the eyes of decision makers so it does not feel like you are challenging them or overseeing them. Remember, people only like to be challenged when they are proved right, and no one likes to be oversighted!

Shifting to Risk Leadership 2020s Style

Your influencing challenge of shifting to Risk Leadership 2020s style is shown in Figures 3 and is based on the extent leaders in your organisation ensure each decision holds true to organisational values and follows a process to manage unconscious bias. They key to excellence in decision making.

Figure 3: The Pathways to Risk Leadership 2020s Style



If your organisation has leaders that are consistently making decisions that do not hold true to your organisation's declared values and they lack awareness of their unconscious biases that affect their decision making, then your job is a tough one. Some shock and awe will be required. Hopefully shocks you can generate through strong analysis and your influence, not by waiting for organisational calamities.

A little easier is when your leaders for the main are aware of their unconscious biases but are letting themselves down by not living true to organisational values. Here the board or senior executive will need you to provide oversight by way of close support until you and they are able to cultivate a strong values-based culture. You must use your influencing skills to constantly remind leaders how their decisions align or fail to align with the organisation's values.

Similar but different is when your leaders are working to do their best to fulfil organisational purpose while holding true to the organisation's values but are lacking in their awareness of unconscious biases. Here the board or senior executive will need you to use your influencing skills to subtly challenge decisions where you see fit. More importantly your role is to educate them about bias.

Finally, once you have moved your organisation into a position where leaders are making decisions in full consideration of organisational values and they are aware of unconscious bias, then it is time to step to the side and lead alongside. And the secret to getting to into the top right of Figure 3 is to drop the language of challenge and oversight and start talking about values-based decision making and unconscious bias.

What you need to do next

Flipping risk from an oversight or challenge role to true leadership advisory role can't happen overnight in your organisation. First you need to choose you want it. Second you need to make it happen by taking on the following challenges:

Skilful Design

– Design your framework so it drives the right behaviours, ensures insights from the risk process using a range of analytical tools and is intertwined with standard business processes so it has a bare minimum of red tape. For help, check out the RMIA's Enterprise Risk Course.

Change Perceptions

– Develop a change management approach that will tackle entrenched perceptions and shift the conversation to values-based decision making and unconscious bias. This will require influencing skills of the highest order. For help, check out my Persuasive Adviser Program.

Ongoing Engagement

– Drive the program relentlessly but be patient. Some directors or executives who have completed a short course on risk as part of governance training will think they are experts. However, you need to keep your eye on the main game of values and bias awareness. Nurture executives and staff alike. And finally, get some help. Enlist a tribe of advocates. For help, read my Experts Need Advocates paper.

By the way, make sure you have the right people in place with the right support to make this happen. Beware of risk staff who have been indoctrinated into risk is a compliance function. It's not!

Got you thinking?

Drop me a line, I'd be interested in your views.

bryan@bryanwhitefield.com

About Bryan

Bryan is a management consultant operating since 2001. He is a specialist in risk-based decision making, strategic leadership and strategic planning born from his more than twenty years of facilitating executive and board workshops. Bryan's experience as a risk practitioner includes the design and implementation of risk management programs for more than 150 organisations across the public, private and not-for-profit sectors. Bryan is the author of **DECIDE: How to Manage the Risk in Your Decision Making**, a book for strategic leaders who wish to minimise the time taken to get to the right decision; **Persuasive Advising: How to Turn Red Tape into Blue Ribbon** that teaches you practical methods to cut through with your advice and make the impact you want to make; and **Risky Business: How Successful Organisations Embrace Uncertainty (#1 Amazon Best Seller)** that is a guide to the most successful way to design and embed an effective risk framework.

Bryan also authored the Australian Government's Risk Management Benchmarking Survey for more than 120 Government agencies from 2002-2005, lectured in the Principles of Risk Transfer in the Masters in Risk Management program of Monash University from 2002 – 2006 and designed and delivers the Risk Management Institute of Australasia's flagship Enterprise Risk course since 2019.

Bryan has assisted clients across all sectors including:

- Australian Government agencies such as the Departments of Foreign Affairs, Environment, Finance, Industry, Defence, Health and Social Services.
- State Government Agencies Fire and Rescue NSW, NSW Police, NSW Health local health districts, TAFE and the Victorian Department of Health and Human Services.
- Not-for-Profit organisations such as AWI, Cancer Council Australia, CBM, Cerebral Palsy Alliance, HCF, IRT, QSuper, Ronald McDonald House Charities, Uniting Care and Unitywater.
- Private Sector organisations such as Brisbane Airport, Brookfield Multiplex, Employers Mutual, FM Global, Downer, G&S, McConnell Dowell, Navitas, Pro Pac, QBE, Santos, Suncorp, Symbion, Weir Minerals and Xstrata.

Bryan was President and Chair of the Board of the Risk Management Institute of Australasia (RMIA) from 2013 through 2015, and is licensed by RMIA as a Certified Chief Risk Officer (CCRO).

Bryan is also a certified Virtual Presenter.

Bryan's **Consultant Profile** is attached. To hear first hand what Bryan's clients say about him, please check out this video.

www.bryanwhitefield.com
Bryan's LinkedIn Profile

Copyright

Disclaimer

This paper does not constitute the giving of advice. Please be sure to take specialist advice before taking on any of the ideas. This paper is general in nature and not meant to replace any specific advice. Risk Management Partners T/A Bryan Whitefield Consulting, its officers, employees and agents disclaim all and any liability to any persons whatsoever in respect of anything done by any person in reliance, whether in whole or in part, on this paper.