Risk Maturity

Delivering Value

Repeat after me:
'Risk is not a compliance function!'

Dec 2025

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 80% of goals 20% faster and 20% of goals 80% faster because of less rework and the elimination of big calamities unless luck is against you!

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 on how risk teams will increasingly deliver value.

Let's start with a little context. This diagram says it all! We are in an era that will take human progress on a trajectory never seen before (see image below) which means increasing complexity for leaders to navigate.

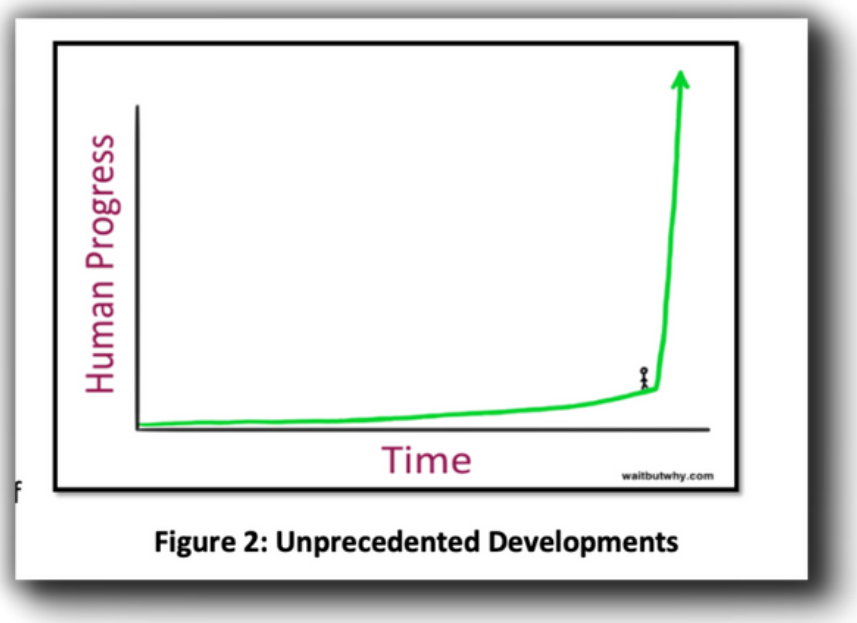


Figure 2: Unprecedented Developments

This paper is for:

Senior leaders: To help you get the support you need from the risk function to help you navigate complexity.

Risk leaders: To help you look at some of your challenges and opportunities in a new light.

Risk team members: To help you ensure your team delivers value!

What value has the risk function delivered?

Risk functions the world over have delivered value by helping decision makers make sense of and lead in uncertainty. In some organisations I have had the pleasure to work with, the risk function has delivered value far exceeding the investment.

Unfortunately, this is not the norm, and while some senior risk professionals talk a good risk game, their organisations have unraveled 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.

As you may know, the first national standard on risk management was jointly published by Australia and New Zealand in 1995 and the first international version was published in 2009, which followed the Global Financial Crisis (GFC). The GFC saw 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. And while you and I know the risk function was not to blame, it was not effective. The fines continue to this day for abhorrent behaviour by some in the sector and, for others, an inability to manage the complexity of their businesses.

Meanwhile, in Australia, 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 at the time came 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."

"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."

Ouch!

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

Let's start with Ardent Leisure and the Dreamworld amusement park accident that killed four tourists. The press acting as jury 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."[1] Following the accident in October 2016, the share price fell 57% and while many factors contributed 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.[2] The share price dropped 44% in less than three months.

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 the perceptions of risk management as compliance and a negative for business: That risk management is a handbrake on business, or a wet blanket taking any of the fun out of it. In fact, in the late 1990s and early 2000s, when I walked into a room for a risk workshop for a new client, many of the participants 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.

[1] https://www.theguardian.com/australia-news/2018/dec/07/dreamworld-reputation-in-tatters-as-inquest-wraps-up
[2] 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 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.

In the finance and many other sectors, it has been the audit firms that 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

I recently worked 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 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 we made it complex. The result: boards the world over had incomprehensible risk reports. The reporters were looking for a pat on the back. Board members looked underwhelmed 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.

Ironically, we are the victims 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 as 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 '90s, 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 many have never recovered from. The responsibility for the risk function was pushed well down in organisations. Now, instead of 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. And responsiblity for the risk function became further removed from senior management.

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

2000s - The decade of assuring

Following major corporate debacles in the '90s and early 2000s like the Barings Bank in the UK, Enron and Worldcom in the US, FlowTex in Germany, Parmalat in France, and HIH Insurance and OneTel in Australia, it was hardly surprising that boards and their stakeholders were demanding better management of risk. Better all-round governance, in fact.

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

This was 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, the Audit team were usually 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 and the attitude that the only reason this "risk stuff" needs to be done is to placate the auditors who need to placate the Audit and Risk Committee. And the whole shebang resulted in a lot more red tape.

2010s - Analytics to provide insight

As we exited the teenage years of the previous decade, risk management had made good headway in some organisations while others still languished in the 2000s, and some even in the 1990s' approach to risk.

Those that had strode ahead developed a forward-looking culture by using analytics to derive strong insights for decision making. Industries such as chemicals, finance, mining and retail have led the way. The chemical industry in particular, with the severe consequences of mismanaged complexity, has found more and more means of sophisticated risk modelling supported by a strong risk management culture. By embracing complexity, they have maintained their licence to operate and to achieve bigger and bigger goals.

The success of analytics is also highlighted by the finance sector. In Australia, for example, insurance companies are not as vulnerable to collapse as they were in the days of HIH. Under heavy pressure from the regulator, the industry gained more insight into the risk profile of certain products and industry sectors using concepts such as stress testing and scenario analysis.

However, analytics alone does not guarantee success. With the growth of AI and machine learning, analytics is being used to gain insight into the culture of organisations. As an example, organisations can now analyse staff emails to detect inappropriate behaviour. However, it's one thing to do the analysis, its quite another to change behaviours, as evidenced by the Financial Services Royal Commission.

2020s - The decade of influence

This decade we need the kind of leadership that helps organisations navigate complexity. 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."

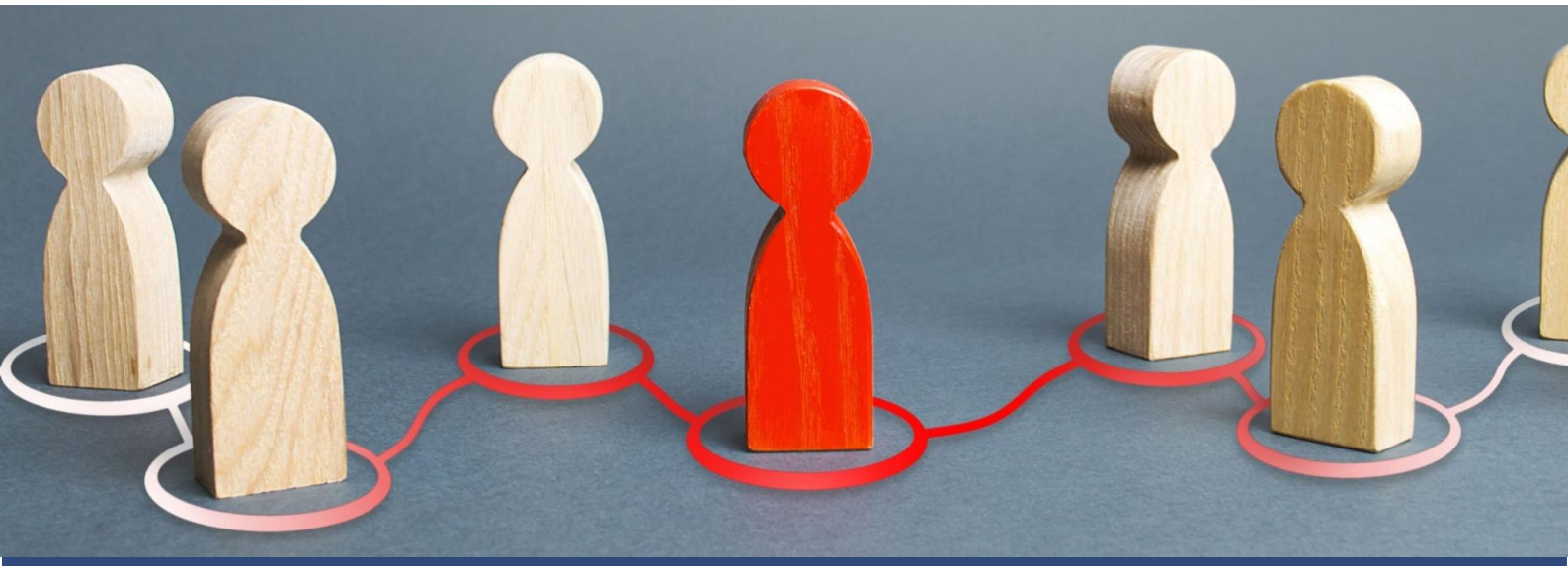
We need leaders who

- are aware of unconscious bias in their decision making and that of others.
- put in place the mechanisms to manage their own bias and to challenge those leaders that don't.
- instill a strong values-based culture in their organisations.

We also need leaders who 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 second half of the 2020s. For the risk function, it means delivering the "decade of influence".



How 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, however it won't happen if it doesn't 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 because of the level of complexity leaders are dealing with.

What needs to change?

The risk profession must provide a better product for the businesses served and must convince them that "This time, it's different." Time to move from red tape to blue ribbon.

It is up to the risk profession - not business leaders - to break out of the mire where risk is seen as a compliance function.

A new approach to risk is clearly needed

A new approach is needed to help organisations achieve greater and sustained success.

My approach, developed from my 30 years in risk and strategy, involves transforming ERM programs from limiting compliance tick-the-box exercises to programs that facilitate effective decision making and provide greater clarity around strategy and risk: essentials for improving agility, resilience and growth.

Got you thinking?

Drop me a line at info@bryanwhitefield.com to share your views on risk and on my approach to enterprise risk management and start a conversation about how we can create a new program together that's designed for greater organisational success.

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 **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; **Risky Business: How Successful Organisations Embrace Uncertainty (#1 Amazon Best Seller),** a guide to the most successful way to design and embed an effective risk framework; and **Team Think: How Teams Make Great Decisions.**

Bryan has 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'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.