
Is your risk framework adequate? Questions directors, investors and the C-suite should ask

Todd Davies TODD DAVIES & ASSOCIATES

Key points

- Despite organisations making significant investments in risk management, they still fall short in dealing with disruptive change.
- Regulatory changes seem unlikely to get to the heart of what really matters in avoiding significant destruction of shareholder value in the future.
- Seven key areas of risk management areas are discussed that investors, boards and the C-suite should be looking for.

In the months leading up to the global financial crisis (GFC), I was having a conversation with the head of audit and risk at a large listed organisation. We discussed the usual topics: Were we making a difference? Were we fulfilling our duties and responsibilities? Were our organisations engaged?

Every now and again there's a pregnant pause in a conversation, and someone says something that needs to be said. This conversation had one of these moments: "I know this sounds terrible, but ... sometimes I find myself hoping for a near miss or a minor catastrophe. There's some complacency setting in at all levels of the organisation, and nothing short of a shock will snap them out of it."

Well, as the saying goes, be careful what you wish for. Twelve months on from the collapse of Lehman Brothers and the global credit crunch, we're through our darkest hours, back to business as usual and investing in risk management again. The newspapers tell us that "risk is the new black", and at the same time we're bracing ourselves for the next wave of regulatory reforms, and trying to anticipate what they might be.

What form should more regulatory reform take?

I've been lucky enough to participate in some of the discussions and consultations in Australia and abroad on what could and should be done in the regulatory reform process, particularly with regard to risk management and lessons from the GFC.

On the one hand, increasingly there's an understanding that overly specific regulatory responses can create bigger problems than those they are attempting to solve. This is particularly the case when different jurisdictions put different solutions in place, as it can create needless complexity or encourage "regulatory arbitrage" between jurisdictions. As a result, deep thinking is required, and meaningful progress is slow — particularly when multiple jurisdictions are involved.

On the other hand, there is a need to move forward, take action and deal with the local political environment. Unfortunately, what we've seen so far in Australia and abroad looks more like tinkering at the edges and dealing with peripheral issues than getting to the heart of things. The various changes to executive remuneration and token efforts around risk governance are good examples of this. In my opinion, most of these regulatory responses would have done little to prevent the enormous destruction of value we've just experienced, let alone the next round of market dislocation.

Around the world, organisations had invested in risk management and had assured investors and stakeholders that their risk management systems were effective, only to make significant earnings downgrades or discover more significant issues which shot to the core of their future viability. When quizzed on this, the standard line from chairmen and CEOs was that "no one could have reasonably foreseen these circumstances". A sad indictment, indeed — damning of their investment in risk management. This response is unacceptable to stakeholders and shareholders. It's no coincidence that we've just been through an abnormally high turnover in CEO ranks.

A number of taskforces I've been involved with are asking this question: How do we know that a company's risk framework is delivering the right outcomes, and is not just bureaucracy gone mad?

What directors, managers and investors should look for

Here are some views drawing on the collective wisdom of institutional investors, directors, internal

auditors and professional advisers on what directors, managers and investors should be looking for to move beyond compliance and deliver risk approaches that we can really rely on.

1. Sort the wood from the trees

Do you ever get the feeling that despite being assured that best practices are being implemented, the risk reporting you are receiving is missing the point? Chances are you're right.

Risk management approaches are often an aggregation of data from individual business units, with the aim of providing an overall picture of the organisation. If you've invested in a risk system or enterprise risk management, and implemented the latest standards, there's a good chance you are swimming in "aggregated minutia".

While there is enormous and often untapped power in the "wisdom of crowds", the reality is that if people don't understand the big picture, they don't have the context to comment on it. You could be getting great information on what's happening with the deckchairs on the ship, but not know whether the ship is heading for any icebergs.

The Australian Securities Exchange (ASX) Corporate Governance Council has rightly said that the focus must be on understanding the material business risks, rather than having an enterprise-wide risk management approach which is bottom-up only.

2. Foresight

When Al Gore was last in Australia, he made the following statement: "We have a habit of confusing the unprecedented with the unlikely."

This statement is particularly relevant in risk management and points out one of the big challenges for risk management.

Risk processes and risk participants tend to be very good at *hindsight*. If something is happening now, or has happened in recent history, there's a good chance it will feature prominently in your risk profile. If it's been a while since something has happened, corporate memory should, it is hoped, also pick things up.

Where risk processes and participants tend to fall down is in identifying situations that haven't been experienced before. And while staff retention and drawing on experience can help us reflect back over multiple economic cycles to give us greater hindsight over a longer period, if events are unprecedented or manifest themselves in new ways, they're unlikely to be flagged or considered seriously.

Life evolves. Conditions change. The risks we face today are different from those we faced in the past. Similarly, the risks we face in the future will be different and will manifest themselves in different ways from those we faced in the past. If your risk processes are not informed by a range of sources — including futurists, whole-systems thinkers and emerging conditions — to give you true foresight, at worst you are driving forward through the rear view mirror, and at best you've probably got material blind spots.

3. Understanding disruptive change

Strategic risk is a specific class of risk which ultimately results in an organisation not being able to continue with its current business or operating model.

It is human nature to operate within a business-as-usual mindset. In mature organisations, budgets and targets are usually set up to deliver single digit performance growth year on year. Success is predicated on narrow ranges of variability and people don't dare think

about disruptions which could change the fundamental assumptions in their business models. True strategic risk is thinking about exactly that.

While many are quick to add the word "strategic" in front

of "risk management" to make their work sound more interesting, the reality is that strategic risk as a class is not well addressed. While there are notable exceptions, most risk assessments I see are well and truly grounded in business-as-usual, even when disruptive change is foreseeable.

Look out for organisations that anticipate, understand and seek out disruptive change. But *watch out* for organisations that are consistently on the back foot and claiming the "reasonably foreseeable" defence. No one actually believes that one anyway.

4. Beware of projections using historical data

The great thing about historical data is that if all things remain equal, it's a great predictor of the future. The downside, of course, is that few things actually do remain equal.

Think about the major changes you've experienced in recent years. Were these predictable based on past trends? Perhaps, but the reality is that change often happens in an exponential rather than a linear fashion. The GFC, climate change, and resource and technology changes mean that a one-in-100-year event yesterday might be a one-in-five-year event today. Of course, this

if people don't understand the big picture, they don't have the context to comment on it

poses real challenges for actuarial and financial models which draw on historical data to project forward with some sense of certainty.

Data models are incredibly useful, but we need to be careful about relying on projections without testing if the underlying assumptions have changed or understanding the environment in which these assumptions actually operate.

5. CEO-driven risk and learning from risk events and near misses

My view is that accountability for risk management has to lie with the CEO, and there is no realistic alternative to this.

While the notion of a “chief risk officer” is gaining prominence — particularly in Europe and in financial services — ultimately, the CEO has to drive risk in the organisation. If the CEO isn’t driving it personally, get out of the stock.

Risk events and near misses provide real tests of the risk framework and pose some fundamental questions, such as: Were these risks previously identified and considered at the right level in the organisation? If not, why not? A steely gaze from the CEO asking “Is this because you were attempting to keep things from me, or because you don’t understand your business?” is not easily brushed away, and is a great way to sharpen the minds of executives. Similarly, in testing why response plans didn’t stand up, was it because the executive didn’t take risk management seriously, or were the plans half-baked?

An annual signoff from the CEO to the board that the risk management system is effective, and that all material risks have been reported, certainly sharpens the mind.

6. Beware of a “good news” culture

Any risk system and process is only as good as the information which flows into it.

In a large proportion of cases where the board was blindsided by risks to the point of organisation failure or a “near death experience”, there was a “good news” culture, whereby good news flowed up the line and bad news was spun into good news or didn’t flow at all.

While a dominant CEO or board can drive results, a culture where people are afraid to communicate bad news is a dangerous place to be.

Reward people for telling it as it is and taking actions to respond. And, again, look out if you see a CEO who’s dominant to the point of creating a good news (yes men) culture. Again, a signoff that all material risks have been considered at an appropriate level in the organisation is a great way to drive focus, and face up to reality.

7. Independent review/assurance

If you’re on the board or in the C-suite and not a specialist in risk management, how do you know whether risk management is working well in your organisation?

The ASX Corporate Governance Council suggests that boards should get independent assurance over the risk management framework in a holistic sense, and that one of the best functions to provide this is internal audit.

This is great advice, and a smart move by any board.

Of course, to make sure that internal audit is truly independent and not “in management’s pocket”, you would do well to make sure you are covering all the points in the Institute of Internal Auditor’s policy agenda

(covered on p 10 of this issue).

In summary

It’s possible for organisations to invest heavily in risk management, tick all the boxes and produce all the standard verbiage in the annual report. But risk management has to be integrated into the organisation’s culture — it needs to be part of how the organisation does business.



Todd Davies,
Consultant, non-executive director and independent audit and risk committee member,
Email: todd@todddavies.com.au,
Todd Davies & Associates,
www.todddavies.com.au.

Todd is an expert in the areas of risk management and risk assurance and has contributed to major developments in these areas in Australia and abroad.