Aligning growth and risk

pwc

"The experience since the global financial crisis and recent global events have challenged the fundamentals about risks and their impacts – risk management has to change for the good of the business and for the good of the economy"

Enterprise resilience – an important business capability today

Risk management as a business discipline has been through the wringer since the global financial crisis. Eight years on the business environment has still not returned to its former state and many are wondering if it ever will. Given the ongoing uncertainties in global economics and geopolitics, it's not surprising the confidence of business leaders has taken a hit.

Our recent Global CEO Survey found Australia's CEOs are less confident about their companies' growth prospects than a year ago, and less optimistic about growth in the world economy. And as confidence falls, concerns are rising: over three quarters see more threats today than they saw three years ago.

The reaction of CEOs, including many in financial services, has been to 'de-risk' their businesses by implementing cost-cutting measures and reducing headcount. But in an environment of increasing complexity, change and opportunity, is this really the path to sustained growth?

PwC considers that enterprise resilience is one of the most important capability business needs today. Enterprise resilience is not traditional risk management; it's an organisation's capacity to anticipate and react to change – not only to survive, but also to grow.

To explore what resilience could offer Australia's financial services sector, we brought together a roundtable of executives and thought leaders, including PwC's Global Leader of Risk Consulting, Dennis Chesley and Rick Crethar, PwC's Australian Risk Leader. Here's a snapshot of the ideas that emerged from our discussion.

About the authors

Dennis Chesley is PwC's Global Risk leader with over 24 years of experience across a broad range of public and private entities with global operations. Dennis helps clients evaluate and choose among risk strategies and treatment options – to help them realise opportunities from the risks the chosens strategies and options can bring. Dennis' clients include global financial institutions, NGOs, federal agencies and industry utilities, and he has been responsible for leading several of the firm's larger and/or more complex projects. Most recently Dennis leads PwC's work on the Committee of Sponsoring Organizations of the Treadway Commission (COSO) update to the Enterprise Risk Management (ERM) framework, slated for release in 2017.

Rick is a Partner in PwC Australia who leads the Risk Consulting Business nationally. He helps clients manage risk successfully so that they can continue to drive change, achieve growth and improve the resilience of their organisations. Rick engages with C-suite management and board members to help them see that risk is far more than value protection; when managed effectively and strategically, it can have a positive impact by capitalising on the opportunity that often accompanies it.

At PwC, we call this your *risk advantage*. Whether clients are embarking on large scale projects, responding to a specific risk, weighing up investment decisions, investigating anomalies, or striving for greater confidence in governance, Rick works with them to evaluate risk with a focus on improving business performance and minimising the impact of any adverse events.

COSO update: The emerging alliance of growth and risk

First up, participants were keen to hear about the upcoming changes to the *Enterprise Risk Management – Integrated* Framework issued by Committee of Sponsoring Organizations of the Treadway Commission (COSO) which has been released for public comment. The framework is widely accepted and used by organisations around the world to manage uncertainty and grow value.

As one of the main contributors to both the original and revised versions of the framework, Dennis offered key insights into how it's evolving.

The big difference this time around is the heightened focus on the relationship between risk and strategy, which is becoming much more pronounced globally.

"As operating environments become more complex, subject to constant change and disruption, there is an increasing need for companies to actively consider risk in the context of strategy, mission and values.

"In the act of strategy setting, understanding the risk profile in each strategic option and carrying that through from an execution standpoint, is going to be extremely important."

"Risk to the strategy" has traditionally been assigned to strategy functions, in an effort to prevent the potential erosion of value. However, the "implications from the strategy" and the "risk of a strategy not aligning" have potentially bigger impacts on performance.

Indeed, a strategy's risk profile, the assumptions and implications underpinning its selection, drives the creation of value. And that's what the draft Framework update helps to make clear: ERM can do its part in the selection of strategy, rather than solely managing risk after the strategy is selected.

A new COSO framework: what's different

- emphasises the relationship between strategy, risk and value
- enhances the alignment between performance and ERM
- conduct, behaviour & risk-based decision making
- leveraging data and analytics
- reputation, brand and trust is at the core
- role of the CRO and the key lines of defence. Steps in the revision process:
- draft released for comment on June 15.
- public comment period until September 30.
- final release early 2017.

Find out more at erm.coso.org

Risk taking risks

The need for risk and strategy to talk to each other more led to a discussion about how the risk management function can reposition itself within an organisation in order to be part of these conversations.

PwC's Risk Consulting Leader, Rick Crethar, asked whether the risk function should re-brand itself from being a gatekeeper to being more influential in helping businesses realise upside.

According to Dennis, effective risk management is about recognizing that risk evolves throughout the business lifecycle. Risk should have the conversations that are about identifying the opportunities which build the business while also keeping the ship steady.

"When you talk to business executives – you need to have a certain mindset. You can't simply come in and be the wet blanket saying 'you can't do this and you can't do that'; you need to say 'here's what we need to do to make this happen."

This means influencing the strategy which drives the business. Whether it's giving positive guidance on transactions, or helping in with the view of what customers mean to the business – taking risk and reward together.

For example, if a company's strategy is dependent on third parties, risk can collate insights and run analytics so that the third party relationships can really deliver. In essence, it's about turning risk into a commercial advantage.

Some participants raised the point that the calibre of risk people is critical; they need to have the skills, capabilities and different attitude to have these kinds of conversations.

Risk capabilites will shift more to mathematical, analytics and business collaboration/translation whereby data can be analysed and translated into business insight.

Another said that the risk culture in the organisation is important too: "if you've got a business which understands risk, then the organisation will engage with risk not as the 'police', but as advisors.

Enterprise Resilience fosters a change of mind-set and culture, moving organisations from a defensive position to proactively seeking opportunities.

It serves as the baseline for entrepreneurial thinking and leverages values for decision taking to promote greater initiative and business partnering which seeks to understand what the business values.

Everyone agreed that this change in attitude presents a tremendous opportunity, but that risk must take a risk and re-think the way it engages with, and positions itself within the organisation.

enterprise resilience

[en-ter-prahyz ri-zil-yuh ns]

Resilience is an organisation's capacity to anticipate and react to change, not only to survive, but also to evolve

Cybersecurity: better integration of risk and strategy

Because it's among the top concerns of CEOs and boards, cybersecurity presents an opportunity for risk to drive a conversation about business strategy.

Dennis said that the traditional risk management approach has not been effective for Cyber risk. The instinct has been to build greater defences, through stronger walls – but this is a recipe for continuous spending in areas which may not pose the greatest risks.

What's missing in the conversation, from a risk and strategy perspective, is to ask: 'What should we change in our business to chop cyber threats off at the knees?'

Companies that have taken a different approach started by challenging what their most critical areas were – for example – 'We don't necessarily need to collect credit card information on our customers, however, we must properly manage our authorisation codes, in order to reduce our exposure to stolen data'.

In other words, they reviewed their business operations to zero in on the real threat and reduce it. Thinking differently about risk management fundamentally changed the nature of the conversation between risk, IT, business executives and ultimately the Board.

One participant recognised how taking such an approach could help build trust in the business: "Greater alignment between risk and strategy can be used as a competitive advantage, to build trust with customers, completely turning around the traditional understanding of the role of risk in the business."

Turning risk into advantage

Dennis gave the example of a Chief Risk Officer in a software company who was struggling to understand how risk could be turned into an advantage.

"She had done a great job at methodically analysing their products to understand how they could be compliant with rules in the many countries that they shipped to. She was proud of the system they had developed and how effectively it worked.

"I asked whether she had thought about taking that system to the firm's customers which shipped internationally as well, to see if it could help them with their own risk and compliance.

"At that point she grabbed her cell phone and called the head of marketing and set up a meeting for the next day.

"Whenever we've been proud of what we've been able to do to deal with a risk, there's often an opportunity to turn that into a commercial advantage; we just need to think about it a bit differently."

The need for speed leads to a new manifest

Another aspect of cybersecurity which has changed the way companies think about risk is the speed required to respond to threats. Cyber threats change so quickly – nation states, hacktivists and organised crime are now all involved – that the normal risk management cycle simply can't keep up.

Companies are realising that cyber risks 'live, breathe and morph' over time. So the way they think about the risk can't be just in one-off treatment options, such as coming up with controls and testing them. They might be totally ineffective the next day.

"Trying to deal with cyber has led risk professionals to say 'we need a new manifest'. And it was out of those conversations that the concept of enterprise resilience evolved," explained Dennis

Cyber Security is one of the top risks facing financial institutions

Financial services executives are already depressingly familiar with the impact that cyber-threats have had on their industry. In PwC's 19th Annual Global CEO Survey, 69% of financial services' CEOs reported that they are either somewhat or extremely concerned about cyber-threats,

Cyber-security is the leading challenge to the adoption of the Internet of Things because insecure interfaces increase the risk of unauthorized access. Here are some concerns:

- Attack surface: hackers can gain entry to a corporate network through an IoT device.
- Perimeter security: IoT rechnology relies on cloud-based services, so it will be challenging to implement effective perimeter defenses.
- Privacy concerns: the pervasiveness of IoT data collection coupled with advanced analytic capabilities could result in consumer privacy breaches.
- Device management: Many IoT devices currently do not support implementation of strong security controls. Maintaining a robust security baseline will get harder as IoT devices proliferate.

From compliance to enterprise resilience

Both regulators and companies have traditionally looked into the past to identify and manage

risk. But this backwards-leaning view has led to compliance, not resilience. It has also been somewhat 'clunky', with different risks being managed in isolation throughout the business.

Dennis explained that resilience is not traditional risk management: "It's about an organisation having the capacity to anticipate and react to change, not only to survive, but also to evolve."

The critical word is change. To be resilient, you need to manage through a major crisis, like a critical supplier's factory being destroyed by an earthquake, as well the disruptive megatrends which are reshaping the global business landscape – demographic change, shifts in economic power, rapid urbanisation, climate change and technological breakthroughs.

"But change doesn't have to be large scale; you also need to manage the shifts in your own market, or among your own stakeholders," said Dennis.

The key is being 'fit' to capitalise on opportunities. Enterprise resilience is sometime referred to as the corporate immune system. If it's in good shape and something strikes, the company can bounce back. It also means the business is fitter to jump further, be more flexible to evolve, and see and seize opportunities ahead of its competitors.

What a resilient enterprise looks like

Resilient organisations exhibit the following six traits:

- ***Coherence*** – The ability to make mutually beneficial decisions
- ***Adaptive capacity*** – The ability to reorganise for change
- ***Agility*** – The ability to make and implement decisions at the required speed
- ***Relevance*** – Consistently delivering on stakeholder needs
- ***Reliability*** – Consistently delivering to expected quality, on time
- ***Trust*** – Knowing how to create investment-worthy relationships

Looking ahead: The role of Risk?

If an organisation builds resilience into its very DNA, the question arises as to the role of the Chief Risk Officer. Are they an administrator of risk, an overseer of the compliance function, or someone who provides specialist advice?

According to one participant: "The executive teams in our bank really look to risk to provide specialist advice. Ideally, they'd be permeated across the business and giving strategic analysis and insights."

Rick Crethar asked: what do people need to be thinking about now, so that in five years' time risk professionals are in high demand right across the business?

It is near impossible to prepare a plan for how a risk function will look in five years' time. This would require a crystal ball on how the megatrends will play out. "We can't predict how technology will advance, nor what the next macro-economic event or scandal will be."

CRO's who will be ready are those which start transforming their risk functions now by leveraging technology to streamline current processes, piloting advanced analytics, enhancing risk management reporting to provide greater insight in making better risk decisions, changing the gene pool as a result and building a stronger risk culture.

This led to discussion about the role of boards in risk, strategy and resilience. Dennis believes that the gap between boards and executives will continue to close.

"Boards we talk to don't want to see risk treated as just a compliance function. What they want is a good sense that risk is connected to executive management, helping them to 'look around corners' to identify the things most likely to impact on the company achieving its strategic objectives.

"Boards are also demanding more transparency around risk management's capabilities, to understand how it is evolving in response to the megatrends and the environment, and how it connects back to strategy.

"Resilience is becoming increasingly important to boards. In fact, we are seeing more and more senior risk professionals being sought to take board positions," said Dennis

Developing your organisation's resilience

With greater resilience, financial services organisation will be better positioned to capitalise on change and manager through a crisis so that they come out stronger. They will have the confidence to take risks necessary to achieve desired returns within their risk appetites.

There are logical triggers in business activities or the external environment which should prompt actions on resilience. For example:

- in setting or reviewing strategic objectives how aligned is the strategy to purpose, vision and values?
- Do you have evidence your corporate immune system is weak? Perhaps a breach has occurred which was not detected quickly
- if a competitor fails – could it happen to your organisation?
- at times of major change – a transformation project or changes in your external environment – do you have the right capabilities to drive change and realise the benefits it may bring at the right speed?

But there's no need to wait until something happens to test your resilience. Here are four steps to building your resilience:

- Get everyone heading in the same direction. Understand what really matters, align how the functions work, and create a shared understanding of what resilience means and how you can create advantage.
- Assess how you invest. Many organisations spend more on insurance than building resilience. But insurance cannot salvage a damaged reputation or rebuild customer trust.
- Check in on your resilience. Stress test your resilience in a safe environment. There are effective ways now to give your corporate immune system regular and thorough health checks.
- Measure resilience. The factors that define what makes your organisation resilient can and should be identified and measured. Embed resilience into your operating model and monitor it continuously by building robust metrics into your KPIs.

90%

*90% of organisations believe that resilience is greater when functions such as strategy risk management, business continuity, IT and security are joined up, but…**

*… only 37% of organisations believe that these areas are properly joined up**

37%

Source: London first PwC Resilience Survey

PwC contacts

Rick Crethar

Partner

+61 (2) 8266 7809
rick.crethar@pwc.com

Access the latest thinking on Enterprise Resilience at PwC's Resilience Journal:

www.pwc.com.au/resilience

Julie Coates

Financial Services Leader

+61 (2) 8266 2006
julie.coates@pwc.com

Peter Burns

Financial Services Consulting Leader

+61 (2) 8266 4726
peter.burns@pwc.com

Nicole Salimbeni

Partner – Risk & Regulation

+61 (2) 8266 1325
nicole.salimbeni@pwc.com

www.pwc.com.au/resilience

WL 127042745