SPEECHES

APRA General Manager of Governance, Culture, Remuneration and Accountability, Stuart Bingham – Speech to the Financial Services Assurance Forum

Thursday 24 November 2022

The power of "Why"

Thank you for the invitation to speak at the Financial Services Assurance Forum. It is a pleasure to be here.

Let me start with a question: were you ever that annoying child who kept asking why? Until the point your parents said, in a very exasperated tone, something like "because it just is!"

I was.

While it may have been frustrating for my parents, I've come to realise that asking "why" is a sign of curiosity and wanting to understand things – something that comes in very handy working at APRA.

As Australia's financial safety regulator, we are very much in the business of risk management, with a mandate to prevent, fix or mitigate problems before they cause harm. When this doesn't happen at a bank, insurer or superannuation fund, we are naturally curious. "Why did the issue occur?" "Why was the risk not well understood?" "Why was a process not followed?"

For APRA supervisors, it is about getting to the root cause of an issue. Understanding "what" and "how" is important, but we firmly believe that fixing an issue or managing a risk requires an understanding of "why".

Discovering "why" requires someone to ask a question, but it also needs an answer. Cast your mind back to your childhood and consider whether you were satisfied with your parents' explanation that you couldn't have an ice cream "because I say so". Your disappointment at not getting a treat was no doubt only magnified by the lack of an explanation that led to increased understanding: of tooth decay, poor diet or – heaven forbid – ruining your appetite before dinner.

While APRA has the ability to compel answers from the banks, insurers and superannuation trustees we regulate when things go wrong, we expect to see questions being asked and answered internally by these entities well before a problem arises and APRA comes calling.

Our observation, however, is this type of inquisitive culture doesn't always flourish within our regulated population to the extent that it should. Not everyone in some organisations believes that reporting problems is their responsibility. More junior employees might be frightened to speak up, while executives can have an overly optimistic view of how well risks are being identified and managed. Too often, analysis of problems doesn't penetrate to the heart of the issue because of a failure to really ask "why?".

Over the past 18 months, APRA has been delving more deeply into the issue of risk culture in our regulated entities through a series of surveys and industry webinars. In the time I have today, I'd like to talk you through APRA's perspective on why a strong risk culture is so important to prudential soundness and financial success. I will also provide an update around three significant issues regulated entities will need to navigate over the coming year: the commencement of the new Financial Accountability Regime, the growing spectre of cyber risk and APRA's enhanced prudential requirements around operational resilience.

Why risk culture?

A strong risk culture is essential for effective risk management outcomes that support an organisation's financial and operational resilience. Risk culture refers to an entity's attitudes and behaviours towards risk management. Specifically, it is the behavioural norms and practices of individuals and groups that shape an entity's ability to identify, understand, openly discuss, escalate and act on its current and emerging risks.

emerging risks.

A strong risk culture creates an environment where employees are comfortable speaking up and voicing concerns with their leaders. It produces better decisions by ensuring a broader range of views is considered, and allows ideas that present heightened risks to be appropriately challenged during decision-making. It incentivises boards and senior executives to prioritise effective risk management. In doing these things, a strong risk culture helps to deliver better business and customer outcomes for organisations.

Pretty much everyone in business today recognises its importance, but not everyone does it equally.

For example, sound risk management requires appropriate systems, processes and frameworks. We therefore – quite rightly – spend a significant amount of time focused on assessing the systems, processes and frameworks that support risk management.

Too many risk assessment reports APRA reads, however, only review design effectiveness. We also want to see a focus on operating effectiveness – how these things work in practice.

You can also go even further. If risk management systems, processes and frameworks don't operate as intended, then we encourage you to assess why that is occurring. The answer invariably comes back to risk culture.

Over the past 18 months, APRA has conducted risk culture surveys across 61 regulated entities in banking, superannuation, and insurance. The survey has now been sent to over 230,000 employees.

The surveys provide insights from employees within financial institutions on perceived risk behaviours and the effectiveness of the risk management architecture they work within. Over time, the responses will help identify the extent to which positive changes are (or are not) taking place within individual institutions, as well as areas for improvement. They also provide APRA with the ability to benchmark results across institutions, facilitating peer analysis and comparison. At this stage, we are one of only a few supervisory bodies worldwide that directly collects such survey data, although a number of our peers are interested in following suit.

In addition to meeting with each entity that took part in the survey to discuss their results, we also recently published an Insight article on our website on the ADI risk culture survey results.

Key themes emerging from the survey were:

- Three-quarters of executives believed that sufficient resources had been committed to improving risk management, while Legal, Risk and Compliance employees were far less positive. This observation serves as a reminder that the critical "voice of risk" needs to be heard and acted upon, particularly regarding the need for sustainable investment in risk management capability and architecture.

- The risk culture survey results highlight a need to continue to ensure that sufficient resources are committed to improving risk management within ADIs.

- Executives and senior management were positive about employees communicating and escalating risk issues, suggesting high levels of psychological safety. This view, however, was not matched by the experiences of individual contributors (i.e. employees with no people management responsibility). This highlights potential blind spots by executives and a missed opportunity for ensuring that people continue to feel safe to speak up.

- There was a wide variation in responses regarding whether individuals are clear on their risk management accountabilities and whether the risk management roles and responsibilities across the organisation (i.e. three lines of defence model) are well understood.

- Executives and individual contributors agreed that risk management was regularly considered in decision-making. Executives also believed that leaders were appropriately challenging decisions, and that constructive challenge was encouraged in their organisation. Individual contributors experienced this differently, indicating more could be done to facilitate an environment that supports constructive challenge and diverse viewpoints within and across all levels of the organisation.

These findings should be considered more broadly by the industry to determine what more can be done at an entity level to improve these issues. Assurance and audit teams can help drive improvements.

Risk culture is also a theme in work undertaken to improve or transform risk management at entities. Risk transformation programs are becoming more common in regulated entities and vary in scope, scale and the businesses impacted. Sometimes these programs are at APRA's urging, but sometimes the entity has identified the need to uplift risk management itself. Either way, your profession has a stake in ensuring these are successful.

The tough news is that research shows that 70 per cent of risk transformations fail.[1]

A recent report I read stated:

"Nonetheless, [the entity] has been unsuccessful in implementing a group-wide operational risk and compliance framework despite multiple attempts over time. Given this context, it is not surprising that our findings on the root causes emphasise a set of cultural reasons that underlie the longstanding implementation problems in this area. It is these cultural challenges, rather than technical aspects of the design of the framework, that have inhibited success."

To emphasise the point, the root cause in the majority of cases is failure to successfully transform both the organisational culture and the risk culture.

It's not the plan that will make the biggest difference – it's the leadership attitude to the transformation program that will shape success. Starting with the "why" makes a difference. Why are they bothering? Why does it matter? Why will their business be better off because of this change? Or worse off if they don't change?

Transformation or change management starts with mindsets, not structure and systems.

But culture runs deep. It is very difficult to change mindsets (what we don't see and often don't attempt to address) as well as behaviours (what we do see and do attempt to address).

Accountability

Powerful levers to influence organisational and risk culture are performance incentives and consequence management. As you know, CPS 511 Remuneration is coming into force next year for significant financial institutions, and all financial institutions by 1 January 2024.

In addition, the Financial Accountability Regime (FAR) is getting closer to starting. The FAR is due to commence for authorised deposit-taking institutions (ADIs) six months after Royal Assent and for insurance and superannuation 18 months after Royal Assent. But with the legislation yet to pass the Senate, it's not clear when the Governor-General will give his stamp of approval.
APRA and ASIC are working closely together to jointly administer the FAR. Industry communication and guidance will be published to support industry to implement and comply with the new regime.

The regulators have established a single point of contact for engagement with entities in relation to the FAR. APRA Connect, APRA's new data collection system, will be used as a single portal to avoid the need for entities to report to APRA and ASIC separately. In addition, a single point of contact for entity queries and issues will be established.

Now is a good opportunity for ADIs to evolve their accountability framework. And it is never too early for insurers and superannuation trustees to start reviewing and reflecting on their governance and accountability arrangements in preparation for the FAR.

We have seen a number of benefits from the Banking Executive Accountability Regime (BEAR) that we expect to translate to the FAR. It is beyond simply doing what the legislation requires, including:

- greater clarity and transparency of individual accountabilities;
- sharpened challenge by boards on actions taken by accountable persons to meet their obligations; and
- more targeted engagement between APRA and entities to deliver prudential outcomes.

Combined with the uplift in remuneration practices under CPS 511, we expect FAR to drive improvements in how entities respond when things go wrong in order to better understand the why.

CPS 230 Operational Resilience

But of course, even better is when we mitigate risk before it crystallises. CPS 230 Operational Resilience sets out APRA's minimum expectations for the management of operational risk as well as incorporating requirements for outsourcing (existing CPS 231) and business continuity management (existing CPS 232). As well as setting foundational operational risk management principles, the design of the standard:

- reflects changes in entity business models since existing standards were made (both from a technology perspective and the general operating environment);
- evolution of approaches to operational risk management by entities, and international regulatory developments; and
- lessons learned through APRA's supervision as well as various reviews that have highlighted deficiencies in operational risk management in the financial sector.

CPS 230 establishes new requirements for each financial institution to:

- identify, assess and manage their operational risks, with effective internal controls, monitoring and remediation;
- be able to continue to deliver its critical operations within tolerance levels through severe disruptions; and
- effectively manage the risks associated with the increased usage of service providers, through a comprehensive service provider management policy, formal agreements and robust monitoring.

A key element of the new standard is an increased emphasis on data and analytics to inform risk management and decision-making. For example, the standard requires each institution to:

- undertake an assessment of its operational risk profile, with a defined risk appetite supported by indicators and limits;

- maintain appropriate and effective information systems to monitor operational risk, compile and analyse operational risk data and facilitate reporting to the board and senior management; and

- ensure that operational risk incidents and near misses are identified, escalated, recorded and addressed in a timely manner.

CPS 230 deliberately moves away from the prescriptive and process-driven approach of the current standards to an approach that is principles-based and outcomes-focused. There is an emphasis on the need for entities to have regard to how disruptions will impact on their customers.

Consultation on CPS 230 has now closed. We are currently assessing the submissions and expect to respond in the new year.

Cyber security and improving resilience of the financial system

Cyber security has been a high priority for regulated entities for some time now. The events of recent weeks have only served to highlight its importance.

Everyone in the financial sector takes this very seriously. There's no lack of awareness of the issues involved, and all entities are investing considerable effort and expense to protect themselves from cyber-attacks. This includes continued investment in people, tools, partnerships and testing to more effectively respond to the evolving nature of cyber-attacks.

The main challenge, of course, is that the job is never done. Everyone needs to be constantly updating their defences and response plans in a manner that is effective in dealing with the latest threats.

Probably one of the biggest issues at present is that entities don't exist or operate in isolation; they're just one part of an interconnected ecosystem with numerous service providers that form part of, and enable, the financial system. While it's important that everyone keeps their own house in order, third party suppliers can create vulnerabilities, and that is where our work – and indeed, that of the international regulatory bodies – is increasingly focused. Certainly, our own Cyber Supervision Strategy, which we published a while ago, sought to give that issue much more prominence.

The audience in this room know better than anyone that cyber-attacks are relentless, so we don't worry

about any lack of awareness. But the increasing interconnectedness of the financial system, and the fragmentation of business processes, with increasing reliance on unregulated service providers, makes the task of staying ahead of the game much more difficult.

CPS 234 Independent Assessments

Execution of CPS 234 independent assessments to establish a baseline of cyber controls have generated significant interest in the industry to uplift the cyber posture. While still in the early stages, the CPS 234 assessments are pointing to a number of areas where the industry is struggling to uplift.

The CPS 234 independent assessments are being rolled out in tranches. The first tranche is concluding at the end of this year with approximately 80 entities involved. The second tranche has commenced mid this year and will be followed by a third tranche kicking off next month.

Early insights from the tripartite reviews point to number of areas of weakness in the industry, including:

- insufficient information security control testing program (i.e. lack of rigour in the nature and frequency of testing);
- insufficient board oversight on cyber (roles and responsibilities are unclear, including inadequate reporting to the board);
- inadequate asset management (information assets identification and classification still to be improved); and
- insufficient testing of incident response plans (while entities have a response plans, more rigour should be applied in testing of those plans).

Conclusion

The assurance profession has an important role to play in the prudent management of regulated entities. As the third line of defence you are often tasked with assessing the effectiveness of risk management systems, processes and frameworks. I am also aware that boards are placing increased expectations on you. This is an opportunity that we hope and expect you to embrace.

As you will note from today's comments, while a focus on risk management systems, processes and frameworks is important, assessing design effectiveness alone is not enough.

There is a need to assess the operating effectiveness of risk management systems, processes and frameworks. There is also a need to be outcomes-focused.

As a further step, where the risk management systems, processes and frameworks are not operating as intended, I encourage you to consider why this is the case. This will require the consideration of attitudes

and behaviours towards risk or the risk culture. Discover your inner child and keep asking why until you get a satisfactory answer – one that is not "because it just is".

Footnotes

[1] Isern, Joseph and Pung, Caroline, "Organizing for successful change management: A McKinsey global survey", The McKinsey Quarterly, June 2006. The McKinsey survey revealed only 30% of business executives considered their change programs "completely/mostly" successful.

Risk

Media enquiries

Contact APRA Media Unit, on +61 2 9210 3636

All other enquiries

For more information contact APRA on 1300 558 849.

information by email