NEXT

PROACTIVE RISK MANAGEMENT

A CULTURE AND STRATEGY IMPERATIVE BEYOND THE CRISIS MOMENT

Tidal Marks 1 by Marilyn Wallace-Mitchell

EDITION SEVEN
BUSINESS. PURPOSE. FUTURE.

KING&WOOD MALLESONS
金杜律师事务所

FEW WOULD SUGGEST THE AFTERMATH OF A CRISIS AS A GOOD TIME TO ANALYSE RISK MANAGEMENT FLAWS.

Too often, it is only while organisations are mopping up mess that they see the importance of investing time and money in proactive risk management. However visceral, these realisations are also costly. Risk mitigation and cultural reviews become a reactionary measure – often hastily commissioned at great expense to explain the inexplicable, tell us what we should already have known and salvage what is left.

We wonder how things might be different. What might be possible by making the leap from reactive to proactive; from minimising liability and repairing reputational damage, to putting organisational purpose and stakeholder interests first? What might be possible if we ask 'how can we be prepared for the known unknowns' or even, 'what might a "market-leading" program look like to guard against "x" risk'?

AUTHORS

ANNAMARIE ROODING

PARTNER
EMPLOYEE RELATIONS & SAFETY
MELBOURNE

ANDREW GRAY

PARTNER
EMPLOYEE RELATIONS & SAFETY
SYDNEY

Done right, risk management can be a foundational building block for resilient and sustainable growth in the longer term - strengthening an organisation's defences against the foreseeable challenges of today and tomorrow. Building a strong risk culture is a strategic and cultural imperative to empower people, develop organisational capability and bring sophisticated, values-aligned responses to challenges well before they turn into crises.

'Risk culture' and 'risk management' are terms the Banking Royal Commission firmly entrenched in the Australian corporate vernacular. Our experience is that sophisticated market participants understand that they are required to develop and document risk management processes addressing both financial and non-financial risk and that at various levels they will be held accountable for not managing those risks effectively.

In the financial services sector this has been driven by stakeholder expectations (both shareholder and regulators) but also the statutory accountability regimes that have been imposed on the sector. The Banking Executive Accountability Regime (**BEAR**) has applied to the largest Authorised Deposit Taking Institutions (**ADIs**) since 1 July 2018. It requires ADIs to map accountability across their operations and assign accountability for key responsibilities (including risk management) to accountable individual executives. The legislation imposes statutory obligations on both the ADI and accountable individuals - to exercise due skill, care and diligence in the conduct of their business and responsibilities and to take reasonable steps to prevent matters arising that would adversely affect the ADI's prudential standing or reputation. These statutory obligations extend to maintaining sound risk management practices and risk culture and taking a proactive approach to these issues, as is typically reflected in the mandatory individual accountability statements agreed with executives under the regime. Failure to comply with the statutory accountability obligation requires a mandatory remuneration adjustment and potentially banning orders from Australian Prudential Regulation Authority (**APRA**). This is also reflected in regulatory expectations with APRA consistently looking to understand who is accountable for material risk and compliance incidents in the industry and what proactive steps accountable executives took to prevent these risks.

This statutory obligation for enhanced risk management will soon extend beyond banks to other financial services companies. Over the next 18 months the Financial Accountability Regime (**FAR**) will extend the BEAR to all APRA regulated entities (e.g. insurers and superannuation entities). Significantly, this will include a new statutory obligation for an accountable person to take reasonable steps to prevent a material contravention of specified financial services laws, which should focus attention on risk and compliance frameworks. ASIC will also be a co-regulator under the FAR and can be expected to be an active regulator of conduct in the industry.

The APRA remuneration standard (CPS511) also requires remuneration frameworks to support the sound management of non-financial risks. This includes providing material weight to non-financial performance metrics and the downward adjustment of remuneration for significant risk management or accountability failures. APRA guidance indicates that a prudent entity should be able to demonstrate how non-financial performance measures incentivise risk management. Illustrative examples of non-financial performance measures include control effectiveness, regulatory and audit findings, risk culture surveys and conduct risk measures including incidents and customer complaints (see CPG 511). The underlying theme of APRA's regulation of remuneration is that remuneration should be used as a tool to drive effective risk management including both as an incentive for positive risk performance and as a consequence for material risk management failures.

In a different context, under the model work health and safety laws that now apply in every Australian jurisdiction except Victoria, officers are required to take reasonable steps to undertake due diligence to ensure the organisation complies with its obligations under those laws (in other words, to proactively manage the risk of non-compliance with the primary health and safety duty). The positive duty to eliminate sexual harassment and related unlawful conduct, now enforceable by the Australian Human Rights Commission (**AHRC**) under the *Sex Discrimination Act* 1984 (Cth), similarly requires the taking of reasonable and proportionate measures: demonstrable actions that are aimed at preventing the conduct or related harms, from occurring in the first place. Indeed, in identifying in its Guidelines that risk management is 1 of the 7 'standards' organisations are expected to meet to comply with the positive duty, the AHRC notes that organisations should take a risk-based approach to prevention and response, expressly acknowledging that risk management is a standard part of running any organisation or business.

But effective risk management is more than a compliance exercise.

PROACTIVE RISK MANAGEMENT IN PRACTICE

What can organisations be doing to elevate their risk management practices from a compliance posture to a proactive, market-differentiating resilience tool?

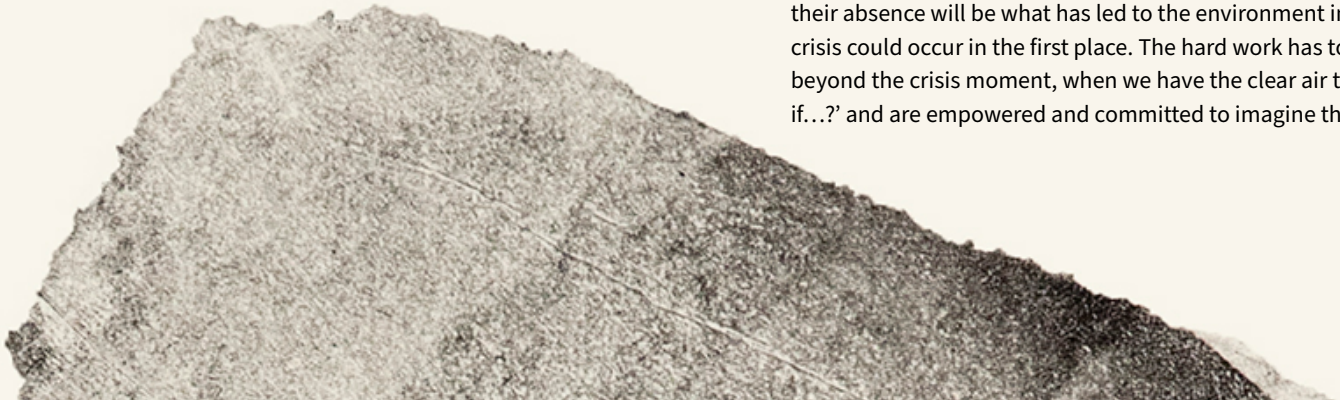
A fundamental aspect of proactive risk management is scenario planning. It is not uncommon for boards in 2023 to be 'war-gaming' cyber incidents, using hypothetical cyber crises to establish the guard rails for how real-life decisions might be made about the most challenging issues, such as whether the organisation will be willing to pay a ransom to a cybercriminal, under which circumstances if so and with a nuanced appreciation of the implications for compliance with various complex laws and stakeholder expectations. This is proactive risk management at work.

We observe that effectively managing risk also bakes a valuable level of literacy, capability and confidence into the organisation's DNA. This is because practical features of a risk-aware culture include things like transparency, open communication and a shared (rather than siloed or function-driven) commitment to identifying and eliminating risks. It means fostering an environment where employees are not only permitted and encouraged to address challenges and speak up about concerns, but are equipped with (and regularly trained in) the necessary skills to do so and similarly, where they are trained to listen to others. On the flip side, an organisation that downplays the importance of risk as an integral part of its culture may implicitly encourage or permit silence or complacency and render ineffective even the most sophisticated risk management systems. As convincing as the 'tone from the top' might sound in an echo chamber, the Board and the Executive will not create an effective risk culture if nobody else understands what it means in practice or knows what it feels like to operate safely within one.

In discussing risk management, the AHRC Guidelines for complying with the positive duty to prevent sexual harassment call out the importance of meaningful engagement and consultation with workers. These people are an organisation's eyes and ears - they understand the practical risks of their workplaces because they live with them every day. And remember, most large organisations are not monocultural, but are comprised of several heterogenous cultures each adapted to the particular contexts of their environment and composition. Effective risk management includes considering how you can tap into those mini-cultures' rich veins of on the ground knowledge to fully understand the risks they present. It is also about acknowledging the positive impacts of doing so on an organisation's risk culture.

NEXT STEPS

Legislators' and regulators' heightened focus on effective risk management is the 'stick' to encourage thinking critically about what kind of risk management culture an organisation has and whether it meets the minimum required standards. The carrot is the precious opportunity you have outside of crisis moments, to undertake a richer analysis of where your organisational risks truly lie and what that might enable you to do. Both in terms of preparedness for unforeseen events and the building of a genuinely risk-aware culture. One of continuous improvement, where leaders actively encourage and value open communication and feedback. One where people at all levels are trained in the identification and mitigation of potential risks and how to speak up about them effectively and with impact. One where leaders lead by example, exhibiting and valuing transparency, accountability and adaptability. One which is ultimately resilient and equipped for sustainable success. These goals are not only not achievable in a crisis when the toothpaste will not get back in the tube and someone has to be to blame – their absence will be what has led to the environment in which the crisis could occur in the first place. The hard work has to be done beyond the crisis moment, when we have the clear air to ask 'what if…?' and are empowered and committed to imagine the answer.



JOIN THE CONVERSATION

SUBSCRIBE TO OUR WECHAT COMMUNITY.
SEARCH: KWM_CHINA