What we’ve learned talking to 150 directors about trust and modern slavery 03 /

A non-financial crisis 04 /

Cultural drivers of organisational performance – why the ‘soft stuff’ matters 06 /

Board talk – dealing with data privacy 08 /

From discussion to decision – effective board decision-making 11 /
Creating and retaining a position of trust amongst community stakeholders has never been more important, or indeed complex, for corporate Australia. In today’s environment, the impact that a company – its people, products and services – has on the community in which it operates is under constant public scrutiny.

In this edition of Across the Board we reflect on recent discussions with more than 150 directors on the intersection between trust and board accountability for non-financial risks. In particular, we discuss the introduction of modern slavery reporting legislation in Australia, which will require boards to approve a mandatory, public, annual statement on the risk of forced labour, debt bondage, trafficking and other slavery-like practices in their operations and supply chains.

We also dissect the findings and recommendations from APRA’s Prudential Inquiry into the operations and governance of CBA, as well as delve into topics around the cultural drivers of organisational performance, data privacy, and removing bias from board decision-making.

Finally, I encourage you to consider the Top 10 issues Australia’s C-level leaders say they are most concerned about as they look towards 2019 in our Keeping us up at night report.

If you would like to discuss any topics in more detail, please contact me or your local KPMG partner.

We hope you find this issue of Across the Board interesting and insightful.

Best regards

Alison Kitchen
National Chairman
KPMG Australia
What we’ve learned talking to 150 directors about trust and modern slavery

It is hard being a director, and it should be. Corporations reach into our everyday lives. They shape and influence societies and economies. The decisions directors make impact all of us. During 2018, board accountability was once again in the spotlight. Royal Commissions, the APRA Prudential Inquiry into the Commonwealth Bank of Australia, and proposed changes to the ASX Corporate Governance Principles all indicate that there is a fundamental question that boards must answer.

How do we earn and maintain trust?
During October and November 2018 we spoke to 150 directors across Australia. All of these discussions centred on the intersection between trust and board accountability for non-financial risks. The non-financial risk we focused on was the introduction of modern slavery reporting legislation in Australia, which will require boards to approve a mandatory, public, annual statement on the risk of forced labour, debt bondage, trafficking and other slavery-like practices in their operations and supply chains.

1. Human rights is not a zero sum game
Directors are clearly grappling with how to balance ideas that seem diametrically opposed. We heard three clear positions in response to the introduction of Australia’s Modern Slavery Act.

Strategy or compliance: A compliance-based approach to the legislative requirement to report on modern slavery is the easiest path.

Opportunity or risk: Responding to modern slavery is about risk management.

Trust or profit: Making decisions that support growing trust comes at a cost to growth and company profit.

The collegiate conversation demonstrated that these are not ‘either or’ propositions. In fact, profit, and in particular growth, are only secured with stakeholder and community acceptance of your business. While you comply with the modern slavery legislation by reporting, you manage your risk by responding. This means business needs a strategic approach to dealing with the impact of its decisions on people.

We’ve all been thinking about harm to people ‘inside the fence’ for years. For those that haven’t already, it’s time to start thinking about those ‘outside the fence’.

While it is appropriate to take a risk-based approach to prioritising the most severe and likely modern slavery practices in your operations and supply chains, leading directors are clearly examining this through an opportunity lens. We heard about opportunities to create supply chain efficiencies, deeper supplier relationships, and to cultivate community partnerships. Others were already creating differentiated products in the market using technology to assure quality, origin, and the absence of harm to people.

Directors showed us that this is not a zero sum game. Profit, compliance and risk management are central considerations to appropriately exercising director duties. However, prioritising human rights considerations can build trust, offer a framework for strategic decision making, and create opportunities for doing business better.

2. Director accountability for non-financial risks is not going away
No-one outright accepts slavery. Well, except it is complicated, isn’t it? What about when we operate in, or procure from, a country where child labour is a way of life? Or where any job, irrespective of the conditions under which it is performed, is better than nothing? Or where choosing to cut off a supplier could destroy a region’s economy?

We were surprised by how often directors wanted to talk about the difficult intersection between human rights, culture and values. The most frequent question underlying this discussion is: Where does it end?

So where does it end? This is in no way to minimise the challenge that business faces in performing these tasks, but there are now well-trodden paths to follow and innovative approaches from which to learn.

The honest answer is that it won’t end. Director accountability for non-financial risks is not going away. Set your risk appetite and start where the risk of harm is greatest. Examine your assumptions about who your stakeholders are, and then listen to them, and learn from leading practice.

If you choose to not listen, then beware the consequences of your business having a ‘tin ear’.
A non-financial crisis

Whilst the Global Financial Crisis (GFC) began as a liquidity, market and credit dislocation – after the immediate economic issues subsided it was clear that another crisis was underlying the financial industry – a crisis of culture, governance and accountability. Australia, on a relative basis, managed well through the financial repercussions of the GFC, with our prudent stability and financial management respected globally. However, a range of poor risk management and conduct issues have most recently been exposed through the Royal Commission, significantly damaging trust in the industry.

Preceding the Royal Commission, but addressing many of the issues head-on, APRA’s Prudential Inquiry into CBA explored the root causes of how such incidents could occur in a bank of such high standing. The findings and recommendations around frameworks, operating effectiveness and culture have informed industry inside and outside of financial services.

Global lessons

In the global financial centres, response from the general public and their elected representatives was severe, with regulators accused of not policing the industry adequately. This was swiftly followed by funding increases to bolster regulators’ capabilities, and broad political support and demands for them to take a stronger position. Oversight and pressure increased substantially, with significant new regulation in the US, Europe and US implemented. Estimates of fines received by the global banking industry reached $300 billion USD.

As part of this acute pressure to manage risk more effectively, a number of key components of the risk management framework evolved substantially at global firms – and continue to do so. These themes are instructive given Australia’s current challenges, and are reflected in APRA’s Prudential Inquiry into CBA.

The board’s role

The board’s role has become far more prominent, albeit posing challenges in maintaining a working line between governance and management. Boards are increasingly expected to have a public and internal voice, to set their expectation and tolerance for risk, and to emphasise the importance of integrity. They need to trust their executive team, but have measures to verify this trust.

For example, to provide additional data points outside their formal executive updates, boards internationally have supplemented existing formal committees with informal and occasional opportunities to meet with risk owners. These allow board members to gain a better understanding of specific risks, understand how management monitors these risks on a day-to-day basis, and agreeing from an informed position as to what makes sense for a board member to monitor. Existing aggregated or averaging risk metrics can be substituted with more meaningful and pinpointed measures that can highlight emerging risks more quickly, minimising reputation risk.

Accountability in focus

Accountability has become a core focus, with a swing toward ensuring that business owners (‘first line’) own their offering end-to-end. Increasingly business heads are tasked with making sure that they and their firms have everything in place they require to adequately manage the inherent risk in their business: no matter who they are dependent on. Accountability has become a core focus, with a swing toward ensuring that business owners (‘first line’) own their offering end-to-end. Increasingly business heads are tasked with making sure that they and their firms have everything in place they require to adequately manage the inherent risk in their business: no matter who they are dependent on.

Arguably these business heads wield the most influence within organisations, so pairing their typically higher compensation with unambiguous accountability for oversight aims to minimise the risk that something ‘falls between the gap’ between the many divisions and functions that support a business.

Boards are asking: do we set the tone that my business heads are fully accountable? Do our business executives have enough authority to influence those they are dependent on, or is this accountability in name only? Does the way we engage executives send a clear message that ‘first line’ or the business is on the hook? Have any of our executives ever been penalised for ‘dragging their heels’ on managing risk, or do we only wait for outright misconduct to act?

Compliance has changed

The role of the Compliance function has also evolved significantly. Historically, Compliance tried to eliminate risk by carefully checking against regulatory or legal compliance (i.e. “Can we do this?”). Now the role at most global institutions is expected to assess and manage risk by asking the question: “Should we do this?”

This has compliance staff effectively playing the role of the independent ethical challenge within organisations, which has a number of implications that boards are increasingly considering. Are the key people in this role equipped for the new expectations? Are they properly interleaved in the organisation’s decision-making processes including strategy and investment governance, or are they confined to more operational activities? Does this ethical ‘release valve’ (Compliance or an equivalent) have a genuine line to the board to provide them with that alternative viewpoint which will protect the board when it really matters?

Risk culture needs assessment

Risk culture (or at least firm culture as it pertains to managing risk), needs to be assessed multi-dimensionally across the organisation, and will typically need more than a staff survey.

What does the board and executive team think and communicate to the rest of the organisation? What does middle management hear, and how do the actions of those above them influence them to act, irrespective of the official communicated corporate ‘values’? What are the competing pressures in middle management that might create conflicting incentives? In addition, what do the rest of the staff perceive, and do they see management ‘walk the talk’?
Remuneration and incentives

Linked to accountability are the complexities of remuneration and incentives. Global financial institutions have increasingly adopted deferred compensation including malus and clawback policies that allow them to apply consequences in the future for today’s poor behaviour. Risk measures in scorecards and risk modifiers are becoming standard, and Risk division input into compensation is being used to demonstrate that financial performance at all costs has a counterweight.

Board members are evaluating: Does my remuneration committee have Risk representation? Is Risk input on compensation limited to group executives only? Are risk considerations in my performance and remuneration structures balanced enough with incentives for financial or operational performance? Will our incentive structure lead our staff to prudent risk/reward trade-offs, or are they actually structurally geared to encourage risky behaviour?

The journey ahead

Boards and executives are in the process of evaluating how their firms’ shape up to these themes and questions that were identified in the APRA CBA Inquiry, as well as during the Royal Commission. There is a significant multi-year journey ahead of the financial services industry, but a wealth of experience from other jurisdictions that are further down this path.

As the industry collectively reflects, and many firms highlight their gaps, careful thought should be given to the remediation efforts that are proposed. Are these proposed changes realistic? Are they sustainable or will they deteriorate when profits are challenged? Are we comfortable that we can achieve these in the targeted timeframe given the likely increase in oversight anticipated?

Finally – whilst financial services responds to the intense pressure to reform, a number of non-financial sector organisations are using this opportunity to assess their own operations. Many, if not all of the findings have a parallel outside financial services, and addressing these proactively before problems arise has obvious financial and reputational benefits.
Cultural drivers of organisational performance - why the ‘soft stuff’ matters

Over the past year, almost half of Australian company directors indicated that their board has had to deal with issues that can affect trust in their organisation. The most critical issue relating to trust was reported to be ‘internal culture and practices’.

The number of large corporate collapses in the past two decades has shed light on the importance of establishing effective internal control systems in organisations to protect stakeholders’ interests, and has elevated corporate governance to prominence. In much the same way on a more recent scale, corporate scandals including those affecting Volkswagen and the Banking Royal Commission, have brought organisational culture to the forefront of consideration when it comes to impact on internal control systems.

For those corporate failures in the early 21st century, the common themes involved a lack of commitment and accountability across the organisation, and the acceptability of self-interest and unethical behaviours.

Now, these same themes are echoed from the findings of the Banking Royal Commission. The prevalence of similar conduct occurring across all of the major entities indicates that characterising misconduct as merely ‘a few bad apples’ ignores the root causes of conduct, which often lie within the systems, processes and culture cultivated by an entity. Such culture risks are pervasive across all levels of an organisation, and unless identified and accounted for within an organisation’s culture, can critically undermine the effectiveness of even the most robust internal control system.

Organisational culture

Organisational culture is set by top management and is essentially ‘what people do without being told to do’. Cultural norms are a critical driver of control, both at a process and an entity level, by conveying expectations for acceptable behaviours and compliance with internal processes. These norms require continuous management to ensure that desired and ethical behaviours are exhibited, and to ensure that behaviour-influencing factors, or so-called ‘soft controls’, do not undermine the achievement of organisation objectives.

The upshot of this is that a positive organisational culture can effectively mediate gaps in an internal control system by influencing behaviour as part of a holistic internal control system. Similarly, it can prevent the negative impacts on efficiency and effectiveness associated with excessive and redundant layers of hard controls.

Culture and the role of Internal Audit

Whilst traditional Internal Audit methodologies do not sufficiently assess culture or consider behavioural drivers, leading Internal Audit functions are acting now to evolve their audit programs to include cultural assessments of these soft controls.

Historically, when things go wrong within an organisation, the response has been to add layers of hard controls such as additional authorisations, reduced delegations, or extra performance metrics to attempt to close the gap. However, we know from experience that increasing layers of hard controls does not necessarily improve organisational performance. People are at the heart of every organisation, and it is the human factors that drive decision-making, organisational performance, and the effectiveness of the system of internal control.

Assessing these human factors can be incorporated in several ways, most notably:

- adding cultural considerations to existing internal audits (e.g. behavioural root cause analysis)
- performing stand-alone culture internal audits and
- expanding the typical Internal Audit universe to include areas with cultural salience, or that may indicate red flags (e.g. whistle-blower hotlines, incentive programs, employee engagement).

Across these three approaches, Internal Audit is well placed within organisations to support increased awareness and capability to manage cultural and behavioural considerations, particularly in the following capacities:

Figure 1. Cultural red flags
- Pursuit of short-term financial benefits with little to no consideration of customers.
- Focus on the letter rather than the spirit of the law and regulations.
- Regarding risk management and controls as an inconvenience.
- Lack of prompt, proper management action to address known issues.
- Active concealment of problems, lack of openness.
- Failure to challenge the status quo.

- Serving as a culture promoter: Starting and supporting dialogue with boards and executive leadership about the critical connection between culture, strategy and risk; helping the board understand their role in culture and to gain buy-in from top management.
- Understanding the current state: Considering how cultural expectations have been defined, communicated, understood and embedded. To measure the organisational culture, internal auditors may apply root cause analysis, observe behaviours and consider what data is available in the organisation to gain insight into culture (e.g. exit interviews, engagement survey results, hotline reporting). Traditional data inputs can then be complemented by other audit procedures including surveys, facilitated workshops, focus groups and advanced analytical techniques like sentiment analysis.
- Evaluating culture over time: Understanding perceptions about what is happening within the organisation, what is working well, and what are the barriers to achieving organisational goals, including key red flags that may be present (see figure 1).
- Providing insights and promoting collaboration: Sharing what other organisations are doing, and collaborating with different lines of defence to evolve the framework.
As a result, Internal Audit can play a strategic role as a culture advisor within an organisation without overstepping its remit or abandoning current approaches to conducting audits. Deficiencies in either cultural or behavioural factors can lead to significant risk exposure, and should be reported to leadership and boards to allow for more informed decision making and to drive meaningful cultural change. Considering soft controls in internal audits will enable boards to receive thematic analysis of behavioural trends over time, challenge management insights, uncover hidden behavioural drivers to allow for improved remediation, and provide a better understanding of what is ‘really’ going on in the organisation.

Similarly, as culture is a critical factor in the achievement of organisational objectives, Internal Audit can add value by assessing existing culture and providing recommendations to management as input for the design of more efficient internal control environments that are able to account for both hard and soft controls, and take advantage of their respective strengths and weaknesses.

Our approach
It is necessary to consider the human factors that influence culture to really understand what is happening within an organisation. In response to this, KPMG has developed a model that integrates a consideration of soft controls into our audit and assurance methodology to help us identify, measure, monitor and report on staff behaviours and its impact on the control environment. The model is based on extensive scientific research by Prof. Dr. Muel Kaptein, a partner from KPMG Netherlands and global subject matter expert, and has been in use in the Netherlands for over 10 years. Visit our website for more information on the model.
Data is fast becoming one of the most important intangible assets for organisations. Data sets organisations apart, enabling better product development, and personalised service offerings, making it a source of competitive edge.

However, the growing commoditisation of data and the advent of serious data breaches across jurisdictions and industries has called for sweeping regulatory change to codify accountability and transparency.

Regulations such as the Notifiable Data Breaches scheme (NDB scheme) and General Data Protection Regulation (GDPR) are lifting the standard on security measures, organisation-wide data awareness, and restoring trust and ownership of personal data with consumers. These regulations also seek to increase accountability for breaches. Fines are only the beginning of the likelihood of breaches.

Boards are increasingly facing data related risks and issues. New regulation, and community expectations, need to be balanced with strategic objectives for digital transformation, reducing operational costs, and retaining competitiveness while delivering on the value proposition. Data lakes and organisation-wide practices need to be understood, and the controls for ethical use and protection of this data need to be monitored and communicated at all levels.

Some of the key data related issues facing boards today are governance, regulation, consumer trust, security, preparation and response, and data strategy and technology innovation.

Goverance
Good governance has never been more critical. In an environment of sweeping regulatory change and heightened consumer awareness of data risks, conflicts often arise between data mining mandates, legal requirements and ethical consumer considerations. Asymmetrical dissemination of privacy risk appetite throughout the organisation, and disempowered risk governance across delegations of authority, usually result in revisiting decisions and potentially higher costs to rectify poor privacy compliance solutions.

Without clear guiding principles regarding how an organisation treats consumer data, there remains risk of grey areas. In relation to consumer data, good governance means:
- data principles that align with consumer expectations, board risk appetite, and organisation values
- enforcing, monitoring and reporting in relation to data governance and controls
- mechanisms for monitoring regulatory change
- clearly defined roles and responsibilities, with empowering delegations of authority
- managing conflicts with business uses of data, and secondary uses
- ensuring data principles are instilled throughout the organisation through regular training, enforcement and real consequences.

Without good governance, the framework for data management will not be clear, and there is likely to be less visibility of data practices, therefore leading to a higher likelihood of breaches.

Regulation
Since 22 February 2018, notification of eligible data breaches became mandatory in many cases to the Office of the Australian Information Commissioner and affected individuals through the NDB scheme. This is the first time in Australia that all entities that are covered under the Australian Privacy Principles have clear obligations to report on eligible data breaches. A critical part of being able to comply with the NDB scheme is preparation. Entities need to know what information they have, where it is stored, how it is protected, how they’ll know when a data breach has occurred, and then how they’ll respond.

Since 25 May 2018, the GDPR came into force with extraterritorial reach that has implications for Australian businesses that offer goods and services to individuals in the EU, and/or monitor EU individuals. This regulation introduced significant requirements for understanding organisation data processing activities (records of processing), providing significant data subject rights such as the right to be forgotten, and data breach reporting requirements of 72 hours from the point of awareness. Broadening the brush stroke of this regulation are the fines, which range from £20 million to 4% of annual global turnover or whichever is higher.

There is significant compliance burden, and risk of reputational and financial loss entailed in meeting these imposing obligations. In raising the bar for transparency and accountability for personal data managed by organisations, these regulations are also a source of many unknowns for non-EU organisations as the enforcement has yet to be tested by privacy regulators.

Upcoming regulation called the Consumer Data Right will start with Open Banking and ultimately be implemented across the entire market, with the energy and telecommunications industries next.

Consumer trust
The Australian Community Attitudes to Privacy Survey 2017 found that privacy awareness was growing, however the majority of respondents did not use, or did not know how to use, simple safeguards such as clearing cookies to protect their privacy.

In 2018:
- Approximately 150 million customer accounts, including personal emails and passwords, were affected by the MyFintech breach of March 2018.
- Orbitz, a travel site owned by Expedia, also disclosed a breach that resulted in unauthorised access to 880,000 personal credit card details for customers who booked travel over 2016 and 2017.
- Cambridge Analytica used the data of 50 million Facebook customers without consent to build psychological profiles so voters could be targeted with ads and stories.

Such data breaches, and the approaches to resolution for affected individuals, indicate a shift in accountability and transparency. The NDB scheme and GDPR most notably brought into effect mandated data breach investigation and reporting timeframes. These laws also increased accountability through introducing significant fines. Breaches also impact reputation due to public reporting.
However, regulation alone is not enough. Attitudes of organisations towards their customer’s personal data and consumer expectations about the fair use of their data need to align. Customers expect organisations to fulﬁl service and product obligations, remain competitive and proﬁtable, while also protecting their privacy interests.

One way organisations can achieve this is through transparency over internal and external data ﬂows, communicated through clear, concise privacy statements. Giving consumers control over how their data is collected, and making the processes for setting such preferences easy and amenable to different customer groups, also need to be considered.

Underpinning this is how serious organisations are about data protection. Organisations must be assured that third party arrangements preserve customer privacy interests. Further, investments in sustainable technology solutions, and automation of manual processes can improve the efﬁcacy of privacy management.

Security
Strategic objectives for technology transformation, use of social media engines and upgrading legacy systems increase exposure to the risk of cyber-attacks. With organisations becoming more interconnected and reliant on complex IT systems, exposure to cyber-attacks has become more sophisticated, frequent, targeted and difﬁcult to detect. As a result, cyber-related crime is one of the highest rated risks facing organisations today.

New regulation seeks to instil requirements for having adequate safeguards that are commensurate with the scale/impact of threats to which an organisation is exposed. Organisations should also have active measures to protect personal information held, while also having measures to ensure data troves are not retained unnecessarily. These requirements are reﬂected in APP 11, Article 32 of the GDPR, and current draft APRA prudential standard CPS234 information security.

It is incumbent on organisations to take appropriate and proportionate technical and organisational measures to manage security risks. Organisations can achieve this by integrating preventative measures to safeguard privacy, raising awareness of every employee’s role in data protection, and distributing responsibility across all levels of an organisation. To tackle the increasing threat of cyber security, common controls embedded throughout organisations include:

- pseudonymisation and encryption
- conﬁdentiality, integrity, availability and resilience of processing systems
- restoring availability and access to personal data following a cyber-attack
- monitoring and supervision of technical and organisational measures.

Preparation and response
The ability to quickly detect, respond and recover from a cybersecurity event has never been more critical, with the volume of cyber-attacks at an all-time high, and the ever-evolving local, and global legislative environment.

Cyber risk poses an asymmetric threat to governments and businesses alike. Hacktivists, insiders, criminals and nation states have a range of motives for stealing, disrupting or destroying information and the systems that they rely upon. Couple this with the increasing pace of technological development, and the growing dependence of organisations on digital information and interconnectivity, and you have a challenging business risk which requires a dynamic solution.

Investors, governments and regulators are increasingly challenging board members to demonstrate diligence in the area of cybersecurity. Regulators expect personal information to be protected, and systems to be resilient to both accidental and deliberate attacks.

One of the most common causes of a failed response is inadequate preparation, and many organisations suffer signiﬁcant brand, reputational and ﬁnancial impact as a result of poor planning processes, and disproportionate or inadequate incident response capabilities. It is critical that cyber risks are understood, clear and deﬁned responsibilities exist, and response plans are current, practical, and most importantly, tested.

Restoring trust and minimising reputation damage is a signiﬁcant challenge to organisations, and without a strategy that encompasses more than just security, the fallout from a breach is likely to be signiﬁcant. The combination of people, privacy, information governance and business resilience is key to managing cyber risk.

Data strategy and tech innovation
As organisations seek to improve the customer experience and secure the competitive advantage associated with brand trust, it is crucial to leverage customers’ personal information assets in the most appropriate way. Organisations strategies often lean on the analytics potential of big data to drive competitive positioning for operational efﬁciency and improved product offerings. However, this needs to be tempered with the risk of cyber and data breaches, and requirements for data minimisation.

Quality data is at the heart of a strong data strategy which includes automation and AI initiatives to replace and enhance existing business processes. However, large lakes of unstructured data can hinder the ability to access effective insights. Further, boards are concerned about the mismatch in maturity of organisation-wide data governance practices with the speed of automation deployment. This generally results in organisations taking on more risk than contemplated in project phases. This is where effective Privacy Impact Assessments (PIAs) are critical to ensuring personal data risks are detected and managed.

Further, automation and AI bring new risks, such as potential biases in those writing algorithms, ineffectiveness of existing controls to monitor performance of algorithms, and lack of suitability of existing risk frameworks to extend over analytics practices. Therefore, existing employees will need to invest in training to learn new skills as their roles evolve.
Looking forward

We have explored some key risks facing boards today. As the pace of automation, investment in new technologies, and machine learning accelerates, new regulations and community expectations will need to be navigated to ensure personal data is adequately protected. However, new regulation and the fear of customer expectations should not be a hindrance to evolving business practices, being courageous in exploring analytics, and designing tailored products for consumers that offer price, choice and flexibility. While consumer awareness of data privacy is currently at its highest measured levels, organisations need to finely balance these heightened expectations with meeting efficiency and competitiveness objectives. Organisations should not be afraid to use the data they have, as long as they have confidence that it is well protected, backed by lawful processing and anonymised or pseudonymised where appropriate.

Building consumer trust by enforcing strong policies around data governance, protection and consumer control will be the difference between organisations that thrive and those that fall behind.

For further information, view the videos here.
Operating in today's complex and dynamic world, boards are constantly challenged to respond to emerging macro and micro economic trends and disruptions in their markets. Business agility and robust decision-making are critical to boards and executives for organisations to stay competitive and on top of emerging trends.

The right skills and diversity at the boardroom table are needed for good decision making. However, considering diverse views, and making effective and efficient decisions is not a simple task. The dynamics in a boardroom when we look at the different personalities, communication styles, perspectives and politics that can be brought to the discussion, makes decision-making difficult, even with the presence of a skilled Chair and collegiate director.

Arriving at a decision in the face of difficult or contentious topics takes time, often requiring consultation, analysis and engagement.

The science of making good decisions tells us that:

- The wisdom of the crowd (relevant and diverse skills) gives a better decision than the individual.
- Removing as much of the bias, including leading, anchoring, or the risk of following the most senior or loudest person’s view in a group discussion is critical for effective team decision-making.
- Replaying a group’s views for further discussion and analysis helps better quality decisions.

To achieve the best possible decision making process we need to reduce the bias from board decision-making through:

- giving equal weight to every director’s perspectives
- contributing views independently and anonymously
- using a data-based, quantifiable and objective approach.

For boards to foster an environment where directors feel their individual perspectives will be considered equally and without recourse, online collaboration and data aggregation is a powerful way to achieve this. The ability to include everyone’s views quickly and easily online, playback to directors objectively in a way that reflects the sentiment around the boardroom table, and to focus the discussion on key points of difference, all contributes to more effective board decision-making.

Digital tools to achieve this offer the benefit of enabling physically absent directors to participate in key decisions by participating remotely online.

KPMG has developed a tool called Facilitator View, that achieves all of the above objectives and provides not only real time reporting of aggregated views, but intelligent heat-mapping of individual perspectives versus the aggregated group position on an anonymous basis. It enables time to be spent clarifying understanding and reaching consensus.

The application is designed to enable discussion and collaboration, and is a game changer in helping directors make effective and efficient decisions quickly.

For further information, click here.

Authors:
Kevin Smout
Partner
Risk Strategy & Technology
KPMG Audit, Assurance & Risk Consulting, ASPAC
Head of KPMG Internal Audit & Risk Consulting Services

Jane Barker
Associate Director
KPMG Audit, Assurance & Risk Consulting

From discussion to decision – effective board decision-making

What we’ve learned talking to 150 directors about trust and modern slavery

A non-financial crisis

Cultural drivers of organisational performance – why the ‘soft stuff’ matters

Board talk – dealing with data privacy

For further information, click here.
For further discussion on boardroom topics, join us at the KPMG sponsored AICD Governance Summit from 4 and 5 March 2019 at the International Convention Centre Sydney.