Managing Culture

A good practice guide

First Edition, December 2017

The Institute of
Internal Auditors
Australia

THE
**ETHICS
CENTRE**

**Governance
Institute**
of Australia

CHARTERED ACCOUNTANTS™
AUSTRALIA + NEW ZEALAND

Contents

Foreword

It's a common perception that regulators retreat from risk. Not so – risk is a part of all business activity.

The emphasis an organisation pays to its business risks sets the scene for the conduct of its employees and determines how risks are identified, understood, discussed and acted upon.

From an ASIC perspective, we have a regulatory interest in risk of misconduct and culture because it is part of our vision that investors and consumers have trust and confidence in the financial system.

As a conduct regulator, we invite boards and senior executives to take action and consider conduct issues, particularly where poor conduct has the capacity to cause damage to customers or to the integrity of the markets. In our view, it is in the interests of organisations for senior managers and the board to be focused on conduct within their firm, and this is about asking the right questions and seeking the right information to deal with conduct risk.

In this book, the Institute of Internal Auditors – Australia (IIA-Australia) in collaboration with The Ethics Centre, Chartered Accountants ANZ and the Governance Institute of Australia, have explored the foundational elements of a sound risk culture. Appropriately, these elements set the management of risk within a broader organisational culture context, and the perspectives of a broad field of researchers, regulators and thinkers in culture and ethics are presented.

The multidimensional approach to exploring risk culture written about here draws out best practice and informs pathways to change. Importantly though, a chapter is assigned to the roles and responsibilities for those who govern and direct businesses. The book explores good governance principles, and the way established systems of work can influence conduct and culture.

Trust, like beauty, is in the eye of the beholder. If consumers don't like the way a firm has behaved, they can take their business elsewhere and tell everyone else about it through the wonders of social media. Loss of reputation due to poor conduct destroys value in a firm. Even more challenging is that poor conduct may be technically within the law, but still have a negative impact on a firm's reputation.

It can take a long time to build trust and confidence. However, the same trust and confidence can be lost very quickly when there is misconduct, and can take even longer to restore. The possible loss of trust and confidence is a key business risk. If the culture and conduct of a firm genuinely reflects 'doing the right thing', this mitigates conduct risk and will be rewarded with longevity, customer loyalty and a sustainable business.

I acknowledge that improving organisational culture can be hard work.

Culture can be viewed as a deal made between executives and their staff, between the company and its customers and investors, and with the broader public.

Boards and senior executives have the opportunity to make sure that the kind of deal an organisation makes with its employees, customers, investors and the public is a fair one.

John Price
Commissioner, Australian Securities & Investments Commission
December 2017

Executive summary

In Australia, the regulators Australian Prudential Regulation Authority (APRA) and Australian Securities and Investments Commission (ASIC) have both signalled that there are significant risks around poor corporate culture. ASIC recognises that culture is at the heart of how an organisation and its staff think and behave, while APRA directs boards to define the institution's risk appetite and establish a risk management strategy, and to ensure management takes the necessary steps to monitor and manage material risks. APRA takes a broad approach to 'risk culture' – including risk emerging from a poor culture.

> 'Poor culture can undermine ... trust and confidence. By contrast, good culture, which is more conducive to good conduct, helps maintain trust and confidence.'
>
> John Price, ASIC Commissioner

Regulators across the globe are grappling with the issue of risk culture and how best to monitor it. While regulators generally do not dictate a cultural framework, they have identified common areas that may influence an organisation's risk culture: leadership, good governance, translating values and principles into practices, measurement and accountability, effective communication and challenge, recruitment and incentives. Ultimately, the greatest risk lies in organisations that are believed to be hypocritical when it comes to the espoused versus actual culture.

The board is ultimately responsible for the definition and oversight of culture. In the US, Mary Jo White, Chair of the Securities and Exchange Commission (SEC), recognised that a weak risk culture is the root cause of many large governance failures, and that the board must set the 'tone at the top'.

Culture also has an important role to play in risk management and risk appetite, and can pose significant risks that may affect an organisation's long-term viability.

However, culture is much more about people than it is about rules.

This guide argues that an ethical framework – which is different from a code of ethics or a code of conduct – should sit at the heart of the governance framework of an organisation. An ethical framework includes a clearly espoused purpose, supported by values and principles.

There is no doubt that increasing attention is being given to the ethical foundations of an organisation as a driving force of culture, and one method of achieving consistency of organisational conduct is to build an ethical framework in which employees can function effectively by achieving clarity about what the organisation deems to be a 'good' or a 'right' decision.

Culture can be measured by looking at the extent to which the ethical framework of the organisation is perceived to be or is actually embedded within day-to-day practices. Yet measurement and evaluation of culture is in its early stages, and boards and senior management need to understand whether the culture they have is the culture they want.

In organisations with strong ethical cultures, the systems and processes of the organisation will align with the ethical framework. And people will use the ethical framework in the making of day-to-day decisions – both large and small.

Setting and embedding a clear ethical framework is not just the role of the board and senior management – all areas can play a role. This publication provides high-level guidance to these different roles:

- **The board** is responsible for setting the tone from the top. The board should set the ethical foundations of the organisation through the ethical framework. Consistently, the board needs to be assured that the ethical framework is embedded within the organisation's systems, processes and culture.
- **Management** is responsible for implementing and monitoring the desired culture as defined and set by the board. They are also responsible for demonstrating leadership of the culture.
- **Human resources** (HR) is fundamental in shaping, reinforcing and changing corporate culture within an organisation. HR drives organisational change programs that ensure cultural alignment with the ethical framework of the organisation. HR provides alignment to the ethical framework through recruitment, orientation, training, performance management, remuneration and other incentives.
- **Internal audit** assesses how culture is being managed and monitored, and can provide an independent view of the current corporate culture.
- **External audit** provides an independent review of an entity's financial affairs according to legislative requirements, and provides the audit committee with valuable, objective insight into aspects of the entity's governance and internal controls including its risk management.

Introduction

The discussion around corporate culture has increased around the globe and regulators have progressively focused on the importance of a good risk culture and strong governance frameworks.
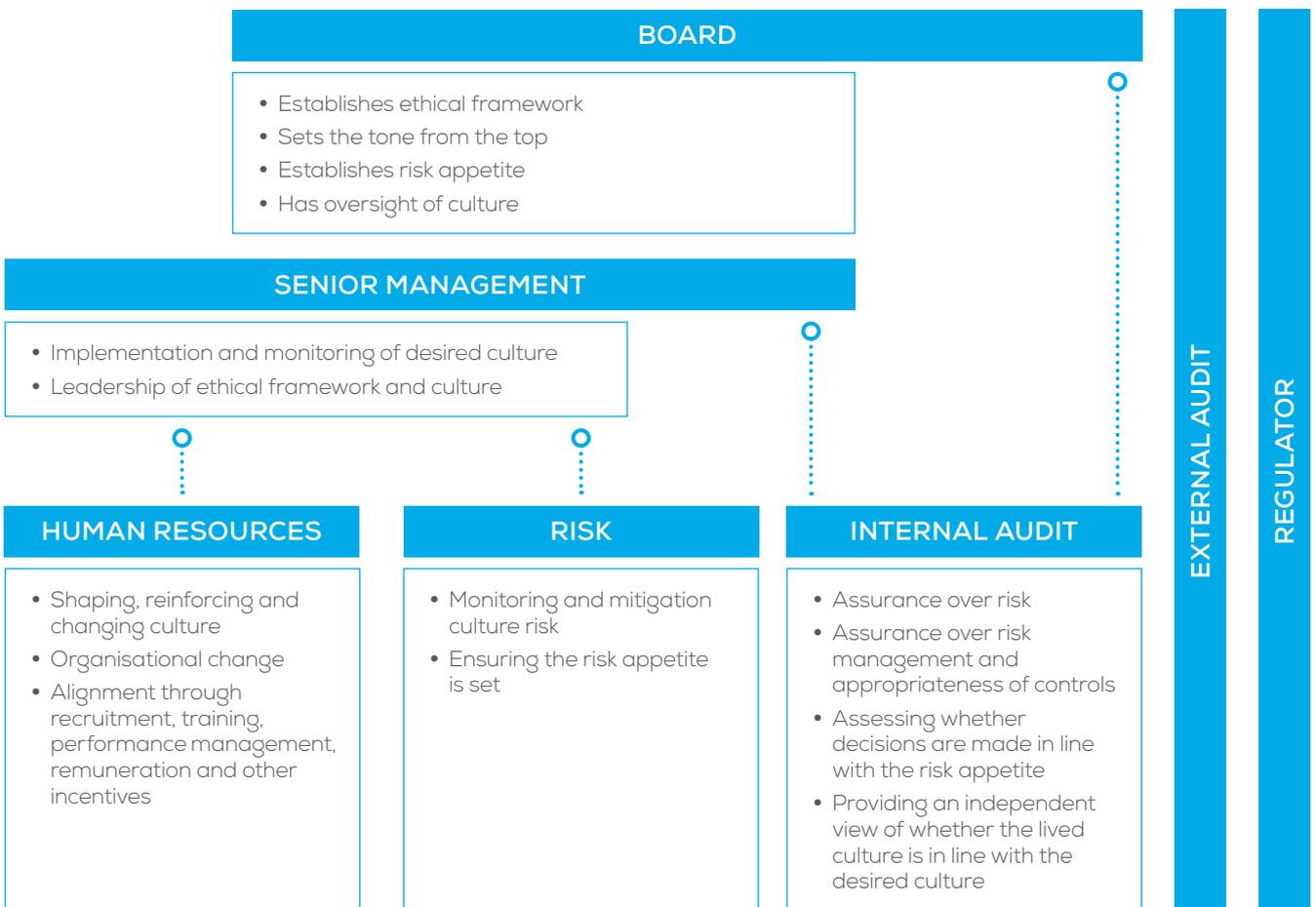
There are a number of approaches to better understand and have oversight over corporate culture. This guide outlines how organisations can approach the topic of culture, the role of ethics, and recent regulatory developments in Australia and overseas. It will assist directors, boards, audit committees and senior managers in understanding the connection between ethics, culture and risk governance, risk appetite and compensation as 'foundational elements of a sound risk culture' (as the UK Financial Stability Board has outlined).

In Australia, the regulators Australian Prudential Regulation Authority (APRA) and Australian Securities and Investments Commission (ASIC) have both signalled that there are significant risks around poor corporate culture. Indeed, regulators across the globe are grappling with the issue of risk culture and how best to monitor and evaluate it. While regulators generally do not dictate a cultural framework, they have identified common areas that may influence an organisation's risk culture: leadership, good governance, translating values and principles into practices, measurement and accountability, effective communication and challenge, recruitment and incentives.

An organisation's culture is the sum of its shared values, principles and behaviours. Culture is a key determinant in the performance of an organisation and its ability to achieve its objectives. It goes to the heart of the openness and transparency needed for effective stewardship and informed decision-making.

This guide argues that an ethical framework – which is different from a code of ethics or a code of conduct – should sit at the heart of the governance framework of an organisation. It gives direction as to how an organisation might understand the state of their current culture, as well as monitor the culture going forward. It also provides direction on how to achieve an ideal culture, which is in alignment with the ethical framework of the organisation.

Setting and embedding a clear ethical framework is not just the role of the board and senior management – all areas can play a role. The UK Financial Reporting Council noted in *Corporate Culture and the Role of Boards* that human resources, internal audit, ethics, compliance and risk functions should be empowered and resourced to embed values and assess culture effectively. This guide sets out the roles of different players across the organisation, outlining how they can contribute to an effective culture.

BOARD

- Establishes ethical framework
- Sets the tone from the top
- Establishes risk appetite
- Has oversight of culture

SENIOR MANAGEMENT

- Implementation and monitoring of desired culture
- Leadership of ethical framework and culture

HUMAN RESOURCES

- Shaping, reinforcing and changing culture
- Organisational change
- Alignment through recruitment, training, performance management, remuneration and other incentives

RISK

- Monitoring and mitigation culture risk
- Ensuring the risk appetite is set

INTERNAL AUDIT

- Assurance over risk
- Assurance over risk management and appropriateness of controls
- Assessing whether decisions are made in line with the risk appetite
- Providing an independent view of whether the lived culture is in line with the desired culture

EXTERNAL AUDIT

REGULATOR

Chapter 1 – Regulatory context

Culture in regulator standards and governance codes

Following the events of the global financial crisis (GFC), prudential and corporate regulators have strongly emphasised the importance of restoring trust and integrity to financial markets and have focused on culture as a key risk area and therefore central to governance and risk management frameworks within companies. This shift in focus arose from widespread agreement that failures of culture, which permitted excessive risk-taking, were at the heart of the GFC.[1] The Financial Stability Board, which coordinates national financial authorities and international standard-setting bodies, cited weak risk culture as 'a root cause of the global financial crisis, headline risk, compliance events.'[2]

While concentrating on financial services organisations in the first instance, many regulators have clarified that all organisations participating in the markets should focus on culture as a key to achieving and rewarding good conduct and good outcomes for customers and restoring trust and confidence in markets.

Australian regulatory responses

ASIC has repeatedly addressed the need for companies to address culture in a range of speeches given by the Chairman and Commissioners.[3] In Australia too, the emphasis at first was on financial institutions, but ASIC soon made it clear that it considers that all companies need to reflect upon how they are addressing the risks of poor culture and poor conduct. ASIC has defined conduct risk as[3] 'the risk of inappropriate, unethical or unlawful behaviour on the part of an organisation's management or employees which can be caused by deliberate actions or may be inadvertent and caused by inadequacies in an organisation's practices, frameworks or education programs.'

ASIC's legislation includes a key responsibility to promote the confident and informed participation of investors and consumers in the financial system. In many speeches, ASIC makes the point that since ASIC is a conduct regulator, it plays an important supervisory role, particularly where poor culture has the capacity to undermine trust, confidence and market integrity. The Chairman of ASIC has stated more than once that 'Culture matters to ASIC because poor culture can be a driver of poor conduct – and we regulate conduct.' ASIC considers culture to be a key risk area with respect to its role as a conduct regulator, as often it is a red flag to broader regulatory problems.

ASIC has indicated it will be focusing on poor culture as a way to detect early warning signs, which will help it to identify pervasive problems within a company as well as individual instances of misconduct.[4] It has incorporated culture into its risk-based surveillance reviews, covering the individual elements of culture, for example remuneration, breach reporting, whistleblower policies and complaints handling.

The Chairman has noted that 'Where we think there may be a problem, we will ask questions and do a "deeper dive". This helps us to not only identify instances of misconduct, but also broader, more pervasive conduct problems. We want to uncover these problems early – and to disrupt and address them.'[5] As part of those 'deeper dives', ASIC has held discussions with boards where it has detected signs of poor culture, as it is focused on the role of boards and management in driving culture.

APRA has also taken a direct interest in culture, linking it to the governance and risk management responsibilities of boards. APRA has noted that the GFC not only revealed deficiencies in how the financial services sector managed risk but also in the attitude taken towards risk by financial institutions. APRA has stated that:[6]

> In combination, a poor risk culture and weak risk management (the former often being the root cause of the latter) led to unbalanced and ill-considered risk-taking, to significant losses and, in some cases, to institutional failures. The impact on the financial stability of affected countries was significant.

APRA, as part of its CPS 220 requirements, directs boards to define the institution's risk appetite and establish a risk management strategy; and to ensure senior management takes the necessary steps to monitor and manage material risks consistent with the strategic objectives, risk appetite statement and policies approved by the board.[7] In its regulation of 'risk culture, APRA's standard CPS220, effectively requires that regulated Boards must[8]:

- Specify the quality and character of the culture that they seek to attain typically done in terms of core Purpose, Values and Principles. Most importantly, Boards are responsible for shaping the organisation's culture – not APRA.
- Measure the extent to which the actual culture aligns with the ideal.
- Develop and implement measures to close any identified gaps between actual and ideal.

1   International Monetary Fund, *Global Financial Stability Report: Risk Taking, Liquidity, and Shadow Banking – Curbing Excess While Promoting Growth, October 2014; Financial Stability Board, Guidance on Supervisory Interaction with Financial Institutions on Risk Culture: A Framework for Assessing Risk Culture*, 7 April 2014

2   Financial Stability Board, *Guidance on Supervisory Interaction with Financial Institutions on Risk Culture: A Framework for Assessing Risk Culture,* 7 April 2014

3   See page 35 Speeches. ASIC, Market Supervision Update Issue 57, 2015 <http://asic.gov.au/about-asic/corporate- publications/newsletters/asic-market-supervision-update/asic-market-supervision-update-previous-issues/market-supervision-update-issue-57/>.

4   'ASIC's focus on culture – digging into the detail digging into the detail', a speech by John Price, Commissioner, ASIC to the GIA's Corporate Governance Forum 2016 (Sydney, Australia), 25 May 2016, http://asic.gov.au/about-asic/media-centre/speeches/asic-s-focus-on-culture-digging-into-the-detail/.

5   'Culture shock', a speech by Greg Medcraft, Chairman, ASIC at ASIC Annual Forum 2016 (Hilton, Sydney), 21 March 2016.

6   APRA, 'Information Paper: Risk Culture', October 2016.

7   APRA Prudential Standard *CPS 220 Risk Management,* January 2015.

8   APRA Prudential Standard *CPS 220 Risk Management,* January 2015.

APRA's 'Information Paper: Risk Culture', it has specifically linked the oversight and implementation of risk management with culture.

Following on from the House of Representatives Standing Committee on Economics *Review of the Four Major Banks,* the Commonwealth government in its 2017/18 budget has brought forward a comprehensive package of reforms aimed at strengthening accountability in the banking system. As part of this package the government has announced that it will legislate to introduce a new Banking Executive Accountability Regime, which, among other things, is aimed at making it easier to hold senior individuals to account for poor conduct and behaviour in carrying out their responsibilities, and implementing changes in banks' remuneration policies to better align the realisation of risk with reward.

UK regulatory responses

In the UK, both the prudential regulator (the Prudential Regulation Authority – PRA) and the conduct regulator (the Financial Conduct Authority – FCA) have highlighted the importance of culture. The PRA has stated that 'The culture of a firm has a significant impact on the PRA's objectives of promoting the safety and soundness of firms, and, for insurers, an appropriate degree of protection for policyholders.'[9] The FCA has stated that culture is a priority as 'Culture drives individual behaviours which in turn affect day-to-day practices in firms and their interaction with customers and other market participants.'[10]

The PRA has stated that it will use its powers to address cultural issues, as part of its overall approach to supervision.[11] This includes ongoing contact with the organisation; reviews of the prudence of valuation methods; assessments of the firm's risk management processes and overall risk awareness; remuneration policies; the ability to challenge senior management; and board effectiveness reviews.

In the UK context, there is a recognition that a culture of personal responsibility has to be embedded in firms, in order to drive the appropriate culture. Following the recommendations of the Parliamentary Commission on Banking Standards,[12] the Senior Managers and Certification Regime was created in statute. At the core of this regime is ensuring that personal accountability is clear, and that managers are accountable.

US regulatory responses

In the United States, former Securities and Exchange Commission (SEC) Chair Mary Jo White spoke of weak risk culture as the root cause of many large corporate governance failures, and of deficient corporate cultures being frequently the cause of the most egregious securities law violations.[13] The SEC has significantly increased its focus on board oversight of corporate culture generally, and risk culture in particular.

Hong Kong responses

The Hong Kong Regulatory Authority has also recognised the importance of a sound corporate culture. In their letter of 2 March 2017 to all authorised institutions, it noted that more needs to be done to promote a sound culture in banks, and requested that banks adopt a 'holistic and effective framework for fostering a sound culture', advising that attention should be given to the pillars of governance, incentive systems and assessment and feedback mechanisms'.[14]

Developed economies

The governance codes in most developed economies also include requirements for the boards of listed entities to take responsibility for the governance and oversight of culture and risk. The codes require boards to delegate to senior management the responsibility to implement the desired culture and establish a sound system of risk management and internal control, and to report regularly to the board on the lived culture and the effectiveness of the risk management system.[15] Regulators and governance codes, therefore, place culture, risk attitude (or risk appetite), risk tolerance, and the oversight of culture and the maintenance of sound risk management and internal control systems at the centre of corporate governance and the role of the board in steering organisations.

While different regulatory bodies worldwide have all cited the importance of a good risk culture, and have various measures in place to encourage a responsible culture, they have stated that they cannot dictate culture, as it is something that companies need to foster and advance themselves. For example, the Financial Conduct Authority in the UK has said:[16]

> Culture is not something we can prescribe, nor would we want to – it is for firms to decide the type of culture they want. But whatever a firm's corporate culture looks like, the fair treatment of customers and market integrity should be central – and it should not be undermined by people or business practices.

9   PRA Statement of Policy – The use of PRA powers to address serious failings in the culture of firms, June 2014.

10 FCA report, *Culture in Banking,* 2015.

11 PRA Statement of Policy – The use of PRA powers to address serious failings in the culture of firms, June 2014.

12 House of Lords/House of Commons, *Changing banking for good,* Report of the Parliamentary Commission on Banking Standards, June 2013.

13 'A few things directors should know about the SEC', a speech by Chair Mary Jo White, Stanford University Rock Center for Corporate Governance, 20th Annual Stanford Directors' College Stanford, CA, 23 June 2014.

14 Hong Kong Monetary Authority, 'Bank Culture Reform', 2 March 2017.

15 ASX Corporate Governance Council, *Corporate Governance Principles and Recommendations, 3rd ed., 2014; UK Corporate Governance Code,* 2014; *King Code of Governance for South Africa, 2009; Singapore Code of Corporate Governance,* 2012; *Hong Kong Corporate Governance Code,* 2012; *Canada – Corporate Governance Codes and Principles.*

16 'Building a common language in the mortgage market', a speech by Linda Woodall, then Director of Mortgages and Consumer Lending, Financial Conduct Authority at the Council of Mortgage Lenders – Mortgage Industry Conference and Exhibition, 6 November 2013.

ASIC has stated that:[17]

Culture is at the heart of how an organisation and its staff think and behave. It is an issue that companies themselves must address. For firms, this means that it is important to have a culture that:

- Seeks and acts on customer feedback
- Promotes effective communication
- Encourages challenge
- Guards against complacency, and
- Is genuine in putting customer outcomes at the centre of what they do. And the customer must believe it. It is not enough to talk the talk; firms must truly embed this in their business.

In the UK, the Financial Reporting Council has conducted research on how boards and senior management are addressing these responsibilities, noting that 'A healthy culture both protects and generates value. It is therefore important to have a continuous focus on culture, rather than wait for a crisis.'[18]

For a table containing a summary of the responsibilities and duties of directors in relation to culture, see Appendix 3, page **28**.

> 'It's important to have a continuous focus on culture, rather than wait for a crisis. Poor behaviour can be exacerbated when companies come under pressure.'
>
> Sir Winfried Bischoff, Chairman,
> UK Financial Reporting Council

---

17 'Culture shock', a speech by Greg Medcraft, Chairman, ASIC at ASIC Annual Forum 2016 (Hilton, Sydney), 21 March 2016.
18 Financial Reporting Council, *Corporate Culture and the Role of Boards: Report of Observations,* July 2016.

Chapter 2 – Definition of culture

What is culture?

An organisation's culture is the sum of its shared values, principles and behaviours. A useful working definition is: 'a set of shared mental assumptions that guide interpretation and action in organisations by defining appropriate behaviour for various situations'.[19] A colloquial definition frequently heard in workplaces is 'the way we do things around here' or 'what we expect around here'.

A formal legal definition of 'corporate culture' is provided in the *Commonwealth Criminal Code 1995.* It is 'an attitude, policy, rule, course of conduct or practice existing within the body corporate generally or in the part of the body corporate in which the relevant activities takes place'.

References are commonly made to an organisation's innovation culture, safety culture or compliance culture – these are simply dimensions of the organisation's culture. It includes the values and behaviours of its people as they relate to various dimensions such as risk, safety and compliance, but those dimensions are not separate cultures.

Organisational culture operates at three levels.[20]
They are:

- Artefacts and behaviours – the characteristics of the organisation that can be easily discerned by individuals, but which may be hard for a newcomer to the organisation to understand. They encompass matters such as governance frameworks, codes of ethics, statements of business ethics, remuneration policies and risk frameworks, and can also include the dress code of the employees, office furniture, stories, work processes, policies and organisational structure
- Values and principles – these encompass the espoused values and principles of the organisation, such as underpin the mission and vision of the organisation, and influence the conscious objectives and philosophies of the organisation
- Assumptions – these are the beliefs that remain hidden, but which influence how certain practices are followed in the organisation. They are difficult to discern but provide the key to understanding why things happen the way they do.

Culture is also influenced by the character of the individuals that make up its collective. Individual character is implicit and subjective, and stems from an individual's values, principles, beliefs and history. Character encompasses an individual's biases and intuitions – their unconscious and conscious intuitions and desires. To ensure ethically aligned behaviours and culture, recruitment, professional development and remuneration

decisions must consider the character of the individual employee, and ensure their alignments with the organisation's ethical framework (see Chapter 3, page **11**).

Organisational identity and culture are entwined. An organisation's identity 'manifests as organisational members draw on organisational culture, as well as on other meaning-making systems (professional culture, national culture, etc.), to define "who we are as an organisation".'[21]

Culture does not exist in isolation, but is influenced by other organisational factors such as leadership, governance, systems, policies and the stakeholders of the organisation. Fundamentally, culture will collectively give priority to, and bring life into, the directives of the leadership.

Until recently, organisational artefacts – including policies, architecture and processes – have been the predominant mechanism by which an organisation's identity has been defined and its people's behaviour influenced and controlled within an organisation. While these artefacts have a significant influence over decision-making,[22] there is evidence emerging that character and culture have a stronger influence than artefacts in affecting the decisions, behaviours and actions of an organisation's people, and in avoiding ethical failure.[23]

Culture, then, is the implicit collective relationships, shared assumptions and power structures that exist within an organisation.

> Behaviour and culture are an integral part of operational management: effective management is only feasible if organisational structure and culture go hand in hand.
> DeNederlandsche Bank 2015,
> *Behaviour and Culture in the Dutch Financial Sector*

Why is culture important?

Culture is a key determinant in the performance of an organisation and its ability to achieve its objectives. It goes to the heart of the openness and transparency needed for effective stewardship and informed decision-making.[24]

Culture is inextricably linked to governance. The ASX *Corporate Governance Council's Corporate Governance Principles and Recommendations* note that acting ethically and responsibly is key to strong governance frameworks, and involves more than abiding by the law. It includes being, and being seen to be, a 'good corporate citizen'. In the UK, the Financial Reporting

---

19 Ravasi, D and Schulz, M, 'Responding to Organizational Identity Threats: Exploring the Role of Organizational Culture', *Academy of Management Journal,* 2006, vol. 49, no. 3, 433 – 458.

20 Schein, E H, *Organizational Culture and Leadership,* John Wiley & Sons, 1992.

21 Ravasi and Schulz, 'Responding to Organizational Identity Threats' Pages 433-458.

22 Chartered Accountants of Australia and New Zealand, A Question of Ethics, 2016.

23 Sheedy, E and Griffin, B, *Empirical Analysis of Risk Culture in Financial Institutions: Interim Report,* 2014.

24 Opening remarks of the Hon Justice Owen in the *Final Report of the HIH Royal Commission* (2003): 'From time to time as I listened to the evidence about specific transactions or decisions, I found myself asking rhetorically: did anyone stand back and ask themselves the simple question – is this right? … Almost every facet of life is governed by rules, regulations, proclamations, orders, guidance notes, codes of conduct, and so on … There is no doubt that regulation is necessary: peace, order and good government depend on it. But it would be a shame if the prescription of corporate governance models and standards of conduct for corporate officers became the beginning, the middle and the end of the decision-making process … I think all those who participate in the direction and management of public companies, as well as their professional advisers, need to identify and examine what they regard as the basic moral underpinning of their system of values. They must then apply those tenets in the decision-making process.'

Council states that strong governance underpins a healthy culture. Referencing the concept of the 'social licence to operate' and the UK Corporate Governance Code, its report on boards and culture is clear that it is the board's role to determine the purpose of the company and establish the culture, values and ethics of the company.[25]

ASIC has also linked a company's social licence to operate to the board and management's role in driving corporate culture in many speeches. ASIC has clarified that companies and their boards and senior management need to be interested in culture, not as a compliance measure, but because there is sufficient research to show that good culture is a business advantage and enhances long-term shareholder value. In various speeches, ASIC has also made it clear that the ways in which a good culture can benefit organisations include:

• Increasing customer loyalty, brand and reputation
• Reducing or avoiding the financial impact of fines or remediation, and
• Attracting and retaining staff.

Culture is also closely linked to risk management and risk appetite, as boards need to consider the risks that the culture may create and the effect of this on the organisation's long-term viability. A governance framework underpinning a healthy culture will support the achievement of the organisation's strategic objectives by clarifying that decision-making is tied to risk and that there is accountability for the exercise of authority.

In a world of rapid information dissemination, organisations need to be able to make decisions quickly. All decision-makers – including client- and customer-facing employees, as well as senior managers – need the freedom to be able to make decisions. However, appropriate boundaries on decision-making need to be in place, clearly understood and respected. The culture of an organisation will affect whether appropriate boundaries on decision-making are in place and monitored, and whether consequences are applied to any breach of those boundaries. It should be noted that the concept of 'boundaries' is not limited to formal regulatory delegation and the associated option of control. Boundaries also include ethical limitations – the difference between what 'could' and 'should' be done.

There is no 'one-size-fits-all' approach to culture, just as there is no 'one-size-fits-all' approach to governance or risk management. Indeed, Sheedy and Griffin[26] found that the subcultures that exist in organisations can be one of the strongest determinants of risk culture. The culture will always need to be appropriate for the context in which the organisation is operating. Cultural variation in itself can be an important driver of innovation; however, internal alignment around a core organisational purpose, values and principles are needed to ensure an overall cultural coherence. Just as members of a family will be separate individuals but share some common DNA, different cultures of a single organisation can also be drawn together through a common purpose, values and principles (their 'shared DNA'), which is then expressed – according to context – in a manner that is both distinct and related.

Risk-aware culture

The risk culture of an organisation is the shared values and behaviours of individuals regarding the management of risk in an organisation. The organisation's culture will be a key determinant in its ability to respond and adapt to changes in the environment in which the organisation operates.[27]

Risk-taking is what organisations do; risk encompasses the opportunities to be realised by the organisation, as well as the hazards to be avoided, with recognition of the uncertainties attached to the opportunities and hazards alike. To effectively manage risk and leverage the opportunities created by uncertainty, an organisation needs a risk-aware culture. A risk-aware culture is a critical subset of the broader organisational culture that incorporates the way directors, managers and employees think, communicate and behave about all aspects of risk.[28]

The Financial Stability Board notes that:[29]

> A sound risk culture consistently supports appropriate risk awareness, behaviours and judgements about risk-taking within a strong risk governance framework. A sound risk culture bolsters effective risk management, promotes sound risk-taking, and ensures that emerging risks or risk-taking activities beyond the institution's risk appetite are recognised, assessed, escalated and addressed in a timely manner.

25 UK Financial Reporting Council, *Corporate Culture and the Role of Boards: Report of Observations,* July 2016, p. 2.

26 Sheedy and Griffin, *Empirical Analysis of Risk Culture in Financial Institutions.*

27 Another definition of risk culture, from the 2009 International Institute of Finance report *Reform in the Financial Services Industry: Strengthening Practices for a More Stable System,* defines 'risk culture as the norms of behaviour for individuals and groups within an organisation that determine the collective ability to identify and understand, openly discuss and act on the organisation's current and future risk'.

28 APRA's Prudential Standard (enforceable) for authorised deposit-taking institutions (ADIs), general insurers and life insurers states that the board must ensure that it 'forms a view of the risk culture in the institution, and the extent to which that culture supports the ability of the institution to operate consistently within its risk appetite, identifies any desirable changes to the risk culture and ensures the institution takes steps to address those changes'.

29 Financial Stability Board, *Guidance on Supervisory Interaction with Financial Institutions on Risk Culture: A Framework for Assessing Risk Culture,* April 2014.

Chapter 3 – Identifying and setting culture

Identifying the desired culture

Successful companies are those companies that make more 'good' decisions than 'bad' ones and do more things that are 'right' than 'wrong'. But how do employees know what makes a decision 'good' or 'bad'? Increased attention is being given to the ethical foundations of an organisation, to help people know how to make good decisions, thus shaping the culture of the organisation.

The attainment of coherence and consistency in decision-making is a foundational aspect of setting culture and one of the principal tasks of those responsible for the governance of organisations. Failure to undertake and complete this task limits the capacity of an organisation to act consistently and with integrity.

One method for achieving coherence and consistency of organisational conduct is to build a strong and comprehensive 'scaffold' of rules and regulations that bind and shape individual decision-makers when acting on behalf of the organisation. These rules and regulations depend upon compliance and limit or remove the capacity of individuals and groups to exercise judgement and discretion when making decisions. In their most extreme form, rules and regulations might be designed with the intention of defining and constraining the totality of all decision-making. It is the overreliance on this scaffolding that has led regulators to increase their focus on culture.

An alternative (and complementary) approach to governance is to establish an ethical framework that guides (rather than directs) decision-makers. In this approach, decision-makers are required to exercise judgement, in accordance with reasons that they are willing and able to defend with reference to an established framework of values and principles that serve the defined purpose of the organisation. That is, coherence and consistency in decision-making grows out of judging 'like cases' in a 'like manner', rather than out of the automatic application of a particular rule.

> 'We think that the voice and authority of risk has been the channel through which abstract narratives of doing the right thing land in the wider organisation. In essence, risk is the vehicle for ethics. They are not two different things.'
>
> M Power, S Ashby and T Palermo,
> Risk Culture in Financial Organisations, 2013

The answer to this is found in purpose, values and principles – the ethical framework (see Figure 1). Together these form the bedrock for all decisions, behaviours and artefacts of organisations.
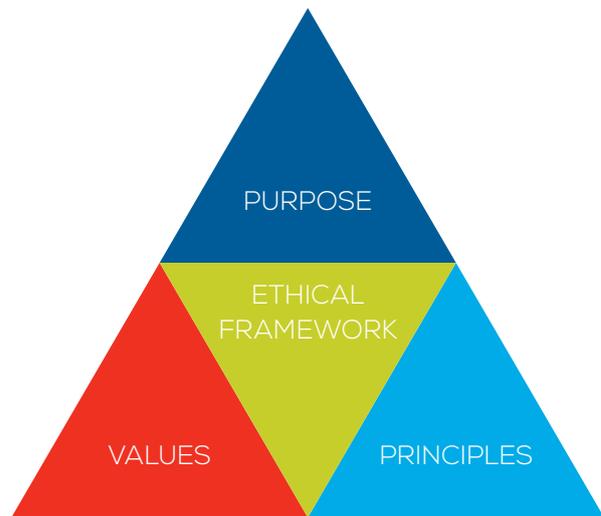
Figure 1: The ethical framework

An ethical framework enables the delegation of authority to a distributed network of responsible decision-makers while maintaining organisational integrity. Such a framework should sit at the heart of the governance structures of an organisation, serving as a common and authoritative point of reference for all decision-makers, and giving shape to organisational culture.

Once established and formally adopted by an organisation's principal governance body, all aspects of the organisation (current and prospective) should be assessed and, if required, aligned with the tenets of the framework. If misalignment is to be allowed, then the specific exception must be justified and approved.

In this way, an ethical framework is different from a code of ethics or a code of conduct, in that codes articulate decisions to be made in specific circumstances. An ethical framework, however, provides guidance on any decision, regardless of its unique circumstances. Typically, a code of ethics or a code of conduct will take the values and principles espoused in an ethical framework and apply them to specific circumstances, but will never cover every possible decision an employee might face.

A good framework will be:

- Practical – able to be applied in practice and with consistency
- Authentic – it will 'ring true'
- Stable – it will not change much (in its essence) over the long term
- Understandable – by all of those required to apply it in practice.

Beyond this, companies should choose what is appropriate for the type of organisation they are (their purpose), and the culture that they want to cultivate.

Purpose

In a world of accelerated disruption, changing customer and community expectations and employees seeking meaning in their work, a growing number of executives are looking to purpose to drive strategy and decision-making.[30] A survey by *Harvard Business Review* found that although 90% of executives valued the importance of purpose, only 46% said that it was effectively informing their strategic and operational decision-making, despite the evidence that it supports growth, innovation and transformation.

> 'Leaders die, products become obsolete, markets change, new technologies emerge, and management fads come and go, but core ideology in a great company endures as a source of guidance and inspiration.'
>
> J Corrin and J Porras, *Built to Last,*
> *HarperCollins,* 1994

Organisations describe their purpose in a simple and concise statement to explain why they exist. This statement goes beyond self-interest and profit motives to demonstrate its ethical core. It explains how an organisation seeks to improve people's lives and make a contribution to a better society or world.

A purpose statement is different from an organisation's vision or mission. A mission describes *what* an organisation does. It's a focused and clear statement defining the business one is in. A vision, on the other hand, describes what one *wants to be.* It's inspirational and future-oriented.

Purpose describes why an organisation exists. It's aspirational and provides meaning. It fuels passion and creates a binding culture. It is the shared language, stories and practices that underpin everything the organisation does. The purpose statement is a centrepiece of that 'core ideology'.

> '53% of executives surveyed whose organisations were strongly purpose led said that their business was successful in innovation and transformation; compared with 19% of those who had not yet considered purpose.'
>
> *Harvard Business Review,* 2015

Values are an expression of what we think to be *'good'.*[31] They capture the essence of what one should choose if available. So, if one of a company's core values is trust, then that company (through its directors and employees) should choose those things that build, display and support trust. However, if that company claims to value trust but in practice only ever acts in a way that is cunning, then one might reasonably conclude that the company is insincere or profoundly irrational. In summary, values determine the direction a company should take whenever there is a fork in the road.

> 'Well-chosen values typically stand the test of time, but need to be tested for continuing relevance as society changes and business adapts.'
>
> FRC, *Corporate Culture and the Role of Boards,*
> July 2016

Principles are an expression of what is *'right'.*[32] Their task is to shape the means by which one obtains the things that are good. If values tell us where to go, principles tell us how to get there.

Examples of principles include things like: 'Do unto others as you would have them do unto you', 'Only do those things you would be proud to do in the full light of day', 'Treat every customer as if they are your friend', etc.

Together, the ethical framework shapes our choices and, therefore, the organisations we make. If the ethical framework is changed, then the organisation changes with them. They are the most powerful determinant of culture.

Stating the ethical framework alone, however, is insufficient. Once the ethical framework has been established, it needs to be embedded throughout the organisation.[33] That is, it needs to be embedded within the purpose, strategy and business models; it needs to be interpreted into policies and systems; and it needs to be translated into expected behaviours, so that employees understand how the purpose, values and principles can be effectively lived in day-to-day decision-making. It also needs to be widely and consistently communicated, including through codes of ethics/conduct, and reinforced through recruitment, performance management and rewards.

---

30 Harvard Business Review, *The Business Case for Purpose,* 2015.

31 The Ethics Centre, 2016, <www.ethics.org.au/on-ethics/blog/october-2016/values-principles-are-your-organisations-dna>.

32 The Ethics Centre, 2016, <www.ethics.org.au/on-ethics/blog/october-2016/values-principles-are-your-organisations-dna>.

33 FRC, *Corporate Culture and the Role of Boards.*

Drivers of culture

Both ASIC and the UK's Financial Reporting Council have identified common drivers of good corporate culture. (See Appendix 4, page **32**, for an expanded version of this table.)

Figure 2: Drivers of good culture[34]

ASIC
• Tone from the top
• Cascading values to the rest of the organisation
• Translating values into business practice
• Accountability
• Effective communication and challenge
• Recruitment, training and rewards
• Governance and control

FRC
• Demonstrate leadership
• Embed and integrate
• Recognise the value of culture
• Assess, measure and manage
• Be open and accountable
• Aligned values and incentives
• Exercise stewardship

Identifying and monitoring the current culture

Measuring the alignment of organisational culture to the ethical framework is key in understanding the culture of an organisation.

In a recent report by APRA,[35] it was found that measurement of culture in relation to risk culture was at the early stages of maturation, with most prudentially-regulated organisations seeking to understand the current state of culture and risk culture.

There is a wide range of approaches to assessing culture. The focus of and the triggers for assessment, as well as the scope of assessment, vary widely across institutions.[36]

There are not yet common indicators in Australia or internationally to measure culture. This said, some are using their ethical framework as a starting point for considering the types of indicators that would assist them in measuring the extent to which they are living their purpose and values. Further, the common areas of interest as identified by ASIC and the FRC provide a starting point for considering possible scope for measurement.

In any analysis of culture, it is important to ensure that data is collected from a range of sources to ensure findings can be triangulated and findings assured. APRA found that the most common methods of data collection for measuring risk culture included:[37]

- Surveys – including both staff engagement surveys, either generally or with specific culture/risk culture questions, or specific culture/risk culture surveys
- Reports and dashboards that include/leverage existing data such as breach limits, whistleblower events, exit interviews, etc., and also HR data.

Interviews and focus groups are also frequently used to add depth to findings. More sophisticated approaches also look to organisational artefacts, such as policies and procedures, to determine the extent to which they encourage the desired behaviours or detract from them.

Increasingly, communications monitoring through social media, email and other sources of data are also starting to be analysed at scale, to better understand how decisions are informed, and what shapes culture and decisions.

Cultural change

Once a clear desired state is articulated, and the current state assessed, the next step is to take steps to close the gap between the aspired-to culture and the actual culture. A culture transformation sets out to do this.

Changing culture is hard. The interlocking nature of the artefacts, behaviours and values makes culture enduring. A single-dimensional approach to change will not suffice; rather, a multifaceted approach is necessary and it will take time to ensure its sustainability.

The role of the ethical framework in a cultural change process

In order to facilitate positive organisational change towards one bound by the ethical framework, the change process itself must be reflective of the ethical framework. If a company values transparency, the change process should be transparent.

Change initiatives are often dressed up to be something they are not, ultimately resulting in cynicism among staff towards the whole change process. Trust is hard to win and easy to lose. In any change process, the change can threaten people's sense of certainty, so trust in the process must be nurtured to assure people that important decisions that affect them will be made for the right and appropriate reasons. Winning back trust in a change process after it has been lost can be a costly exercise.

---

34 'Why culture matters', a speech by Greg Medcraft, Chairman, ASIC at BNP Paribas Conduct Month (Sydney, Australia), 24 May 2016; FRC, *Corporate Culture and the Role of Boards*.
35 APRA, 'Information Paper: Risk Culture', October 2016.
36 APRA, 'Information Paper: Risk Culture', October 2016.
37 APRA, 'Information Paper: Risk Culture', October 2016.

A cultural change model that focuses staff on the higher-order purpose, values and principles of the organisation will naturally link change with meaning, and provide the umbrella under which 'levers of change' will make operational the required change. This will include embedding the ethical framework in:

- The governance mechanisms of the organisation, including the setting of strategy and risk appetite
- Leadership development
- The first, second and third line of defence controls, including risk management, internal audit, and performance management
- Internal and external communications, and
- Human Resources, including recruitment, induction, training and professional development.

Figure 3: Human psychology and change

Our understanding of human psychology and decisions has accelerated profoundly since the creation of MRI scanners that allow us to see the impact of our decisions on the functioning of the brain. This, together with the volatile, uncertain, complex and ambiguous environments that we operate in, has led to traditional change models being transformed through contemporary psychology, philosophy, and behavioural economics.

Policy development leaders such as Harvard University Professors Cass Sunstein and Dr David Halpern of the UK's Behaviour Insights Team, among others, show how 'rational-choice theory', the foundation of much of modern economic, political and social modelling (which suggests people make rational decisions based on self-interest) is fundamentally flawed. A new approach, which was used widely by the Obama Administration and UK policy units, coined as 'Nudge',[38] brings a scientific rigour and transparency to what marketing companies have been doing for many years. That is, observing how people actually behave and designing promotional activities in light of this.[39]

This work builds on that of Professor Daniel Kahneman, a Nobel Laureate and professor of psychology at Princeton, who along with others showed how human behaviour is more complex than rational-choice theory proposes.[40] He shows how humans are programmed to use heuristics, or 'mental short-cuts', to make decisions. While in most cases they serve humans well, they also become biases that blind people to rationality in certain circumstances, and make them prone to error.

In a dynamic environment, organisational cultural change must be able to become part of 'business as usual', not be bound tightly by rules and regulations (or even popular theories), and transparently adapt to the unique challenges of each organisation. That said, 'business as usual' must avoid falling into the trap of becoming 'unthinking custom and practice' – the most potent source of ethical failure.

However, if the overall change process appears to undermine the ethical character historically espoused by the organisation – for example, replacing its moral compass with acrimonious legalistic negotiations between employer and employee groups to identify what is good and right – the organisation's culture becomes the casualty. All the observable artefacts (such as policies and procedures) may, in the end, be pushed into place, but the underlying culture may be rendering the artefacts a hollow façade.

As technological changes paradoxically place greater focus on the human element in control structures, organisational ethical frameworks are likely to be integral to contemporary organisational control in constantly changing environments. Complex change models outside traditional organisational change frames, such as Nudge, offer helpful new insights into how an ethical framework can be instrumental in achieving cultural change.

---

38 'The HOW Report: A Global, Empirical Analysis of How Governance, Culture and Leadership Impact Performance', LRN, 2016, <http://howmetrics.lrn.com/>.

39 'The HOW Report'.

40 'ADKAR change management model overview', <www.prosci.com/adkar/adkar-model>.

Chapter 4 – Embedding culture

Governance and risk management

Boards are called upon to articulate the purpose, values and principles of their company, in order to connect purpose to strategy and culture. One UK report notes that:[41]

> Establishing a company's overall purpose is crucial in supporting the values and driving the correct behaviours. The strategy to achieve a company's purpose should reflect the values and culture of the company and should not be developed in isolation. Boards should oversee both.

Those exercising authority and making decisions within an organisation have the power to facilitate the strategic objectives of the organisation. The board is the governing body of an organisation, but good governance extends beyond the board room. It provides the framework through which the organisation's strategic objectives are set and cascaded, and the means of attaining them are determined.

Governance has four key components:[42]

1 **Transparency:** being clear and unambiguous about the organisation's structure, operations and performance, both externally and internally, and maintaining a genuine dialogue with, and providing insight to, legitimate stakeholders.
2 **Accountability:** ensuring that there is clarity of decision-making within the organisation, with processes in place to ensure that the right people have the right authority for the organisation to make effective and efficient decisions, with appropriate consequences for failures to follow those processes.
3 **Stewardship:** developing and maintaining an enterprise-wide recognition that the organisation is managed for the benefit of its shareholders/members, taking reasonable account of the interests of other legitimate stakeholders.
4 **Integrity:** developing and maintaining a culture committed to ethical behaviour and compliance with the law.

Good governance encompasses not only the systems by which authority is exercised in organisations and how they are controlled, but also the mechanisms by which organisations and those who exercise authority within them are held to account.[43]

Directors have a fiduciary duty to act in the best interests of the company. In order to discharge their duties, directors need to know, and properly assess, the nature and magnitude of risks faced by the entity. Risk management is a critical area of responsibility for the board. An integrated governance and risk management framework is central both to informed decision-making by the board and adapting to changes in the environment in which the organisation operates. However,

unless an organisation also establishes a culture that promotes risk awareness in everything it does, it is unlikely to achieve – let alone exceed – its objectives and will most likely fail to avoid damaging risk events and take hold of opportunities. In order for a risk culture to exist, risk management must be embedded into the organisation. It should be built into the organisation's policies, procedures and practices – not treated as a separate business activity.

Management has the task of implementing a risk culture where everyone in the organisation:

- Is aware of the risks for their span of responsibility
- Takes responsibility for the controls for managing those risks
- Is confident that they can raise issues at the time they arise.

Management must ensure that the right competencies and the appropriate level of resources are available. An effective risk culture is one where people are aware not only of the risks in relation to their own area of responsibility, but also how those risks impact across the organisation. That said, this is not just a matter of risk management and conformance. High performance is also linked to culture – especially to ethical alignment.

The role of the board

Directors' duties include setting the ethical foundations for corporate culture and monitoring and correcting any evident misalignment between what is espoused and what is practised within the organisation they govern.

The ethical foundation that the board sets will ultimately be expressed in ways that set the culture of the organisation. This is commonly referred to as setting the 'tone from the top'.

As noted earlier, regulatory requirements and governance codes hold boards responsible for setting the tone from the top.

ASIC has stated that in setting the right tone from the top, the board might wish to consider:

- How the board is modelling the firm's desired behaviours and values when interacting with management and staff
- How the actions and behaviours of the board support and advance the firm's desired culture
- How the board sees its role in relation to cultivating the firm's values and ensuring that the firm has a culture of integrity.[44]

Former SEC chair Mary Jo White noted:

> Ensuring the right 'tone at the top' for a company is a critical responsibility for each director and the board collectively. Setting the standard in the boardroom that good governance and rigorous compliance are essential goes a long way in

---

41 Financial Reporting Council, *Corporate Culture and the Role of Boards: Report of Observations,* July 2016, p. 2.

42 Governance Institute of Australia, 'More thoughts on governance', <www.governanceinstitute.com.au/knowledge-resources/governance-foundations/more-thoughts-on-governance/>.

43 ASX Corporate Governance Council's *Corporate Governance Principles and Recommendations,* 3rd edn, p. 3: 'Corporate governance is the framework of rules, relationships, systems and processes within and by which authority is exercised and controlled in corporations. It encompasses the mechanisms by which companies, and those in control, are held to account'. Definition taken from Justice Owen, HIH Royal Commission, *The Failure of HIH Insurance, Volume 1: A Corporate Collapse and Its Lessons,* Commonwealth of Australia, April 2003, p. xxxiii.

44 'Directors' duties and culture', a speech by Greg Medcraft, Chairman, Australian Securities and Investments Commission (ASIC) at Law Council of Australia, Business Law Section Corporations Workshop (Gold Coast, Queensland), 19 June 2016.

engendering a strong corporate culture throughout an organisation.[45]

Regulators are of the view that ethics and honesty can become core corporate values only when directors and senior executives embrace them.

The board is also responsible for ensuring there is oversight of how that tone is implemented. The board cannot 'set and forget' culture. It has a critical responsibility to monitor how management is implementing the 'tone from the top'. A prudent board will need to ensure that the company is not setting policies, building systems or establishing practices that might reasonably be expected to drive conduct that is at odds with the declared ethical framework.

Board oversight of culture

One of the key characteristics that members expect of a well-governed organisation is the exercise by its board of independent judgement made in the best interests of the organisation and its members generally.

To successfully develop a culture of openness and transparency, the behaviours of directors need to be commensurate with the stated values and principles of the organisation, and that can only be facilitated by robust and open discussion and debate. Behavioural expectation involves a readiness to test and challenge and, in respect of risk matters, a readiness to seek external advice in doing so if it is felt to be appropriate.

The independence of mind of non-executive directors provides a foundation for enquiry and for building openness with, and trust from, senior executives. In turn, management needs to recognise the contribution that non-executive directors make to such cultural values.

Challenging specialist knowledge is particularly important, as the willingness to listen to, and respond to, a contrary opinion is one indicator of an open and transparent culture. The expertise of non-executive directors is therefore an important tool in assisting a board to review the degree to which the culture is one of being open to challenge.

Board evaluation of the lived culture

For a board of directors, it can be very challenging to understand the degree to which the culture reflects the values it espouses. The question for boards is whether the defined culture is known and understood within the organisation and whether the actual culture (the lived culture) represents the necessary and desired culture.

It is an essential element of governance for a board to understand if there is any disjunction between the desired and stated culture and the actual culture, for it is only the actual culture – the enacted values – that ultimately matter.

All organisations will have subcultures, which are intra-organisational groups of people who exhibit a set of shared values and behaviours that are identifiably different from those in other areas of the organisation. Boards and management need to identify if there are subcultures within the entity that do not align with the desired culture of the organisation as a whole: any 'rogue' subcultures should be identified.

Rules are necessary but not sufficient to inculcate a culture where the enacted values align with the desired values. Also, without an open and transparent culture, the questioning that will test if the enacted values align with the desired values will not be undertaken. Both go to the heart of governance and risk management if they are to create and protect value.

Comments such as 'noses in and fingers out' speak to the responsibility of boards to have oversight of culture by monitoring whether the lived culture aligns with the desired culture without becoming involved in the day-to-day operations of the business.

ASIC has noted that boards may wish to consider the following questions to help gain insights into a company's culture:[46]

- Is culture a regular feature on the board and audit committee agenda?
- Do directors have regular interaction with staff across the organisation and not just with the CEO and executive management?
- Are there good relationships with key employees, such as line managers, to help with gathering insights about team-specific issues and subcultures?
- Is there periodic engagement with all stakeholders to get a broad perspective on the issues impacting on customers, suppliers, regulators and the community? This should help with balancing various competing and conflicting interests.

Risk appetite

It is the role of the board to set the risk appetite for the entity, to oversee its risk management framework and to satisfy itself that the framework is sound. Setting appropriate boundaries for risk-taking is the core function of risk appetite and risk tolerance. The risk appetite will influence the culture of the organisation.

Setting the risk appetite explicitly articulates the attitudes to risk that the board expects senior management to take. The board provides a series of licences to senior management to act in particular ways or implement particular decisions that align with these attitudes. Senior management in turn sets in place a further series of licences that cascade the risk appetite through the organisation to align decision-making at all levels with the attitudes to risk set by the board.[47]

---

45 'A few things directors should know about the SEC', a speech by Chair Mary Jo White, Stanford University Rock Center for Corporate Governance, 20th Annual Stanford Directors' College Stanford, CA, 23 June 2014.

46 'ASIC's focus on culture – digging into the detail', a speech by John Price, Commissioner, ASIC to Governance Institute of Australia's Corporate Governance Forum 2016 (Sydney, Australia), 25 May 2016.

47 ASIC's report on AFS licence holders indicated that determination of risk appetite is a board responsibility. APRA's Prudential Standards (enforceable) for ADIs, general insurers, life insurers and superannuation require boards to maintain and approve a 'risk appetite statement'. The Committee of Sponsoring Organisations of the Treadway Commission (COSO) proposes that management, with board review and concurrence, should develop risk appetite; communicate risk appetite; and monitor and update risk appetite.

It is good governance for organisations to articulate and communicate their appetite for risk with a formal risk appetite statement. Regulators may require the board to set a risk appetite statement. The concept of risk appetite seems easy to grasp, yet in practice answering the question of the amount and type of risk an organisation is willing to pursue or retain can be very difficult. The risk appetite statement is necessarily broad, yet should be descriptive enough to give its audience an understanding of the approach the organisation takes to managing risk. Risk appetite is strategic and directly related to the achievement of business objectives, including the allocation of resources.

The risk appetite statement is:[48]

> Commonly the document that articulates the organisation's approach to risk, and would include both the risk appetite and risk tolerances. It can be both quantitative and qualitative. The risk appetite may consist of high-level statements in only one or two paragraphs that in turn drive a more detailed listing of risk tolerances. The two parts work together and in their entirety constitute the risk appetite statement.

The role of management

Management is responsible for implementing and monitoring the desired culture as defined and set by the board.

Forging a culture that is aligned with business strategy is the role of management, with the board having oversight of implementation, but not responsibility for it. This is not unlike risk management, where it is the role of the board to set the risk appetite for the entity, to oversee its risk management framework and to satisfy itself that the framework is sound, while it is the role of management to design and implement that framework and to ensure that the entity operates within the risk appetite set by the board.

For example, it is the responsibility of management to ensure there is training on culture and ethics as well as due diligence, and that monitoring programs are in place to enable staff to understand the ethical framework and relevant codes of conduct and apply them effectively. Boards would not monitor training, although they are likely to request reports from management as to the functioning and effectiveness of training programs as part of management's responsibilities to implement the 'tone from the top' set by the board.

The UK report *Corporate Culture and the Role of the Board* clarifies that it is the board's role to determine the purpose, values and principles of the company and that the CEO has the responsibility of implementing those ethics.

At an operational level the focus will be on obtaining assurance that the company's operations are aligned with its culture. In this way, boards and executive management can ensure that decisions around value creation and values are fully integrated.

It has been noted by regulators that the tone and behaviours manifested by middle management are as important as those exhibited by senior management. Middle-level managers channel the culture as set at the top to the business lines whose operational responsibilities take risks in line with the risk appetite set by the board. These operational roles usually are those responsible for identifying, assessing and controlling the risks of their businesses.

Monitoring culture

In order for changes to occur, an organisation's culture must be monitored, measured and reported on. As the saying goes, 'What gets measured gets done.' A number of areas in an organisation can fulfil this function, from a specific 'culture' team to HR and sometimes Risk. Results need to be fed back regularly to the executive, as often it is assumed that the desired culture exists throughout the organisation when this is not the case.

Cascading governance through the organisation

Board governance is but one part, but an important driver in producing the desired culture for an organisation.

Whole-of-organisation governance is about how authority is exercised and controlled below the board in an organisation. Authority cascades from the board to the CEO to the executive management team and throughout the organisation. How an organisation is governed is best not left to chance, but should be actively considered by the board and the executive management team and structured accordingly.

Governance Institute defines whole-of-organisation governance as 'a principles-based approach to good governance from the board through management to the whole organisation in order to achieve strategic objectives'.[49] Its guidelines note that key elements in enabling organisations to achieve their objectives are to:

- Understand the risks of not achieving the strategic objectives so that these can be managed
- Ensure that the effort undertaken by all employees across the organisation is aligned with the strategic objectives
- Clarify individuals' roles, authorities and accountabilities in achieving strategic objectives
- Empower individuals to make decisions that are aligned with strategic objectives
- Clarify the controls and boundaries that apply to the exercise of authority
- Provide for clear and effective accountability for the decisions taken and authority exercised.

48 Governance Institute of Australia, *Good Governance Guide: Risk appetite statement,* <www.governanceinstitute.com.au/knowledge-resources/guidance-tools/good-governance-guides/?category=Recognise+and+manage+risk>.

49 Governance Institute of Australia, *Guidelines: Whole-of-organisation governance,* October 2015.

All decision-makers in the organisation should understand the purpose for which authority is to be exercised – to facilitate the strategic objectives of the organisation (the why). All decision-makers should understand how authority is exercised, who has authority to do what, and what boundaries apply (the how). Appropriate monitoring mechanisms should be in place to provide assurance that decisions are being made in the right way for the right purpose (the safeguard).

A clear whole-of-organisation governance framework supports the achievement of the organisation's strategic objectives by clarifying that decision-making is tied to risk and there is accountability for the exercise of authority. Whole-of-organisation governance is inextricably linked to good risk management.

This aligns with ASIC's focus on cascading and translating the values set at the top into business practice and ensuring there is accountability for this.

A whole-of-organisation governance framework also provides the board with visibility on whether – and how – the desired culture is the enacted (lived) culture. It also provides the board with the means to make adjustments if there is a slippage in the alignment between the desired and enacted culture. A whole-of-organisation governance framework empowers employees to make good decisions where the enacted values align with the desired values of the organisation. (See also Appendix 5, page **34**, which sets out the key elements in whole-of-organisation governance and outlines the role of the board.)

Delegated authorities

The board needs to know that an effective framework is in place clarifying who is authorised to make what decisions and in what circumstances. Comprehensive delegated authorities should be put in place by management, clearly articulating to each decision-maker within the organisation their capacity to make decisions in relation to their specific responsibilities and duties.[50] The delegations of authority framework needs to align with the strategic objectives of the organisation.

The delegations policy should clarify that setting out the delegations of authority is a fundamental component of a risk management framework. It is not a stand-alone policy, but central to the governance framework of an organisation both at and below board level. It provides a framework for decision-making and accountability within the organisation.

When framing delegations of authority, management needs to consider them within the risk management framework through scenario testing. This could include considering the risks of unintended consequences if this particular form of empowerment is granted. Management needs to ensure that all material decisions, both financial and non-financial, are covered by the delegations of authority.

Incentives

Incentives play a powerful role in influencing the values and behaviour of individuals, and hence the culture.

Incentives may have unintended consequences. Research has shown that individuals will seek to do those things that are rewarded, often to the exclusion of activities that are not rewarded. This can create cases of folly, however, where the types of behaviour rewarded are those which the organisation is trying to discourage, while the desired behaviour is not rewarded at all.[51]

Examples include:

- We hope for long-term and sustainable growth – but reward quarterly sales.
- We hope for team work – but reward individual effort.
- We hope for safer workplaces – but reward productivity and cost reduction.
- We hope for candour – but reward reporting of good news and agreeing with the boss and punish reporting of bad news or disagreement with the boss.

The board needs to align both the overt and implicit incentives with either the stated values and principles of the organisation or the mitigation framework to prevent undue risk-taking. Financial and non-financial incentives should be appropriately balanced and linked to behavioural objectives. This then needs to be monitored constantly and adjusted as necessary.

The board also needs to ensure that current remuneration practices align with the risk appetite and the risk tolerance/capacity of the organisation. Risk management and cultural/ethical alignment should be a criterion for executive evaluation and risk-related objectives should be built into the company's executive remuneration structures.

Regulator and investor interest in incentives

The International Monetary Fund noted that 'The causes of [such] risk taking [in the financial sector] were many and complex, but there is general agreement in the financial industry, the public sector, and academia that incentive structures at some financial institutions played an important role'.[52]

---

50 Governance Institute of Australia's *Good Governance Guide: Issues to consider when developing a policy on delegations of authority* is a useful reference.

51 Kerr, S, 'On the folly of rewarding A, while hoping for B', *Academy of Management Journal,* 1975; vol. 18, no. 4, p 769.

52 International Monetary Fund, *Global Financial Stability Report: Risk Taking, Liquidity, and Shadow Banking – Curbing Excess While Promoting Growth,* October 2014; Financial Stability Board, *Guidance on Supervisory Interaction with Financial Institutions on Risk Culture: A Framework for Assessing Risk Culture,* 7 April, 2014.

Regulators were therefore concerned not just with requiring boards to take responsibility for oversight of risk management, but also to focus on executive remuneration to ensure that it aligned with risk appetite. Investors were keen to see that boards were putting in place remuneration structures and performance targets that align with shareholders' interests.

While this focus is required, boards need to consider that taking risks to innovate and create value in an increasingly competitive and complex global economy is also their responsibility.

Human Resources

Many of the responsibilities of the human resource function (HR) are fundamental in shaping, reinforcing and changing corporate culture within an organisation. Employees take their cue from HR around what is acceptable within the organisation from the moment they are hired. By helping to strengthen desired behaviours in leaders and staff, identifying weaknesses and their relevance to business results, and measuring progress, HR professionals are well placed to make the link between culture and business performance. To impact culture, HR leaders must work with company executives to help define what the organisation considers appropriate with regard to how people think, act and behave. They need to help executives understand the strengths and weaknesses of the cultures they create. One could cite the cultures at Enron and Arthur Andersen as examples of leaders not realising the impact of their corporate cultures. HR can play a pivotal role in ensuring that how results are achieved is considered just as important as the results themselves.

HR can play a part in communicating culture throughout the organisation. For example, in order to create a culture of openness and honesty, it is important that employees hear about the policy toward whistleblowing. HR can assist management in communication of their commitment to ethical behaviour in memos, newsletters and speeches to company personnel.

All HR activities have a direct role in reinforcing an organisation's culture. Recruitment, remuneration and performance management all need to be directed towards employing and rewarding those who behave in accordance with the organisation's culture. Training activities educate leaders and teams in what are the desired behaviours. Also, while executives tend to believe that the espoused culture exists throughout the organisation, often this is not the case. HR can have a role to monitor the culture through training, through undertaking surveys and providing feedback to the executive. As guardians of corporate culture, HR professionals need to play an ongoing role in upskilling, coaching and supporting leaders and their teams. HR is also typically responsible for taking the lead on any culture change initiatives.

The following HR activities have a significant impact on culture.

Remuneration and other incentives

This is one of the centrepieces of HR's role. When rewards are directly linked with values, behaviours and culture, they act as a powerful reminder of what is important in the business. While responsibility for setting C-suite remuneration usually resides with the board, the HR team plays a key role in the remuneration process for the rest of the organisation. They also explain how compensation works, provide advice and help managers with both informal and formal staff recognition systems for outstanding performance. To effectively impact corporate culture, pay systems should reward not only job outcomes, but also behavioural expectations. Pay systems that reward based simply on productivity could be creating a culture that is counter to organisational success.

Once values, principles, business objectives and desired behaviours are determined, then compensation plans can be put in place to support them. For example, if a value of the organisation is trust, then the compensation strategy will reward observable behaviours that reflect the actions of someone who is trustworthy.

The role of compensation in an organisation and the compensation strategy must be clearly defined and communicated, and HR plays a key part in communicating that strategy. For example, if the organisation espouses a value of trust, then it needs to help its people understand the behaviours that uphold trust, as well as those that don't. It needs to help people practise and live those behaviours, and to reengineer systems and processes to assist people to act in a trustworthy way. HR, then, needs to clearly communicate these expectations through multiple channels, both internally and externally.

Performance management

An important component of developing employees is a comprehensive and well-executed performance management system, which creates a work environment or setting in which people are enabled to perform to the best of their abilities, acting in accordance with the desired behaviours to achieve the organisation's objectives. A performance management system can incorporate elements such as regular one-to-one meetings, performance appraisals and processes to manage underperformance. It can include corrective actions or sanctions such as fines and warnings. This system must be designed to encourage and reward the desired behaviours and values and discourage those behaviours that are inconsistent with the organisation's culture. Culturally aligned performance management systems have a strong element of differentiation. This means that those who think, act and behave according to the desired culture are given higher ratings, increases and/or promotions than those that do not.

A company's performance management system can have a negative influence on its culture. Though once extremely popular, ranking employees against each other can generate a fear of failure, which leads to low risk-taking and innovation. Once-a-year performance reviews can also hinder modernisation and learning agility by failing to provide coaching and feedback at a pace that matches industry changes.

Training

HR plays a crucial role in designing and delivering training of employees and leaders to help disperse desired behaviours throughout the organisation. By facilitating internal training, 'town hall' meetings and cross-functional group meetings HR professionals can help bring these behaviours to life through story-telling, case studies and experiences. By focusing on training and development efforts that help employees to think, act and behave in an ethically and culturally aligned way, HR can impact culture. Also, those who are successful within a culture should be given additional development opportunities so that they can assume positions of greater responsibility. By developing and promoting those who support the values and corporate culture, the desired behaviours are reinforced.

Organisations that promote employee development as part of their corporate culture should ensure that enough resources are allocated to HR's training and development budget. The allocation of scarce resources is a sign that employees look for when determining if an organisation is serious about creating the culture they espouse.

Recruitment and orientation

Recruitment practices should aim to increase the probability of recruiting those who reflect or can readily adapt to the values, principles and culture of the organisation. This ensures the new employee's assimilation to the company and further strengthens corporate culture. It's important that, when hiring managers, interviewers and recruiters can identify critical characteristics and values and principles that mesh well with the company's ethical framework and desired culture – although hiring someone who will be a good fit culturally should not be used as an excuse for a lack of diversity in recruitment. Hiring different types of people lessens the risk of the kind of group think that often contributes to breakdowns in organisational culture.

Job descriptions and other recruitment literature should reflect desired characteristics. For example, if a strong sense of entrepreneurism is a cultural hallmark, ensuring that potential candidates are entrepreneurial, with a track record of thriving in similar environments, will be important; these characteristics should feature in job descriptions and interviews. If flexible working arrangements are upheld as desirable characteristics of an organisation's culture, interviewing managers should respond positively when job applicants seek to obtain information about such arrangements.

Interview questions such as the following may assist in the recruitment process:

- What type of culture do you thrive in? (Does the response reflect your organisational culture?)
- What values are you drawn to, and what's your ideal workplace?
- Why do you want to work here?
- How would you describe our culture, based on what you've seen? Is this something that works for you?
- What best practices would you bring with you from another organisation? Do you see yourself being able to implement these best practices in our environment?

New employee orientations should focus on helping employees connect to and navigate the culture of the organisation. They should build on (not contradict) the individual's cultural education, commenced during the recruitment process. Facilitated case studies that highlight cultural norms and practices, videos and profiles (of customers and employees) can be useful tools in illustrating the culture of the organisation during orientation.

Chapter 5 – Gaining assurance over risk culture

Given the regulatory expectations regarding risk culture, and the importance of developing a 'desired state' which is embedded throughout the organisation, boards need to understand whether the culture they want is the culture they have.

The setting and monitoring of risk culture is a board responsibility with senior management responsible for implementing the desired culture. However, as with any risk, both the board and senior management will require an independent assessment of how the desired culture is being embedded, and whether the lived culture aligns with that. Assurance providers in the form of internal and external audit can advise on how robust the framework for risk culture is, as well as providing an independent view of the 'as is' risk culture and flagging where the desired culture is not embedded.

Internal audit

Regulatory expectations

Internal audit is increasingly being requested by boards, senior management and some regulators to review and provide an assessment on culture, but in many cases specifically targeting risk culture. In the UK, the financial services regulators have a specific requirement for internal audit to review and comment on risk culture. Internal audit's role in auditing culture can be to provide independent assurance that the culture and values the board and senior management have set are being lived throughout the organisation.

In the UK, the *Effective Internal Audit in the Financial Services* recommendations produced by the Chartered Institute of Internal Auditors in 2013 and 2017 recommends that internal audit should include within its scope the risk and control culture of the organisation, and should also evaluate whether the organisation is acting with integrity in its dealings with customers and the wider market.

The Hong Kong Monetary Authority (HKMA)[53] expects that firms should have a dedicated board-level committee to assist the board in discharging its responsibilities for culture-related matters, noting that this committee should be assisted by internal audit functions to 'review and confirm the effectiveness of the overall culture enhancement initiatives pursued by the institution'.

In Australia, for many internal audit departments, an assessment of risk culture is an intrinsic part of their independent reviews of Prudential Standard CPS 220. The Standard (which came into effect on 1 January 2015) requires that the board should ensure a sound risk management culture is established and maintained, and that the risk management strategy should instil an appropriate risk culture within the organisation.

The role of internal audit

Internal audit has a unique position – it is based within the organisation, but is also independent and objective. Its knowledge of practices across the organisation (gained through ongoing audit reviews) means that it is well placed to provide a perspective on practices across the organisation, and also to assess risk culture, based on the practices and behaviours they observe.

The Chartered Institute of Internal Auditors in the UK (in *Organisational Culture: Evolving Approaches to Embedding and Assurance*) identified a number of enablers that need to be in place to allow internal audit to review and comment on risk culture:

- Organisational culture has been analysed, properly defined and disseminated by the board/senior management – that is, what is required behaviour in the organisation has been made explicit.
- Appetite from the top of the organisation.
- Internal audit has been given a clear mandate.
- The mandate has been written into the audit charter.
- There is a relationship of trust between the audit committee chair and the head of internal audit that allows informal discussion about subjective judgements on culture.
- Position, treatment and regard for internal audit and a non-adversarial relationships with their clients.
- Clients have the ability to report or respond to surveys confidentially.
- There is a good level of risk maturity in the organisation.

In order for internal audit to succeed in this role, it is vital that the value that they can add is recognised and supported. Part of this value is the aforementioned organisation-wide view of practices that the department has. This gives the team the ability to comment on the framework around risk culture, including challenging whether the desired culture has been defined and whether it is appropriately embedded.

Another element is the trust that internal audit has within the organisation and the ability of the team to have honest conversations. This is especially pertinent when assessing the lived culture, calling out where the actual culture is out of step with the desired state.

---

53 Hong Kong Monetary Authority, 'Bank Culture Reform', 2 March 2017.

Indicators of sound culture and 'red flags'

As previously mentioned, the role of articulating the desired risk culture rests solely in the hands of the board and senior management, who should define the desired state and the values and principles. These will be different from organisation to organisation. Regulators (including the PRA and FCA in the UK, and ASIC and APRA in Australia) have stated that they will not define what 'good' culture is, but many of them have articulated some expectations of what characteristics should be in place for a good culture. William C Dudley (CEO of the New York Reserve Bank),[54] noted in a speech that the focus and values of banks should be on 'sustainable success, not short-run profit'. In their June 2014 paper,[55] the FCA stated that 'we expect firms to have a culture that places customers and market integrity at the heart of their business'. The UK Banking Standards Board[56] cites these characteristics of good culture: honesty, respect, openness, accountability, competence, reliability, responsiveness, personal and organisational resilience and shared purpose. The HKMA[57] identifies three 'pillars' for promoting sound bank culture – governance, incentive systems, and assessment and feedback mechanisms (including whistleblowing). Andrew Bailey, CEO of the PRA said in a speech in 2016[58] that 'my assessment of recent history is that there has not been a case of major prudential or conduct failing in a firm which did not have among its root causes a failure of culture as manifested in governance, remuneration, risk management or tone from the top.'

A number of regulators have clarified what behaviours contribute to a poor culture, or what would indicate a poor culture. The FCA[59] has articulated the failings that would lead them to enhance their supervision of a firm:

- The observation of numerous or especially significant conduct failings or repeated failings that when examined individually might not be considered serious
- The occurrence of failings in several business areas, as this is an indicator of wider cultural issues within the firm
- A poorly functioning board – for example, failing to challenge executives or take a lead in considering conduct
- Evidence of control areas such as risk, compliance and internal audit being poorly managed, under-resourced, or unable to make their voices heard at board level
- Evidence of weak risk management, or
- Evidence of other weaknesses in the way in which the board and senior management influence key cultural factors, for example 'tone from the top', pay and incentives, and their adherence to the organisation's values.

The PRA[60] has also articulated their indicators of culture failings, which are very similar:

- The observation of multiple examples of firms failing to conduct their business in a safe and sound manner, including failings in different business areas, that may not be related or that when examined individually may not be considered serious
- Evidence of a poorly functioning board that fails to challenge executives or take a lead in consideration of conducting business in a safe and sound manner, which can include setting, articulating and embedding an appropriate culture in the firm, and drawing up clear policies and guidelines that are linked to staff objectives, training, evaluation and incentives
- Evidence of weak control areas such as risk, compliance and internal audit that may indicate poor management, lack of resources, or insignificant representation at board level
- Evidence of other weaknesses in board or senior management behaviour and the influence of these on board culture, including incentives and adherence to the firm's values
- Any other evidence of failings in culture identified by the PRA's supervisory approach.

APRA[61] identifies the following behaviours as indicators of culture failings:

- Pursuing short-term financial interests, including personal interests, with little or no consideration of customer interests
- Observing the letter of relevant law and regulation while contravening the spirit of those laws and regulations
- Treating risk management processes and/or controls as inconveniences which can be disregarded when it is expedient to do so
- Poorly defining management accountability for risks
- Failing to reward good risk management and/or apply consequences for poor management of risks
- Senior executives and/or directors failing to take timely actions to mitigate significant risks
- Concealing problems, rather than resolving the underlying causes of the problems, and
- Failing to challenge the status quo and consider alternative viewpoints, resulting in a false sense of security and risk blind spots.

Auditing culture

'Culture' is not just behaviour. Andrew Bailey, CEO of the FCA, noted in a speech in 2016 that 'culture is a product of a wide range of contributory forces: the stance and effectiveness of management and governance, including that well used phrase 'the tone at the top'; the structure of remuneration and the incentives it creates; the quality and effectiveness of risk management; and, as important as tone from the top, the willingness of people throughout the organisation to enthusiastically adopt and adhere to that tone".[62] Greg Medcraft, ASIC Chair, spoke about the key drivers of a positive culture,

54 'Reforming culture for the long term', a speech by William C. Dudley to the Banking Standards Board, 21 March 2017.

55 FCA, *Tackling Serious Failings in Firms – A response to the special measures proposal of the parliamentary commission on banking standards June 2014.*

56 Banking Standards Board, Annual Review 2016/17.

57 Hong Kong Monetary Authority, 'Bank Culture Reform', 2 March 2017.

58 'Culture in financial services – a regulator's perspective', a speech by Andrew Bailey at City Week 2016 Conference.

59 FCA, *Tackling Serious Failings in Firms – A response to the special measures proposal of the parliamentary commission on banking standards June 2014.*

60 PRA Statement of Policy – The use of PRA powers to address serious failings in the culture of firms, June 2014.

61 APRA, 'Information Paper – Risk Culture', October 2016.

62 'Culture in financial services – a regulator's perspective', a speech by Andrew Bailey at City Week 2016 Conference.

which included tone at the top, accountability, effective communication and challenge, and recruitment, training and rewards.[63] Within this context, then, there are four key ways in which internal audit can provide assurance relating to the culture in an organisation. The first relates to the definition of the *desired culture* – has it been clearly articulated and communicated? The second relates to *embedment* – has the desired culture been embedded into every part of the organisation? The third relates to *monitoring and measurement* – how is the board and senior management monitoring the culture? Lastly, internal audit also has a role in assessing the *actual culture versus the desired state* – are behaviours in line with the desired culture, as articulated by the board and senior management?

Desired culture – APRA, in its review of risk culture,[64] observed that 'clarity and a shared understanding of organisational purpose and values were central to driving cultural and behavioural outcomes.' However, they also noted that many organisations are still maturing when it comes to identifying both their desired risk culture and weaknesses in the current culture. Greg Medcraft noted that 'a firm should have a statement of its purpose and values, which sets out what it is trying to achieve (purpose) – and how it will go about achieving this (values).'[65]

While internal audit does not have a role in challenging the organisational purpose, values and principles, it does have a valuable role in ensuring that the culture, through shared purpose, values and principles is clearly defined and communicated throughout the organisation. This should specifically focus on the desired culture the board and senior management wish to implement and how it is communicated throughout the organisation, so that it becomes part of 'how we work around here'. Here, internal audit can usefully 'test' the communication through their ongoing audit work – for example, by asking staff whether they are aware of the values and behaviours expected of them. As part of the organisation themselves, internal audit will be recipients of key messages from senior management and the board, and will be able to form a view based on their own understanding of the desired culture.

Embedding the culture – While articulating the desired state is the first step, providing assurance over how this is embedded across the organisation, and assessing whether core documentation and policies are aligned to the purpose and values, is a valuable role that internal audit can play. A review of core information can identify whether there is a misalignment in any area. Potential areas for review include:

- Is the **business strategy** in line with the desired purpose, values and principles?
- Is the **risk appetite** set in line with the desired values and principles, and how is performance against the stated risk appetite monitored?
- Are **product development** and **product pricing** decisions aligned?

- Are **credit policies** aligned with the desired values and principles?
- How are **customer and supplier complaints** responded to?
- How are **problems and mistakes** identified and fixed, including **breaches**?
- Are the appropriate **delegated authorities** in place, and are these procedures complied with? How are **conflicts of interest** identified and assessed?
- Does the **recruitment** process support hiring people whose ethics, values and principles are in line with the organisation?
- Does the **induction** and **training** offered enable staff to connect to the values and principles, and desired culture, and reinforce the desired culture?
- Is the appropriate **incentive and remuneration** structure in place? Does it have any unintended consequences? Is the **performance management** process robust? Does it support both the values and principles of the organisation, and is it linked with the incentives that are in place?

Also, the 'tone' of how these policies and procedures are put in place is critical. PwC, in their paper on generating a positive culture,[66] noted that behaviours change depending on whether an individual is trying to avoid a loss or wanting a reward, and so positioning positive culture and behaviours as something to be rewarded and encouraged is critical.

Monitoring and measurement – An important element of culture is the oversight that board and senior management have over culture. A number of regulators have commented on the need for appropriate governance structures around culture, including an expectation that the board and audit committee will regularly discuss culture, and that reports are provided that give updates on cultural indicators, and provide insights into the current state of the culture. These dashboards will vary between organisations – internal audit can play a role in challenging the completeness and veracity of the information provided, as well as challenging what information is collected.

There are a number of performance metrics that can be used to provide an indication of the current state of culture. These include:

- Customer complaints
- Breaches, and timelines of breach reporting
- Whistleblowing reports
- Loss events
- Response to audit issues.

In addition, a number of HR metrics can be used, including levels of sick leave and untaken leave; information from exit interviews; code of conduct warnings, etc. Another measure is the results of staff surveys.

There are a number of challenges in developing these reports, including the challenge of identifying and aggregating the data, as well as being able to draw sufficient conclusions and identify trends.

63 'The importance of corporate culture', a speech by Greg Medcraft at the AHRI Senior HR Directors Forum, 5 April 2017.
64 APRA, 'Information Paper – Risk Culture', October 2016.
65 'The importance of corporate culture', a speech by Greg Medcraft at the AHRI Senior HR Directors Forum, 5 April 2017.
66 PwC and London Business School, 'Stand out for the right reasons – why you can't scare bankers into doing the right thing', June 2015.

Actual culture versus desired state – In addition to reviewing the governance and monitoring of risk culture, internal audit can play a role in providing the board and senior management with an independent assessment of the actual culture 'on the ground', as observed from their work. While this is still maturing in many organisations, there are predominantly two main approaches – auditing culture, or looking at the cultural aspects of what is being audited.

Some internal audit departments are using organisational psychologists to perform stand-alone reviews of culture, separate from their ongoing assurance work. This generally involves the use of surveys and focus groups to ascertain the culture in place. In this approach, the internal audit team is able to provide management with an overview of the culture that is in place, and the key drivers behind that culture. This then allows management to assess whether the culture is in line with the desired values and behaviours, and to make changes as appropriate. This assessment is a useful 'deep dive' into individual areas. However, this approach is also time-consuming, and requires a very specific skill set that not all internal audit departments may have. In addition, this role may also be played by other areas of the organisation (such as HR), who may be tasked with assessing the culture within the organisation.

Some internal audit teams are embedding a review of culture into each audit. This approach is dependent on the organisation having clearly articulated the desired purpose, values and culture, in order to have something to assess against. Typically in these reviews, the audit team will survey relevant staff. These surveys are often developed by organisational psychologists, who develop the questions based on the desired state of the organisation, and where the questions could indicate there that desired state has not been communicated, or has not been fully embedded. The results of these surveys are then used to drive a series of focus groups, performed at the same time as the ongoing internal audit work, to draw out key themes and drivers. While specialist skills are still required for performing this part of the audit review, it provides useful information which could explain wider control deficiencies and gaps.

The Chartered Institute of Internal Auditors, in their 2016 paper on culture,[67] noted that 'many auditors feel that there is more mileage to be had in looking at the cultural aspects in their standard audits than in separating out culture itself', echoing a previous report.

There are a number of ways of incorporating a cultural review into each audit in addition to that described above:

- **Focus on 'red flags'** Wolters Kluwer noted that one way that internal audit teams are assessing culture and behaviours through their audit work is by looking at how management engages with the audit process itself.[68] In this method, behaviours such as pushback from management, guarded conversations on issues or management disregarding issues raised, and inappropriate reactions from management could all indicate a poor culture.

- **Assessing management's control awareness** Some internal audit departments have developed a process for assessing management's overall awareness of risks and controls, as a proxy for assessing the culture. This is more comprehensive than the 'red flags' approach, and focuses on a number of key areas. EY, in their 2015 report on risk culture,[69] listed three main areas:
  - risk identification – covering ongoing risk assessment, monitoring and reporting
  - risk remediation – covering management's proactive approach to addressing issues
  - governance and attitude – covering engagement with internal audit, as well as internal management challenge on risks and remediation plans, and resourcing of second-line functions.
- **Clear focus on root cause analysis** another proxy for assessing the culture of the area under review is a focus on root cause analysis. The Chartered Institute of Internal Auditors noted that many internal audit teams in the UK are using this to explore *why* things happened, and what cultural aspects (including reward and remuneration, targets, appraisals, etc.) may have contributed to the issue.

Methods for auditing culture are still maturing, and there is no one right approach. However, internal audit does have a key role to play in providing the board and senior management with an independent assessment of how risk culture is being embedded and measured, and whether the 'as is' culture is aligned to the desired state. How internal audit is able to do that depends on the maturity of the organisation and the needs of the board, but, given the focus from regulators in various jurisdictions, it may well become a standard part of the role of internal audit over time.

External audit and culture

The external auditor may consider culture as part of their audit process. Working together and sharing insights around culture, the external auditors, internal auditors and management have the potential to deliver powerful insights regarding an organisation's internal culture.

While it is not the role of the external auditor to consider culture, some of the auditor's procedures examine areas which are often a reflection of an organisation's culture. External auditors are most commonly engaged to perform an audit required by legislation, the objective of which is to form an opinion as to whether the financial statements are prepared in accordance with accounting standards and/or relevant legislation. In order to achieve this objective, external auditors need to understand the entity and its environment. Gaining this understanding will involve gaining an understanding of the entity's culture, as this will have an impact on how susceptible the financial statements are to material misstatement due to fraud or error.

67 Chartered Institute of Internal Auditors, 'Organisational Culture – evolving approaches to embedding and assurance', May 2016.
68 Wolters Kluwer, 'Auditing risk culture, part 2: Where to begin', November 2016.
69 EY, 'Risk culture – the role of internal audit', 2015.

Although the term 'culture' is not used explicitly, a number of auditing standards imply that it must be considered throughout the course of the audit. External auditors are required to obtain an understanding of the control environment. This may include obtaining an understanding of whether management has created and maintained a culture of honesty and ethical behaviour. External auditors may also need to understand how management communicates and enforces integrity and ethical values. It might encompass determining matters such as management's consideration of the competence levels for particular jobs. They may need to consider the extent of the board's involvement with the business; how appropriate its actions are, including the degree to which difficult questions are raised and pursued with management; and its interaction with internal and external auditors. External auditors may need to understand management's philosophy and operating style, including their approach to taking and managing business risks. Understanding the organisational framework for achieving objectives, how authority and responsibility for operating activities are assigned and how reporting relationships and authorisation hierarchies are established, may also be necessary. Auditors sometimes need to understand HR policies and practices that relate to, for example, recruitment, orientation, training, evaluation, counselling, promotion, compensation and remedial actions.

Similarly, the auditor's obligations relating to fraud include performing risk assessment procedures relating to management's views on business practices and ethical behaviour. Other standards require the auditor to be on the lookout for instances of management bias. These are also useful indicators of the organisation's culture. Before even taking on a new client, auditors must also consider the integrity of each prospective client.

The following are examples of where culture might come into focus for the auditor as they obtain an understanding of the control environment:

- Poor staff engagement survey results, staff absenteeism and high levels of customer complaints are occurring in the retail arm of a client. This could indicate a higher risk of control failure, but is also evidence of a culture problem within that part of the business.
- A remuneration structure in a property investment company that incentivises short-term focus, a culture of fear and bullying, previous incidents and high staff turnover are all indicators of a higher fraud risk, but also very serious culture problems that may need to be addressed before they become embedded within the organisation.
- Use of significant assumptions that yield fair value accounting estimates in a financial intermediary may indicate possible management bias and potentially fraud. Again, instances of management bias may indicate a culture where manipulation of results is acceptable.

- Early consideration of remuneration of, and incentives offered to, financial planners could highlight the sale of large volumes of products to investors that breach licensing or regulatory requirements, which may impact the valuation of related business unit assets and result in impairment of those assets. This is an example which may result in direct financial statement implications, but also indicates a culture that emphasises results and not how those results were achieved.
- Before taking on a new client the auditor considers the attitude of key management towards such matters as aggressive interpretation of accounting standards and the internal control environment and whether the client is aggressively concerned with maintaining the firm's fees at as low a level as possible. If the prospective client exhibits these attitudes it can indicate a culture where quality and ethical behaviour are not respected.

The above examples show that while the objectives of a financial statement audit do not explicitly relate to culture, auditors play an important role in understanding and assessing an organisation's culture and values as part of their assessment of the control environment and fraud risk.

As discussed in the previous section, internal auditors may provide assurance to the board over culture. Benefits may also be achieved by engaging independent assurance practitioners to perform specific 'culture audits' which are separate to financial statement audits. With their knowledge of the entity, external auditors of financial statements may be well placed to perform such engagements. They can offer a benchmark on culture from their work with other entities. Additionally, smaller entities that do not possess an internal audit function can engage external auditors to provide desired assurance.

Elements of culture can be objectively assessed. An engagement might deliver assurance over specific assertions made by management which form a part of the cultural framework and which are supported by internal controls. For example: 'Our cultural framework is annually reviewed and available on our web site', or 'All of our staff are trained on our core values and decision-making process.' It may be challenging to measure and evaluate actual behaviours, but external auditors could give directors some level of assurance that the culture they believe is in place at board level is actually being promulgated throughout the organisation.

Auditors already implicitly consider aspects of business culture through many facets of their existing audit. Strengthening that focus can deliver better insights and preventative benefits. A targeted consideration of culture by the board, HR, risk management, internal audit and external audit could help identify failings before they start to threaten the organisation's existence.

Appendix 1 – Glossary

ASX Corporate Governance Council's Corporate Governance Principles and Recommendations – These set out corporate governance practices for entities listed on the ASX that are likely to achieve good governance outcomes and meet the reasonable expectations of most investors.

APRA-regulated entities – Entities that are regulated by the Australian Prudential Regulation Authority (APRA), which includes banks, building societies and credit unions (authorised deposit-taking institutions), life and general insurance companies and reinsurance companies, friendly societies and superannuation funds (excluding self-managed super funds).

Culture – The sum of an organisation's shared values and behaviours.

Delegated authorities – Boards can identify that an effective framework is in place clarifying who is the authorised decision-maker in what circumstances. The delegations of authority framework needs to align with the strategic objectives of the organisation.

Ethical framework – The ethical framework sits at the heart of the governance structure of an organisation, and enables the delegation of authority to a distributed network of responsible decision-makers while maintaining organisational integrity.

External audit – An engagement in which an assurance practitioner expresses a conclusion designed to enhance the degree of confidence of the intended users, other than the responsible party, about the outcome of the evaluation or measurement of a subject matter against criteria. There are levels of assurance, with an external audit providing reasonable assurance to users, which is the greatest degree of assurance available.

Governance Codes – Include requirements for the boards of listed entities to take responsibility for the governance and oversight of culture and risks.

Human Resources (HR) – The HR function is fundamental in shaping, reinforcing and changing corporate culture within an organisation.

Internal audit – 'Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes' (Chartered Institute of Internal Auditors, UK).

Operating and financial review (OFR) – Forms part of the annual report and is one of the key sources of information about entities, particularly disclosure of the key features of the business model, and should include environmental or other sustainable risks.

Orientation – New employee orientation helps employees connect to and navigate the culture of an organisation. Facilitated case studies that highlight cultural norms and practices, videos and profiles (of customers and employees) can be useful tools in illustrating the culture of an organisation during orientation.

Performance management – An important component of developing employees which can incorporate regular one-to-one meetings, performance appraisals and processes to manage underperformance. The performance management system should be designed to encourage the desired behaviour and values and discourage those behaviours that are inconsistent with the organisation's culture.

Remuneration – Rewards to employees can be directly linked to culture behaviours and outcomes, and act as a powerful reminder of what is important in the business.

Risk appetite – The level of risk an organisation is willing to accept as manageable.

Risk culture – The risk culture of an organisation is the shared attitudes (values) and behaviours of individuals concerning the management of risk within an organisation.

Risk management framework – The risk management framework is a set of components that support and sustain risk management throughout an organisation.

Risk management strategy – The risk management strategy provides a structured and coherent approach to identifying, assessing and managing risk across an organisation.

Training – HR impacts culture through internal training and development of employees, along with 'town hall' meetings that help them to think, act and behave in a culturally aligned way.

UK Corporate Governance Code – Ascribes a board's responsibility for setting the company's values and standards in dual-listed entities.

Values – An expression of what we think to be 'good'.

Whole-of-organisation governance – How authority is exercised and controlled below the board in an organisation.

Appendix 2 – List of abbreviations

AFS	Guidance to Australian Financial Services
APRA	Australian Prudential Regulation Authority
APESB	Accounting Professional and Ethical Standards Board
ASIC	Australian Securities and Investments Commission
ASX	Australian Securities Exchange
CA ANZ	Chartered Accountants Australia and New Zealand
FCA	Financial Conduct Authority (UK)
FRC	Financial Reporting Council (UK)
FRC	Financial Reporting Council (Aus)
GIA	Governance Institute of Australia
GFC	Global Financial Crisis
IMF	International Monetary Fund
IIA	Institute of Internal Auditors – Australia (IIA-Australia)
NZX	New Zealand Stock Exchange
OFR	Operating and Financial Review
PRA	Prudential Regulation Authority (UK)
SEC	Securities and Exchange Commission (US)
TEC	The Ethics Centre

Appendix 3 – Responsibilities and duties of directors in relation to culture

Legislation, governance code or regulatory standard	Responsibilities and duties of directors
Corporations Act 2001 (Cth) Given the evident importance of corporate culture in defining and shaping the conduct of corporations, these statutory duties extend to the engagement of directors on issues of corporate culture.	s 180 (duty to act with reasonable care and diligence) s 181 (duty to act in good faith in the best interests of the company and for a proper purpose) ss 182 and 183 (duty not to improperly use their position or information)
The common law also imposes fiduciary duties on directors.	The courts have classified these fiduciary duties under four headings: • To act bona fide in the best interests of the company • To exercise powers for a proper purpose • To retain discretion • To avoid conflicts of interest.
Division 12 of the *Commonwealth Criminal Code 1995* provides that culture can be used by a court to establish fault for corporate criminal culpability. The definition of corporate culture includes policies and rules, but also extends more broadly to attitudes and courses of conduct or practice. That is, written policies and what is actually done within an organisation constitute the corporate culture.	Under the Criminal Code, culture can be used by a court to establish fault for corporate criminal culpability. The Code permits fault to be imputed to a corporation which maintains a culture of non-compliance with the law in question or fails to maintain a culture of compliance and includes familiar common law principles that impute to the corporation the intentions, knowledge or recklessness of the board of directors or high managerial agents.
ASIC *Regulatory Guide 247: Effective disclosure in an operating and financial review*	The Operating and Financial Review (OFR) forms part of the annual report, which is one of the key sources of information about entities and therefore plays an important role in promoting the accountability of boards. It requires disclosure of the key features of the business model of the entity – that is, how the entity makes money and generates income or capital growth for shareholders, or otherwise achieves its objectives. It should also include a discussion of environmental and other sustainability risks where those risks could affect the entity's achievement of its financial performance or outcomes disclosed, taking into account the nature and business of the entity and its business strategy. Culture may be a non-financial risk that could affect the entity's achievement of its financial performance.
ASIC *Regulatory Guide 104 Licensing: Meeting the general obligations* (RG 104)	Guidance to Australian Financial Services (AFS) licensees about what ASIC expects in relation to their meeting the obligation to have adequate risk management systems
ASIC *Regulatory Guide 3 AFS Licensing Kit: Part 3 – Preparing your additional proofs* (RG 3)	The risk management system of a licensed financial services organisation is required to describe the main risks the business will face, focusing particularly on those that adversely affect consumers of market integrity, including: details of identified risks; how those risks will arise; their likelihood; their potential impact; mitigation and monitoring measures that the organisation has put in place; and the person responsible for managing each risk.

Legislation, governance code or regulatory standard	Responsibilities and duties of directors
Australian *Prudential Regulation Authority (APRA), Prudential Standard CPS 220 Risk Management,* January 2015	The board of an APRA-regulated institution is ultimately responsible for the institution's risk management framework and is responsible for the oversight of its operation by management. In particular, the board must ensure that it: **a** sets the risk appetite within which it expects management to operate, and **b** forms a view of the risk culture in the institution, and the extent to which that culture supports the ability of the institution to operate consistently within its risk appetite; identifies any desirable changes to the risk culture; and ensures the institution takes steps to address those changes. CPS 220 effectively requires that regulated boards must: • Specify the quality and character of the culture that they seek to attain (typically done in terms of core purpose, values and principles). Most importantly, boards are responsible for shaping the organisation's culture • Measure the extent to which the actual culture aligns with the ideal • Develop and implement measures to close any identified gaps between actual and ideal.
APRA *Information Paper: Risk Culture,* October 2016	The paper confirms that risk management is a critical area of responsibility for the board and a core component of a governance framework, and that boards are responsible for ensuring that risk-taking in financial institutions is conducted within reasonable bounds.
In the UK, the Senior Managers Regime and Conduct Rules introduced by the Financial Conduct Authority (FCA) and Prudential Regulation Authority (PRA) emphasise the importance of culture in dual-listed financial institutions.	The UK Senior Managers Regime holds individual managers accountable for poor conduct occurring in businesses for which they are responsible. The regime involves firms mapping out responsibilities for senior managers and having them pre-approved by regulators. Firms will also need to identify staff who could pose a risk of significant harm and assess their fitness and propriety. The Conduct Rules set out a basic standard for behaviour that all those covered by the new regime will be expected to meet.
The UK Financial Reporting Council's paper Corporate Culture and the Role of Boards	The paper addresses how boards and executive management can steer corporate behaviour to create a culture that will deliver sustainable performance. It specifically addresses the role of culture in long-term value and the role of the board in shaping, monitoring and overseeing culture.

Legislation, governance code or regulatory standard	Responsibilities and duties of directors
Principle 3 of the ASX Corporate Governance Council's *Corporate Governance Principles and Recommendations,* 3rd ed., 2014

Principle 3 requires listed entities to act ethically and responsibly.

The governance guidelines developed for listed entities are frequently adopted, or adapted for use, in other corporate structures and also in not-for-profit organisations and public sector entities. | The commentary to Principle 3 clarifies that the board of a listed entity should lead by example when it comes to acting ethically and responsibly and should specifically charge management with the responsibility for creating a culture within the entity that promotes ethical and responsible behaviour.

Recommendation 3.1: A listed entity should:

a have a code of conduct for its directors, senior executives and employees; and

b disclose that code or summary of it.

The commentary to the Recommendation states that the board delegates to senior management responsibility for the promotion of the code of conduct, proper training and proportionate disciplinary action if breached. |
| Principle 7 of the ASX *Corporate Governance Council's Corporate Governance Principles and Recommendations,* 3rd ed., 2014

Principle 7 clarifies that the board of a listed entity is ultimately responsible for setting the risk appetite for the entity, overseeing its risk management framework, and satisfying itself that the framework is sound. | Recommendation 7.1: The board of a listed entity should have a committee or committees that oversee risk.

Recommendation 7.2: The board should review the entity's risk management framework at least annually to satisfy itself that it continues to be sound.

Recommendation 7.3: The board should disclose if it has an internal audit function, how that function is structured and what role it performs.

Recommendation 7.4: The board should disclose whether it has any material exposure to economic, environmental and social sustainability risks and, if it does, how it manages or intends to manage those risks.

The commentary clarifies that the board delegates to senior management responsibility for the operational effectiveness of the management of risk and for operating within the risk appetite set by the board. |
| *UK Corporate Governance Code,* April 2016, ascribes to boards a responsibility for setting the company's values and standards in dual-listed entities. | Supporting principle A.1: The Role of the Board states that the board should set the company's values and standards.

The Preface states that a key role of the board is to establish the culture, values and ethics of the company and set the correct 'tone from the top'. The directors should lead by example and ensure that good standards of behaviour permeate throughout all levels of the organisation. |
| *UK Corporate Governance Code,* April 2016, ascribes to the board the responsibility oversight of risk management in dual-listed entities | Principle C.2: Risk Management and Internal Control states that the board is responsible for determining the nature and extent of the principal risks it is willing to take in achieving its strategic objectives. The board should maintain sound risk management and internal control systems. |

Legislation, governance code or regulatory standard	Responsibilities and duties of directors
New Zealand Stock Exchange, *Consultation Paper: Review of the NZX Corporate Governance Code*	The consultation paper outlines NZX's proposed amendments to the governance code, including Principle 1 – Ethical Standards, which requires boards to set high standards of ethical behaviour, model this behaviour and hold management accountable for delivering these standards throughout the organisation. Proposed Recommendation 1.1 requires boards to develop a code of ethics applicable to both directors and employees, and training on the code should be provided regularly.
US Securities and Exchange Commission (SEC) proxy disclosures: Companies operating in the US	The commentary clarifies that the board delegates to senior management responsibility for the operational effectiveness of the management of risk.
Financial Stability Board, *Guidance on Supervisory Interaction with Financial Institutions on Risk Culture: A Framework for Assessing Risk Culture,* April 2014	The guidance notes that 'While various definitions of culture exist, supervisors are focusing on the [financial] institution's norms, attitudes and behaviours related to risk awareness, risk–taking and risk management, or the institution's risk culture.'
APRA, *Prudential Standard SPS 220 Risk Management,* July 2013	**23** An RMS is a strategic document that describes the RSE licensee's strategy for managing risk and the key elements of the risk management framework that give effect to this strategy. At a minimum, an RSE licensee's RMS must describe: **f** the approach to ensuring all persons within the RSE licensee's business operations have awareness of the risk management framework and for instilling an appropriate risk culture across the RSE licensee's business operations.
Basel Committee on Banking and Supervision 2014, *Guidelines: Corporate governance principles for banks* (item 27)	'A fundamental component of good governance is a demonstrated corporate culture of reinforcing appropriate norms of responsible and ethical behaviour.'
Hong Kong Monetary Authority 2010, Supervisory Policy Manual, Risk Management Framework	In the section 'Key elements of an effective risk management framework': 'effective risk governance requires a strong risk culture which promotes risk awareness and encourages open communication and challenge with regard to risk–taking across the AI (including vertically to and from the Board and senior management).'

Appendix 4 – Drivers of good culture

ASIC	FRC
Tone from the top	**Demonstrate leadership**
• The board and senior management are responsible for creating a culture where everyone has ownership and responsibility for 'doing the right thing'. • The board and senior management should set the values and principles of an organisation's culture and ensure they are reflected in the organisation's strategy, business model, risk appetite, and compliance and governance frameworks. • The board and senior management should lead by example, by demonstrating the conduct that supports the organisation's values.	Leaders, particularly the CEO, should embody their desired culture, embedding it throughout the business and at all levels of the organisation. Boards should act when leaders fail to deliver.
Cascading values to the rest of the organisation	**Embed and integrate**
• Senior management needs to ensure the organisation's values are cascaded and understood throughout the organisation. • This is important, because quite often the message gets lost in the middle and is not received by the front line. It is important that middle and front line managers model the organisation's values, because this is how new and junior employees learn 'how things are done around here'.	• Company values need to inform the behaviours of all employees and suppliers. • Human resources, internal audit, ethics, compliance and risk should be empowered to embed the values and assess the culture effectively.
Translating values into business practice	**Recognise the value of culture**
Senior management should ensure the organisation's values are incorporated into all of its business practices. For example, how problems and mistakes are identified internally, elevated and fixed. Translating the organisation's core values into business practices is important, because it ensures there isn't a gap between the organisation's desired values and the actual conduct that occurs.	• Good corporate culture is an asset and source of competitive advantage. The board's role is to determine the purpose of the company and to ensure that the strategy, values and business models are aligned to it. • Directors should be pro-active on company culture.
Accountability	**Assess, measure and manage**
Senior management should ensure the compliance and governance frameworks that are in place are monitored and enforced.	• Indicators and measures used should be aligned to the desired outcomes and material to the business. • The board has the responsibility to understand the behaviours in the organisation and challenge where they see misalignment. • Boards should commit resources to evaluating and reporting on their culture.
Effective communication and challenge	**Be open and accountable**
• The board and senior management should promote a culture of open communication and effective challenge to allow current practices to be tested. • The board and senior management should encourage a positive critical attitude among employees, and promote an environment of open and constructive engagement.	• Openness and accountability matters at every level. Good governance focuses on how this takes place and those who act on its behalf. • It involves respecting a wide range of stakeholder interests, and is concerned with how the company conducts its business, engages with and reports to stakeholders.

ASIC	FRC
Recruitment, training and rewards	**Aligned values and incentives**
• The board and senior management should include behaviours and attitudes that lead to good conduct and outcomes for customers as part of the selection of all staff. • The board and senior management should ensure training is available to maintain staff knowledge about the organisation's values and the attitudes and behaviours expected of staff. • The board and senior management should also ensure that the company's remuneration and incentives (including promotions) across the organisation are linked to good conduct and good outcomes for customers. • Rewards play a big role in driving culture and conduct, because they impact on priorities and act as a motivator and reinforcer of conduct. It is therefore crucial that organisations recognise performance in a way that not only promotes good conduct, but penalises poor conduct as well.	The performance management and reward system should support and encourage behaviours consistent with the company's purpose, values, strategy and business model. The board is responsible for explaining this alignment to internal and external stakeholders.
Governance and control	**Exercise stewardship**
Under the board's stewardship, the leadership team should promote, monitor and assess the impact of the organisation's culture on conduct and make changes where necessary. It's important that there is direct access to the board and leadership team. It's also important that there is a process in place for periodic reporting to the board on culture, conduct and compliance issues.	• Effective stewardship should encourage engagement about culture and encourage better reporting. • Investors should challenge themselves about the behaviours they are encouraging in companies and to reflect on their own culture.

Appendix 5 – Key elements in whole-of-organisation governance

There are six key elements set out in Governance Institute of *Australia's Guidelines: Whole-of-organisation governance,* which include the dimension of risk governance:[70]

1 **Objectives:** The board should set the strategic objectives of the organisation (this includes the organisation's mission, key performance indicators and remuneration incentives) and ensure these are appropriately cascaded throughout the organisation.

2 **Risk appetite:** The board should apply a risk lens to the organisation's strategic objectives and incentives. This means asking questions such as: What are the risks that could hinder the organisation from achieving its objectives? What is the board's appetite or tolerance for those risks?

3 **Risks and opportunities:** The board should consider the risks and opportunities that could affect the organisation's ability to achieve its strategic objective, and also the controls that management should put in place to mitigate the risks and deliver the opportunities.

4 **Delegated authorities:** The delegated authorities (that is, the decision rights of individuals or committees) should be designed within the context of ensuring that the organisation pursues its objectives while operating within its desired appetite for risk.

5 **Boundaries on conduct:** The boundaries on behaviour and decision-making (through policies, procedures, standards, systems and controls) are developed within the context of ensuring the organisation pursues its objectives and opportunities while operating within its desired appetite for risk and the tone from the top as set by the board.

6 **Assurance mechanisms:** The assurance mechanisms, such as audits, reporting and sign-offs, provide the means of monitoring whether the framework is operating as intended.

The role of the board

In setting whole-of-organisation governance, it is the board's responsibility to:

• Set the mission and overall strategic objectives
• Form a top-down view of the risks and opportunities that could impact on the ability to achieve the overall objectives
• Determine the organisation's risk appetite (what level of risk the organisation is willing to accept)
• Align the organisation's incentives with achievement of the objectives
• Delegate authority to the CEO
• Set the top-down view of the mandatory requirements (policies) and controls, having regard to the risk appetite and risks
• Ensure that the strategic objectives, delegated authorities and policies are implemented and resourced properly
• Approve key documents (for example, the code of conduct)
• Establish the assurance mechanisms
• Monitor performance and conformance, ensuring the whole-of-organisation governance framework is both adequate and functioning effectively
• Set the 'tone from the top' in relation to culture
• Setting and appraising the core purpose, values and principles

---

70 Governance Institute of Australia, *Guidelines: Whole-of-organisation governance,* October 2015.

End Notes ASIC Speeches

'Conduct in the spotlight: Views from ASIC', a speech by John Price, Commissioner, ASIC at the Institute of Internal Auditors Australia's Financial Services Internal Audit Conference (Sydney, Australia), 29 November 2016; 'The current state of corporate culture', a speech by John Price, Commissioner, ASIC at the Governance Institute of Australia (GIA) 33rd National Conference (Sydney, Australia), 28 November 2016; 'A question of risk', a speech by John Price, Commissioner, ASIC at RMA Australia and PricewaterhouseCoopers (Sydney, Australia), 22 November 2016; 'Regulatory perspective on conduct risk, culture and governance', a speech by Cathie Armour, Commissioner, ASIC at Risk Australia Conference (Sydney, Australia), 18 August 2016; 'The importance of corporate culture in improving governance and compliance', a speech by Greg Medcraft, Chairman, ASIC at the Challenger Legal and Corporate Affairs team offsite (Sydney, Australia), 28 July 2016; 'Good corporate culture, values and ethics', a speech by Greg Medcraft, Chairman, ASIC at the launch of GIA's inaugural Ethics Index (Sydney, New South Wales), 20 July 2016; 'Tone from the top: Influencing conduct and culture', a speech by Greg Medcraft, Chairman, ASIC at the Thomson Reuters 4th Annual Australian Regulatory Summit (Sydney, New South Wales), 21 June 2016; 'Directors' duties and culture', a speech by Greg Medcraft, Chairman, ASIC to the Law Council of Australia, Business Law Section Corporations Workshop (Gold Coast, Queensland), 19 June 2016; 'ASIC's focus on culture – digging into the detail', a speech by John Price, Commissioner, ASIC to the GIA's Corporate Governance Forum 2016 (Sydney, Australia), 25 May 2016; 'Why culture matters', a speech by Greg Medcraft, Chairman, ASIC at BNP Paribas Conduct Month (Sydney, Australia), 24 May 2016; 'Why are we talking about culture?', opening remarks by Peter Kell, Deputy Chairman, ASIC at AFR Banking & Wealth Summit 2016 (Sofitel Wentworth, Sydney), 5 April 2016; 'Culture shock', a speech by Greg Medcraft, Chairman, ASIC at ASIC Annual Forum 2016 (Hilton, Sydney), 21 March 2016; 'Corporate culture and corporate regulation', a speech by Greg Medcraft, Chairman, ASIC at Law Council of Australia BLS AGM seminar (Melbourne, Victoria), 20 November 2015; 'Putting the customer first: Creating a win – win', a speech by Greg Medcraft, Chairman, ASIC at CFA Australia Investment Conference (Sydney, Australia), 13 October 2015; 'Trust and culture: What consumers want', a speech by John Price, Commissioner, ASIC at 2015 Customer Owned Banking Convention (Darwin, Australia), 21 September 2015; 'Trust and confidence, culture and ethics: The right nudge in shaping communities globally and locally', a speech by Greg Medcraft, Chairman, ASIC, delivered at the annual dinner of the Paddington Society, Cipri Italian Restaurant, Paddington, Sydney, 6 August 2015; 'The importance of culture to improving conduct within the financial industry', a speech by Greg Tanzer, Commissioner, ASIC, at Thomson Reuters' Third Australian Regulatory Summit (Sydney, Australia), 27 May 2015.

Appendix 6 – Contact details

The Ethics Centre (EC) Level 2, Legion House, 161 Castlereagh St, Sydney, NSW 2000 02 8267 5700

Chartered Accountants Australia New Zealand (CA ANZ), 33 Erskine Street, Sydney NSW 2000 02 9290 1344

Governance Institute of Australia Ltd (GIA) Level 10, 5 Hunter Street, Sydney NSW 2000 02 9223 5744

The Institute of Internal Auditors-Australia (IIA-Australia) Level 7, 133 Castlereagh Street Sydney New South Wales 2000 02 9267 9155.

CHARTERED ACCOUNTANTS™
AUSTRALIA + NEW ZEALAND