The Institute of Internal Auditors Australia

Auditing Risk Culture:
A practical guide

July 2021

Connect › Support › Advance

About the Institute of Internal Auditors

The Institute of Internal Auditors (IIA) is the global professional association for internal auditors, with global headquarters in the USA and affiliated Institutes and Chapters throughout the world, including Australia (IIA-Australia).

As the Chief Advocate of the internal audit profession, the IIA serves as the profession's international standard-setter, sole provider of globally accepted internal auditing certifications, and principal researcher and educator.

The IIA sets the bar for internal audit integrity and professionalism around the world with its International Professional Practices Framework (IPPF), a collection of guidance that includes the International Standards for the Professional Practice of Internal Auditing and the Code of Ethics.

Authors:

Elizabeth Arzadon, Kiel Advisory Group

Regardt Du Preez, Head of Internal Audit, QSuper

Professor Elizabeth Sheedy, Macquarie University

Copyright – IIA Australia ©

Disclaimer

July 2021

CONTENTS

INTRODUCTION

The idea of writing *Auditing Risk Culture – A practical guide* had its origins during the development of the Institute of Internal Auditors – Australia's publication *Internal Audit Better Practice Guide for Financial Services in Australia* which was released in November 2020. Included in this latter publication was Principle 6: 'Adopt appropriate methodologies for auditing risk culture'.

Given the broad scope that auditing risk culture entails, the IIA-Australia decided that a more comprehensive guide could benefit internal auditing professionals in not only the financial services sector, but across all industries.

The Institute approached Macquarie University's Professor Elizabeth Sheedy, who had worked on Principle 6 of the Better Practice Guide, to produce an outline for this guide. In addition, risk culture expert Elizabeth Arzadon, from Kiel Advisory Group, and QSuper's Head of Internal Audit, Regardt Du Preez, were engaged to assist by providing first-hand industry experience.

As Phaedrus observed in 1st-century Rome, 'Things are not always as they seem; the first appearance deceives many.' So it is that the culture of an organisation affects behavioural norms, which may help or hinder effective risk management. This is why measuring risk culture is necessary.

This guidance has been written by a group of experts to benefit internal auditors, board audit committees, senior managers and other assurance providers. This guidance is not mandatory. It is up to individual organisations to decide if auditing the risk culture is necessary. Having said that, poor culture can be the root cause of many problems.

This guide provides a practical evidence-based approach to auditing risk culture, with a robust model at its core. There are other risk culture models in the market, and these too should be thoroughly investigated. The approach adopted in this paper can be used with any such model.

This guide presents the internal auditor with information so they can decide to perform a risk culture audit themselves, or be in a position to discuss such audits in an informed way with internal functions (such as ERM) or external providers. We have assumed that any internal audit activity using this guide is a mature operation with a comprehensive understanding of the operation of the three lines in their organisation.

This guide outlines a ten-step model, which is not a checklist but guidance, as every organisation has a unique set of stakeholders, organisational context and audit capability. It also recognises that each sector in the economy functions differently.

As is pointed out in the guide, 'auditing risk culture is still a relatively new concept for organisations. This means that senior leaders, managers and staff – and auditors themselves – are still getting used to the idea.' Also, 'different organisations will be at different stages of their risk culture audit "journey".'

The guide outlines several methodologies for a risk culture audit program, from a surface level assessment to a more comprehensive audit. In addition, this guide contains a Toolbox of risk culture audit techniques which should be of use to internal audit practitioners.

While the guide was developed in the context of Australian financial services organisations, we believe that it will be useful more broadly: in non-financial organisations and both within and outside Australia.

I commend this publication to you.

Peter Jones
Chief Executive Officer
Institute of Internal Auditors – Australia

1

Risk culture and its context

1.1 Defining risk culture

Culture is a characteristic of a group of people – the shared perceptions about what behaviour is 'correct', prioritised and likely to be rewarded. Organisations pursue many different strategic priorities and operate in different political, economic and social contexts, so their cultures vary.

Individual behaviour is affected by the way in which actions are rewarded or punished. In the workplace, people learn what is acceptable behaviour by observing the behaviour (including speech) of peers and managers. Behaviour that is repeated regularly becomes the norm, or 'the way we do things around here'. Behaviour of managers and leaders is particularly important in demonstrating the priorities of the organisation.

Risk culture is an aspect of broader organisational culture. Risk culture refers to the behavioural norms that help or hinder effective risk management. Some definitions of risk culture also incorporate the group's underlying values and assumptions about risk management, and others incorporate policies and systems. In large organisations, subcultures often form in different areas and even in specific teams with different managers. Internal audit teams should not assume that risk culture is consistent throughout an organisation, or even within a large division or function or tier of management of that organisation. Culture normally forms in groups of people that have regular interaction with one another, often with a common manager.

1.2 The importance of risk culture

Risk culture is a crucial element within the risk management framework. Together with effective policies and systems, sound risk culture encourages desirable risk management behaviours such as open and regular discussion of risk, with concerns about business practices raised and acted upon promptly. Collectively, these behaviours help organisations stay within the risk appetite set by the board and achieve performance aspirations in a sustainable way.

An unfavourable risk culture can compromise the effectiveness of the risk management framework in a range of ways. When risk management is seen as a 'tick-box' exercise rather than a genuine priority, investment in risk capability and systems may be insufficient to really achieve adequate effectiveness. An overemphasis on short-term profits, growth in market share or cost minimisation can override risk management considerations in decision-making.

1.3 The role of regulators

Risk culture has been a focus of prudential regulators since the global financial crisis. The Financial Stability Board (an international body that monitors and makes recommendations about the global financial system) has issued guidance to prudential supervisors on assessing an entity's risk culture.[1]

The European Banking Association has stated that 'An institution shall develop an integrated and institution-wide risk culture, based on a full understanding of the risks it faces and how they are managed, taking into account its risk tolerance/appetite.'[2]

Australia's prudential regulator, the Australian Prudential Regulation Authority (APRA), requires boards of regulated entities to form a view of risk culture, and oversee action to enhance risk culture where necessary.[3]

Over the recent past a number of misconduct scandals have emerged in financial institutions including LIBOR-rigging (manipulation of market interest rates), the UK's PPI scandal (sale of inappropriate insurance products), Wells Fargo's opening customer accounts without their knowledge, and numerous problems in Australia that led to the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry. These conduct scandals are a particular concern to conduct regulators such as the Australian Securities and Investments Commission (ASIC).

1.4 Ethics and risk

Some people have questioned whether risk culture is adequate, on its own, to address issues of misconduct. This is because risk culture in some organisations is only indirectly concerned with customer outcomes. Poor customer outcomes may be seen not as a concern in their own right, but rather because they could result in long-term losses to the organisation through fines, legal costs, customer remediation programs and reputational damage.

A number of organisations increasingly promote ethical values, making clear that good customer outcomes are an objective for the organisation. When this happens, risk management takes account of customer objectives, and assessments of risk culture in such organisations should therefore emphasise risks to the customer as well as risks to shareholders.

The remainder of this guide reflects this approach.

1 FSB (2014). 'Guidance on Supervisory Interaction with Financial Institutions on Risk Culture: A Framework for Assessing Risk Culture'
2 European Banking Association (2011). 'EBA Guidelines on Internal Governance (GL 44)', Part C, paragraph 20.1
3 APRA (2017). 'Prudential Standard CPS 220 Risk Management', paragraph 9(b)

2

The role of internal audit

As a function that is independent of line management, an internal audit activity is well positioned to provide assurance on the design and operation of processes around risk culture and reporting, and to provide an objective view of the risk culture itself.[4]

2.1 Expectations of stakeholders

Although there is no prescriptive requirement in Australia for the internal audit activity to audit risk culture, there are a range of expectations from regulators, industry bodies, boards and management that imply a need for the internal audit activity to get involved.

2.1.1 Regulatory expectations

There is an increasing trend from regulators around the world to expect the internal audit activity to provide an assessment on risk culture. For example, in the UK, the Internal Audit Financial Services Code of Practice[5] (IIA Code) developed in cooperation with UK regulators has specific requirements for the internal audit activity to review and comment on risk culture; and the Monetary Authority of Singapore expects the internal audit functions of financial institutions to assess behaviour and culture.[6]

4 IIA Australia (2020). *Internal Audit Better Practice Guide for Financial Service in Australia*, Principle 6.1

5 The Internal Audit Financial Services Code of Practice was produced by an independent committee established by the Chartered Institute of Internal Auditors (IIA-UK & Ireland), with representation and observers from leading banks, insurers, the Financial Conduct Authority, the Prudential Regulation Authority and the Bank of England.

6 Monetary Authority of Singapore (2020). Information Paper: *Culture and Conduct Practices of Financial Institutions*. www.mas.gov.sg/-/media/MAS/MPI/Guidelines/Information-Paper-on-Culture-and-Conduct-Practices-of-Financial-Institutions.pdf

In Australia, Prudential Standard CPS 220 requires a board to ensure that it forms a view of the risk culture in an organisation and the extent to which that culture supports the ability of the organisation to operate consistently within its risk appetite.[7] In addition, the board must identify desirable changes to the risk culture and ensure that steps are taken to make those changes. The risk management strategy, approved by the board, must outline the approach for instilling risk culture in the organisation (paragraph 30(e)).

While the primary responsibility for the assessment and management of risk culture lies with management, internal auditing can play an important role in assessing how well this is being done and providing independent advice to the board.

For some internal audit activities, an assessment of risk culture is a key element of their periodic independent reviews of compliance with Prudential Standard CPS 220 (paragraph 44). The Hayne Royal Commission and APRA's Prudential Inquiry into the Commonwealth Bank of Australia highlighted the important role internal audit activities can play in the governance of an organisation.

2.1.2 Professional standards

The International Standards for the Professional Practice of Internal Auditing (The Standards) require the internal audit plan to be risk-based (Standard 2010). This implies that internal audit activities should consider what behavioural or cultural issues pose a risk to the organisation.

The Standards also require internal audit activities to add value to the organisation (Standard 2000) and to coordinate assurance activities (Standard 2050). This implies that internal audit activities need to understand the existing behavioural or cultural assurance processes within the organisation. There is little value in telling management or the board about a risk culture problem if it is already known and being prioritised.

Lastly, The Standards require internal audit activities to allocate appropriate resources to an engagement (Standard 2230). This implies that, as with any specialist area, appropriately skilled staff must be assigned to risk culture audits.

2.1.3 Professional guidance

IIA-Australia's recent *Internal Audit Better Practice Guide for Financial Services in Australia* is another reference that may help stakeholders understand that it is an accepted best practice for internal audit activities in the financial services sector to include risk culture within their scope.

The IIA has also published two relevant Practice Guides: *Auditing Conduct Risk* (2019) and *Auditing Culture* (2020).

2.1.4 Boards and management

The board and management of an organisation is responsible for setting and monitoring the desired risk culture. As with any aspect of governance, the board and management will require an independent assessment or view of how the desired risk culture is being embedded across the organisation.

The internal audit activity acts as the eyes and ears of the board and is ideally placed to observe everyday practices though the execution of the audit plan. Therefore, the internal audit activity is in a position to form a view of the risk culture across the organisation, independently of management. It can flag concerns with the board and management where the desired risk culture is not embedded. Internal auditing can also assess the appropriateness and effectiveness of the risk culture model if a formal model has been adopted (see Section 3 of this guide). The opinion of the internal audit activity is provided to the board directly and is not mediated by management.

For the internal audit activity to succeed, it needs a clear mandate from the board to review and comment on risk culture. The mandate should form part of the internal audit charter. The internal audit activity also needs a good working relationship with the chair of the board audit committee which includes regular discussions about risk culture observations.

2.2 Distinguishing the role of internal audit from other internal assurance activities

A common discussion point for internal auditors embarking on a new or augmented approach to auditing risk culture is the intersection of their role with other teams engaged in risk culture related activities such as second line[8] risk management, people and culture, or first line compliance. Clearly articulating the internal audit activity's mandate in relation to risk culture, and how it differs from the focus of other functions, is essential. Open discussion on respective roles and responsibilities also prevents misunderstandings about coverage, accountabilities, frameworks and principles, and efficient use of resources. Maintaining multiple independent lines of information to the board and management is important to balance the different priorities and unavoidable inherent bias that are to be found in any reporting line.

7 APRA Prudential Standard CPS220: *Risk Management*

8 The terms 'first line' and 'second line' refer to the three lines model, as explained in IIA Australia (2020), *Internal Audit Better Practice Guide for Financial Service in Australia*. While compliance is often a second line function, there are some examples of first line compliance teams.

Although there is no prescribed approach to delineating responsibilities for different functions in relation to risk culture, some common differentiators include internal audit's unique role in providing:

- Objective assessment of the formal processes through which the desired culture is articulated, embedded throughout the organisation, monitored and reported, and necessary corrective action taken.
- Independent assurance to leaders and the board on first and second line assessments of risk culture.
- An additional opportunity for staff to provide anonymous feedback on behaviour and risk culture in their area.
- A risk-based approach that focuses resources on areas of highest risk to the organisation.
- The capacity to leverage observations and data gathered by auditors who have regular interactions with all parts of the business in the course of their regular internal audit work.
- Existing governance mechanisms that offer reinforcement of improvement via issue and action logging, monitoring and progress reporting, as necessary.

First and second line management should be the primary source of risk culture information for the board. However, in some organisations (especially smaller organisations with an immature second line) it will be the internal audit activity. Where risk culture is already being assessed by other functions, the internal audit activity should evaluate the assessment methodology and challenge resulting assessments as necessary. (*Implementation Guide 2050 – Coordination and Reliance* provides relevant guidance.) Internal audit also can play an important role in considering the effectiveness of risk culture governance and reporting to the board.

EXAMPLE:
Coordination and reliance

A large organisation had a range of risk culture activities occurring across the first, second and third line of defence. However, discussions with the board and senior management were beginning to question the impact and relevance of the investment in these activities, especially in light of several material risk incidents. Internal audit agreed to enhance its coverage of risk culture across the organisation. The first step involved an evaluation of the organisation's group-wide risk culture model and governance mechanisms. This work considered the validity of the model being used to articulate expected standards of risk behaviour, and the effectiveness of key processes to identify, evaluate and escalate cultural risks to the board. After addressing these fundamental issues related to formal oversight and governance of risk culture, internal audit turned its attention to its own methodology for independently assessing risk culture outcomes in specific areas of high risk across the organisation.

The Standards require internal audit conclusions to be based on 'sufficient, reliable, relevant, and useful' evidence (Standard 2310) and appropriate analyses (Standard 2320), so internal audit teams should adopt a demonstrably valid risk culture audit model that reflects these standards. Risk culture audit findings are also likely to carry more weight if the assessment is conducted using an accepted, demonstrably valid model.

3

Risk culture model

3.1 Evaluation criteria for your risk culture audit

Adequate criteria are needed to evaluate any activity. Standard 2210.A3 requires that internal auditors:

- Ascertain the extent to which management and/or the board has established adequate criteria to determine whether objectives and goals have been accomplished.
- Use such criteria in their evaluation, if they are adequate.
- Identify appropriate evaluation criteria through discussion with management and/or the board if adequate criteria have not been established.

To determine whether risk culture is appropriate and whether appropriate processes are in place, a reference model is required. Assessment of culture may appear to be straightforward, but in reality it is complex and requires the robust discipline that validated models provide. There are many risk culture models available and the organisation may already have adopted one. If the organisation has formally adopted a model, then the internal auditor should assess it for adequacy and, if it is adequate, use it in their work.

Risk culture is still a relatively new concept, especially when compared with constructs, such as safety culture which have been studied for more than 30 years. A good model should have some evidence of validity that goes beyond just case studies.

Many models exist and choosing among them may be difficult. The most robust models provide statistical evidence that they measure the concept accurately ('construct validity') and predict outcomes the practitioner cares about ('criterion validity'). Independent peer review and scrutiny are both important, since there could be other factors that do an even better job of predicting those outcomes. The independent validation that comes from publication and peer review can provide some confidence in the validity of a model. Similarly, independent regulatory agencies and industry bodies can be a useful source of guidance for important factors that should be included in models

The best model for an organisation is not necessarily the one that produces the most favourable result. Arguably, a model that finds the weaknesses in an organisation may be best for promoting and tracking improvement.

Over time research and understanding of risk culture may also evolve and new factors emerge as important and relevant. Internal auditors should pursue ongoing professional development to stay abreast of such advances.

3.2 Example – the Macquarie model

For purposes of this guide we have used a model developed at Macquarie University. It will provide a vehicle for our examples and has a number of features that make it useful for this purpose. It is available for internal use by any organisation at zero cost; it has an evidence base that validates it; and it has been subjected to peer review.

The use of the Macquarie model does not imply that other models are invalid or should not be used for this purpose. Each organisation should choose a model that suits its individual requirements.

This model was developed by a multi-disciplinary team (risk governance and organisational psychology), including one of the authors of this guide. It has been validated in numerous financial institutions and in four separate peer-reviewed studies using a range of methods and published in top international journals.[9] This research suggests that when combined with well-designed risk management policies, frameworks and systems, favourable risk culture, as defined by this model, is likely to produce desirable risk outcomes. That is, desirable risk management behaviour will flourish and the organisation should achieve its objectives with few unwelcome surprises.

The model identifies four dimensions of risk culture:

- *Proactive* is a group of favourable behavioural norms that are associated with effective risk management by employees – for example, discussions about risk issues are constructive and focused on problem-solving rather than blaming/shaming.
- *Manager/leader* is another set of norms that specifically relate to the risk management behaviour of managers and leaders, who play a fundamental role in the development of risk culture – for example, managers and leaders are good role models of risk management behaviour such as reporting and resolving risk issues, and complying with policies.
- The *valued* dimension refers to risk management being genuinely valued by the organisation, and seen as an enabler for success, as opposed to being begrudgingly implemented at regulator behest – for example, where there is a sense of 'chronic unease' regarding risk management (the sense that, despite progress to date, we can and should do better).
- The *avoidance* dimension has been found to be one of the most important for predicting poor risk and control outcomes, such as misconduct and non-compliance with policy. Including it in your risk culture model is therefore highly recommended. Omitting it may mean that your organisation is not sufficiently focused on identifying the issues that might work against risk management. Avoidance is not just a lack of the 'proactive' culture dimension – it is indicative of the fact that other strategic priorities are undermining the risk culture, usually undue focus on short-term profits or cost reduction. In other words, there is a conflict between risk and other priorities that remains unresolved. Low levels of avoidance are preferred – for example, a high level of avoidance may be that employees perceive that top performers can get away with non-compliance with risk policy.

Detailed behavioural examples of each dimension are presented in Appendix 1.

9 Sheedy, E. A., Griffin, B., & Barbour, J. P. (2017). 'A framework and measure for examining risk climate in financial institutions'. *Journal of Business and Psychology*, 32(1), 101–116; Sheedy, E., & Griffin, B. (2018). 'Risk governance, structures, culture, and behavior: A view from the inside'. *Corporate Governance: An International Review*, 26(1), 4–22; Sheedy, E., Zhang, L., & Tam, K. C. H. (2019). 'Incentives and culture in risk compliance'. *Journal of Banking & Finance*, 107, 105611; Sheedy, E., Garcia, P., & Jepsen, D. (2019). 'The role of risk climate and ethical self-interest climate in predicting unethical pro-organisational behaviour'. *Journal of Business Ethics*, 1–20.

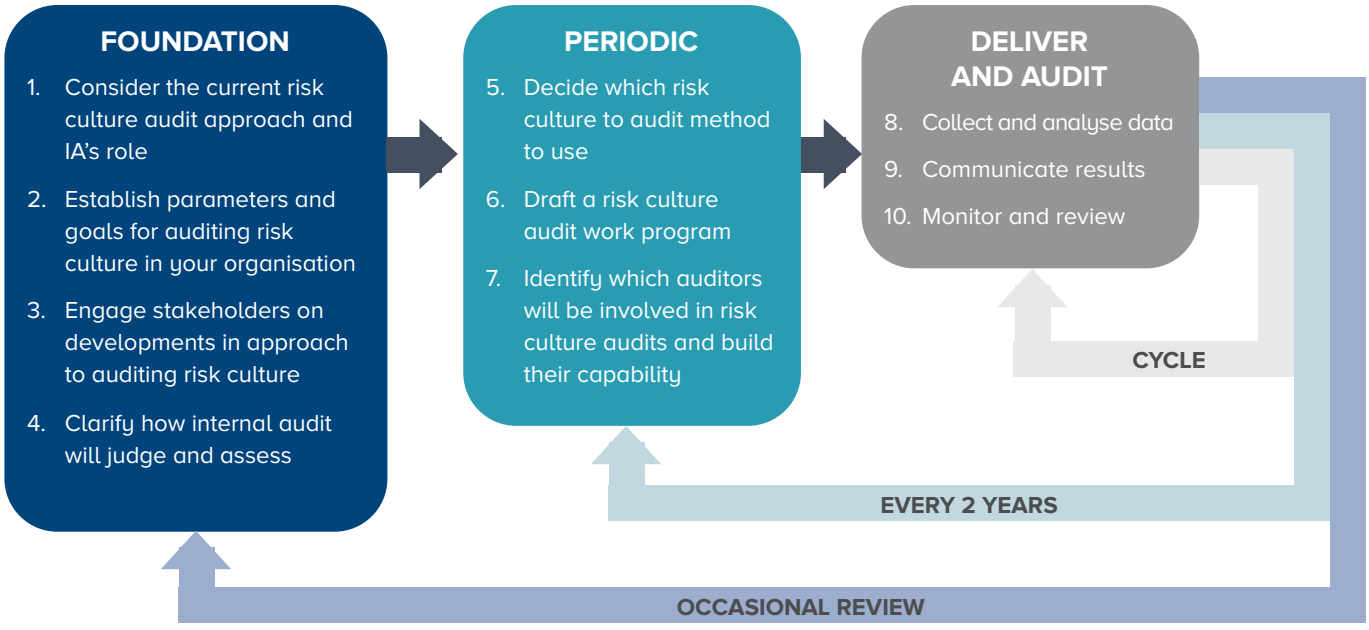
4

Auditing culture in practice

The IIA Practice Guides Auditing Culture (2019) and Auditing Conduct Risk (2020) provide some general guidance that will be useful to internal audit practitioners. In this guide we present a ten-step model that provides a roadmap for introducing or enhancing risk culture audits in your organisation.

Some steps (1 to 4) are undertaken initially and then reviewed from time to time to ensure continuing relevance to the organisation. Other steps (5 to 7) will be reviewed more frequently and adjusted as the organisation becomes more mature. The final steps (8 to 10) form a review cycle that continuously informs the organisation.

FIGURE 1 THE TEN-STEP APPROACH



The ten steps should be applicable to any organisation. However, this is a guide, not a checklist. Every organisation has its own unique set of stakeholders, organisational context and internal audit capability. The guide therefore requires your judgment to determine which options will suit your specific situation best. Some of these steps will be limited in scope in the first instance and coverage will expand as your organisation gains maturity.

Your risk culture audit program should be designed to deliver what best helps the board and management to govern culture, and improve management of risk.

Step 1: Consider the current risk culture audit approach and IA's role

Compared to auditing of financial and operational risks and controls, auditing risk culture is still a relatively new concept for organisations. This means that senior leaders, managers and staff – and auditors themselves – are still getting used to the idea. It also means that different organisations will be at different stages of their risk culture audit 'journey' or 'evolution'.

Getting started

The first step is to identify the objectives of an effective risk culture and the internal auditor's role in assessing it. Ask: what outcomes should an internal audit of culture achieve?

Then review the current approach to auditing risk culture if an approach has been established. If none exists, start to build one. If an approach has been established, consider whether it is fit for purpose.

In addition to reflecting on this question yourself, ask a range of stakeholders and your team for their opinions – for example:

- *The board and executive leadership:* does the information the internal audit activity currently provides on cultural drivers of effective risk management help you oversee risk culture and ensure weaknesses are adequately addressed? If risk culture information is being provided by other functions, how should internal auditing complement this information, and/or does the current information provided meet this expectation?
- *Business and functional stakeholders:* how well do you think the internal audit activity understands the cultural drivers of effective risk management in the organisation, and constructively ensures they are addressed?
- *Internal audit colleagues:* How confident are you that we are identifying, evaluating, reporting and reinforcing adequate improvement in risk culture across the organisation?

There may be value in a self-assessment (using the existing knowledge of the internal auditors) against a robust risk culture model.

Success factors

It is worth considering whether you see evidence of the following:

- Committed sponsorship from internal audit leadership (including the audit committee).
- Willingness to develop technical expertise on risk culture, or outsource expertise as required.
- Collaboration across relevant disciplines in the business (such as HR, risk, and internal audit).
- Alignment with the Core Principles for the Professional Practice of Internal Auditing.
- Ability to leverage (and adapt, if applicable) internal auditing mechanisms to ensure improvement is achieved where necessary.

EXAMPLE:
Consider the current approach

As part of the annual internal audit planning cycle, the chief audit executive meets with the audit committee and executives to discuss their expectations and the role of the internal audit activity as it relates to risk culture. The outcomes from these discussions then inform the principles (Step 2) and approach (Step 3) to auditing risk culture.

Step 2: Establish parameters and goals for auditing risk culture in your organisation

Before jumping into the task of auditing risk culture, it is important to stop and consider how to make sure the methods used by the internal audit activity are fair, fit for purpose, and in line with the broader goals and values of stakeholders. Stakeholders can feel defensive when questions are raised about leadership and culture. Investing in this step will help keep everyone focused on common goals and values when difficult discussions and decisions inevitably arise. Start by deciding on the general parameters the internal audit activity wants to observe when conducting risk culture audit work. You can then look at the more specific goals of the internal audit activity's risk culture audit program, which will likely reflect the organisation's broader goals.

Parameters

Internal audit activities are ultimately striving to support their organisation's purpose overall: internal auditing 'promotes organizational improvement'.[10] Risk culture audits, like all audits, must also be independent exercises built on strong audit parameters. The parameters underpinning risk culture audits should:

- provide a reference point for making decisions
- clarify competing priorities
- align with the expectations of the audit committee and other stakeholders, subject to the need for independent challenge
- explicitly incorporate professional standards and values
- anticipate risk and opportunities.

Some parameters are clearly established by The Standards:

- **Impact-oriented** – audit work is focused on a valid risk culture model that predicts outcomes and identifies root causes, providing the necessary foundation for action to drive genuine improvement (Standard 2210).
- **Sustainable** – the process must be managed with integrity, be cognisant of risks (to all parties) and ensure conclusions are reliable (Standard 2300).
- **Evidence-based** – all conclusions must be underpinned by sufficient, reliable, relevant and useful information (Standard 2310) such as triangulated qualitative and quantitative data sources.
- **Objective** – the methodology must employ techniques that minimise bias, both conscious and unconscious (Standard 2420).
- **Insightful** – conclusions should seek to highlight and provide evidence on issues that have been difficult to see, understand or act on in the past (Core Principles).

Other, organisation-specific parameters may be appropriate.

Goals

Identifying your organisation's goals in auditing risk culture will help you decide on the most appropriate approach and methodology.

EXAMPLE:
Goal of the risk culture audit program

If the ultimate aspiration of the risk culture audit is to directly contribute to overcoming the cultural barriers that are blocking effective management of risk, the audit approach and methodologies will need to include coverage of cultural root causes, not just observed behaviours and outcomes.

On the other hand, if the risk culture audit aims to focus only on reporting of risk culture, then a more limited coverage focused on key risks and effectiveness of risk culture assessment, reporting and improvement efforts may be appropriate.

In identifying goals, it may be helpful to consider the following:

- Is it important for risk culture audits to produce information that helps the executive to improve risk management outcomes? This would require significant depth of insight, and therefore greater capability.
- Are there any barriers to internal audit effectiveness that risk culture audits could help improve?
- What technical and/or leadership capability might be developed via a risk culture audit program?
- Could risk culture audit work be a vehicle for strengthening internal stakeholder relationships?
- Could the internal audit activity's risk culture work help the organisation improve its standing and reputation with external stakeholders?

10 *Core Principles for the Professional Practice of Internal Auditing*

Step 3: Engage stakeholders on developments in approach to auditing risk culture

You will already have engaged with stakeholders to gather feedback on the effectiveness of the internal audit activity's approach to auditing risk culture (see Step 1). The next stage of these discussions involves sharing the internal audit activity's response to various feedback, and its preliminary view on how it intends to audit risk culture.

This process exposes the internal auditor's outline assessment criteria to management as part of the process of developing the criteria.

Importantly, this is also the point where the internal audit activity may need to consider and raise any preliminary concerns about the organisation's risk culture framework (if they have one) and decide how to address these concerns. Such an approach may be prompted by stakeholder discussions in Step 1, or general observations that the framework does not appear to be based on research, regulatory expectations, or other evidence of validity. There are many ways internal auditors could proceed if they believe the organisation needs to revisit the risk culture framework and the criteria for 'what good risk culture looks like', but it would be unusual for the internal audit activity to proceed to other forms of culture audit work if they have serious concerns about the framework being used to define risk culture across the organisation. Addressing any issues at this stage also provides a strong basis for the internal audit activity's future work by ensuring stakeholders are aligned in their expectations of the scope and criteria for risk culture across the firm. Two options to consider include:

1. A formal audit of the existing risk culture framework against a set of criteria including primary and/or published research on the validity of key dimensions, regulatory expectations and other forms of evidence-based best practice insight related to risk culture models. The expected outcome from such an audit would be the adoption of an appropriate model and a set of criteria for 'what good risk culture looks like' across the organisation.
2. Alternatively, the board, executive, internal audit and other key functions might come together to identify, evaluate, challenge and agree on a framework that meets the needs of all parties. This process would ultimately aim to achieve the same outcome as (i), but in a less formal manner.

The time required for this step will depend on whether there is any need to change the organisation's risk culture model and whether any such changes involve minor tweaks or a major overhaul.

Which stakeholders to engage with at this stage

Assuming reasonable alignment on the model and criteria for risk culture, there is still work to do to ensure stakeholders understand how the internal audit activity will assess the effectiveness of risk culture in different parts of the business. Your team probably has a good idea of which stakeholders to keep engaging closely on IA's risk culture audit work. The following roles and functions are often good to engage in some way:

- executives with accountability for risk culture under relevant accountability regimes (such as the Financial Accountability Regime[11]).
- any relevant remediation or transformation programs
- second line risk culture team (if any)
- people & culture/Human Resources
- risk management
- compliance
- communications
- regulatory affairs
- operations
- controls assurance
- first line risk culture teams.

Anticipating concerns from auditees

It may be beneficial to anticipate which parts of the risk culture audit process are likely to cause particular concern in auditees, due to either misconceptions or legitimate risks. Discussing and preparing a standard approach to these kinds of issues will be helpful in establishing early buy-in to a new approach. Typical concerns are:

- How the internal audit activity will manage situations where misconduct is disclosed during a confidential discussion.
- Whether the business will know who the internal audit team have interviewed as part of the process (even if their specific feedback remains anonymous).
- Whether current members of the audit team will be involved in risk culture reviews, and whether information gathered will be used to inform their other audit activities.

11 See treasury.gov.au/consultation/c2020-24974

Addressing stakeholder resistance

The development or evolution of a risk culture audit program has potential to provide significant value, but it may also face stakeholder resistance – 'Why should I waste my time on this?' To address concerns, internal audit teams should:

- Engage leadership and peer opinion shapers within the internal audit team.
- Select pilot reviews carefully to demonstrate insight and build credibility.
- Engage sources of expertise outside the internal audit activity where possible (for example, HR and second line).
- Develop a robust capability-building strategy (develop/hire/co-source/outsource).
- Ensure findings are balanced, reflecting both strengths and challenges.

> ***Positioning the new approach as a pilot***
>
> Most new methodologies benefit from an initial pilot (or series of pilots). This provides the IA team with an opportunity to test and learn, and for the business to gain confidence in the new approach. It may also build reference cases and champions who can help others understand benefits in the approach. Be aware, though, that the internal audit activity should be genuine in this positioning – a review should be conducted after the pilot, and any learnings should be incorporated into the methodology.

Step 4: Clarify how internal audit will judge and assess risk culture

Even once there is agreement on the dimensions or 'topics' to be included in a risk culture model (proactive, manager/leader, etc.), how the internal audit activity will assess the degree to which these characteristics are evident is a practical question.

A key tool for conducting a behavioural assessment is a set of specific statements (sometimes referred to by social scientists as 'behavioural anchors') that describe desirable versus undesirable behaviours. Some internal audit activities go one step further and develop a series of statements that describe behaviours that might be expected at different stages of maturity. In addition, they may also define expected mechanisms, outcomes and/or mindsets or attitudes that might be displayed at each stage of maturity. Highly detailed maturity model descriptions are probably not required in many organisations, but a basic description has a range of advantages, in that it:

- supports transparency and alignment of objectives between the internal audit activity and their stakeholders
- reinforces a standardised audit approach across different auditors, businesses and timeframes
- reduces unconscious bias in an auditor's observations by providing a common reference point
- provides a view of what auditees should aim for if improvement is required
- focuses attention on observable elements of culture rather than less visible elements that are more reliant on judgment.

How to develop behavioural anchors

The process involved in developing a set of behavioural anchors commonly includes the following activities:

- Use the risk culture model that you have agreed is a valid model as your basic structure. Define key behavioural anchors for each dimension of the risk culture model – each dimension might include multiple behaviours that differentiate desirable from undesirable outcomes. See Appendix 1 for more ideas that relate to your business context.
- Consider existing collateral – most organisations have a range of existing documentation that may include reference to the kinds of risk management behaviour expected of staff and managers/leaders. These can be a useful source when defining behavioural anchors.
- It may be helpful to compare and contrast critical incidents where very poor versus very good risk management outcomes were achieved, and identify key behaviours that may have distinguished success from failure.
- Draft behavioural anchor statements – these statements should be specific descriptions of behaviour that define each end of the spectrum (and possibly the midpoints) for each behavioural dimension. It may be helpful to gather suggestions from the broader internal audit team, leadership and/or stakeholders for this exercise.
- Test, challenge and socialise with stakeholders – finally, the statements should be discussed with appropriate internal/external subject matter experts and/or stakeholders to ensure it aligns to external best practice, internal expectations and leadership aspirations.

EXAMPLE:
Behavioural anchors

Sample behavioural anchors for 'proactive' and 'avoidance' from the Macquarie model

Dimension: Proactive			
Behaviour	**Unacceptable**	**Acceptable**	**Desirable**
Raise concerns about risk	Staff rarely discuss risks within or outside their area of responsibility	Staff raise concerns related to risk, including issues outside their area of responsibility if asked	Staff are proactive about raising risk concerns, even if they are outside their area of responsibility
Report risk events	Staff conceal risk events and mistakes	Staff report risk events and mistakes with adequate level of detail	Staff are diligent about reporting events and mistakes thoroughly and in a timely manner
Personal ownership	Staff expect others to take care of risk matters	Staff understand and accept their role in risk management	Many staff are risk advocates, reminding peers of their risk

Dimension: Avoidance			
Behaviour	**Unacceptable**	**Acceptable**	**Desirable**
Risk management is de-prioritised in important situations	People breach risk policy to help meet sales/cost targets	People spend the minimum time on risk requirements in order to focus on other priorities	People maintain strong compliance with risk policies even when they are under pressure to focus on other priorities
Performance management policies not applied consistently (reward, promotion, etc.)	Exceptions are made for 'top' performers who breach risk policies	'Top' performers are permitted lenience with small breaches of risk policy (but not significant breaches)	Performance management policies are applied equally to all staff, regardless of performance on revenue or other dimensions
Respect for risk management and compliance	Staff speak disparagingly about risk management and compliance	Tension between front office and risk management sometimes exists, but is managed appropriately	Front office and risk management staff consistently exhibit mutual respect in their interactions

Step 5: Decide which risk culture audit method to use

Based on the goals identified in Step 3, you can now decide how to structure your risk culture audit. There is a broad range of individual data collection and analysis techniques that can be applied when auditing risk culture. The overarching method your internal audit activity has chosen will help guide these choices:

- Method I: surface-level cultural risk[12] assessment
- Method II: deep dive risk culture audits
- Method III: comprehensive risk culture audit program.

The key difference between these methodologies is 'how much of the iceberg' each one aims to understand:

FIGURE 2 STYLES OF COVERAGE

Method I (breadth)

Method II (depth)

Method III (breadth + depth)

12 This paper has made a distinction between 'risk culture' and 'cultural risk'. The latter refers to warning signs that raise concerns about the current/future culture of an organisation (see the Glossary).

Method I – Surface-level cultural risk assessment

Summary

- Provides an indication of cultural risk broadly across the organisation.
- Assesses visible aspects of culture (behaviours and outcomes).
- Highlights where problematic behaviours may be occurring and where deeper examination by specialists may be warranted.
- Possible tools are survey, traditional business data and behavioural observation as part of the regular audit program.
- Not sufficient for identifying whether behaviours are norms or isolated instances, or what their systemic drivers are.

Description

Method I involves broad, cultural risk assessment. Unlike deeper and/or more comprehensive methods of assessing risk culture, an assessment of cultural risk aims to identify where cultural issues are likely to develop due to pressure from external and internal conditions. It may also uncover evidence that problematic behaviours are already emerging and may become embedded. This method has the potential to provide an early warning sign of future risk culture issues. In response, cultural risk assessments also offer the opportunity to intervene early, rather than waiting until poor risk culture has already become systemically entrenched and more difficult to address.

Inherent cultural risk is related to factors that increase pressure on behavioural norms within a particular part of the business. These factors are often reasonably self-evident: for example, geographical expansion, an aggressive growth strategy, under-resourcing in key oversight or control roles, or intense cost reduction targets. Estimates of cultural risk can be made by considering various risk, people, customer and regulatory metrics, as well as evidence of observed behaviour collected by internal auditors in the course of their regular audit work. Certain audits such as employee life cycle audits (e.g., recruitment, training and performance review audits) may provide particularly rich data for this purpose. Properly conducted employee surveys can also provide a broad cultural risk assessment, identifying teams that may benefit from further investigation.

Taken together, this data can provide an indication of emerging materialisation of cultural concerns. It is important to note, however, that this kind of assessment is usually limited to the surface dimensions of culture, rather than a more complete view which includes the less visible (and less conscious) drivers of culture.

Method II – Deep dive risk culture audits

Summary

- Deep assessment of risk culture in defined teams, divisions or functions.
- Areas for review may be selected on the basis of known issues or leadership/board interest.
- Evaluates all elements of risk culture, from outcomes to behavioural norms and their systemic root causes.
- Not sufficient to gain an organisation-wide picture of culture, since risk culture often varies in different parts of the organisation.
- Uses a wide range of methods, as discussed in Step 8.
- Conducted by specialists in assessing risk culture, whether internally or outsourced.

Description

Method II involves a narrower, targeted review of risk culture itself. Targeted reviews seek to form a thorough assessment of risk culture in a particular subgroup. Such ‘deep dive’ reviews identify behavioural norms that are helping versus hindering effective management of risk, the systemic root causes driving these behavioural norms, and their impact on risk outcomes. Subgroups are usually divisions or teams, and could number from the tens to the hundreds. They could also be processes, controls or even risk types.

Depending on appetite, capability and capacity, a limited number of areas are generally selected on a risk-based approach. This approach can be a very effective method for introducing stakeholders to the value of internal audit, providing an independent assessment of risk culture in high-risk areas of the business, but may also be a valid routine model. One drawback is that such reviews are somewhat resource-intense, so the number of reviews that can be conducted each year tends to be limited. It is also important to select areas carefully, to ensure resources are directed to areas of most risk and impact.

Inevitably a risk culture review reflects the situation at a particular time and may be influenced by short-term contextual factors.

Method III – Comprehensive risk culture audit program

Summary

- Deep assessment of risk culture in areas that have been systematically identified as high risk.
- Combined breadth and depth.
- Uses a wide range of tools.
- Builds capability required for application of behavioural science to other internal audit activities – for example, identification of behavioural barriers to control effectiveness.

Description

Method III is a comprehensive, risk-based model, a hybrid of Methods I and II, but also potentially offering more than the sum of these two models. At higher levels of maturity, this model combines both a broad, data-driven assessment of cultural risk, and a program of deep dive reviews. This method offers the benefit of an independent perspective on where cultural risk is highest across the audit universe, as well as thorough reviews in high-risk subgroups. Internal audit activities adopting this method may also be in a position to balance the selection of review targets, with some aimed to preventative intervention (that is, areas where inherent pressure is high, but evidence this risk is translating into problematic behaviour norms is only just emerging) and others responding to identified areas of concern.

A comprehensive approach usually requires a range of tools and methodologies to be developed, as well as capability in both the generalist audit team and specialist risk culture auditors. Given these requirements, this method usually takes two to three years to develop, pilot and embed into business-as-usual practice. This may be undertaken through evolution from Method I, which can be implemented immediately.

How to decide which method to use

A broad range of factors will influence which method is best for your organisation. Depending on your situation, Method I versus Method II will have different advantages and drawbacks. There is no objectively right answer, and the best choice may change over time. In making their decision, the chief audit executive (with input from senior stakeholders such as the audit committee) will probably want to consider the following issues:

- board risk appetite
- executive focus on risk culture
- group-level strategy
- specific expectations of external stakeholders
- practices of peer organisations
- internal audit leadership aspirations
- other risk culture activities being undertaken in the first and second line
- existing internal audit capability
- access to expert capability
- history of auditing risk culture
- the dynamic between the internal audit activity and its stakeholders.

Phased introduction

It is not necessary to address the whole organisation at once. We have already discussed the advantages of running a pilot program. Once the pilot has been conducted and evaluated, culture audits can be rolled out progressively across an organisation.

Method I reviews may be conducted independently in different parts of the organisation. This allows the organisation to become accustomed to them and allows the internal audit activity to develop its competence in the process. While it might be a longer-term goal to develop a unified picture of culture across the organisation, such audits should be reported as they are completed – especially if problematic issues are identified.

Care should be taken to maintain a consistent approach throughout the process. The aim is to educate internal auditors in conducting a rigorous culture audit and not to allow the method to deteriorate through variations in the approach of individual teams.

While culture may change slowly, it does change. Therefore, you must be careful to keep various forms of data collection aligned in time and allow that different parts of an organisation may not be comparable if the reviews of some of them are conducted much later than the reviews of others.

Step 6: Draft a risk culture audit work program

Now that you have clarified the basic parameters, goals and method you will be using to audit risk culture, it is time to develop a plan for implementing any enhancements to your current approach.

Factors to consider

Drafting your risk culture audit work program involves considering a range of factors:

- selection of business areas to be assessed
- reporting of findings and observations
- monitoring of improvement actions
- capability-building required
- integration of risk culture audits into annual audit plan
- resourcing
- time requirement.

Some of these factors will require input from stakeholders outside of internal audit, and others are matters for the internal audit leadership team to decide. How you apply the factors will also depend on the method you have chosen in Step 5, as the following table shows:

I. FACTORS REQUIRING STAKEHOLDER ENGAGEMENT

Factors	Method I Surface-level cultural risk assessment	Method II Deep dive risk culture audits	Method III Comprehensive risk culture audit program
Selection of areas to be assessed	The scope of 'risk culture audit' activity needs to be defined (and may or may not be aligned to the scope of regular internal audit activity); most entities within the prescribed scope should then be assessed.	Generally less formalised than Method I; triggers may be risk-based ('push'), based on internal audit leadership and/or board consultation, or in response to a manager's request ('pull').	Deep dive reviews are generally selected on the basis of formal cultural risk assessment, supplemented by additional reviews in response to current events and/or at the request of other stakeholders
Reporting of findings	Reporting can be by individual audit, but it may be easier to report 1¬–2 times per year. Longer time periods are not recommended as it can be difficult to align collection, analysis and benchmarking of cultural risk ratings to timing of individual audits.	Reporting is by audit.	Multiple reporting cycles occur during the year including an annual/ semi-annual risk assessment, as well as targeted review reports.
Monitoring of improvement actions	May be limited to management-initiated actions, unless the risk assessment triggers a deep dive risk culture audit.	As above, resources may need to be allocated to design, monitoring and closing out of actions; some activities may be shared with other specialist functions such as people and culture or risk management colleagues.	As for Method II.

II. FACTORS FOR INTERNAL AUDIT LEADERSHIP TO CONSIDER

Factors	Method I Surface-level cultural risk assessment	Method II Deep dive risk culture audits	Method III Comprehensive risk culture audit program
Capability-building required	Period of methodology development and training and/or pilot required for general audit team.	More limited capability-building required initially – focus on deep dive audit team and internal audit leadership.	As for Method I.
Integration of risk culture audits into annual audit plan	Fieldwork may be integrated if data is being collected via audits – consideration of how much additional time is required per audit.	Generally reviews are conducted independently and do not have too much impact on the rest of the plan unless there is sensitivity regarding total time spent on audit activities.	As for Method I.
Resourcing	Generalist audit team, with facilitation and analysis likely guided by a subject matter expert.	Small specialist team (usually 1–2) supplemented with mid-to-senior generalist auditors as required.	Subject matter expert(s) can be leveraged to facilitate risk assessment and deep dive reviews.
Time requirements	Additional time should be factored into planning for each audit (if collecting data via routine audits); a quarterly workshop with internal audit teams to collate, analyse, document and benchmark observations is also necessary.	Deep dive reviews may require several months (depending on the size of the unit being reviewed), with resources dedicated 100%. Time may also need be allocated to post-audit engagement, to support development of appropriate actions, monitoring of implementation, and follow-up review (generally conducted 12–18 months after the initial audit) to ensure sufficient improvement is evidenced.	As for both Method I and Method II.

Step 7: Identify which auditors will be involved in risk culture audits and build their capability

Before embarking on a risk culture audit using your new or enhanced methodology, you will need to consider which team members will be involved in the work. Depending on the methodology you have chosen, this capability-building requirement will vary from just a few selected auditors to the entire department, and the level of knowledge required may vary from deep specialisation to the knowledge and skill necessary to use a standard set of tools.

Method I – Surface-level cultural risk assessment

This method usually leverages insight from a broader set of internal audit colleagues. It requires that the internal auditors be trained in the use and interpretation of the tools, and will initially require specialist support. In the longer term, it should be possible to conduct these audits using a typical internal auditor team. You will need to:

- Determine whether to identify a subset of the internal audit team to act as 'risk culture leads' – this is especially helpful if you have a large team with varying levels of experience, interest and aptitude in the area of risk culture.
  As suggested in the Internal Audit Better Practice Guide for Financial Services in Australia, ongoing investment in postgraduate education may be part of the solution, especially if the decision is taken to develop 'risk culture leads'. A number of universities now offer programs in business psychology that would be of benefit. Courses in qualitative research methods, with their emphasis on observation and ethnography, may also be relevant. See Appendix 5 for resources for further reading.
- Develop standardised templates for gathering and documenting data and behavioural evidence – this is important to promote consistency, decrease unconscious bias and accurately track progress over time.
- Conduct training to build capability – this will probably involve some element of classroom-style training or self-study in risk culture theory, as well as skill-building workshops and coaching on practical techniques such as behavioural observation.

Method II – Deep dive risk culture audits

Deep dive risk culture reviews generally require only a small team of auditors. This eases the burden of training your entire team of auditors. However, deep dive risk culture reviews involve technical skills and knowledge, similar to reviews involving other specialist risks such as IT or market risk. In addition, your lead auditors will need to feel confident to discuss the method in a credible way with their stakeholders, evaluate the appropriateness of actions arising from risk culture audits, and oversee the monitoring of improvement (if necessary) to ensure it is sufficient. Therefore, you should ensure the team includes at least one or two members with specialist experience in risk culture auditing, who can lead and coach generalist colleagues. If your audit team does not include any staff with this kind of experience, you will need to decide how to acquire or develop it. While larger internal audit activities may find it possible to recruit and maintain expertise in-house, many internal audit activities will need to rely on external resources. You could:

- Recruit one or two expert risk culture auditors to join your team full time. They may have expertise in organisational or social psychology, in anthropology/ethnography or in behavioural science – disciplines that develop skills in observation/interview techniques and survey methods.
- Engage an external provider to support the first few risk culture audits and help build capability within your team over time.
- Leverage a co-source or outsource provider to conduct deep dive risk culture reviews so you do not have to invest in a dedicated in-house team.

Example of NatWest Group (formerly RBS)[13]

NatWest Group, a major British bank, has created a behavioural risk team within internal audit. It comprises professionals from organisational psychology, behavioural science and other disciplines. The team conducts reviews in specific parts of the business, using a range of methods. Confidential discussions, focus groups and surveys are used to gain an understanding of staff mindsets and behaviours. Documents such as policies, processes, performance measures, meeting agendas/minutes, organisational charts and plans are examined to understand the formal environment. Team members attend meetings and observe employees working at their tasks, noting the group dynamics and interactions.

13 Engler, H., & Wood, A. (2020). 'How banks are using behavioral science to prevent scandals'. *Harvard Business Review*. hbr.org/2020/04/how-banks-are-using-behavioral-science-to-prevent-scandals

Method III – Comprehensive risk culture audit program

This method is usually selected by large organisations where risk culture is a strategic priority. It requires a larger number of internal auditors to be trained in conducting surface-level cultural risk assessments across the audit universe, as well as a team of specialist internal auditors to conduct deep dive risk culture audits in high-risk parts of the business. Therefore, all of the considerations noted above for Method I and Method II need to be addressed.

It is worth highlighting here that institutions embarking on a comprehensive risk culture audit program usually develop the scale and expertise necessary to expand their audit practices into adjacent issues. Although not strictly covered under the typical definition of 'risk culture', the following are narrower subtopics that could be assessed using the same specialist capabilities, and are therefore good options for audit functions applying Method III:

- behavioural root causes of material/high-risk incidents
- behavioural barriers to key control effectiveness
- change readiness and impact
- leadership team effectiveness.

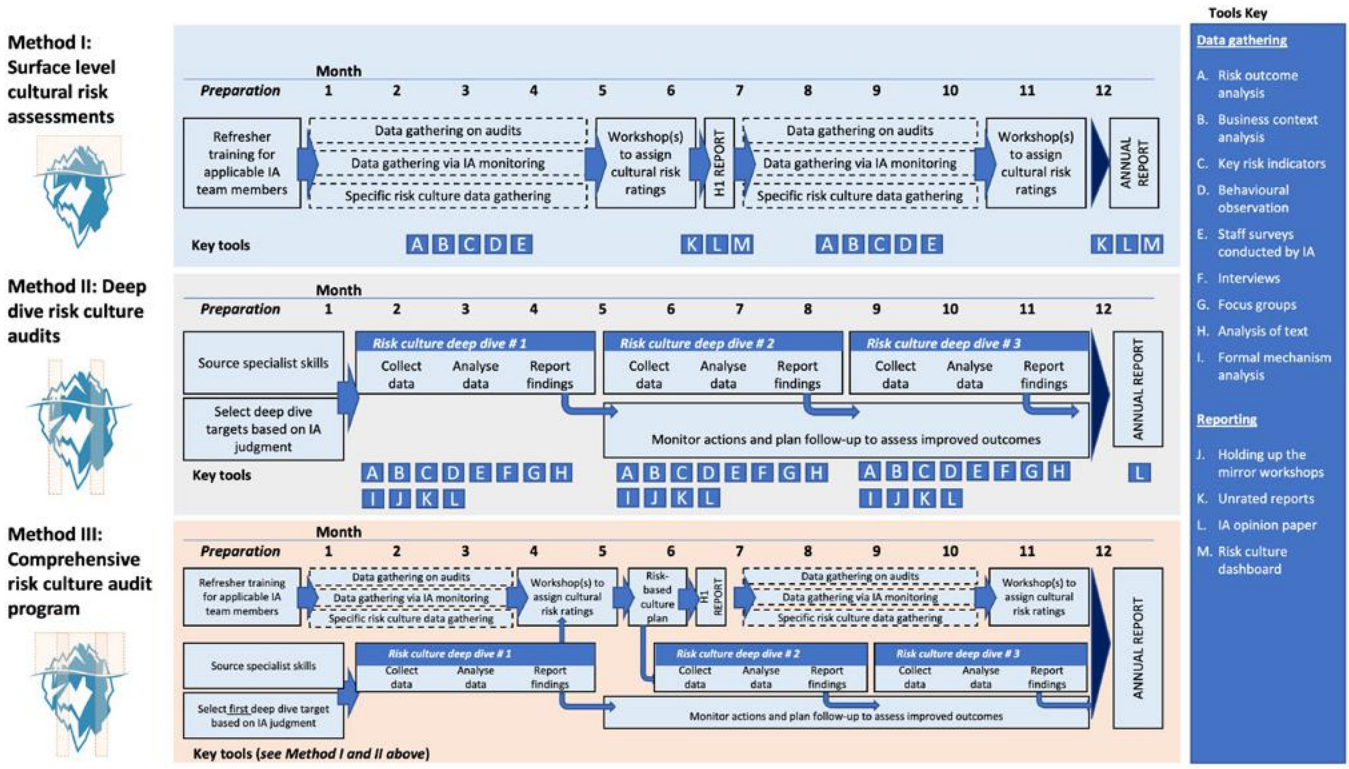
Steps 8–10 Deliver audit program

After all the planning involved in Steps 1 to 7, at this stage you are finally ready to conduct a risk culture audit. Regardless of the method you have selected, at a high level there are three major stages involved:

- collecting data
- analysing data
- communicating results.

The following flow charts provide an overview of the process required for each of these stages, depending on whether you have chosen to adopt Method I, II or III.

FIGURE 3 ANNUAL FLOW CHARTS FOR CONDUCTING RISK CULTURE AUDITS



You will notice that a number of the specific techniques under each stage are common across the different methodologies (it is more the number and combination of techniques that differentiates the scope of potential findings). The techniques are explained in greater detail in the Toolbox (Appendix 2 and Appendix 3).

Step 8: Deliver audit program – collect and analyse data

The Toolbox of risk culture audit techniques (see Appendix 2) serves multiple purposes:

- It provides guidance for internal audit teams wishing to provide an independent view of risk culture.
- It provides techniques that other parts of the business who are involved in risk culture assessment, including first or second line risk and compliance teams, may find useful.
- It provides guidance that could be used by the internal audit activity for the review and critique of methodologies used by the business to assess risk culture.

The internal audit work program should select appropriate sets of tools to give multiple perspectives. Different techniques may be appropriate for different approaches to the review (see Step 5). Appendix 2 discusses each of these in greater detail.

	REVIEW METHOD		
TOOL	**I**	**II**	**III**
A. Risk outcome analysis	✓	✓	✓
B. Business context analysis	✓	✓	✓
C. Key risk indicators	✓	✓	✓
D. Behavioural observation	✓	✓	✓
E. Staff surveys by internal audit	✓	✓	✓
F. Interviews		✓	✓
G. Focus groups		✓	✓
H. Analysis of text	✓	✓	✓
I. Formal mechanism analysis		✓	✓

The discussion of individual techniques includes references to both data *collection* and data *analysis*. This is a contiguous process. For example, in the course of conducting an interview, data is collected – such as in the form of interview transcripts. After conducting a set of interviews, a data set (i.e. a number of transcripts) will be available for analysis. Auditors then need to 'process' this data to develop conclusions or insights, such as ascertaining common themes that appear in multiple transcripts. This will produce an analysis for the interview data set. But what happens once you have analysed several different forms of data – interviews, a survey, and text analysis, for example?

No single method is perfect. By combining multiple methods and data sources, it is possible to mitigate the biases and issues that relate to each. Mixed-method culture assessments add credibility, insight and validity. Triangulation provides cross-validation of multiple types and sources of data to ensure conclusions are well-founded and robust. It enables us to bring together data from a range of techniques and draw conclusions.

First, data sources should be collected and analysed independently and then insights from each analysis compared, to determine whether they support the same conclusion. This could be done very simply in a table that captures evidence and resulting insights/conclusions against each dimension of the risk culture model from separate sources. The aim is to test for consistency.

An example of robust triangulation would be combining 20 unprompted interview comments referencing the idea that 'people avoid admitting mistakes in this business', 80 per cent of survey respondents saying the same thing, data on a lengthy average days-to-report-errors, several critical incidents arising from unreported errors, and an underutilised incident reporting tool. Each data point on its own may be open to challenge, but together they provide a solid set of evidence that the culture does not support escalation.

Practically, triangulation also offers the opportunity for conventional auditors to collaborate with and learn from specialists in other disciplines. Combining cross-functional perspectives often reveals patterns that would not be obvious when viewed from a single angle.

EXAMPLE:
Behavioural root cause analysis

Root cause analysis (RCA) is a common technique within conventional audit toolkits. Typically, the goal of traditional RCA is to identify the cause(s) of a control failure. Reflecting the systemic nature of culture, RCAs conducted as part of a cultural audit are aimed at identifying multiple interconnected factors that all contribute to an event. Usually RCAs conducted in this context start with a particular behavioural norm, and explore the range of formal and informal factors that mutually reinforce the norm. The RCA needs to be based on evidence collected throughout the audit, not just theoretical drivers.

A thorough understanding of how a behavioural norm is being reinforced is a critical first step in developing effective improvement actions. Not all drivers will be controllable (history, for example), but change is unlikely to occur unless something is done to mitigate the effect of environmental reinforcers. Further, cultural RCAs give insight into the likely time and effort required to achieve a shift, which is usually more nuanced than a simple training or compliance reminder.

Step 9: Deliver audit program – Communicate results

There are many ways that internal audit results may be communicated. While there is a long tradition of formal, written reports, these are not a requirement of The Standards, nor are they necessarily the best way of communicating observations. Standard 2400 only requires that we communicate results; it does not prescribe the manner in which this should be done.

There are many different approaches that can be taken to communicating results, and effective communication may require the use of more than one of them. Possible communication tools include:

	REVIEW METHOD		
TOOL	I	II	III
J. Holding up the mirror workshops		✓	✓
K. Unrated reports	✓	✓	✓
L. Internal audit opinion papers	✓	✓	✓
M. Risk culture dashboards	✓		✓

Appendix 3 discusses these techniques in greater detail.

Step 10: Deliver audit program – Monitor and review

Cultural change is notoriously difficult. Under Prudential Standard CPS220, boards of financial institutions are not only required to understand the risk culture that exists in their organisation, but also to 'identify any desirable changes to the risk culture and ensure the institution takes steps to address those changes'. Standard 2600 creates a requirement for internal audit activities that identify risk culture issues to determine whether they are being properly addressed and potentially escalate them to the board. Standard 2500 requires internal audit to monitor improvement efforts.

Three stages are key for effective monitoring of post-audit risk culture improvement:

- *Design and ownership of actions*

  The actions arising from a risk culture audit are often quite different to traditional risk and control audits.

  First, they tend to take a lot longer to execute – cultural change is not usually possible within the time frame required for resolution of high-rated issues in most organisations.

  Second, some additional work may be required to identify and prioritise specific actions required to address root causes of the issues identified. Due to the systemic nature of risk culture, the underlying drivers of issues are almost always multifaceted, and only a subset will be practical to change, eliminate or mitigate. Improvement plans to address cultural issues should involve divisional leaders and support from specialist colleagues (such as people and culture), with an eye to practical opportunities such as how to leverage other initiatives that may already be underway in the business.

  Third, actions need to be designed in stages, with test-and-adjust periods at regular periods to ensure progress is maintained. This is because cultural change can be unpredictable, as external and internal environments shift and interact with change efforts. The ultimate goal in addressing cultural weaknesses is improved outcomes, not a completed action that is no longer relevant.

  Finally (and similar to traditional audits), the most effective risk culture improvement actions are designed and owned by the applicable business area itself – not by the internal audit activity.

- *Close monitoring*

  It cannot be stated strongly enough: cultural change is difficult. Even when leaders are aware of and buy into cultural problems identified by an internal audit, 'old habits die hard'. In practice, this means that close and continuous monitoring is required to maintain momentum, motivation and focus. Internal audit is not the only function responsible for monitoring progress, but the internal audit activity's natural cadence of ongoing stakeholder engagement, traditional audit work and regular interactions with the board mean it can play a very useful role in supporting accountability for addressing cultural issues that have been identified.

- *Formal internal audit follow-up*

  Regardless of post-audit monitoring, a formal follow-up is recommended as a mechanism to close issues that have been raised in a prior 'deep dive' risk culture review. Follow-ups are usually scheduled 12–18 months after an initial risk culture review, and are intended to evaluate whether cultural issues have been adequately resolved. Importantly, this evaluation needs to extend beyond the question of whether initial actions were completed, to an assessment of necessary improvement. This implies that auditees need to take ownership of monitoring and adjusting their program of improvement activities as necessary, rather than just 'ticking off' actions, to ensure the desired outcome (i.e. cultural improvement) is achieved in practice.

  Follow-ups require a similar process to standard deep dive reviews, but tend to be shorter and more focused on the specific issues raised in the original review, as well as any unintended side effects that may have arisen due to improvement efforts or from other factors occurring in the intervening period. Follow-ups are a key step to help reinforce accountability for change, to ensure effective governance during the improvement period, and to provide a sense of closure for the business when successful improvement is achieved.

Plan for next year

Many internal audit activities evolve their approach to auditing risk culture gradually, reaching their desired business-as-usual stage of maturity over several years. Therefore at least every one or two years, it is helpful to consider:

- How 'bought-in' are stakeholders to the internal audit activity's risk culture work?
- Were the right auditors selected for the right tasks?
- What impediments were encountered, and how did we address them?
- Is the selected method still appropriate?
- What worked well, what did not, and what should we do to improve the approach next year?

Tips and traps

The development or evolution of a risk culture audit program has the potential to deliver value to an organisation. On the other hand, there are potential pitfalls that emerge both initially and as the program matures. The table lists some pitfalls to anticipate and avoid at varying stages of development.

Phase	Key challenge	Management strategies
Early	Stakeholder resistance	› Engage leadership and peer opinion shapers within the internal audit team. › Select pilot reviews carefully to demonstrate insight and build credibility. › Engage sources of expertise outside internal audit (e.g. HR and second line). › Develop a robust capability-building strategy (develop/hire/co-source/outsource). › Ensure findings are balanced, reflecting both strengths and challenges.
Embedding	Lack of improvement	› Ensure audit method focuses on outcomes, not just 'interesting' insights about the culture. › Ensure actions are focused on cultural root causes, not process steps that are easy to complete. › Set realistic time frames for expected improvement. › Be disciplined about follow-up to embed accountability. › Resolve instances where businesses can't or won't act.
Mature	Program gaps	› Plan carefully and flexibility to ensure audits are conducted in highest risk areas. › Leverage data science, technology and artificial intelligence to maximise inputs to cultural risk assessments. › Build breadth and depth into overall risk culture program. › Consider a variety of entity 'options' – e.g. divisions, risks, controls, geographies, etc. › Consider the nature and content of reporting carefully.

APPENDIX 1

Evidence-based risk culture model and behavioural indicators

Proactive (desirable)	Avoidance (undesirable)
› Business units (line 1) display accountability for managing the risks of their business. › Communication about risk management is regular/normal. › Staff are proactive about raising their risk management concerns. › Discussions about risk issues are constructive and focused on problem-solving rather than blaming/shaming. › Risk events are reported promptly; under-reporting and recurring issues are rare. › Past risk events and near misses are analysed and information used to adjust business practices where appropriate › Risk reporting is meaningful to the users and guides business decisions. › Staff consistently comply with policies. › Non-financial risks (operational, compliance, conduct) are managed as actively and systematically as financial risks. › Staff understand their role in the risk management framework and what behaviours are expected of them in relation to risk management (i.e. compliance with policy, plus raising issues/concerns). › Risk is generally within appetite (i.e. we take the right amount of the right risks). Exceptions to this are dealt with promptly.	› Employees perceive that managers/leaders don't want to hear bad news; raising issues is a waste of effort. › Employees perceive that top performers can get away with non-compliance. › Risk/compliance/internal audit budgets are under undue pressure; there is a lack of investment in systems, high-quality people resources and their professional development. › There is a sense of complacency about risk management, perhaps due to past strong performance. › There is an undue focus on short-term profits and self-interest (e.g. immediate bonuses). › When the business is under pressure (e.g. sales/ profits low, costs blow out), risk management is de-prioritised. › Risk issues remain unresolved for lengthy periods of time. › Breaches are not reported promptly to regulators. › There is a lack of clarity about what is considered acceptable/desirable behaviour. › There is a lack of clarity about accountabilities. › There is a lack of challenge/discussion about business practices, or evidence of groupthink, perhaps due to an unduly dominating manager or a lack of cognitive diversity. › There is resistance to the assessment of risk culture. › Risk reports are unread or ignored. › Poor behaviour is justified with diffusion of responsibility ('Everyone does it'); euphemistic language downplays the seriousness of the misconduct. › Gaming behaviour is apparent (e.g. manipulation of accountabilities, working to 'appear good' rather than actually do the right thing). › Risk/compliance/internal audit people or policies are mocked or disparaged. › There is a 'tick box' approach to addressing internal audit findings, rather than putting in place appropriate actions to address the findings. › Budgets and performance targets are overly ambitious and/or workloads are excessive, creating inherent conflict with risk management objectives.
Valued (desirable)	**Leaders and managers (desirable)**
› Risk management, compliance and internal audit staff are respected by the business. › There is a sense of 'chronic unease' regarding risk management (i.e. we can always do better). › Staff are thoughtfully engaged with the risk management process/framework, as opposed to 'mere compliance'. › Risk management is seen as an enabler, rather than a barrier, for achieving business objectives.	› Leaders and managers have a good understanding of the business environment, the risks that are present, and how they may be changing. › Managers and opinion leaders in the business are good role models of risk management behaviour, e.g. reporting and resolving risk issues, complying with policies. › People who speak up about risk issues/concerns are valued by managers, their concerns are taken seriously, and managers respond to their concerns appropriately. › Leaders and managers regularly communicate about risk management, in both formal and informal ways. › • When non-compliance occurs or when employees display lack of accountability for their risk obligations, there are direct, fair and proportional consequences in performance reviews, rewards, promotions, etc.

APPENDIX 2

Toolbox of risk culture audit techniques

Tool	Review method	Issues/Problems to consider
A. Risk outcome analysis Ultimately the nature of a tree can be judged by its fruit. Since the goal of risk management is to ensure that the organisation achieves its objectives, an obvious place to start is by considering whether targets have been met. Assess how outcomes relate to risk appetite, on key dimensions that are important for the business such as solvency, liquidity, business continuity, investment performance, efficiency, reputation, compliance with regulations, customer/member outcomes. Examples might be: › # of upheld customer complaints › # of regulatory breaches › # of operational events and impact on earnings, e.g. system downtime, processing errors › # and impact of adverse reputational incidents › investment performance relative to benchmarks/tolerances › major product launch on time and on budget › earnings relative to target/tolerances.	**I, II, III**	One of the biggest challenges of this technique is that the outcome measures are generally lagging rather than leading indicators of risk culture. We would prefer to get predictive measures of poor risk culture rather than waiting to observe bad outcomes.
B. Business context analysis This technique considers the business model (and any changes that may occur), and external and internal context, of individual parts of the business to identity factors that may increase or decrease pressure on behavioural norms. Auditors should consider theory, research and practitioner evidence on the kinds of environmental factors that put pressure on behaviour by affecting clarity of expectations, level of oversight, and drive to prioritise other objectives over maintenance of agreed risk appetite. For example: › Are profits low/negative? This might create pressure to take excessive risk in an attempt to recover lost revenue, or make it difficult to invest adequate resources in risk management capability or systems. › Are the products/services being offered complex relative to the ability of customers to understand them? Exploitation is more likely to occur in such environments. › Are employees in the business eligible for commission or variable remuneration? These are associated with increased misconduct.[14] Over time, new behaviours that emerge in response to these environmental factors can become normalised if not addressed early. It is generally most insightful to consider changes to business context alongside indicators that may suggest risk is materialising or receding as expected such as trends in key risk outcome metrics and KRIs (see sections below).	**I, II, III**	Auditors may need assistance in determining which factors have an evidence-based linkage to cultural risk, and new research is continually being published on this topic, especially in relation to the impact of factors such as remuneration models, customer vulnerability and remote working. Auditors should also take care in positioning this style of reporting to ensure stakeholders do not conclude that these factors are an excuse for poor culture; leaders still have responsibility for mitigating the risk that might arise from the presence of environmental pressures via effective management. Identification of some of these contextual factors relies on judgment and is therefore exposed to bias. There are many behavioural biases that plague risk management, including overconfidence and availability bias. Business leaders often have the most knowledge of risk in their own business but they also have incentives to downplay the inherent risk of their business, so such assessments should be interpreted appropriately.

Tool	Review method	Issues/Problems to consider
C. Key risk indicators We use the term key risk indicators (KRIs) to refer to measures that give early warning to managers of poor risk outcomes. In practice, finding good KRIs that are truly predictive (not lagging) and easy to measure is quite difficult. Suppose that an organisation has an objective and risk appetite statement related to customer outcomes. This is measured using # upheld customer complaints. Some possible KRIs with relevance to this outcome would be: # and type of customer complaints received, # open roles in relevant compliance function, percentage of staff completed relevant training in ethical treatment of customers, use of confidential hotlines and whistle-blower office, # compliance breaches, unusually high profits. Other traditional data sources with relevance to risk culture include: › Analysis of data from staff (e.g. staff or leadership turnover, staff complaints, completion of designated risk tasks). › Analysis of risk/issue reporting (frequency/severity/timeliness trends), evidence of under-reporting by line one, timeliness of issue resolution and repeat/recurring issues, number of breaches of risk policy. › The distribution of rewards/promotions is one of the best indicators of what the organisation truly values. This means that data relating to performance reviews, reward, and consequence management are another useful source of information (e.g. variation in manager ratings, suitability of consequences where misconduct is identified). Are employees with poor risk/compliance outcomes receiving appropriate consequences? › Auditors should especially consider movements in these metrics that reveal a problematic trajectory. As noted above, in conjunction with monitoring of inherent pressures it may be possible to identify areas where closer attention is warranted, therefore intervening before behavioural norms become too embedded.	**I, II, III**	In practice it is often difficult to find effective KRIs that are robust to manipulation. Their ability to predict outcomes of interest should be tested. Some measures have proven to be of limited value as indicators of culture in the field of financial services. For example, the net promotor score works badly as an indicator of customer outcomes because financial services are typically opaque, and many customers lack financial literacy. While customer complaints are likely to be a better source of information, there is evidence to suggest that even these are open to manipulation in certain instances. Measures that are open to manipulation are generally problematic, especially when they are linked to reward. In one organisation there had been a series of severe technology outages, known as Sev-1 outages. It was decided to set a key performance target for Sev-1 outages near zero. Staff in the technology area were informed that no bonuses would be paid unless the target was reached. The target was achieved, but this was done by refusing to classify any outage as Sev-1, even when there had been no connectivity for an hour. Monitoring problems are a major issue for some measures, such as short-term measures of compliance. These are typically overly rosy, since monitoring is imperfect and people will prefer to hide their 'bad' behaviour.
D. Behavioural observation Observations of behaviour can provide deep and supplementary insights into risk culture. It's possible to learn not only what behaviour is occurring, but also to discover what may be contributing to the behaviour – for example, group dynamics and communication style. Observation is a powerful form of triangulating evidence because what people say they do (in surveys and interviews) is often different from what they actually do. Arguably all internal auditors would benefit from some basic training in these skills, as they have an ideal opportunity to observe people at work around the organisation. Specialist observers, however, may be needed for gaining a deep cultural understanding. As specialist observation is time-consuming and requires expertise, it works best for evaluating the culture in small business units or teams. To assist observers in their task, and ensure consistency between different observers, it can be helpful to create a checklist or simple scoring system based on the risk culture model and behavioural indicators. The scoring might address the frequency of the behaviour and/or its strength, and should be designed in a way that aims to strengthen objectivity and standardisation of data, and reduces bias – for example, capturing verbatim quotes of those being observed, rather than the observer's summary or interpretation of what is said.	**I, II, III**	The presence of an observer may change behaviour. The observer effect (reactivity) tends to diminish over time as participants become habituated to the presence of the observer. Most people find it difficult to maintain unnatural behaviour for long periods of time. Reactivity can be reduced if the observer blends in by, for example, wearing similar clothing to those being observed. Reactivity will be heightened if participants think that the observer is looking for socially unacceptable or deviant behaviour. A second concern is the inherent subjectivity of qualitative interpretation, even when using tools aimed at reducing bias. The observer interacts with those being observed, making it difficult to be entirely neutral. Two different observers might draw different conclusions, depending on their backgrounds and biases. In addition, it is difficult to make objective comparisons between different business units, or between the same business unit at different points in time. Various methods are used to (partially) address this issue. See the book by Patton on qualitative research methods listed in Appendix 5 for further information.

Tool	Review method	Issues/Problems to consider
E. Staff surveys conducted by internal audit Provided that survey instruments with demonstrated reliability and validity are used, surveys can provide a useful measure of risk culture. Surveys gather information about the way staff perceive their environment, including their observation of normal behaviour, what drives these norms, and what impact they might have on risk outcomes. It is possible to compare scores between business units, and across time. It is also possible to statistically test whether cultural norms exist at all by examining whether perceptions of group members are similar. Surveys are very efficient; data can be gathered from large samples at relatively low cost. This creates the opportunity to identify and then further investigate, in much greater depth, business units that may be showing signs of cultural problems. Unfortunately, the attraction of efficiency may mean that surveys are overused in some organisations and 'survey fatigue' sets in. When this issue comes up, organisations may need to consider what their survey priorities are: risk culture or other issues (such as engagement). Surveys can offer anonymity, something that is never possible with interviews or observations. Arguably, you can obtain the most candid responses from participants if they are confident in confidentiality. To get maximum benefit from your survey: › Surveys should be anonymous (everyone gets the same link) not invitational (everyone gets a unique link). This helps employees feel safe to give honest responses. › Do not report results for small teams – say fewer than ten responses. Again, this helps employees feel safe to answer honestly. › Separate the risk culture assessment from your staff engagement survey. › Be wary of short surveys with fewer than ten survey items. As explained in Section 3, research suggests that risk culture is a multi-dimensional concept with at least four unique factors or dimensions that influence behaviour in different ways. Each one of these components typically requires 3–6 survey items for reliable measurement.	**I, II, III**	Because surveys measure what staff believe about the norms in their area, it can be difficult to separate 'perception' from 'reality'. On one hand, this may not be so important. since the way people perceive their environment is usually what drives their behaviour, and ultimately good or poor outcomes. However, surveys should not be used on their own to conclude facts – for example, the presence or absence of certain controls – as staff may not have sufficient information to form an accurate judgment. On a related point, surveys results can also be biased by deliberate or unconscious attempts to portray the business in a favourable (or indeed unfavourable) light. This risk is particularly relevant if survey results are linked to consequences, even indirectly – for example, staff may feel inclined to inflate their responses on certain items to be supportive of their manager, or avoid confronting their own role in poor cultural norms. To mitigate the risk of biased survey responding, results should not be used to feed into promotion or reward decisions. Good survey design can also help to mitigate this problem. The benefits of surveys may not be realised if organisations rely on poor survey instruments. Creating a valid risk culture assessment survey, sometimes called a scale, is a task involving specialist psychometric expertise and skills in writing effective survey questions that minimise response biases, as well as expertise in the field of risk governance. Proving validity takes a number of years with testing in multiple samples, applying the established protocols of survey design and validation. An in-house survey may be a 'cheaper' option, but ultimately poor value for money. In the case of risk culture, an invalid instrument may provide a false sense of comfort that all is well, and opportunities for management to intervene may be missed. Validated survey instruments can be used under license, or survey assessment can be outsourced.

Tool	Review method	Issues/Problems to consider
F. Interviews Interviews provide an opportunity to gain insight into the lived experience of interviewees. They provide an opportunity to better understand why behaviour is occurring, which is sometimes only possible by asking people about internal processes such as perceptions, interpretations and beliefs. In a sense, every interviewee is also an observer of the day-to-day environment under study, so collecting these observations provides the opportunity for a larger data set than observations of the internal audit team. Interviewees may include employees and leaders from within the area in the scope of a review, as well as stakeholders who interact with them – for example, key support functions such as complaint handling or operations teams. Exit interviews (with departing managers/employees) can also provide insight from individuals who may be more transparent about perceived challenges within an area. Interviews are often used as an inductive or 'exploratory' technique to elicit feedback without any pre-existing assumptions. To aid consistency and ensure appropriate coverage of relevant issues, interviewers often use a standard set of open-ended questions. Unlike surveys, interviews also provide the option of asking follow-up questions, which considerably expands the potential depth of insight. It is important that interviewers are experienced at asking questions in a way that promotes openness, and does not 'lead' responses in a particular direction. Skills in developing rapport and encouraging self-reflection are also important. To this end, a non-judgmental style is crucial. To enhance the reliability of findings, discussions should be held with a sample of individuals that reflect a cross-section of the population being examined. The more people who independently raise an issue, especially without prompting, the more confident we can be that the issue is representative of norms within an area. Finally, appropriate analysis of interview data is critical. Although interviewers will have a view of what themes have been discussed most often in discussions, these perceptions can be distorted by memory and other forms of error or bias. Content analysis is a common way to analyse interview data (and other text data such as survey comments), which helps improve reliability and validity of conclusions. Content analysis involves systematic coding of verbatim text to generate quantitative counts on the presence of certain themes, words, sentiments, etc. Computer programs are increasingly used to help facilitate this process, but manual coding is still the most common approach, to ensure high quality results.	**II, III**	Like any 'self-report' data source, interview data is limited by what interviewees are willing and able to share. It is critical that auditors consider how to maximise the reliability and validity of information gathered via interviews. Interviewers may need training and experience to apply techniques that effectively surface valid insight into cultural norms, including ways of helping interviewees to identify semi-conscious drivers of their own behaviour, and overcoming reluctance to share sensitive information. Additionally, robust analysis of interview data can also be resource intensive, and require specialist skills.
G. Focus groups Focus groups are more than just a group interview – social dynamics can be leveraged to gain insights that may not be achieved through one-to-one interviews. Focus groups allow an examination of how widespread a view is within the workplace, and participants may feel more confident to share their views if they observe others doing the same. Focus groups also offer the promise of greater efficiency than individual interviews. Confidentiality is difficult to provide in a group setting, which can make it difficult to explore highly sensitive or controversial issues. However, skilled facilitation, and careful consideration of group structure (e.g. keeping groups homogenous in term of function and/or level), can improve candour, even within a group setting. (For further insight on analysis of focus group discussion data, see the section above on content analysis of interview data.)	**II, III**	One risk of focus groups is that differing viewpoints may be less visible – even with skilled facilitation, individuals may be reluctant to share perspectives that appear to diverge from the accepted or group view. Usually focus groups need to be complemented by at least a sample of one-to-one interviews to mitigate this risk.

Tool	Review method	Issues/Problems to consider
H. Analysis of text in formal documents and communication Organisations produce vast realms of text, and this text is often a rich data source about culture. New software tools have become available in recent years to analyse large amounts of text, and these can be applied to a range of text types. Formal documents are often considered 'artefacts' that reflect an organisation's culture in both obvious and subtle ways. The text of formal policies, reporting, procedures and system documents can be 'mined' for insight on both the drivers and outcomes of culture – that is, auditors review the text of policies that guide behaviour in such documents, as well as information about the behaviour shaped by norms in the business. In particular, characteristics such as language, tone, scope, authorship and revision history can be especially revealing. Text is also produced via various forms of day-to-day communication within an organisation, both internally and with outside parties: email, collaboration tools, audio calls, messaging services and social media. Such communication can offer considerable insight into not just the content of discussion, but also the nature of interactions and relationships within an organisation. Finally, insight into an organisation's culture can also be gleaned via external text sources including employee review platforms such as Glassdoor, or customer review websites. These are useful because they offer an anonymous platform for feedback from employees or customers. Some evidence of validity had already emerged in relation to Glassdoor analyses of culture.	**I, II, III**	Although technology-driven text analytics is a rapidly growing field, it is relatively young. This creates some issues and risks to consider. The use of big data gleaned from current employees raises a host of privacy and ethical concerns. Resolving these concerns usually places some limits on what can be extracted from employee communication text. '' Bigdata' approaches that rely on internal correspondence may also be exposed to observer effects. If employees know that their emails and messages are being monitored, they may start to 'sanitise' communication via these channels. This may drive the 'bad' communication onto other, unobserved communication platforms.
I. Formal mechanism analysis On the surface, evaluating formal mechanisms (formal policies, processes and systems) is familiar territory for most traditional auditors. The formal mechanisms that shape behaviour within an organisation are also necessary (but not sufficient) to consider when assessing risk culture. Key mechanisms to consider include performance management mechanisms, remuneration policies, training and development, recruitment and selection, and consequence management frameworks. Assessment criteria is a key issue for auditors to consider when evaluating the effectiveness of formal mechanisms related to culture within an organisation. Although compliance with regulatory or other guidelines is important, for the purpose of identifying risk culture strengths and challenges the key question auditors should be asking when conducting an audit of risk culture is: how are formal mechanisms helping versus hindering behavioural norms that reinforce sound risk management in this business? Using specialist advice, auditors may be able to assess the design of formal mechanisms in a 'desk-based' review. A more robust approach, however, would be testing the way formal mechanisms actually impact behaviour in practice, leveraging some of the other techniques outlined in this toolbox, such as behavioural observation, root cause analysis, cultural risk outcome monitoring or interviews.	**II, III**	A key challenge for traditional auditors assessing the effectiveness of formal mechanisms related to culture is the ability to assess the likely impact of formal mechanisms on behavioural norms. Even for experts, apparently 'effectively designed' mechanisms can create unexpected and undesirable effects on behavioural norms. However, this challenge can generally be overcome by data collection and analysis against appropriate criteria.

APPENDIX 3

Reporting tools

Tool	Review method	Issues/Problems to consider
J. Holding up the mirror workshops A holding up the mirror (HUTM) session is an increasingly common way of communicating the findings from a risk culture deep dive audit. Materials from the session are generally more extensive than may be attached to a short executive summary for reporting to the board. The goal of this kind of session is to 'show, not tell' the auditor's conclusions by illustrating the range of evidence on which findings are based. Such an approach reduces the tendency for cultural observations to be dismissed as subjective and potentially biased, and provides rich information to management about the nature, impact and drivers of culture within their business. Sessions usually follow a similar agenda, including background to the review, methodology used (including sampling), key issues, evidence for the impact, norms and drivers of each issue, and areas to prioritise for improvement. Facilitating these sessions requires a careful balance between confronting leaders with sufficient data so they recognise their view of 'reality' may not be complete (in the event that issues being raised are not already well recognised) and overwhelming leaders to the point they become defensive and/or feel helpless to achieve improvement. This kind of reporting reflects a distinctive characteristic of culture audits: improvement is almost impossible without fundamental buy-in from stakeholders. Mere acceptance of the audit point is not enough, because cultural change almost always requires some degree of behavioural change on the part of leaders, which is unlikely unless the leader truly believes in the need to personally change. HUTM sessions are designed to ensure that culture audit findings have the best chance of improvement once identified.	**II, III**	**Best used when ...** › internal audit has a goal of contributing to better risk culture outcomes within their organisation, not just reporting issues, since HUTM workshops reinforce understanding and ownership of issues by those in the business. › the team includes specialist colleagues with necessary experience and seniority to facilitate the session effectively. › the leader of the business being audited is comfortable being transparent with his/her team regarding the results of the review. **May be less appropriate when ...** › unusual concerns exist related to sensitivity or confidentiality of findings, or protecting the anonymity of those who have contributed key insight.
K. Unrated reports Ratings provide a standardised method for communicating how concerned senior leaders should be about an issue and/or business relative to others across the organisation. However, ratings can also cause significant conflict with auditees – higher ratings generally attract significant direct or indirect consequences, and the ultimate decision is at the auditor's discretion. Although the argument for ratings is generally compelling in conventional auditing, several factors create a strong case for avoiding them when it comes to culture audits. First, achieving leadership buy-in is especially critical to achieving genuine cultural change if required. Unconstructive rating discussions can be particularly counterproductive to achieving improvement, given the real risk of disengaging stakeholders before the report is even issued. Second, it is often difficult to judge an appropriate rating for cultural issues and reports until an adequate number of audits have been conducted for comparison purposes. Third, there are ways to mitigate the risk of not rating issues and reports. Some organisations with a limited number of culture audits on their plan each year choose to escalate every report to the board. This avoids one key reason for including a rating (to determine how far the report is escalated).	**I, II, III**	**Best used when ...** › in the early stages of introducing risk culture audits, when ratings may be an unhelpful distraction from discussion on the actual issues being raised. › when the general internal audit or risk management framework is difficult to align to risk culture context, and/or may create unintended side effects (such as prescribed timelines for action closure). › when there is an accepted practice of unrated reports being used for audits on special topics or other purposes that are relevant. **May be less appropriate when ...** › the internal audit activity has been conducting risk culture reviews for some time and is ready for a more routine/established approach where reports are rated like most other audits. › the broader organisational environment is such that accountability may be limited unless ratings are assigned. › stakeholders are constructive in their approach to ratings and find them helpful to prioritise attention.

Tool	Review method	Issues/Problems to consider
L. Internal audit opinion papers Even in the absence of formalised risk culture audit programs, many chief audit executives (CAE) provide regular commentary for their boards and senior management teams on their independent observations about the way behaviour and culture is supporting or undermining risk management effectiveness across the organisation. These observations do not need to be based on specific internal audit engagements, and may include judgment of the CAE and their team, based on information collected and synthesised from interactions with stakeholders and employees, participation in management meetings, review of reporting, and analysis of audit findings. From time to time, the CAE will share and discuss internal audit opinion papers with the audit committee, as part of the 'in camera' sessions. Internal audit opinion papers may cover a range of observations, including: › Observations of leadership norms and their impact on behaviour culture at lower levels of the organisation. › Independent perspective on the methodology and conclusions offered by first and second line assessments of risk culture. › 'Meta-analysis' of multiple risk culture audits and/or other relevant audit work, to identify patterns and concerns. › Proactive observations regarding external conditions or events that may have implications for governance and oversight of the organisation's risk culture.	**I, II, III**	**Best used when ...** › the internal audit opinion is supplementary to other risk culture assessments by either internal audit and/or other functions within the organisation. › internal audit do not have the resources to implement a formal risk culture audit program. › the internal audit activity has significant positional authority and is a valued source of independent perspective. › the CAE is willing to provide a view on risk culture based on less evidence than might be possible through a more formal program of work. **May be less appropriate when ...** › • regulatory or other key stakeholders expect a more robust or evidence-based approach to auditing risk culture, due to existing or prior concerns.
M. Risk culture dashboards Some boards and senior management expect to see risk culture reporting via a dashboard – a set of key outcome metrics that are monitored against risk appetite levels and reported on a regular basis. To make the dashboard more forward-looking, it may also include judgments about inherent business risk and evidence about emerging materialisation of this risk, e.g. staff survey trends and KRIs. There are drawbacks to this reporting format, most of which are also drawbacks of Method I versus Method II and III (e.g. that individual, predetermined 'proxy' measures can pinpoint where culture may be problematic, but generally struggle to explain why the issues exist, and therefore the difficulty, and steps required to change). However, this reporting style is very appropriate for Method I, and tends to be familiar and aligned to other forms of risk reporting, which can make it appealing. Risk culture dashboards are generally best issued annually or semi-annually, as changes seen in less than 6 months are unlikely to be embedded and systemic in nature. As with inherent risk reporting, this kind of dashboard often provides an evidence-based rationale for conducting a dedicated culture audit. A benefit of the dashboard is that it allows for some limited triangulation between several assessment methods. Where there is consistency of findings, users can be more confident.	**I, III**	**Best used when ...** › stakeholders require a degree of insight into the status of culture across the entire organisation. › there is sufficient quality, reliability and commonality of data across the organisation to populate a dashboard accurately. › there is appetite for engaging with risk culture in a proactive, preventative fashion, not just a reactive one. **May be less appropriate when ...** › there is a danger the dashboard may become 'form over function', due to insufficient availability of robust and/or consistent data, leading to unreliable assurance outcomes.

APPENDIX 4

About the authors

Elizabeth Arzadon
Kiel Advisory Group

Elizabeth is an international expert on cultural factors that impact management of risk, and the Managing Director of Kiel Advisory Group. She is a registered psychologist with extensive experience in corporate and regulatory roles, as well as insight from 15 years as a strategy and independent advisor, diagnosing culture and designing change programs with a range of clients. She has established risk culture internal audit programs for several major financial institutions, and has led over 30 risk culture audits across the Asia-Pacific region, Europe and the Americas. She also works directly with regulators globally to develop their supervisory methodologies, and undertake entity level and industry-wide assessments of culture, behavioural risk and governance. Elizabeth is an active contributor to industry thought leadership. She holds a Master of Psychology (Organisational) and a Bachelor of Science (Psychology)(Hons), and is a member of the Australian Psychological Society.

Regardt du Preez
Head of Internal Audit, QSuper

Reg is an experienced specialist in audit and risk with more than 20 years' experience spanning South Africa, the Cayman Islands and Australia. He currently leads the Group Internal Audit function at QSuper and is responsible for the management and execution of the Group's assurance plan. QSuper is one of the largest superannuation funds in Australia, managing in excess of AUD 100 billion in funds for more than 600,000 members. Reg has held senior roles in each of the three lines of defence and is well placed to comment on the role of internal audit generally, including in the area of culture. Reg presented at the Institute of Internal Auditors' (Australia) Financial Services Forum and South Pacific and Asia Conference (SOPAC®) on the topic of risk culture. Reg holds an Honours Bachelor of Accounting Science degree from the University of South Africa, is a Chartered Accountant and an Associate Member of the Institute of Internal Auditors.

Professor Elizabeth Sheedy
Macquarie University

Elizabeth Sheedy is a risk governance expert based in the Department of Applied Finance of Macquarie Business School. She teaches in the Master of Applied Finance program and the Global MBA program. She is one of the foremost researchers worldwide in the field of risk culture, and as part of this research, has assessed risk culture in some 17 financial institutions in four countries. She publishes in top international journals and her new book on risk governance will be published with Routledge in June 2021. Elizabeth is a popular speaker at industry conferences and a regular media commentator.

APPENDIX 4

Further reading and resources

Helpful for	Resource
Obtaining general background on the design and conduct of internal audits of culture and/or behaviour.	The Institute of Internal Auditors (2019). *Practice Guide: Auditing Culture.* global.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/Auditing-Culture.aspx. The Institute of Internal Auditors (2020). *Practice Guide: Auditing Conduct Risk.* global.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/Auditing-Conduct-Risk.aspx
Developing a valid risk culture survey	DeVellis, R. F. (2016). *Scale Development: Theory and Applications* (vol. 26). Sage Publications. 4th edition.
Understanding psychological safety	Edmondson, A. (2019). *The Fearless Organization. Wiley.* Amy Edmondson on YouTube, 'Building a psychologically safe workplace' (11.26) www.youtube.com/watch?v=LhoLuui9gX8
Six evidence-based principles for influencing others	Cialdini, R. (2009) *Influence: The Psychology of Persuasion*. Harper-Collins. Robert Cialdini on YouTube, 'Science of persuasion' (11.50) www.youtube.com/watch?v=cFdCzN7RYbw
A comprehensive guide to qualitative methods, including observation, interviews, and interpretation of findings	Patton. M. (2015) *Qualitative Research and Evaluation Methods. Sage Publications*. 4th edition.
Useful material on observing and interpreting group dynamics, communication, leadership and error management systems	De Nederlandsche Bank, *Supervision of Behaviour and Culture*. www.dnb.nl/media/1gmkp1vk/supervision-of-behaviour-and-culture_tcm46-380398-1.pdf
For the more scholarly inclined, this book summarises decades of research in the field	Ehrhart, M. G., Schneider, B., and Macey, W. H. (2014). *Organizational Climate and Culture: An Introduction to Theory, Research and Practice*, Routledge.
This resource offers practical guidance on how to assess conduct and culture for internal governance purposes, to report to regulators and to evidence success to stakeholders. Focus is on conduct risk	Miles, R. (2021). *Culture Audit in Financial Services. Kogan* Page.
A primer on risk governance more broadly, with chapters on risk culture and remuneration. This book emphasises the importance of good risk governance and culture for overcoming behavioural biases and ensuring incentives are appropriately designed	Sheedy, E. (2021). *Risk Governance: Biases, Blind Spots and Bonuses*. Routledge.
A paper explaining the various information sources used by the Bank of England for assessing bank culture as part of its program of supervision	Bank of England, Staff Working Paper No. 19*2, Organisational Culture and Bank Risk*. www.bankofengland.co.uk/working-paper/2021/organisational-culture-and-bank-risk

APPENDIX 4

Glossary/Index

Term	Meaning in this document
Add value	Internal auditing adds value to the organisation and stakeholders when it provides objective and relevant assurance, and contributes to the effectiveness and efficiency of governance, risk management and control processes.
Assurance service	An objective examination of evidence for the purpose of providing an independent assessment on governance, risk management and control processes for the organisation.
Audit committee	A subcommittee to which the board has delegated certain functions. The audit committee is responsible for the oversight of the internal audit activity's conformance with the Code of Ethics, the IIA Standards and audit standard.
Chief audit executive	Also known as the head of internal audit, chief audit executive (CAE) describes the role of a person in a senior position responsible for effectively managing the internal audit activity in accordance with the internal audit charter and mandatory elements of the IPPF.
Code of Ethics	The Code of Ethics of The IIA are principles relevant to the profession and practice of internal auditing, and rules of conduct that describe behaviour expected of internal auditors.
Compliance	Adherence to policies, plans, procedures, laws, regulations, contracts or other requirements.
Conflicts of interest	Any relationship that is, or appears to be, not in the best interest of the organisation. A conflict of interest would prejudice an individual's ability to perform his or her duties and responsibilities objectively.
Control environment	The attitude and actions of the leadership team regarding the importance of control within the organisation. This provides the discipline and structure for the achievement of the primary objectives of the system of internal control.
Core Principles	The Core Principles for the Professional Practice of Internal Auditing are the foundations for the IPPF and support internal audit effectiveness.
Cultural risk	The likelihood that culture will differ from what is desired due to inherent pressures in the environment and/or ineffective mitigation of these factors. Heightened cultural risk usually warrants closer examination and monitoring.
Culture	Values and behaviours that contribute to the unique social and psychological environment of a business. Culture influences the way people relate and represents the collective values, beliefs and principles of organisational members.
External co-sourcing	A person from a firm outside the organisation who has special knowledge, skill and experience in a particular discipline.
Governance	The combination of processes and structures implemented by the board to inform, direct, manage and monitor the activities of the organisation toward the achievement of its objectives.
IIA-Australia	The Institute of Internal Auditors – Australia is a company limited by guarantee and without share capital. It is the Australian affiliate of The IIA.

Term	Meaning in this document
Independence	The freedom from conditions that threaten the ability of internal audit to carry out internal audit responsibilities in an unbiased manner.
Internal audit activity	A department, division, team of consultants or other practitioners that provides independent, objective assurance and consulting services designed to add value and improve the organisation's operations.
Internal audit charter	A formal document that defines the internal audit activity's purpose, authority and responsibility. It establishes the internal audit activity's position within the organisation; authorises access to records, personnel and physical properties relevant to the performance of engagements; and defines the scope of internal audit activities.
Internal audit engagement	A specific internal audit assignment, task or review activity, such as an internal audit, control self-assessment review, fraud examination, or consultancy.
Internal auditing	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.
International Professional Practices Framework (IPPF)	The conceptual framework that organises the authoritative guidance promulgated by the IIA. Authoritative guidance is composed of two categories: (1) mandatory, and (2) recommended.
Leadership team	Also known as the C-suite, senior management or executive management, the leadership team refers to the senior management team within the organisation and is overseen by the board of directors.
Objectivity	An unbiased mental attitude that allows internal auditors to perform engagements in such a manner that they believe in their work product and no quality compromises are made.
Policies and procedures	The policies and procedures guide internal audit. The form and content of the policies and procedures will be dependent on the size and nature of internal audit.
Risk	Effect of uncertainty on objectives. Uncertainty arises from a lack of complete knowledge about a situation or future events. Risk is often characterised as the effect a future event may have on objectives. It is measured in terms of the potential consequences of that event and likelihood of experiencing those consequences.
Risk appetite	The level of risk that an organisation is willing to accept.
Risk culture	The behavioural norms that help or hinder effective risk management.
Risk management	A process to identify, assess, manage and control situations or potential events to provide reasonable assurance regarding the achievement of the organisation's objectives.
The IIA	The Institute of Internal Auditors. The IIA is an international professional association with global headquarters in Lake Mary, Florida, USA. The IIA is organised as Chapters within North America and Affiliate Institutes outside of North America.
The Standards	*International Standards for the Professional Practice of Internal Auditing.* Professional pronouncement promulgated by the International Internal Auditing Standards Board that delineate the requirements for performing a broad range of internal audit activities and for evaluating internal audit performance.
Tone from the top	The organisation's risk climate as established by the board of directors, audit committee and leadership team. The tone from the top is a crucial influence on a company's cultural environment and corporate values.

T 02 9267 9155
E enquiry@iia.org.au

www.iia.org.au