ACCA Think Ahead

airmic

PRMIA Professional Risk Managers' International Association

RISK CULTURE: BUILDING RESILIENCE AND SEIZING OPPORTUNITIES

A GLOBAL SURVEY AND REPORT

About ACCA

ACCA (the Association of Chartered Certified Accountants) is the global professional body for professional accountants.

We're a thriving global community of **241,000** members and **542,000** future members based in **178** countries and regions, who work across a wide range of sectors and industries. We uphold the highest professional and ethical values.

We offer everyone everywhere the opportunity to experience a rewarding career in accountancy, finance and management. Our qualifications and learning opportunities develop strategic business leaders, forward-thinking professionals with the financial, business and digital expertise essential for the creation of sustainable organisations and flourishing societies.

Since 1904, being a force for public good has been embedded in **our purpose**. In December 2020, we made commitments to the **UN Sustainable Development Goals** which we are measuring and will report on in our annual integrated report. We believe that accountancy is a cornerstone profession of society and is vital in helping economies, organisations and individuals to grow and prosper. It does this by creating robust trusted financial and business management, combating corruption, ensuring organisations are managed ethically, driving sustainability, and providing rewarding career opportunities.

And through our cutting-edge research, we lead the profession by answering today's questions and preparing for the future. We're a not-for-profit organisation.

Find out more at **accaglobal.com**

About Airmic

The leading UK association for everyone who has a responsibility for risk management and insurance in their organisation, Airmic has over 450 corporate members and more than 1,750 individual members.

Individual members are from all sectors and include finance, sustainability, information and technology, internal audit, and legal professionals, as well as risk and insurance professionals. With our partners, and in collaboration with affiliate associations and institutes, Airmic supports members through learning and research; a diverse programme of events; developing and encouraging good practice; and lobbying on subjects that directly affect our members and their professions. Above all, we provide a platform for professionals to stay in touch, to communicate with each other, and to share ideas and information.

www.airmic.com

About PRMIA

Established in 2002, the Professional Risk Managers' International Association (PRMIA) is a non-profit, member-focused and member-driven professional association represented globally by more than 50 chapters in major cities around the world.

PRMIA's mission is to provide an open forum for the development and promotion of the risk profession through credentialing, learning and development programs, online thought leadership resources, and events.

To learn more, visit **www.prmia.org**

April 2023

RISK CULTURE: BUILDING RESILIENCE AND SEIZING OPPORTUNITIES

Unique collaboration and dedicated special interest group

The Association of Chartered Certified Accountants (ACCA), Airmic, and the Professional Risk Managers' International Association (PRMIA) have teamed up to dig deeper into what our members are doing to enhance risk culture and its effect on the organisation's broader strategy. This collaboration is a 'first of its kind' on risk culture across sectors and regions around the world.

Author

Rachael Johnson,
Head of Risk Management and
Corporate Governance, ACCA

Foreword

In recent years our world has experienced profound behaviour-transforming disruption. In early 2022, we decided to collaborate and explore how these interconnected issues, including climate change and other intensifying global macro threats, are influencing the way members of our three professional bodies approach risk management. Given the new perma-crisis norm, we decided to take a deeper dive into what risk culture means and find out to what extent risk and accountancy professionals understand its impact on performance.

As a continued string of corporate failures also reminds us of the long-standing disconnection between risk management and accountancy, we remain focused on how our professions can collaborate more on fostering cultures that allow organisations to get where they want to be.

Risky behaviours brought down the Wirecards and FTXs. Other collapses continue to grab headlines, indeed even as we write, with Silicon Valley Bank and Signature Bank in the US (Pound 2023). Yet the predictable question that always comes up in the aftermath is: where were the risk managers and accountants? In today's digital, vox pop world, we also see the likes of Trustpilot, Glassdoor and other social media giving regulators a new lens for observing beyond what is stated in annual reports and other public statements.

However, in this new era of accountability, it won't just be the regulators stepping up their scrutiny. With environmental, social and governance (ESG) issues dominating agendas, we see stakeholders from all corners asking for more answers. This is a material aspect of today's corporate world that risk and financial leaders cannot ignore.

Our aim through this report is to empower our professions to improve their risk cultures and, by helping them learn what is working or not, lead their organisations in what is undeniably a new age of risk. As part of our research, we formed a special interest group comprising subject matter experts, who continue to assist us in shaping the research, educating our members, and enhancing our continuous learning resources for risk and financial professionals globally. We would like to thank all who have contributed.

Helen Brand
CEO, ACCA

Julia Graham
CEO, Airmic

Justin McCarthy
CEO, Prmia

Contents

About the report

Global surveys, roundtables, and one-on-one interviews

At the heart of our research is an online global survey designed to help us gauge how members of our professional bodies would describe their risk culture. Is your culture one that is dangerously full of perils and contradictions? Is it a potentially powerful and coherent force full of opportunity? Is it somewhere in the many shades of grey in between? There's much to unveil, revealed by our extensive reach.

The survey, which took place during the last two weeks of October 2022, attracted 1,823 individual responses from risk and financial professionals around the world and across a range of industries. It covered an unprecedented amount of ground on the culture of risk management. With 93% of responders being ACCA members and therefore from accountancy backgrounds, we can compare findings from a wide range of niche roles related to risk with perspectives from people also in financial roles not explicitly in charge of risk management. This has given the research a breadth and authenticity which we have found very insightful.

Several financial supervisory bodies already conduct regular comprehensive surveys on the risk culture of firms, but these are in their separate jurisdictions, which means our joint initiative is the first to do so with such global scale and reach (APRA 2022; FCA 2017). Charts can be found in the Appendix showing the demographic breakdown of our survey respondents by region (Figure A1), organisation size (Figure A2), sector (Figures A3 and A5), roles (Figure A4) and age.

To complement our survey, we held an online community pop-up platform in November 2022 where respondents could log-in and share their views and experiences with risk culture. This platform attracted more than 100 participants, who joined in conversations with members of our special interest group as well as in mini-polls and other interactive engagements, giving us rich qualitative data and a wealth of anecdotes to compare with the survey findings.

We also set up roundtables and one-on-one interviews, along with discussions in our business-as-usual forums, all of which took place between January 2022 and January 2023, allowing us, ultimately, to gather insights from over 2,000 risk and financial professionals around the world. With this triangulation we have been able to analyse in detail the convergences and divergences of all the input.

Overall, we found the survey respondents seemed overconfident about the effectiveness of their risk cultures, given what we heard in the qualitative sessions. Listening to participants in our interviews and forums, we experienced a 'bursting of the floodgates' as participants expressed a pent-up frustration with the short-sighted focus on risk culture inside their organisations. Through those discussions, we perceived a mix of risk perceptions and scepticism across different roles and hierarchies.

Have lessons been learned despite the accounting scandals that have shone a light on the alleged misdiagnoses of external auditors? Are judgements still being based on numbers that only vaguely add up and assertions from senior management that ignore red flags? Hindsight bias always says a different call could have been made, but can audit professionals honestly say that their judgements were valid and reasonable when considering all the information they had at the time? The consensus is a resounding 'no' from those in key risk roles. These interviews produced fascinating insights into risk and financial professionals' hopes and fears day-to-day as they often struggle to get the necessary commitment to create the risk cultures and governance needed to facilitate their organisation's strategy. This struggle arises because the warning signs of failures waiting to happen are definitely present, but respondents recognised that a strong risk culture, consciously built and nurtured by the board, senior and middle management is essential as the best means of avoiding them, and this is often lacking.

> **I HAVE SEEN SO MANY SITUATIONS WHERE MORE JUNIOR STAFF "STAY IN THEIR LANE" BECAUSE SENIOR MANAGEMENT TEND TO USE JARGON THAT IS HIGH LEVEL AND GENERALLY ACT LIKE RISK DISCUSSIONS ARE SECRETS TO BE KEPT LOCKED AWAY IN THE BOARDROOM AND AWAY FROM STAFF.**
>
> ONLINE COMMUNITY POP-UP PARTICIPANT

1. **What** is **risk culture** and **why** is it **gaining recognition**?

From Arthur Andersen and Enron to Lehman Brothers, the LIBOR (London Interbank Offer Rate] manipulation and the never-ending stream of other scandals, we see how risk culture becomes a big topic as a consequence of each incident but then fades down the list of priorities for boards and senior managers until the next spectacular corporate collapse.

But, in recent years, supervisory regulators in the financial services industry, especially, have been turning their attention to risk culture as a means of tackling and preventing further governance failures, and a concerted dialogue on psychological safety has fast emerged (Baunsgaard 2022). The focus is on how to foster an environment where staff believe they are safe to speak up and discuss ethical issues, including views on how their products and services are produced and delivered.

Businesses are increasingly finding themselves forced to consider why their organisation exists and what the role of their business should be within wider society. This includes identifying where conduct and leadership lapses can threaten their competitiveness. So, where is risk culture in all this?

Every risk is driven by human behaviour

For all its concern over regulatory capital, the Basel Committee on Banking Supervision has published corporate governance guidelines for banks after every crisis (e.g., BCBS/BIS 2014) and still defines risk culture as 'norms, attitudes and behaviours related to risk awareness, risk-taking and risk management, and controls that shape decisions on risks' (quoted in Milkau 2017).

The Financial Stability Board (FSB), set up in Basel in April 2009 to represent the G20 economies, also describes a sound risk culture as that which 'bolsters effective risk management, promotes sound risk-taking, and ensures that emerging risks … are recognised, assessed, escalated and addressed in a timely manner' (FSB 2014). The FSB explains how risk culture is not static but 'evolves over time in relation to the events that affect the institution's history (such as mergers and acquisitions) and is affected by the external context within which the institution operates' (FSB 2014).

What we have learned throughout the course of our research and engagement with members of our professional bodies is that individual values, beliefs and attitudes towards risk are naturally influenced by, and contribute to, the wider overall culture of an organisation (Power et al. n.d.). In other words, organisational culture – or corporate culture – is naturally related to leadership, learning and performance, control, ideology and/or oppression (Power et al. n.d.). Culture is about 'how we do things around here' or 'what we expect around here' (Power et al. n.d.). Culture is the 'cause', as it were and what happens as a result, be it good or bad, is the 'effect'.

The workplace transformations accelerated by Covid-19 also posed new questions about what constitutes 'risky behaviour' and how it spreads.

'There are huge points when your organisation is tested. For example, when you do a restructuring or a termination. You won't get it right if you don't have the risk leaders, finance and HR working in tandem. It's like the Freudian triangle. You need all these to have a culture that will have the right impact: the behaviours that get you where you want to be.'

Accountant at a Fortune 500 company

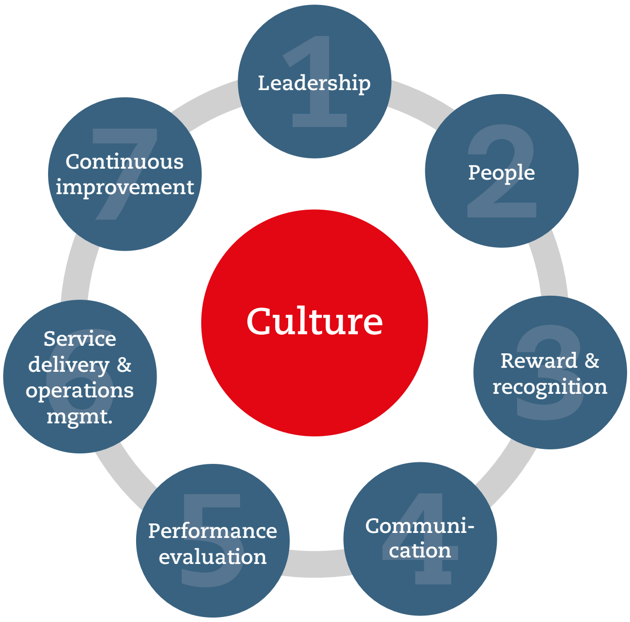
'We have to be careful not to fall into the trap of separating culture from risk culture. Culture is how people behave. Behaviours, whether they lead to risk taking or risk aversion, come from the decisions that you make. Decisions are based on judgements, and judgements are largely based on the values we hold. Yes, there are external pressures which impact these decisions, but we need to track [Risk Culture] back to a clear set of moral and behavioural values that underpin decisions. This is where individual and firm values become intertwined in the firm's business and risk culture.'

Patrick Butler board chair, Net Zero Labs and adviser on culture and conduct management, and member of the special interest group

In our survey, we asked whether respondents believed the risk culture at their organisation could prevent unexpected behavioural issues and we put forward a short suggested definition of risk culture to give them a general base for their answers and comments. It is one that we would say is accurate and reflects our research findings.

> RISK CULTURE IS A TERM DESCRIBING THE VALUES, BELIEFS, KNOWLEDGE, ATTITUDES, CONDUCT, BEHAVIOURS, AND UNDERSTANDING ABOUT RISK AND THE LEVEL OF ACCEPTED RISK SHARED BY A GROUP OF PEOPLE WHO HAVE A COMMON PURPOSE.

FIGURE 1.1: Seven steps of culture



Source: adapted from Airmic-QBE Guide, *The Importance of Managing Corporate Culture*, 2018

Human behaviour is difficult for organisations to define and measure

An organisation's risk culture is hard to measure because whether good or bad, a risk culture that helps an organisation be successful at achieving its goals involves participation up and down, throughout the organisation. Therefore, there are many touchpoints, which individually could be of high or low quality, to consider when developing behavioural indicators.

> *'Organisational culture is about how people behave as members of a group, and risk culture is an aspect of this. For firms, promoting behavioural norms that facilitate good risk management, and identifying and managing any that may undermine it, matters. Doing this well requires both understanding of the wider context in terms of overall workplace culture and avoiding narrowing the focus to conduct as measured by the incidence of misconduct – the latter, identifiable and clearly very important, but only a part of the bigger picture.'*
>
> **Alison Cottrell, chief executive officer of the UK's Financial Services Culture Board**

In the face of these measurement challenges, regulators are requiring firms to demonstrate how they manage human capital, because there is a growing consensus among them that managing risk culture starts by assessing the broader culture, the behaviours it breeds and the risks that they might drive (Starling Insights 2018).

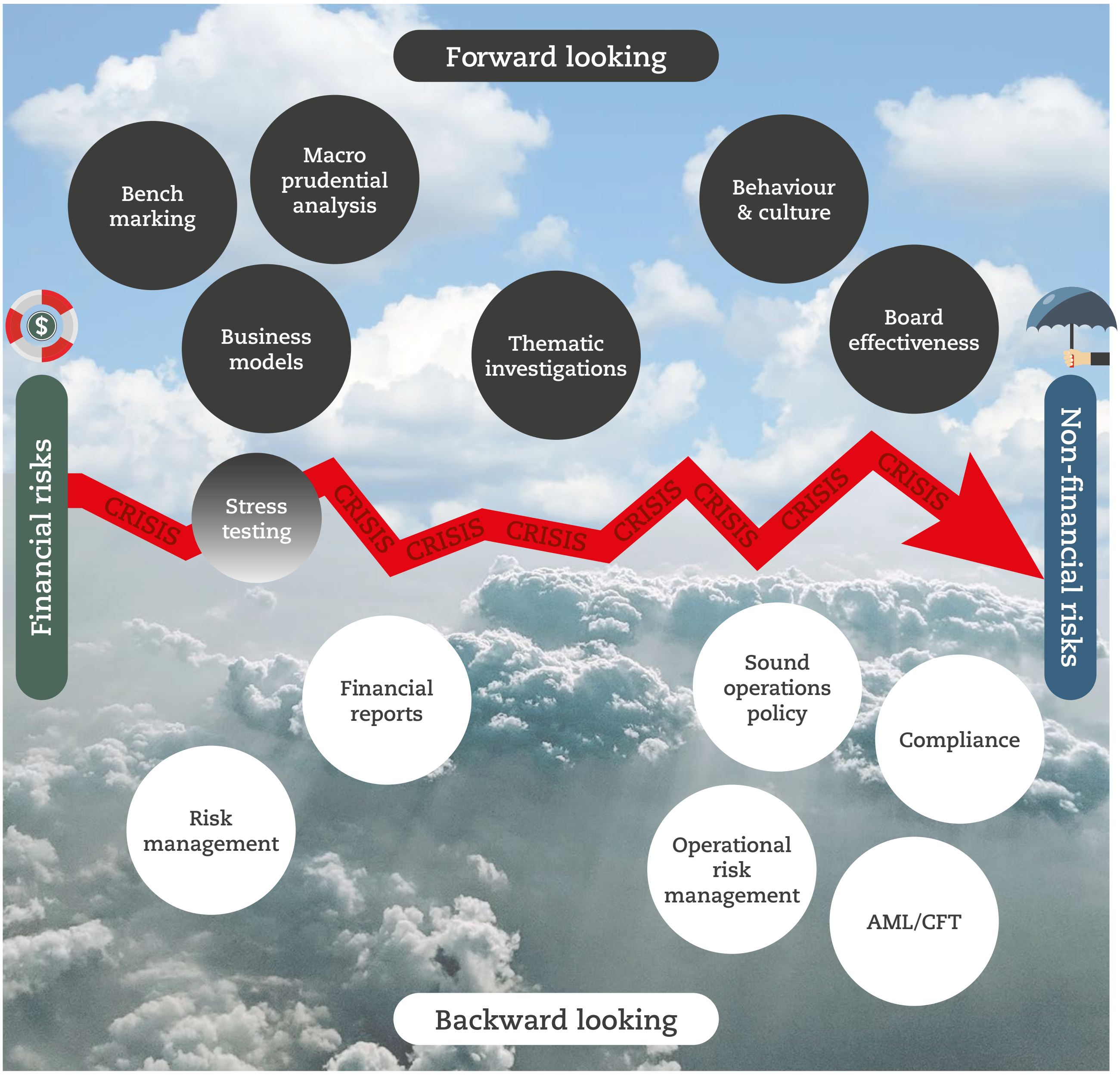
No matter how hard it is to measure, manage or influence risk culture, or how much or how little an organisation's leaders are under pressure to do so, the benefits of getting risk culture right, laid out in this report, underline why boards and executives would be wise to recognise how their risk culture affects performance.

As we see through our survey responses, this requires a new generation of management reporting information (MI) that many members of our professional bodies admit they have yet to grasp. Some respondents in the financial services industry have been gathering culture and conduct MI for as long as a decade now but say they are still struggling to use it strategically and act appropriately on the information they get. Some banks have invested a considerable amount of money in developing the metrics, and respondents in various roles told us they are not only working out what information matters most but trying to share it with the people who could use it in a more effective way.

We also heard how the growing focus on this has led some organisations to discover they are sitting on useful information that they had not previously realised they had and now are considering how to apply it to policies and decision making. This new data paradigm is spelled out more comprehensively in *Culture Audit in Financial Services: Reporting on Behaviour to Conduct Regulators* by Dr Roger Miles, a specialist in behavioural science who is also member of ACCA's risk culture special interest group (see Harwood 2022).

Culture supervision

FIGURE 1.2: Risk culture supervision



Source: adapted from Dr Roger Miles

AN ORGANISATION'S RISK CULTURE IS HARD TO MEASURE BECAUSE WHETHER GOOD OR BAD, A RISK CULTURE THAT HELPS AN ORGANISATION BE SUCCESSFUL AT ACHIEVING ITS GOALS INVOLVES PARTICIPATION UP AND DOWN, THROUGHOUT THE ORGANISATION.

2. **Key findings** from our **online survey**

Survey **respondents** rank **regulatory change** and **cybersecurity** as **top risk priorities**

‘Regulatory, compliance, and legal’ risks came top of respondents’ risk priorities and ‘Technology, data, cybersecurity’ came second. Regulators and hackers top the list of greatest risk concerns, as shown in Figure 2.1.

Data from the first question in the survey speaks volumes and in the subsequent interviews and roundtables led us to debate why being compliant is the top risk priority for organisations (Figures 2.2).

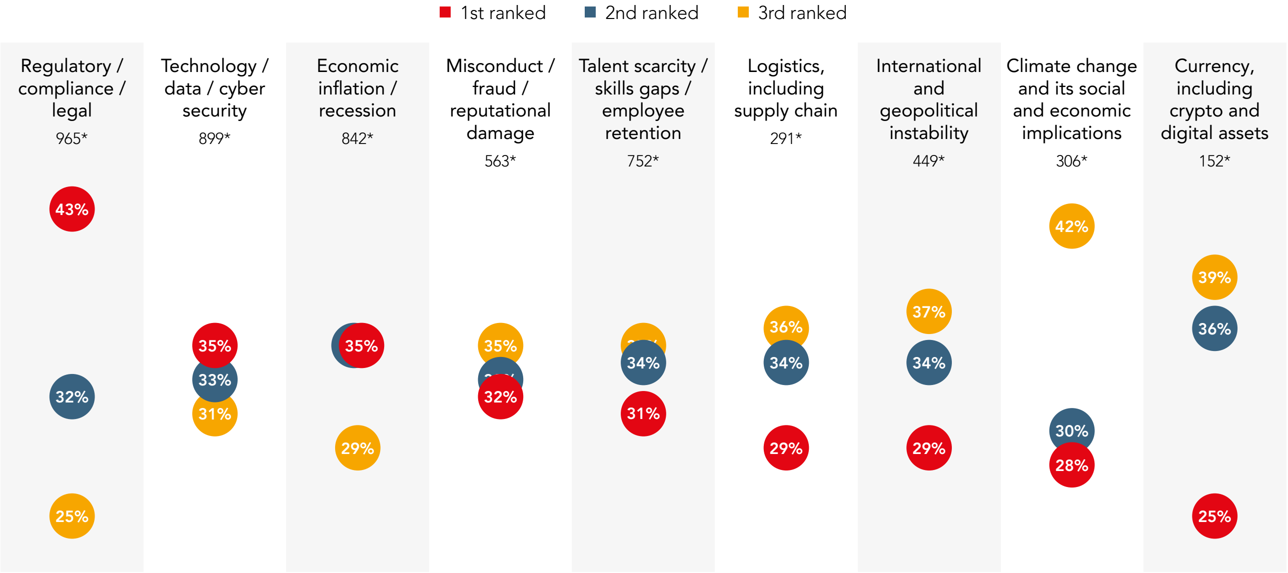
There is no doubt that this reflects the multitude of regulatory and compliance requirements around the globe as the workplace becomes ever more complex. It also indicates that staying on top of these changes requires a great deal of time and effort for those responsible. Regulatory/compliance/legal is in the top three for all sectors except one: not-for-profit/charity.

By region, regulatory/compliance/legal risk is top or close to the top with one exception: North America ranked technology/data/cybersecurity significantly higher than the rest. Also notable is China, where regulatory/compliance/legal risk was a much higher priority than all other risks (Figure 2.3). Respondents based in Africa were more likely to be concerned about misconduct/fraud/reputational damage issues, something that was not a major concern for those in Western Europe.

In terms of sector, respondents in financial services were more likely to raise technology/data/cyber security and regulatory/compliance/legal as their highest risk priorities, whereas those in the corporate sector ranked logistics/supply chain issues as one of their top risk concerns.

> **PLENTY OF ‘BOX TICKING’ IS PREVALENT, BUT THERE IS ALSO A GROWING INTEREST IN RISK CULTURE TO COPE WITH DISCONNECTED ORGANISATIONAL CULTURES AND HARD-TO-DETECT BREADTH OF RISKS.**

FIGURE 2.1: Risk and financial professionals’ top risk priorities (as at October 2022)



*Number of respondents out of the total 1,823 who put this risk in their top three
(Data rounded to nearest whole number)

FIGURE 2.2: Top risk priorities by sector

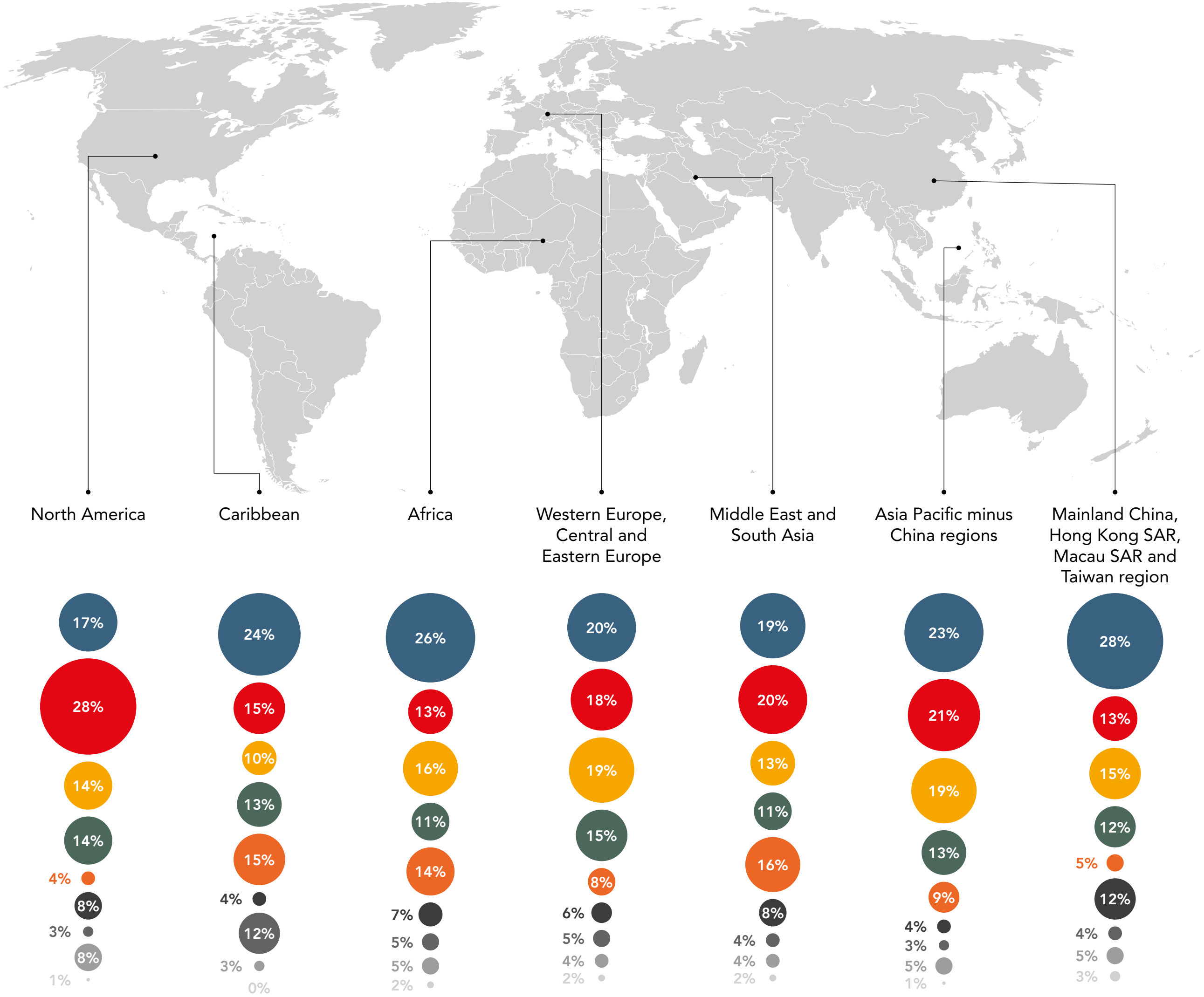
- 🟦 Regulatory / compliance / legal
- 🟥 Technology / data / cyber security
- 🟨 Economic inflation / recession
- 🟩 Talent scarcity / skills gaps / employee retention
- 🟧 Misconduct / fraud / reputational damage
- ⬛ International and geopolitical instability
- ◼ Logistics, including supply chain
- ▩ Climate change and its social and economic implications
- ⬜ Currency, including crypto and digital assets

SECTOR	1st RANKED	2nd RANKED	3rd RANKED
Public practice	🟦 46%	◼ 44%	🟩 39%
Public sector	🟦 41%	🟩 39%	🟨 38%
Financial services	🟦 46%	🟨 36%	🟥 34%
Not-for-profit / charity	🟥 43%	🟧 40%	🟨 39%
Corporate sector	🟦 42%	🟥 40%	🟨 36%
Retired / between jobs*	🟦 43%	🟧 41%	▩ 38%

*Based responses on previous place of work
(Data rounded to nearest whole number)

FIGURE 2.3: Top risk priorities around the world

- 🟦 Regulatory / compliance / legal
- 🟥 Technology / data / cyber security
- 🟨 Economic inflation / recession
- 🟩 Talent scarcity / skills gaps / employee retention
- 🟧 Misconduct / fraud / reputational damage
- ⬛ International and geopolitical instability
- ◼ Logistics, including supply chain
- ▩ Climate change and its social and economic implications
- ⬜ Currency, including crypto and digital assets



('Don't knows' remain the balancing figure for each region)

The outliers by age are the over-65s, who put economic concerns top, then cybersecurity, followed by talent. While there are some interesting age nuances to consider, the main differences throughout the survey are between the under 25s and over 65s (Figure 2.4).

We found variances across roles to be especially insightful for most questions in the survey (Figure 2.5). Of all the roles categories, chief risk officers placed cyber and economic concerns higher than regulatory/compliance/legal, but not by much. Respondents in these roles gave a higher ranking to misconduct/fraud/reputational damage than those in any other roles, putting it in fourth place.

> *'I suspect that most of the CROs and heads of risk responding to this survey would be from highly regulated industries, such as banking and telecoms, and as such have no option but to comply since these are mandatory requirements which could attract fines and have a severe impact on the business as a going concern.'*
> **CRO from a bank in Western Africa**
>
> *'Multinational companies have had to rely on third parties because of all the supply chain disruption and travel restriction pressures since Covid, and this just makes business ripe for bribery and other crimes. Regulators are now stepping up their enforcement and working together to combat the corruption, so this is an increasing concern for our multinational clients. Audit and compliance teams are dealing with a crazy number of changing risks and incidents in this post-pandemic era.'*
> **Monica Young, director of risk and compliance at KMPG LLP in Chicago, and a member of our special interest group**

FIGURE 2.4: Top risk perceptions by age of respondent

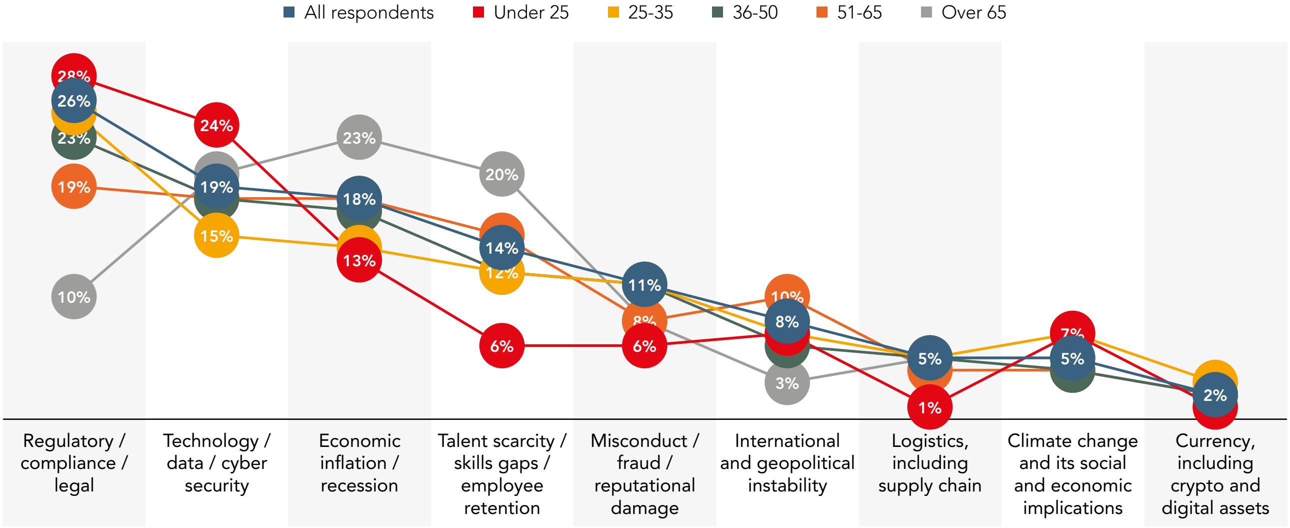
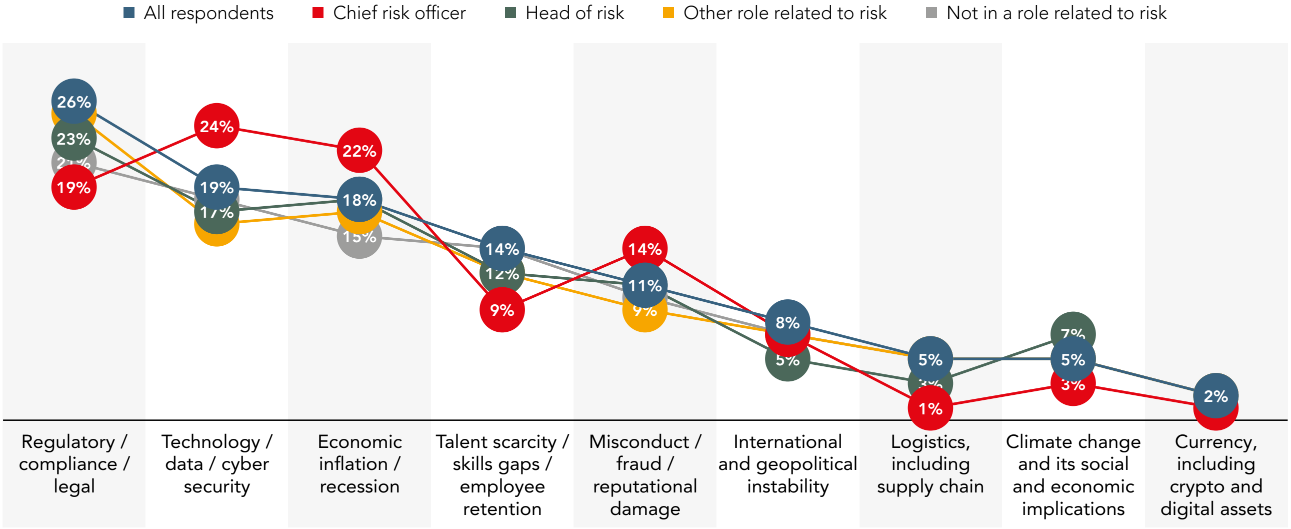


FIGURE 2.5: Who fears what? Top risk perceptions by job roles



There is a realisation, albeit after the fact, of how risk culture affects an organisation's ability to deal with constant regulatory implementations. One audit committee chair at a UK property developer told us that, in hindsight, a greater focus on risk culture could have helped the organisation cope better with fierce and sudden regulatory changes that are being described as the new black swans.[1] But the truth of the matter is that this 'being compliant-style of management' has become a core driver of corporate strategy.

'We had to put some big provisions on the balance sheet because of a regulation that was developed overnight that says any building you've ever built in the last 30 years you have to go and fix, even though you may no longer own it. Ethically, the government is saying 'you've made a load of money in the last 20 years, there's no one around who's left to fix this, so it's over to you, Mr Developers.'

'There's just no way to predict what this or that outcome is going to be, and there's more upcoming. We've got a new consumer code that is like Sarbanes–Oxley on steroids. Regulation has completely changed. Yes, it is for the better because one could argue we should have been doing this stuff and responding to customers in the right way in the first place, but we're not used to working in such a volatile political environment like this. It's a massive paradigm shift in terms of behavioural change and how we need to operate.'

ACCA members in UK

The Russian invasion of Ukraine was also highly disruptive for our respective members at the time of the survey. Many risk leaders started 2022 losing sleep over concentration risk on the Cloud and then came a curveball of geopolitical and economic uncertainty never seen in most of our respondents' careers.

'We had a lot of new issues to sort out and since as much as a third of our branches were in buildings owned by Russian oligarchs there was obviously a blind spot that required different teams coming together given the sanctions.'

CRO in UK

Even where regulators are not springing surprises on organisations, the comment below from a chief financial officer at a construction company in Singapore explains that while the authorities there have been giving the company a reasonable timetable for complying with new sustainability reporting standards, the implications of Covid-19 have changed the industry for ever and such transformations are impossible to keep up with operationally and financially.

'The new requirements definitely give us insights for the long run to see how we can reflect on how we move on from the traditional way of doing things and do it better for the future, but we also have the fact that things are evolving at a very rapid pace.'

CFO in Singapore

The burden of compliance is greater in some areas than others, and that is also a reason why certain priorities at the bottom of the ranking stood out. Climate change, for example, has undeniably become increasingly compliance-intensive, despite coming second to last overall as a priority. With several respondents referring to the 'daunting task' of Scope 3 emissions, we can see how climate change is increasingly viewed as a regulatory issue by our respondents. Regulatory risks also loom large because regulators can present sudden fines and immense implementation costs, with most respondents admitting that while they accept extreme weather and natural catastrophes are also causing costly disruption, they do not have the resources for assessing the scale of the impacts on their businesses.

'We are facing risk everywhere, especially with the unpredictable approach of the authorities, and not just at the state level but also the European level. We have the cost-of-living crisis, which is intensifying daily here, while authorities continue to change the rules, especially when it comes to climate. It's not an easy game to play and makes it harder for us to attract new direct investments.'

An energy sector entrepreneur in Eastern Europe

[1] A reference to *The Black Swan: The Impact of the Highly Improbable* by Nassim Nicholas Taleb.

Regulatory risk ranking at the top can also be explained by the fact that, for some, it is the way they chose to express concern over other risks. Below is a comment from a finance director in North America on cybersecurity, and why it also can be covered under a broad definition of regulatory risk.

'Cybersecurity is one of the biggest problems for the best of us and we don't know how to collectively manage or report on it. New regulations are coming out all the time with new kinds of approaches and we go to the Big Four, but they are also playing catch-up. We have had regulations on cyber risk before, but not to the magnitude it is now.'

Finance director in North America

'Regulators are requiring banks to reimburse customers for phishing and other hacks, so the stakes are high for banks to invest in the right measures for mitigating this added layer of an already material risk. They want us to have zero tolerance, but it is foolish to think anyone could have zero tolerance when you look at the scenarios we are dealing with.'

Head of risk at a bank in Central Europe

As regards to the ranking of technology/data/cybersecurity at second highest overall, one ACCA member at a technology company in Eastern Europe also summed up why cyber risks would remain a priority for everyone.

'Cyber risk is something that is so ingrained in anyone who wants to run a successful business, so I think there is less of a fight or a challenge in getting the buy-in. Leaders also worry about retaining the data security or IT teams because so much subject matter expertise is required. Some might even say it's part of compliance, but compliance is not a security against cyber risk. IT risk is also a worry because the CEO can't prevent who clicks on what. They can only take ownership of the risk from the perspective of investment and prioritisation rather than the day-to-day measurement.'

ACCA member at a technology company in Eastern Europe

Talent shortages ranked mid to high in the priority hierarchy compared with other risk areas and in our conversations seem clearly to have hit some organisations harder than others.

'Another material risk for us is human resources. In the case of Romania, six million people have left in the last couple of years to live abroad, mostly around Western Europe. Most of them are very educated and left due to the difference in salaries, conditions, medical system, insurance, and so on.'

Managing director in Eastern Europe

Demand for certain kinds of talent was a major topic with ACCA members in the Middle East as well, with one risk head who works at one of the US-based big tech companies in Dubai explaining the high demand for risk and compliance professionals in the region.

'Everyone here is looking for risk and compliance people right now and there [are] not enough to go around.'

Head of risk at a tech company in Dubai

Another interviewee who works as a risk governance consultant in Dubai blamed the talent scarcity on 'the ancient and out-of-touch' education models we have created, saying that graduate students, even those coming out of the top universities and finance programmes globally, are not in tune to what is happening in the real world and none of them know how to account for risks or sustainability matters.

'Trade bodies and universities should be working together more on risk training, and that's around the world not just here, because even those coming out of the top universities and finance programmes do not have an inkling about risk and what it means to companies today. I'm working with small-to-medium and public sector entities on learning the ISO 31000 certification, but this needs to be continuous in terms of how you apply it to your business situations in a fast-changing world; how will you use AI and now the consequences, risks and opportunities of ChatGPT and who decides that and creates the governance for it?'[2]

Risk governance consultant in Dubai

[2] ISO 31000:2018, the latest update of the international risk management standard, reinforces the importance of managing risk culture. It requires top management to demonstrate their commitment to risk management and its alignment with the organisation's strategy and culture. Organisations must also evaluate the effectiveness of the risk management framework on the behaviours of their people. Risk and financial professionals therefore have a major role to play in managing corporate culture.

Risk culture has **changed for the better** since the pandemic

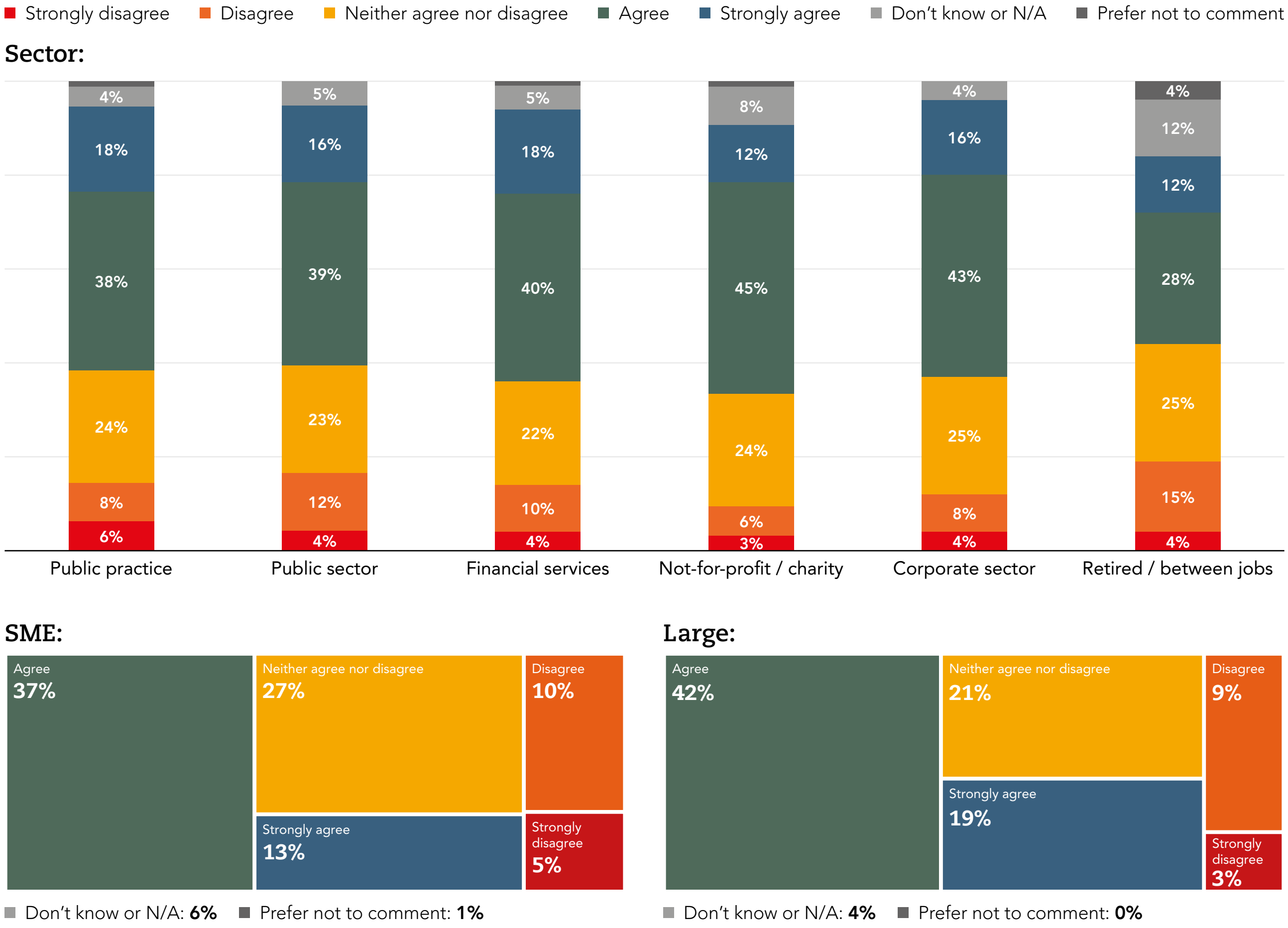
When we asked about risk culture, most respondents, irrespective of sector or organisational size either agreed, or neither agreed nor disagreed, that their organisation's risk culture had improved (Figure 2.6). Respondents in China were generally much more confident in their organisations' risk culture compared to other countries.

> **57%** OF RESPONDENTS SAY THAT THEIR RISK CULTURE HAS CHANGED FOR THE BETTER SINCE THE PANDEMIC.

It might intuitively appear that the number of respondents saying 'oh yes, the pandemic has improved/changed our risk culture' would be higher. What our discussions on the responses brought out is that there is a will to improve, and many things are improving, but at the same time the post-pandemic environment is very challenging, particularly given that scarce resources are coupled with rising costs and the need to put new technologies into practice. These competing forces are why the data shows such a mixed picture. While our survey findings did not indicate a direct link between employee wellbeing and risk culture, certain testimonies in our roundtable discussions implied that employee wellbeing resulted in better employee engagement, which therefore shows some correlation with a better risk culture and management of people risk.

Internal audit members in previous research discussed how, once Covid-19 struck, their roles became less about adding up numbers and more about making judgements in difficult situations (ACCA 2021). The pandemic proved how modernising and more frequent monitoring were required at even the most profitable firms with mature risk frameworks. We heard how organisations could structure governance better, particularly for the relationship between the first and second lines of defence and how the past few years have proved the importance of collaborating while also maintaining independence for the second line.

FIGURE 2.6: The pandemic got more than half of the respondents' organisations to rethink risk culture



(Data rounded to nearest whole number)

We continue to hear members talk about bringing due diligence processes up to date, but this requires resources, and most organisations are struggling with budgeting for the long term, especially as technology advances rapidly and economic conditions become increasingly uncertain. Respondents talked about the conflict between short-term shockwaves and the need to think for the long term and move on from costly legacy systems.

> *'I have worked in both the private and public sectors for decades and can say that while risk culture has become more important, given the circumstances today, it is in its infancy. But, suddenly, being thrust into this economic shift where annual funding or revenue streams disappear, and where we are faced with situations that we had not prepared ourselves for, means we need to rethink how we operate. It has been survival mode for the last three years, meaning you're managing things month-to-month and not thinking about investing in something that has long-term implications.'*
>
> **CFO in Canada**

An ACCA member who had worked as head of internal audit for multinational companies based in Japan, China and India, decided to leave her corporate job during the pandemic to set up a risk advisory business that supports small-to-medium-sized enterprises (SMEs) in Asia, mostly in China.

> *'I saw how much human and manual errors are holding SMEs back. Helping them adopt blockchain, AI and other open-source technologies for processing orders and payments can change the course of direction of their business very quickly. Many of their founders or leaders don't understand how attitude can help them drive that until they start weighing risk and opportunity, and once they start talking about that they see how avenues of investment and growth can happen during stressful times.'*
>
> **Risk adviser, Far East**

RESPONDENTS SAY AN EFFECTIVE RISK CULTURE NOT ONLY AVERTS DISASTERS BUT ALSO PRESENTS OPPORTUNITIES.

If a 'being compliant style of management' or a 'tick the box audit and risk management style' are what drives risk strategy, then we conclude that in itself is a significant risk since it moves away from the specific context of the organisation's purpose and distorts important, high-level decisions, which have to take full account of both threat and opportunity. This distorted perspective essentially implies that the purpose of the organisation is to be compliant with regulatory requirements, and that would seem far from the true purpose and mission of an organisation and its value proposition.

An optimistic portrayal of risk culture was mentioned repeatedly in our research – a risk culture built to take on risks in a more informed way and with the most directly bottom-line focus possible for gaining a competitive advantage. In conversations, respondents admit that they are not seeking 100% compliance but, rather, thinking of risk as a language that everyone in the organisation speaks.

> *'In my mind the overall approach to risk management has been from a defensive perspective for decades and I think culturally as a profession we have not talked enough about how we think the other way; how it can actually give you a competitive advantage. That's why we fall back into ticking the boxes and why it's only the people who are responsible for risk [who have] a more positive view of how we are doing compared [with] others. That is a tough line to cross but as we see more of us thinking about risk culture, maybe we will start to see the real benefits of risk management as opposed to this unconscious bias that it is all about meeting defensive requirements.'*
>
> **CFO at mid-size corporation in North America**

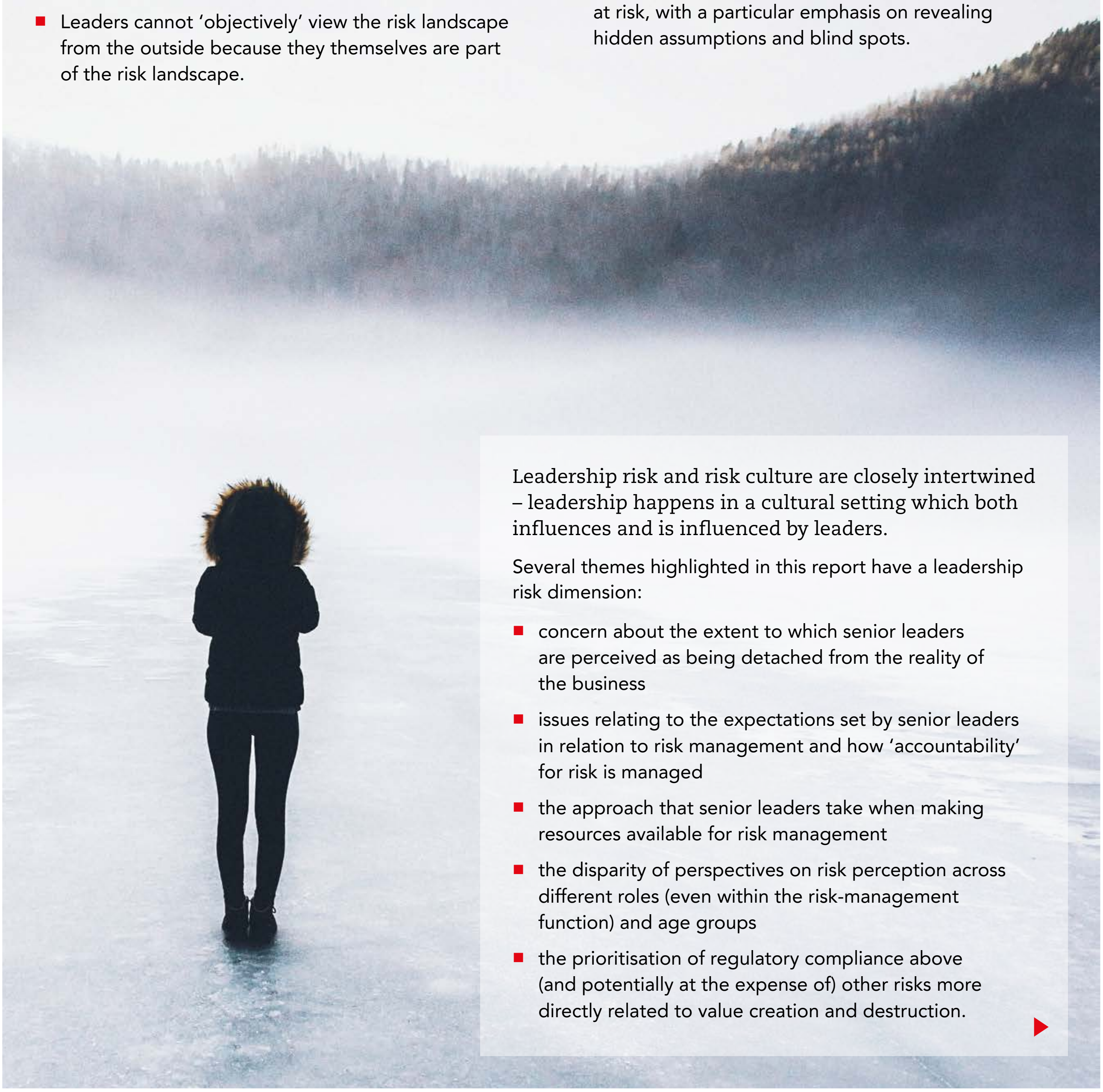
LEADERSHIP RISKS: What to look out for

by **Dr David Cooper**, Cooper Limon

Leadership risk relates to the way in which the process of leadership and the way leaders think and behave determines value creation and destruction. It is often a significant contributing factor when there is a sudden collapse in enterprise value: recent examples include WeWork, Theranos, FTX, Silicon Valley Bank and Signature Bank. Indeed, it is increasingly recognised as being significant for all businesses as understanding the role of leadership provides a richer more contextualised understanding of risk – a counterbalance to overly 'rational' analytical approaches.

The leadership risk perspective has a number of key aspects:

- Leadership risk is not a separate category of risk, it relates more to the wider organisational environment in which risk management happens.
- Leaders cannot 'objectively' view the risk landscape from the outside because they themselves are part of the risk landscape.
- This view encourages those involved in risk management not just to consider what the risks are but also to take account of how they are looking at risk, with a particular emphasis on revealing hidden assumptions and blind spots.



Leadership risk and risk culture are closely intertwined – leadership happens in a cultural setting which both influences and is influenced by leaders.

Several themes highlighted in this report have a leadership risk dimension:

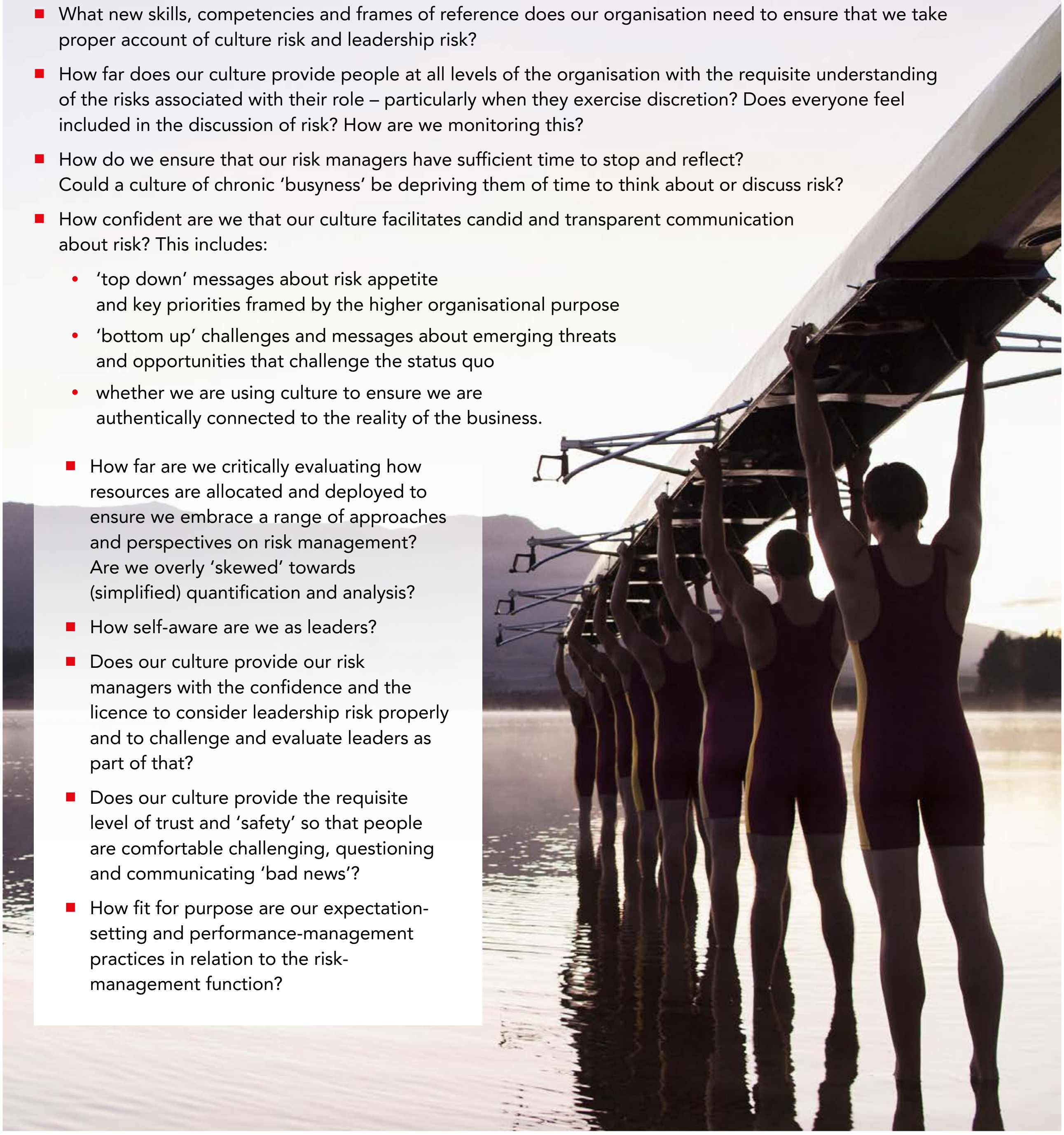
- concern about the extent to which senior leaders are perceived as being detached from the reality of the business
- issues relating to the expectations set by senior leaders in relation to risk management and how 'accountability' for risk is managed
- the approach that senior leaders take when making resources available for risk management
- the disparity of perspectives on risk perception across different roles (even within the risk-management function) and age groups
- the prioritisation of regulatory compliance above (and potentially at the expense of) other risks more directly related to value creation and destruction.

LEADERSHIP RISKS: What to look out for

by **Dr David Cooper**, Cooper Limon

To engage effectively with culture risk, it is important to consider the leadership risk perspective and the ways in which this influences the definitions, decisions, approaches, and reactions associated with the process. Several comments from the respondents in our research underline why senior leaders should consider the following questions:

- How effectively are we capturing culture risk and leadership risk on our high-level risk dashboard? How far do we bring these subjects into discussions about risk and the wider organisational purpose?
- What gets in the way of engaging more actively with the culture risk agenda? How can we address this?
- What new skills, competencies and frames of reference does our organisation need to ensure that we take proper account of culture risk and leadership risk?
- How far does our culture provide people at all levels of the organisation with the requisite understanding of the risks associated with their role – particularly when they exercise discretion? Does everyone feel included in the discussion of risk? How are we monitoring this?
- How do we ensure that our risk managers have sufficient time to stop and reflect? Could a culture of chronic 'busyness' be depriving them of time to think about or discuss risk?
- How confident are we that our culture facilitates candid and transparent communication about risk? This includes:
  - 'top down' messages about risk appetite and key priorities framed by the higher organisational purpose
  - 'bottom up' challenges and messages about emerging threats and opportunities that challenge the status quo
  - whether we are using culture to ensure we are authentically connected to the reality of the business.
- How far are we critically evaluating how resources are allocated and deployed to ensure we embrace a range of approaches and perspectives on risk management? Are we overly 'skewed' towards (simplified) quantification and analysis?
- How self-aware are we as leaders?
- Does our culture provide our risk managers with the confidence and the licence to consider leadership risk properly and to challenge and evaluate leaders as part of that?
- Does our culture provide the requisite level of trust and 'safety' so that people are comfortable challenging, questioning and communicating 'bad news'?
- How fit for purpose are our expectation-setting and performance-management practices in relation to the risk-management function?



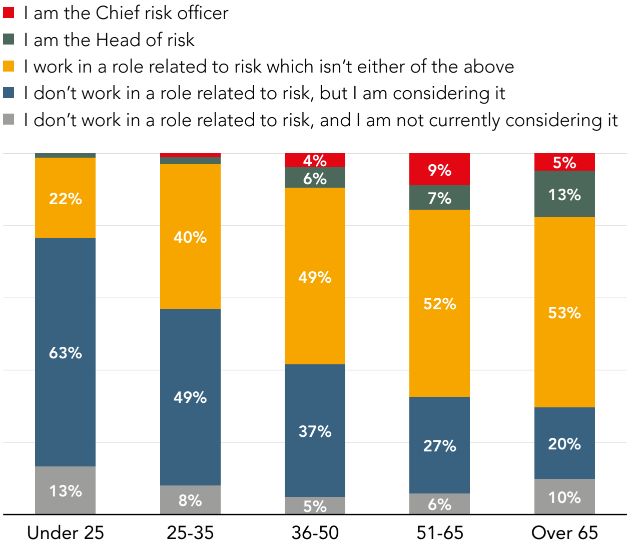
Who is who in risk management?

One of the best aspects of our research is that the survey results allowed us to compare responses between people who are risk professionals and those financial professionals who are not in roles explicitly related to risk (Figure 2.7). We were also pleased that the number of respondents in each role gave us the opportunity to dig deeper into specific roles, such as those of chief risk officers and heads of risk and put them into context in relation to internal audit, for example, especially when we were speaking with them or reading their responses to the two open-ended questions in the survey, which we will discuss later in this chapter.

We also asked about risk versus non-risk functions across other dimensions, such as age. Here it was clear that younger respondents tended not to work in a role explicitly related to risk but interestingly many were actively considering some form of risk role as part of their job activities, and we learned through our discussions that Gen Zs and Gen Ys yearn for more involvement in the risk conversations at their organisations.

During our special interest group discussions, lack of experience was highlighted as a risk from a risk knowledge perspective, and the possible reasons for it went beyond the simple dimension of seniority being linked to age (Figure 2.8).

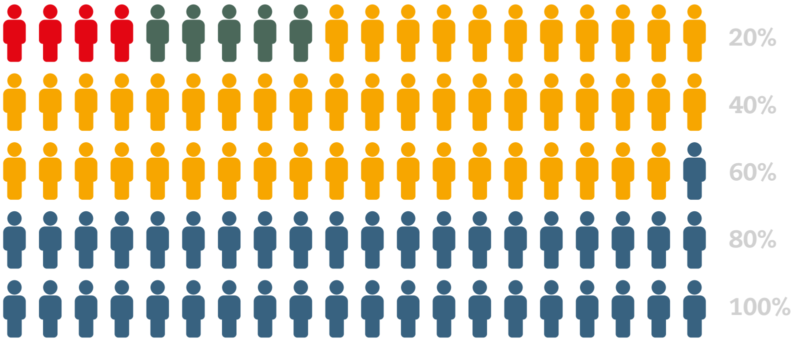
FIGURE 2.8: Roles by age



(Data rounded to nearest whole number)

'Are age groups defining and understanding language in a different way? Or perhaps age groups differ in terms of risk perception? An effective risk culture should provide a consistent point of reference which would hopefully flatten out such differences.'
Special interest group participant

FIGURE 2.7: Who is who in risk?



4% Chief risk officer

5% Head of risk

50% Other role related to risk

41% Not in a role related to risk

(Data rounded to nearest whole number)

CHIEF RISK OFFICERS
Mostly in regulated or large multinational companies with some being regional CROs of big oil, insurance, investment banking, chemicals, pharma companies for example

HEADS OF RISK
Overseeing enterprise risk for medium to large businesses or in charge of certain risks, including operational, credit, market, cyber, as well as culture and conduct. Heads of Risk may be the most senior risk leaders in large multinational companies where sectors are less regulated

RISK ROLES BUT NOT CRO OR HEAD OF RISK
This includes internal audit (though we found some internal audit in the heads of risk if they had 'risk' in the title too; external audit, finance teams, compliance as well as other C-suite)

ROLES NOT EXPLICITLY IN CHARGE OF RISK
Financial controllers, accountancy practitioners, academics, consultants, training, entrepreneurs of different types, many public sector positions, and a range of business development roles

When the differences between age groups came up in one of our CROs Forum sessions, one member, who said he has become 'fascinated by the whole area of behavioural economics and its application to risk management', advised us to be careful not to stereotype different generations, otherwise you may create artificial generational divides that make it even more difficult to get the language right across the organisation. Our findings attest that the needs of all ages are complex and in constant change, and we see how understanding both the similarities and differences between generations is a key first step in both attracting and keeping talent.

> *'The CEO and I are in our 40s and we work well together but that doesn't mean that I do not work just as well with those on the risk committee or in my team who may be on other ends of the generational spectrum. This kind of engagement is another important aspect of risk culture and another reason why culture becomes so important to your competitiveness. Even if technology is making our processes more efficient, at the same time I see the human aspects of risk more than ever before.'*
>
> **ACCA CROs Forum participant**

We also looked at where the responsibility for risk within an organisation sat from a functional perspective. Our data shows that most organisations represented by the survey respondents placed responsibility for risk with either specific risk employees – a CRO or head/director of risk, internal audit or finance teams – and a minority placed the risk responsibility in the hands of a non-executive director or other function.

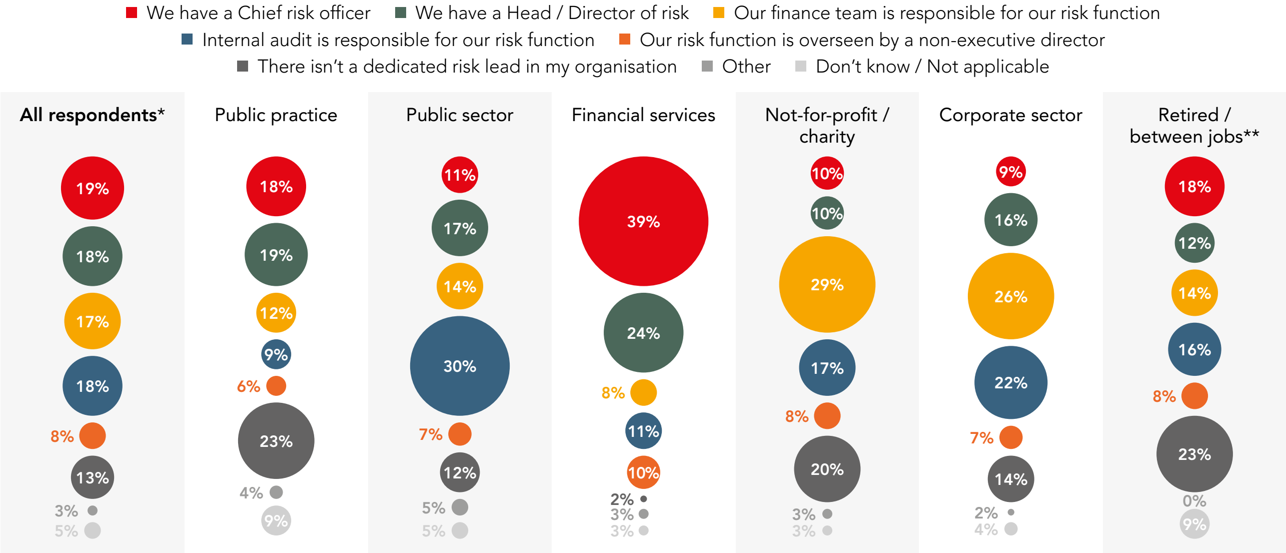
The numbers responding, 'there isn't a dedicated risk lead in my organisation' varied by sector. Overall, 13% of the respondents said there was no specific risk leader in their company. It dropped to 2% in the financial sector and rose to 20% in the not for profit / charity sector (Figure 2.9). Jane Walde, an enterprise risk consultant, and member of the special interest group, emphasises that without risk leadership and adequate tone from the top, it is very difficult to shape and embed a risk culture (Figure 2.10).

> *'8% of respondents said the risk function is overseen by a non-executive director. Perhaps this should open a debate about whether the risk function should be overseen by a non-executive director, or at least have regular conversations with one given that the governing board or trust are ultimately responsible for the risks the organisation is taking.'*
>
> **Jane Walde, enterprise risk consultant, who is also a member of the special interest group and ACCA's Global Forum for Governance, Risk and Performance**

And on the topic of accountability for risk among non-risk functions, the role of HR alongside risk and finance teams arose often in discussions as being an essential part of avoiding blind spots – from bullying to expenses patterns we heard how many are known but not addressed. 'Every business transformation requires a culture transformation', as one respondent also put it.

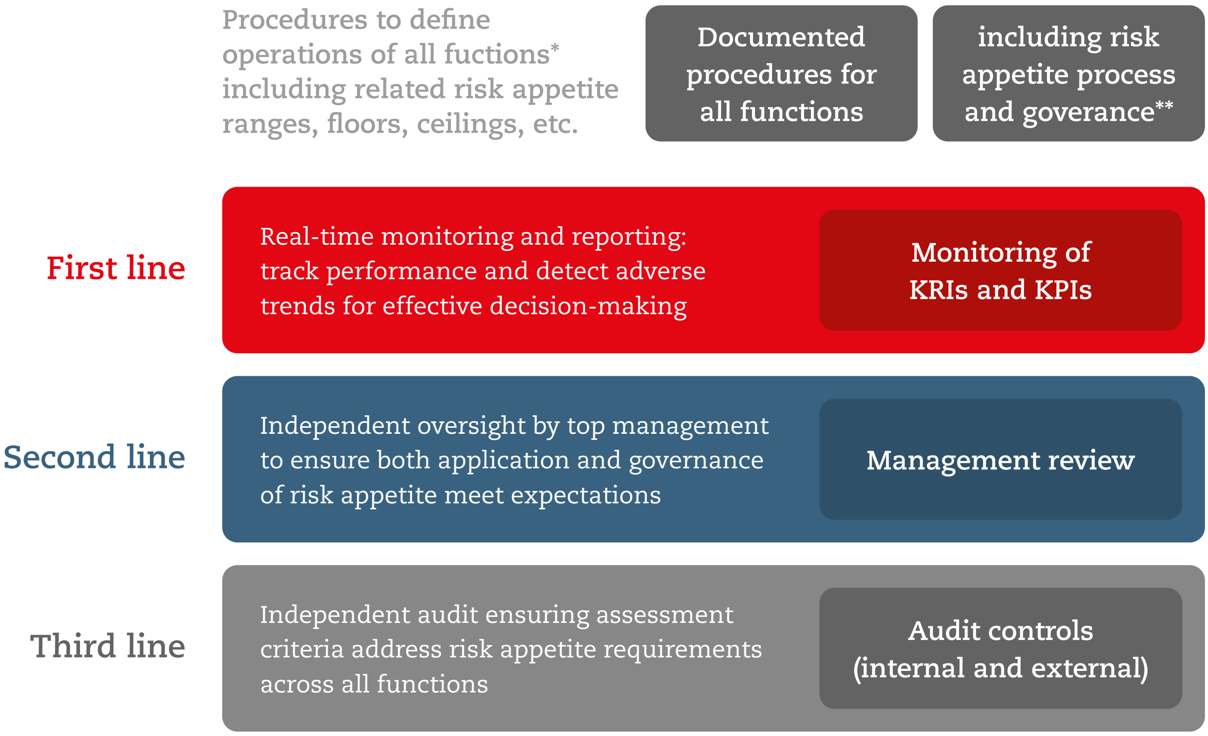
> *'The HR function is just as much a compliance function [as the risk function]. HR sometimes thinks that they are there to develop career growth. That's the sexy part, but when you're dealing with so much change, you need a strong, smart HR department that understands the company's mission and values, or else your culture can really decline. You need an HR department that's going to work with the business and help manage the behaviours during trying times.'*
>
> **Head of internal audit & risk, apparel company**

FIGURE 2.9: Risk organisation varies across sectors



*Data shows the '% of total responses', so 19% of responses were 'We have a Chief Risk Officer'. Note that multiple responses from one person are possible.
**People not currently working were asked to answer with reference to their previous job.

FIGURE 2.10: The ‘Three Lines Model’ and Risk Appetite



Procedures to define operations of all fuctions* including related risk appetite ranges, floors, ceilings, etc.

Documented procedures for all functions

including risk appetite process and goverance**

First line

Real-time monitoring and reporting: track performance and detect adverse trends for effective decision-making

Monitoring of KRIs and KPIs

Second line

Independent oversight by top management to ensure both application and governance of risk appetite meet expectations

Management review

Third line

Independent audit ensuring assessment criteria address risk appetite requirements across all functions

Audit controls (internal and external)

*Make sure there are no ‘black holes’ or ‘glass ceilings’ where process controls and risk appetite parameters do not reach. It may prove difficult to define, control and set metrics for some functions such as those with sensitive information (finances, HR) or creative processes (design, marketing), or managers may try to avoid the process controls applied in the core operations and service delivery. This would very likely have damaging knock-on effects, including avoidance of monitoring, audit and reporting for management oversight, so it is important to map out all functions in your organisation as one connected management system to ensure nothing has been missed.

**Emphasised here to spotlight risk appetite, but in practice, it is likely to be both part of operating procedures and controls defined around risk management / ERM overview itself.

Source: adapted from Airmic-Arthur D. Little-QBE *EXPLAINED Guide, Risk Appetite*, 2021

How **internal audit evolves** with **risk management** remains a big question

Our survey also examined the effectiveness of internal auditors and planning processes. We asked, 'Can internal audit at my organisation verify whether proper internal controls and processes for dealing with risky behaviours are in place and adhered to?' Only around two-thirds agreed that internal audit could verify internal controls for risk taking and approximately one-fifth either disagreed, didn't know, or preferred not to say (Figure 2.11).

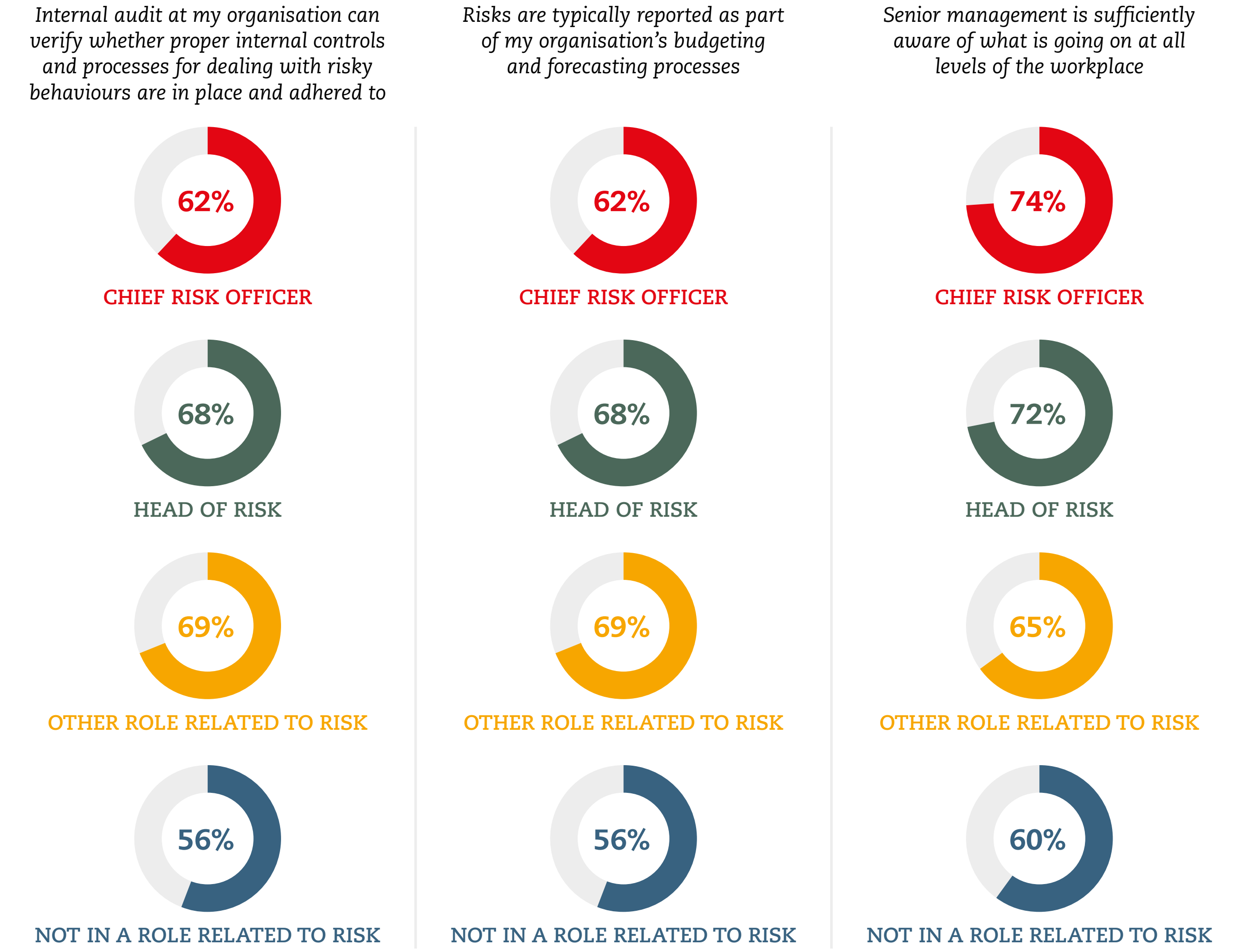
The data could indicate another blind spot, this time in internal auditing. Perhaps the difficulty arises because most intended controls for behaviour are policies and guidelines, and the test should be on how behaviours change in practice.

There is also the possibility that reactive controls, such as penalties for misconduct, can be tested and reported better (or created, if not in place). Other levers and predictors of behaviour, for example, bonuses, might also be risk-assessed for unintended consequences, preferably with the advice of the risk function, which can signpost risk indicators for internal audit to test. Whether risks were typically reported as part of an organisation's budgeting and forecasting processes varied: only roughly two-thirds said that risks were included in the internal financial processes.

Since all controls require resource, any adjustments to budgets should be firmly based on the necessity (or otherwise) of controls. An understanding of how these controls will change the risk so that objectives can be met within the ethical values of the company is necessary when determining whether the budget allocation is sufficient.

Risk gives a basis for prioritising spending, and it should be remembered that meeting behavioural and cultural aims also requires resource, so the question should be not 'Can we achieve our objectives?' but rather 'Can we achieve our objectives in a way that corresponds with our ethical and cultural values?'

FIGURE 2.11: Potential blind spot – only two-thirds of risk and financial professionals believe that internal audit can verify internal controls



Internal audit at my organisation can verify whether proper internal controls and processes for dealing with risky behaviours are in place and adhered to

Risks are typically reported as part of my organisation's budgeting and forecasting processes

Senior management is sufficiently aware of what is going on at all levels of the workplace

Risk appetite: even when people **understand** it, they **behave** differently

Most respondents said they had a good understanding of risk appetite in their organisation, with the under-35s and those not explicitly in a role related to risk rating their understanding lowest. This was still at a very high overall level, at around 80%, which was not only astounding to everyone involved in the data analysis but also contradicted what respondents were revealing in the roundtables and online community pop-up platform (Figure 2.12).

A good understanding of what risk appetite 'is supposed to be' does not necessarily mean the behaviours and culture inside an organisation reflect the stated appetite for risk taking. Culture and risk appetite too often diverge and work against each other as separate forces.

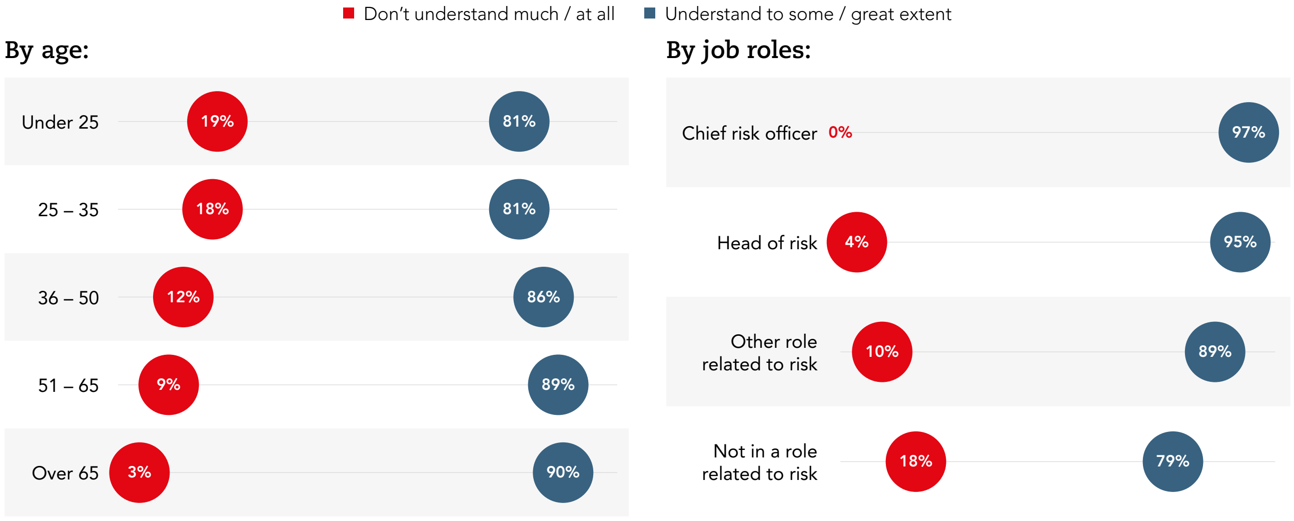
> *'Risk appetite is a key component of enterprise risk management. Willingness to bear risk can be defined as an organisation's desire or aversion to pursue opportunities in an uncertain business environment and as how much volatility around an expected outcome is tolerable in terms of capacity, regulatory compliance, ethics, reputation, and alternative costs for a business. Risk appetite varies between industry sectors and between organisations within sectors, and by geographies and types of risk. The level of regulation and capital intensity of an organisation will also influence its perception of acceptable risk in relation to potential opportunities. The context in which all organisations operate is dynamic, and an approach of continuous improvement should be adopted to ensure that risk appetite is reviewed and updated in synchronisation with change, and signed off by key stakeholders, including the Board. Key is that whatever the business and whatever the context, risk appetite and risk culture should reflect "the way we do things here".'*
>
> Julia Graham, CEO, Airmic

The stated greater understanding of risk appetite in 50 to 65 year-olds and over 65s in the survey data is again perhaps another reflection of overconfidence and therefore, dangerously, a complacent view that it is not necessary to be particularly engaged or concerned. This was one of the viewpoints in one of our special interest group discussions.

> *'Many of that age would be in senior positions or board level and are probably not trained to deal with new and challenging issues around risk culture, so they are more likely to want to keep doing what they have been doing.'*
>
> *'There is a hardening, a sclerosis if you like, across organisations and industries. There'll be a "first man over the wall gets shot – so no one wants to go first" scenario. There's also a defence of sorts in saying "we're doing the same as our peers" and thereby claiming to be "best practice". How about "effective practice" as a better alternative? If you don't have an effective practice, how can you be confident that you really understand the risk appetite of your organisation?'*
>
> Special interest group participants

A GOOD UNDERSTANDING OF WHAT RISK APPETITE 'IS SUPPOSED TO BE' DOES NOT NECESSARILY MEAN THE BEHAVIOURS AND CULTURE INSIDE AN ORGANISATION REFLECT THE STATED APPETITE FOR RISK TAKING.

FIGURE 2.12: Making sense of the overconfidence about understanding risk appetite



('Don't knows' remain the balancing figure for each age/role)

Overconfidence is a result of opting for apparently simple solutions where in practice there are none. One member of our special interest group pointed out the challenges of persuading senior people that simply benchmarking yourself against others is not the answer.

'People can get stuck on benchmarking. How am I doing against others? How are you doing when it comes to the effective management of risk in your business? I tell board members I can compare their organisations to anybody, but it might be different tomorrow morning. Rather, what I suggest is they improve their level of maturity by not obsessing about benchmarking. See where you are instead, and how you can grow. And this is hard, not just because I'm handing them a problem as opposed to a simple solution, but because if they get any of the Big Four coming into their business and doing their version of a risk culture maturity assessment, one of the key things they'll say is "we will benchmark you". I would really like to steer people away from benchmarking as the solution.'

Special interest group member

These comments on benchmarking also remind us of Daniel Kahneman's book *Thinking Fast and Slow*, (Kahneman 2012) in that we can rely too much on making simple immediate judgements because being decisive is a behaviour all senior executives like to display. Kahneman's 'slower thinking' is about the more effortful thinking required to understand complex entities. This is what leaders in effective risk cultures will demonstrate – they will admit 'I don't know'.

Another example of the desire for 'black and white thinking' leading to overconfidence in assessing risk appetite stood out from a comment in our online community pop-up, given there are always going to be two sides to this: qualitative and quantitative.

'You might say that you have zero tolerance for risks that will damage your reputation, such as cyber risks, but nobody in the world can have zero tolerance for reputational or cyber risks because it's not a matter of if they're going to hit you, but when. You can't zero them out so expressing that in a risk appetite statement is ridiculous, it's not real. A risk culture perspective on risk appetite says 'is risk appetite known by every employee and are they acting within it? Are people operating at the top end of your risk appetite so we can give them the best "risk taking assessing reward?" That is a good culture.'

Online community pop-up participant

Since articulation of risk appetite helps guide and inform behaviour and therefore culture, it is logical to suggest that improved communication of risk appetite is going to be beneficial in building a successful risk culture. Respondents also noted, however, that within a single multinational organisation different appetites for risk may be appropriate in different regions and that will warrant different conversations about it.

'Risk appetite it is pretty different across the different regions we work in. For example, in the West we basically have a larger risk appetite for trading activities, and in the China region a larger risk appetite for real estate and property. I also believe there's a difference between the culture of the banks and branches of them within Asia. For example, banks in Singapore and Japan sit somewhere in-between Western and Chinese banking culture.'

CRO at a global investment firm in Hong Kong SAR

'Even for the banking sector there will be different business models. You look from one side of the world to the other and you will see that their appetites or tolerances for risk will be 'night and day', so there's no template for risk culture and that's especially true when it comes to perceptions of risk appetite.'

Non-executive director for Asia-based bank

Risk culture is about both diversity and cohesiveness. Getting that balance right is integral to how an organisation is governed, and it reflects how well an organisation can achieve its objectives. There is no single right or wrong risk culture. This is something borne out in our research. We found that risk culture and how it is framed varies hugely, depending on the organisation: what industry it is in, what regulations it must follow, who the stakeholders are, as well as how its stated purpose and tolerance for risk are defined. Structures within any single organisation might also constantly change as the speed of risk accelerates. Nevertheless, the implications of diversity, cohesiveness and good governance cannot be overlooked.

RISK CULTURE IS ABOUT BOTH DIVERSITY AND COHESIVENESS. GETTING THAT BALANCE RIGHT IS INTEGRAL TO HOW AN ORGANISATION IS GOVERNED, AND IT REFLECTS HOW WELL AN ORGANISATION CAN ACHIEVE ITS OBJECTIVES.

A related point made by members is that there can be very good reasons why risk appetite needs to change, but if it does then culture and communication should be carefully adjusted to ensure that alignment remains.

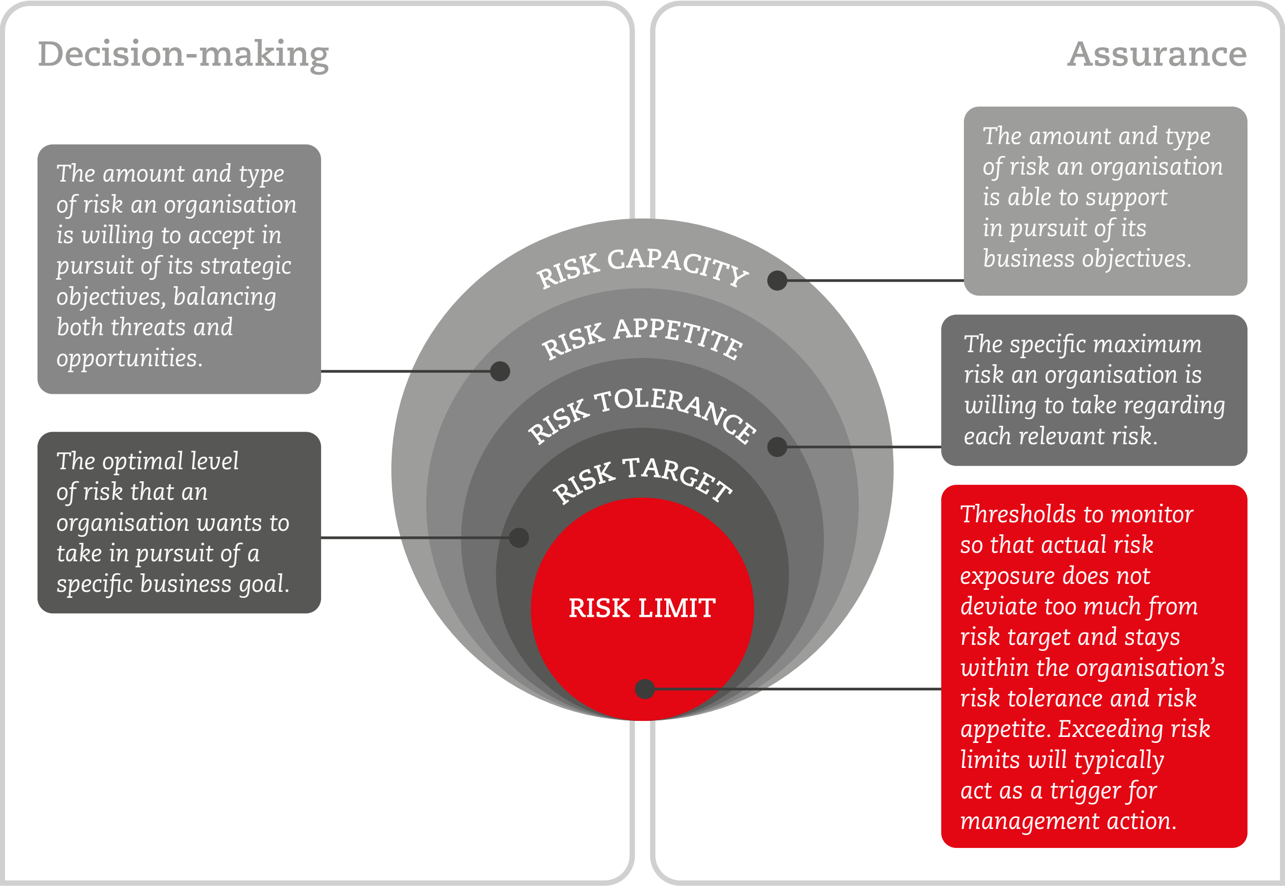
> *'People tend to become more willing to accept a higher level of risks, given [that] every day seems to bring something new and unexpected to worry about. That might be another explanation for overconfidence in the findings related to risk appetite. I think there's going be a sea change in the way we perceive risk. People might be saying that "risk is covered" or that "we are good with our risk assessments", but I would say deep down they know that is not the reality of it, especially when it comes to conduct.'*
> **Chief audit officer in Europe**

THE CONSENSUS IS THAT RISK APPETITE HAS BECOME MUCH MORE THEORETICAL THAN PRACTICAL.

Our research also revealed that even if you have your risk appetite, risk culture and behaviours perfectly in line, when a person has to make a quick decision they may do something completely out of step because of the pressure of the moment. The consensus is that risk appetite has become much more theoretical than practical and that many perhaps claimed to understand risk appetite just because of they were aware of the organisation's risk appetite statement (Figure 2.13).

> *'A risk appetite statement could be something beautiful and flowery, whatever the case may be, but there's no way to measure it since it is changing all the time. I have seen situations where we're not actually taking enough risk, because people want to follow their procedures, and they don't want to grab the ball and be the person who's called out if something goes wrong. On any given day the overall position might not be out of line with the stated appetite, but it may be that someone is just so worried about something going wrong, that they don't want to take the chance.'*
> **Risk manager at bank in North America**

FIGURE 2.13: Key concepts of risk appetite



The amount and type of risk an organisation is willing to accept in pursuit of its strategic objectives, balancing both threats and opportunities.

The optimal level of risk that an organisation wants to take in pursuit of a specific business goal.

The amount and type of risk an organisation is able to support in pursuit of its business objectives.

The specific maximum risk an organisation is willing to take regarding each relevant risk.

Thresholds to monitor so that actual risk exposure does not deviate too much from risk target and stays within the organisation's risk tolerance and risk appetite. Exceeding risk limits will typically act as a trigger for management action.

Source: 'adapted from Airmic-Arthur D. Little-QBE *EXPLAINED Guide, Risk Appetite*, 2021

The inside story of **overconfidence** and **debilitating misalignment** between **culture** and organisational **purpose**

When we asked respondents whether their organisation's risk culture was aligned to its purpose, the results were similar, with around 70% agreeing, chief risk officers scoring highest at 80% and heads of risk lowest at 63% (Figure 2.14).

On the one hand the data shows a clear majority agreeing there is alignment on the difficult topic of alignment between culture and organisational purpose, but at the same time about one-third do not believe there is. But again, what about overconfidence? Do respondents genuinely understand whether their culture is aligned to purpose or were they basing their agreement on statements written on their websites?

The short-sightedness of relying on what you can see was famously illustrated by Donald Rumsfeld, the former US Secretary of Defense: 'Reports that say that something hasn't happened are always interesting to me, because as we know, there are known knowns; things we know that we know. We also know there are known unknowns. There are things that we know we do not know. But there are also unknown unknowns – the ones we don't know we don't know'.

His famous quote came up often during our research discussions and led us to another point that 'claiming you are not biased' is perhaps the worst bias of all. The ability to recognise the limits of your knowledge and say 'I don't know' is key to effective risk management but what is equally important is following up and reducing knowledge gaps as far as possible.

As we learnt through one-on-one interviews, there are diverging definitions of what 'risk' means and indeed how purpose is related to it. This was thought-provoking, since the respondents were all risk and financial professionals.

Nonetheless, respondents did agree that whether it is firefighting or chasing profit opportunities, the overconfidence in 'knowing what our biggest risks are' is just as hazardous. That individuals have different perceptions of where risk appetite fits in was also a common concern, particularly in the banking and professional services environments. This becomes most problematic when distinguishing good versus bad risk taking. Unfortunately, risk registers and risk reports are not going to solve these problems.

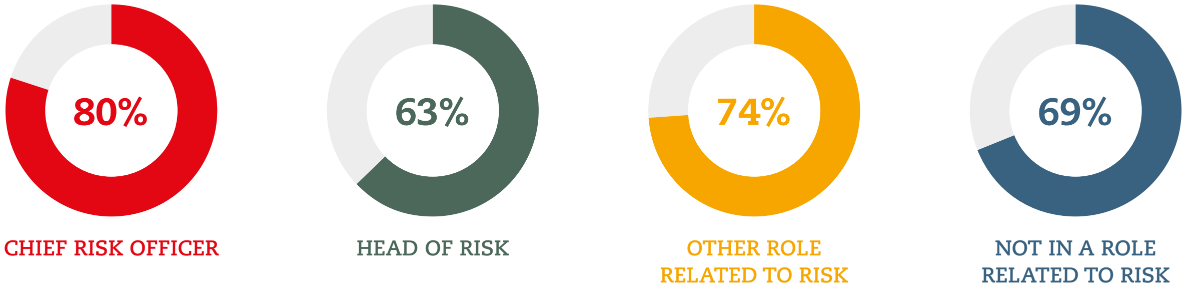
'I'm trying to transform and combine financial and non-financial risk quantification on our risk register and have learned early on how much [understanding behaviours] matters. The real lightbulb moment is when you're trying to get this super aggregate of the different levels of risks and potential control failures. From an accountancy perspective, scenario analysis is at the heart of understanding what can go wrong, but this also is where all these questions and images about customers, safety, and how people think and act come in, so you see how behaviours have so much to do with it now.'

CRO in Europe

'The problem with risk reports is that the details become conveniently averaged out as you read along, so aggregating a core figure for risk proves unhelpful in the end. Quantum[sic] processes can mislead and disguise some of the finer sensitivities, and quite often the behaviour-based sensitivities of these finer details get buried at the back of the report and no one beyond the risk team ever reads them.'

Dr Roger Miles, presenting on Behaviours at Risk at CROs Forum

FIGURE 2.14: One-third say culture and purpose are not in line



AROUND 70% OF ALL RESPONDENTS AGREED THAT THEIR ORGANISATION'S RISK CULTURE WAS ALIGNED TO ITS PURPOSE. CHIEF RISK OFFICERS SCORED HIGHEST AT 80% AND HEADS OF RISK LOWEST AT 63%.

We also considered to what extent the mixed results reflect the constant battle between the culture believers and those more concerned with ticking boxes, and how we verify the risks and their implications.

> *'Some banks have put names on teams to oversee behaviours, culture and conduct risks, but are these window-dressing efforts? It's hard to see whether they have any real power or influence, and the concern could be that they are spending a lot of their time justifying their existence rather than driving true change. The CEOs do not want someone going over their head to the board so you can see how they're able to deflect an issue downward into obscurity if they choose [to do] so.'*
> **Special interest group discussion**

On the difference in confidence between chief risk officers and heads of risk, we saw a similarly more pessimistic view from heads of risk when respondents were asked whether 'risk awareness informs strategy' (Figure 2.15).

We also found those not in a risk role showed lower confidence when we asked whether public commitments are really aligned with risk culture (Figure 2.16).

Thus, misalignment is certainly not something that only risk professionals care about. Some of the respondents in roles not explicitly in charge of risk told us they wished that they were more involved in defining and articulating the purpose and risk appetite statements (Figure 2.16).

We found plenty of those financial professionals from outside the risk team agitating to be heard when we asked two open ended-questions and in the online community pop-up.

The alignment or not of 'an organisation's risk culture with what it says it does publicly' was a hot topic in our interviews. Respondents talked about culture risk – or the 'risks in a culture' – where an organisation with a culture of dysfunction or fear or conversely 'success-at-any-cost' carries the risk that its people will engage in unethical behaviour and wrongdoing, something that is certainly not in line with its publicly stated purpose, risk appetite and values. This could stem from poor management, bad systems, or an environment in an organisation where misbehaviour is not reported.

We also found that the most optimistic respondents, by role, for alignment of culture, strategy and purpose are the chief risk officers. While the top risk for organisations overall is compliance, the 'Job to Be Done' for many risk professionals is not about ticking a compliance box, but fixing the risk culture inside their organisations, because that is how they see these organisations becoming compliant. The message was clear that risk leaders are working passionately to improve culture and align it with purpose. Some perhaps believe they're getting somewhere while others probably do not, but believe that they will or must somehow find a way to get the authority they need to change the mindsets of their peers.

FIGURE 2.15: Heads of risk less confident than others that risk awareness informs strategy

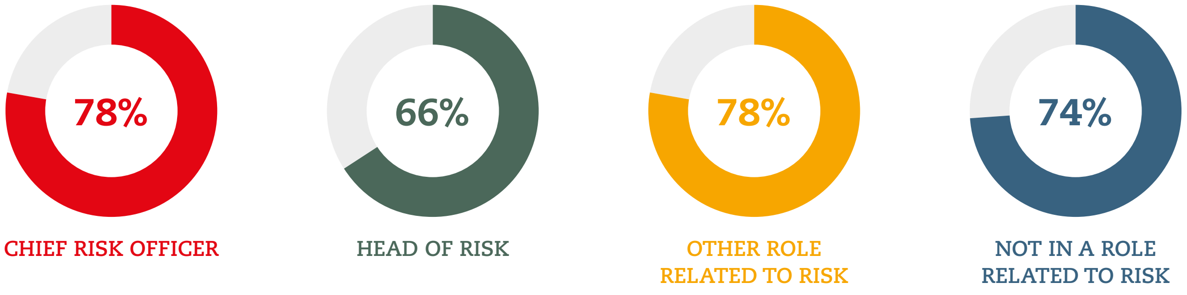
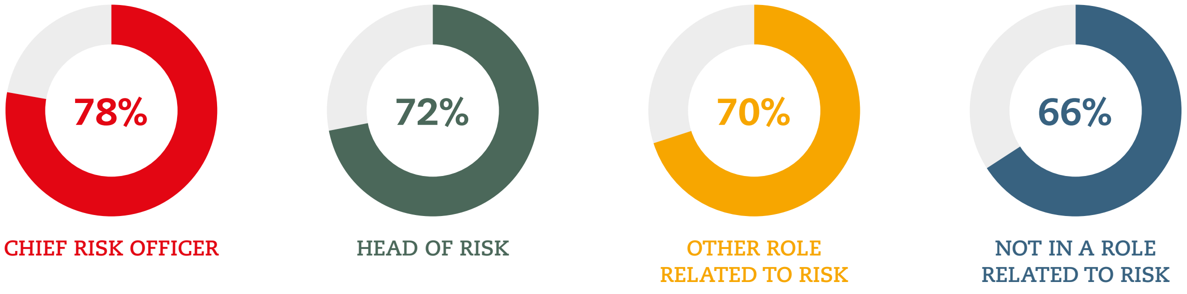


FIGURE 2.16: Those not in a risk role less convinced that risk culture is what the organisation says it is



This question is, for many, a reflection of their own work and the success of what they themselves are responsible for and trying to achieve, but the overriding challenge for them is getting others at the top to appreciate how behaviours in their organisation drive risk.

> *'I think risk management is still seen as a process by most, whereas the effective management of risk is what we need to focus on. It's more about the purpose [being] to support the execution of strategy. When we start looking deeper into the human behaviours that underpin the responses to risk, that's the important shift in mindset we are talking about. It's about the decisions that every employee makes every day in their job at any point in time. It's about the employees having a risk-management mindset. If everyone looks left, right, and left again we have a stronger understanding of how to respond in any given situation.'*
> Horst Simon, risk culture builder, Canada and Namibia, member of special interest group

Respondents talked about how the behaviour of people inside an organisation should be a focus when discussing costs, another 'hard numbers' reason to promote the risk culture agenda.

> *'We have to think about mistakes that our employees can make and how they respond to them. This is something that we are focused on, and we know it can be costly if a customer's satisfaction is affected. But this requires resources, and we need to think about where we innovate, where it matters most; and that is more challenging than you think because of the market we are in and the fast-changing headwinds we face today.'*
> CFO from a US corporate

A member of our special interest group also pointed out the futility of relaxing for a moment simply because you've thoroughly ticked all the boxes you can possibly think of.

> *'You can tick all the boxes and list all the risks that you know, but tomorrow morning that might be totally different due to any kind of external or sometimes even internal factors. There definitely was a risk register for Twitter, which changed overnight and there's a risk register in most organisations which changed overnight when Covid struck. So, if someone expresses assurance that they are brilliant on any one day, that assurance may be worthless the next morning because they totally missed something like a global pandemic. It's not about the plan and testing the plan, it's about how people will respond to that situation when it happens.'*
> Special interest group member

The view of most risk leaders in our survey was clear-cut: if a company has a set of ethical values as a foundation of its culture and these are aligned with an efficient risk framework, in theory, compliance with regulations would be a natural consequence.

> *'Do we need to be reminded of FTX? This wasn't something done in the deep dark recesses of the crypto world. This was about some sophisticated people, some real knuckleheads when it comes to internal controls, approving expenses with emojis. It was just a crazy bad culture that brought it down.'*
> Non-executive director at bank based in North America

We also see how organisations that focused on compliance and processes were falling down the incompetence slide, whereas those that understood the importance of culture and did something about it were more forward-looking. A good risk culture was viewed as an organisational culture that gives staff the capacity to spot emerging risks and act on them. A weak culture was described as 'misaligned', 'bureaucratic' and 'process-driven': one that enables activities at odds with stated policies and values.

One of our respondents also pointed out that investment in technology without appropriate governance often carried huge risks of misfiring. This respondent talked about the scramble in 2020 to rush through digitalisation plans and how the continuous monitoring required to keep up with fast-changing ways of working was not sufficiently maintained.

> *'We threw cash at new digital technologies and cyber risk software but conducted an assessment two years on and realised we didn't get the proper implementation needed to reap the cost-savings benefits we thought we were getting, and in turn just exposed ourselves to more risk than we had before we'd invested in these new technologies.'*
> Survey respondent

A GOOD RISK CULTURE WAS VIEWED AS AN ORGANISATIONAL CULTURE THAT GIVES STAFF THE CAPACITY TO SPOT EMERGING RISKS AND ACT ON THEM. A WEAK CULTURE WAS ONE THAT ENABLES ACTIVITIES AT ODDS WITH STATED POLICIES AND VALUES.

Phil James, a partner at the cyber risk boutique consultancy, CIO-Office, presented to ACCA's Global Forum for Governance, Risk and Performance in February 2023 on developing governance and oversight for cybersecurity and new technologies and argued that only behaviour can stop many scandals, particularly those involving social media. Internet risk culture was a subject that sparked much interest during discussions.

The conflict between 'What somebody has told us we must prioritise, ie, the box needing to be ticked' and 'what actually needs to be done to ensure we are compliant' is a significant factor revealed by the survey, which showed that two-thirds of respondents agreed that culture, strategy, and purpose are aligned and one-third did not.

> *'LinkedIn is the most common offender, but it's not just the posts. You can lose valid usernames, password combinations and other confidential data without being hacked and that's a risk that most organisations fail to look at. People might write confidential things in their CVs that reveal IT and security resources; what systems the company is good at or what projects they're working on. That gives a lot away to the hackers.'*
>
> **Phil James, partner at CIO-Office**

Risk conversations are happening in a **vacuum at the top**

We asked, 'Are risks sufficiently discussed at all levels in your organisation?' Only around 60% of respondents agreed that they were (Figure 2.17). Our discussions about the results pointed to the fact that this is the opposite of what a good risk culture is supposed to do.

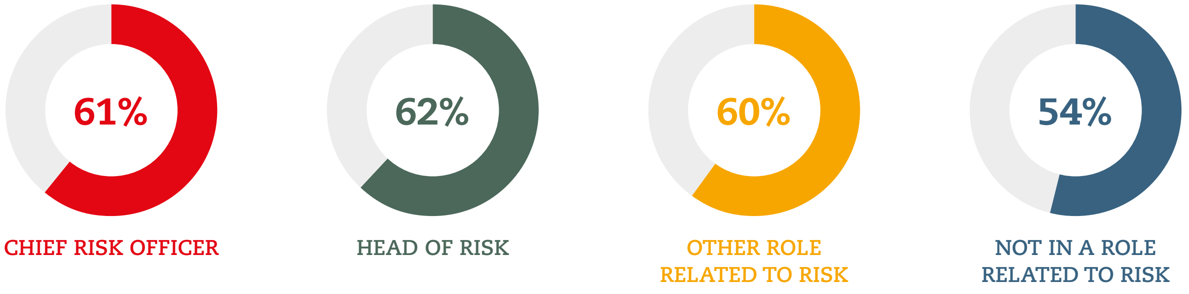
> *'Risk culture should enable leaders to connect with the emerging reality of the business so there would appear to be room from improvement here.'*
>
> **Special interest group member**
>
> *'My biggest challenge as head of risk is getting staff to understand that their responsibilities include acting as risk managers; making them see that while the risk team provides guidance, the business and risk owners still have to make the final decisions and take responsibility for risks'*
>
> **Head of risk on the survey's question about what constitutes the biggest challenge**

The lower level of agreement by those not explicitly in a risk role may also indicate that true enterprise risk management (ERM), where every function engages in risk management, is yet to be embedded in many of the organisations surveyed. Our conclusion is that silos still exist even in what is considered the most mature ERM framework.

In the open-ended questions of the online survey, those respondents in roles not explicitly in charge of risk said that interpreting volatile macro and political conditions and aligning them with risk strategy remained one of biggest challenges. One respondent complained of a general over-confidence, within the business, that risks were all under control.

> *'The capacity to deal with change and that expectation from the board that we can predict the future are all myths.'*
>
> **Respondent to online survey**

FIGURE 2.17: Only 60% of risk and financial professionals believe risk is sufficiently discussed



ONLY AROUND 60% OF RESPONDENTS AGREED THAT RISK WAS SUFFICIENTLY DISCUSSED AT ALL LEVELS IN THEIR ORGANISATION.

Board and **senior management coordination** needs to **improve**

Overall, two-thirds of respondents agreed that their board and senior management have the same approach (Figure 2.18). But there were a lot of 'I've heard enough about tone at the top' comments in our discussions, and many respondents, including those in senior management, said that with the changes in work and virtual board meetings 'tone from the top' is a cliche that has lost meaning. A chief risk officer from an insurance company in Europe helped us understand another perspective behind the data – exactly how potent is the 'tone from the top' and should it also be assessed when we think about expectations of what a risk culture can do?

> *'While the board has overall responsibility for culture, including its alignment with risk culture, it is essential to assess the effectiveness of "tone from the top" when ensuring that the expected risk culture is happening in practice.'*
> **CRO, insurance company, Europe**

One audit committee chair at a Hong Kong SAR conglomerate also commented on the importance of cascading risk awareness throughout the organisation.

> *'Strong risk awareness is important in what we all do, not only in a risk department. Our group board, through the audit committee, defines the tone at the top regarding the culture of our risk management and controls and must lead that by example. Our chief risk officer at the bank subsidiary drafts our risk appetite statement but that is discussed with many others, including other board committees and every business function head. The CRO and chief operation officer coordinate training, townhall and communications with staff about our risk appetite. The government in the China region provides guidance on cultural exchange and promoting people bonds and cooperation, and we follow that.'*
> **Audit committee chair, Hong Kong SAR**

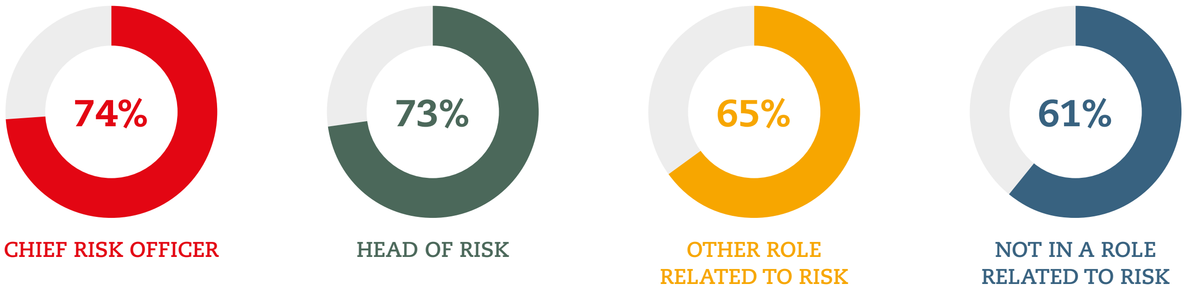
Our online-community platform revealed several reasons why different functions in an organisation may or may not be aligned: 'ticking boxes' again, with the board and senior management talking in a vacuum.

> *'We can talk about tone from the top but what about the tone from the middle? You can't just have your senior management, the C-suite and the board talking about how we've got a healthy risk culture. How do you convey that and how does it cascade to the rest of the staff?'*
> **Online community pop-up**

In a roundtable of European respondents, a risk advisory consultant at one of the Big Four accountancy firms talked about how conversations at each level are critical for people to understand what's behind KPIs or Key Risk Indicators (KRIs). The point is that without conversations there is no possibility of 'being on the same page' and our survey showed low levels of maturity overall.

> *'We can see how misaligned the risk culture is from the first conversation we have with a client, so we do questionnaires and interviews before we help them implement risk management frameworks. Management then has an ongoing communication with the risk takers and the wider audience about what really defines their risk appetite and how those at the end of the curve can pick that up. They then see how alignment can be improved simply by having people be part of the conversation. The more who are involved in the conversation, who know what's behind the KPIs or KRIs, the better. It really is about knowledge and information sharing.'*
> **Risk advisory consultant with a Big Four firm in Europe**

FIGURE 2.18: Different functions speaking different languages about risk



OUR ONLINE-COMMUNITY PLATFORM REVEALED SEVERAL REASONS WHY DIFFERENT FUNCTIONS IN AN ORGANISATION MAY OR MAY NOT BE ALIGNED: 'TICKING BOXES' AGAIN, WITH THE BOARD AND SENIOR MANAGEMENT TALKING IN A VACUUM.

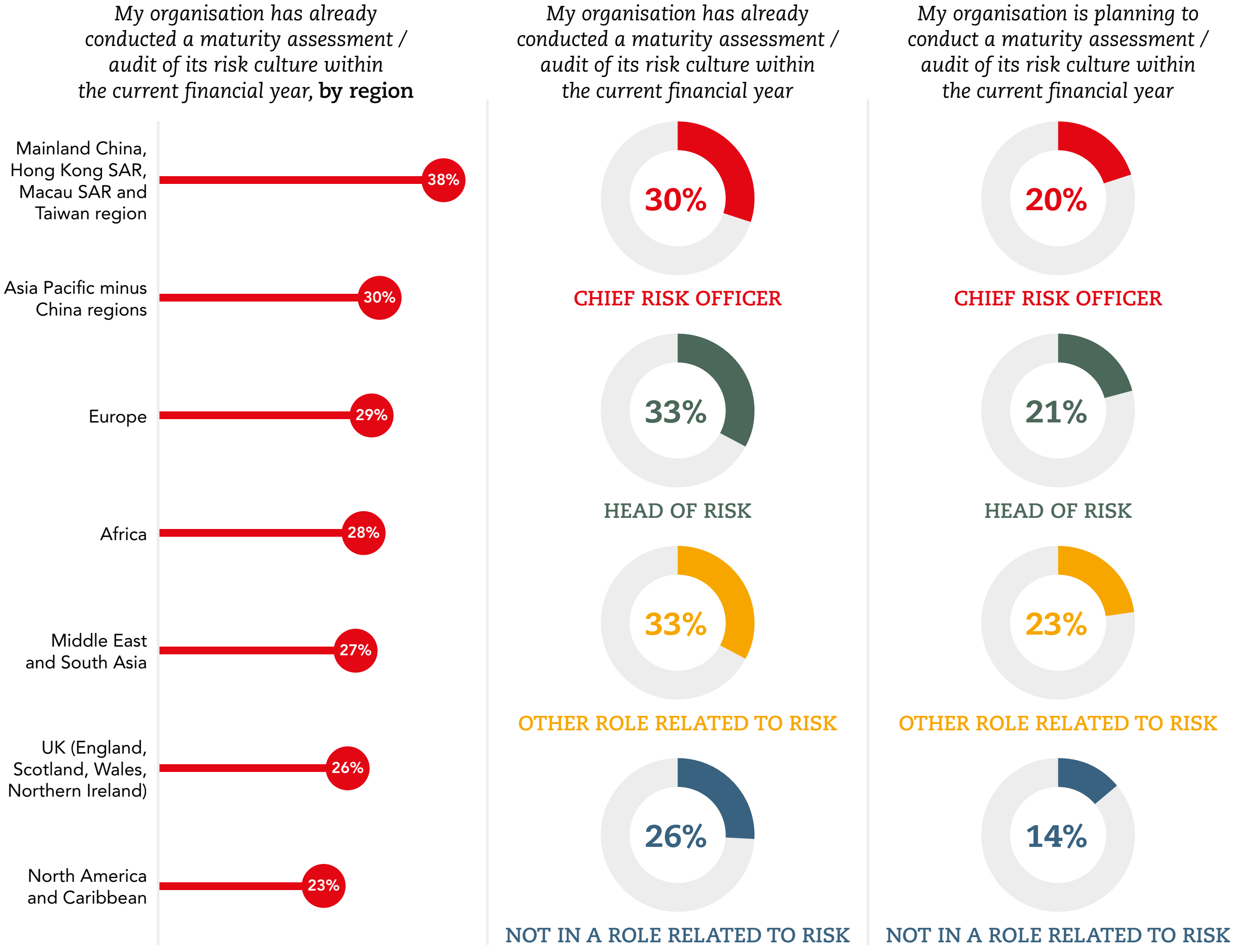
Our online-community platform also provided perspectives about the link behind whether people are 'on the same page' (or not) and incentives and rewards. The difficult question of how you reward someone for contributing to a 'good culture' was highlighted in discussions.

> *'Risk culture, or if you want, culture risk, is always, from a leadership perspective, going to be overwritten by something more existential, like cyber risk, and that's the problem with so many organisations. They have a quarter-to-quarter perspective and it's hard for them to focus on the bigger picture and that's something the CEOs and CROs need to overcome together. Your call to action should be to look beyond the quarter-to-quarter performance. You've got to look at culture and its effect over the longer term. Lagging governance can certainly have a sudden, adverse deleterious effect. But as a CEO or CRO, how is your performance gauged? If you look at all the CEOs of the big US banks, it's the earnings announcements. They get large bonuses based on stock performance, revenue and controlling costs. So, how do we reward someone for [contributing to] a 'good culture'? There are just a number of things that need to be overcome.'*
> **Online community pop-up**

ONE-THIRD OF SURVEY RESPONDENTS HAD CONDUCTED A RISK ASSESSMENT IN THE PREVIOUS 12 MONTHS, BUT HOW DID IT ADD VALUE?

We asked respondents whether they had conducted a risk culture maturity assessment or audit of risk culture, and about one-third said they had conducted one within the current financial year, and around a 20% more said that they were planning one (Figure 2.19). Again, we get the same message: there is interest in the topic, but it is certainly not an automatic feature of an organisation's annual priorities, and interpretations of what an assessment might be vary.

FIGURE 2.19: More than half have worked or are working on risk maturity assessments



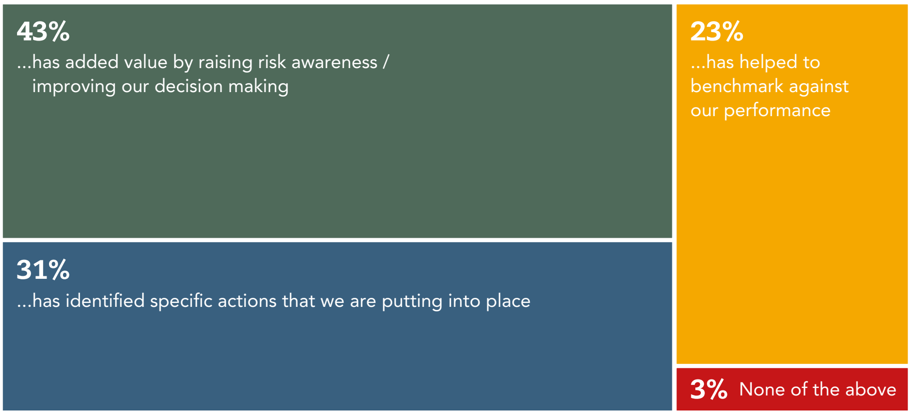
My organisation has already conducted a maturity assessment / audit of its risk culture within the current financial year, ***by region***

My organisation has already conducted a maturity assessment / audit of its risk culture within the current financial year

My organisation is planning to conduct a maturity assessment / audit of its risk culture within the current financial year

Mainland China, Hong Kong SAR, Macau SAR and Taiwan region
38%
Asia Pacific minus China regions
30%
Europe
29%
Africa
28%
Middle East and South Asia
27%
UK (England, Scotland, Wales, Northern Ireland)
26%
North America and Caribbean
23%
30%
CHIEF RISK OFFICER
33%
HEAD OF RISK
33%
OTHER ROLE RELATED TO RISK
26%
NOT IN A ROLE RELATED TO RISK
20%
CHIEF RISK OFFICER
21%
HEAD OF RISK
23%
OTHER ROLE RELATED TO RISK
14%
NOT IN A ROLE RELATED TO RISK

FIGURE 2.20: Which of the following statements are true with regards to the outcome of an assessment / audit of risk culture at your organisation?



43%

SAY RISK ASSESSMENTS HAVE IMPROVED RISK AWARENESS

(Data rounded to nearest whole number)

We also asked about the outcomes of assessments of risk culture, which revealed that they come in many different forms. (See quotes from online community pop-up.)

> *'We have had much success with incorporating behaviour economics and I have to say that when I engage the business in risk assessment exercises, I don't even mention risk. Risk is counter intuitive because the responses range from blank looks or "it's fine" to panic or a tendency to equate risk with a certain outcome. So, instead, I ask about verifiable facts and from this work with the management team I try to understand the risks that these facts give rise to or what risks can be inferred from the data.'*
>
> ACCA CROs Forum

While there appears to be positive feedback, we also saw no lack of alternative views on the effectiveness of risk maturity assessments when we spoke to respondents (Figure 2.20). One ACCA member who sits on company boards around the world said, 'they're often just a filler with little value added'.

> *'I've seen many risk maturity assessments, and they are all …their own versions, but the reality is that [companies are] not really doing anything with them. The results stay in the risk team and don't really get acted on. Any sense of the real risk culture at an organisation is more of a check-list exercise from what I can see. Also, it depends on who you are talking to. So, if you are interviewing the people who are producing these programmes, they well may argue that it is working fantastically, but if you talk to another audience, they might say it's a bit iffy.'*
>
> Board chair

The head of compliance of a bank in Greece couldn't see how risk maturity assessments provide any reliable insight into risk culture and said that she didn't believe any of the respondents from her part of Europe could say that they had completed one during the last financial year. Referring to a new Greek corporate governance rule requiring listed companies to appoint a chief risk officer, the respondent made the comment below.

> *'Right now, most of us are in the process of assessing all the new requirements of the law, but I have not seen many companies conducting actual risk maturity assessments and would add that I have never seen one that takes behaviours and culture into account. That's not to say that people are not aware of wrongdoing or not doing something bad. It's just that most of them are hidden secrets and have never been included. I think that's why people have answered your survey in a confident way at least from what I see in Europe. They feel confident because they genuinely do not know if anything bad has happened. They only know the impact of wrongdoing after the fact.'*
>
> Head of compliance in Greece

A head of risk from a mid-size tech company in Europe also spoke about the difficulties of producing quality risk-maturity assessments, explaining how it is one thing to identify the main risks but when you dig deeper into individual activities and processes to get a bigger picture, you end up with too many biases to piece together.

> *'You cannot assess everything; you need to scope it. We look at a key process, certain geographical spread, or different types of risk drivers. Even if you have only the first line [of defence] submitting self-assessments, that's still a lot of input so it becomes important to have tools to eliminate biases when you consolidate your inputs. Only then do you have a chance to genuinely capture a bottom-up picture to make visible to the board. This is even more of a challenge today when the world is moving faster. The picture changes daily, but that makes it more important than ever to do continuous monitoring, and you can't do that unless you have key risk indicators at various levels within the organisation, not just at the top with the risk team. If you ask yourselves whether something happened when the sickness rate was abnormally high, you need models that interpret how much of a deviation there is and whether that's something you need to look at, so the controls team know what direction that risk is moving in. You need pillars that will pick up the signals everywhere and the means to interpret those signals and analyse them.'*
>
> **Head of risk, technology company, Europe**

Indeed, a common thread across respondents in all regions and sectors was that everyone has their own interpretation of what a risk maturity assessment looks like and how it is conducted and used. A CRO at an insurance company in Europe talked about how theirs is acted on.

> *'We conduct a maturity assessment model each year where we look at several dimensions from questionnaires that rank 1 to 5 on "culture, people and organisation", "risk control cycle", and "organisation and governance". The CEO and CRO own the outcome and calibrate with the group functional heads to define actions and follow-ups. For example, this year with People we saw the team had increased turnover, so we agreed to improve our succession planning and increase our interactions with the rest of the organisation.'*
>
> **CRO, insurance company, Europe**

Alastair Goddin, head of risk at Asta in London – as well as a member of the special interest group, ACCA's Global Forum for Governance, Risk and Performance and ACCA's CROs Forum – says it makes sense that there are no consistent views of what a risk culture or risk maturity assessment should look like, since there is no one-size-fits-all even in one industry, but that in regulated sectors it pays to modify them over time to meet individual needs.

> *'We have implemented a risk culture assessment framework, which has helped us to identify areas for improvement, where our clients are doing well and where we can drive actions to improve the risk culture and therefore overall risk management framework. The approach is based on regulatory guidance but includes specific expectations of the Lloyd's market. It has provided another view of the risk framework for senior management and the board.'*
>
> **Alastair Goddin, head of risk, Asta, London**

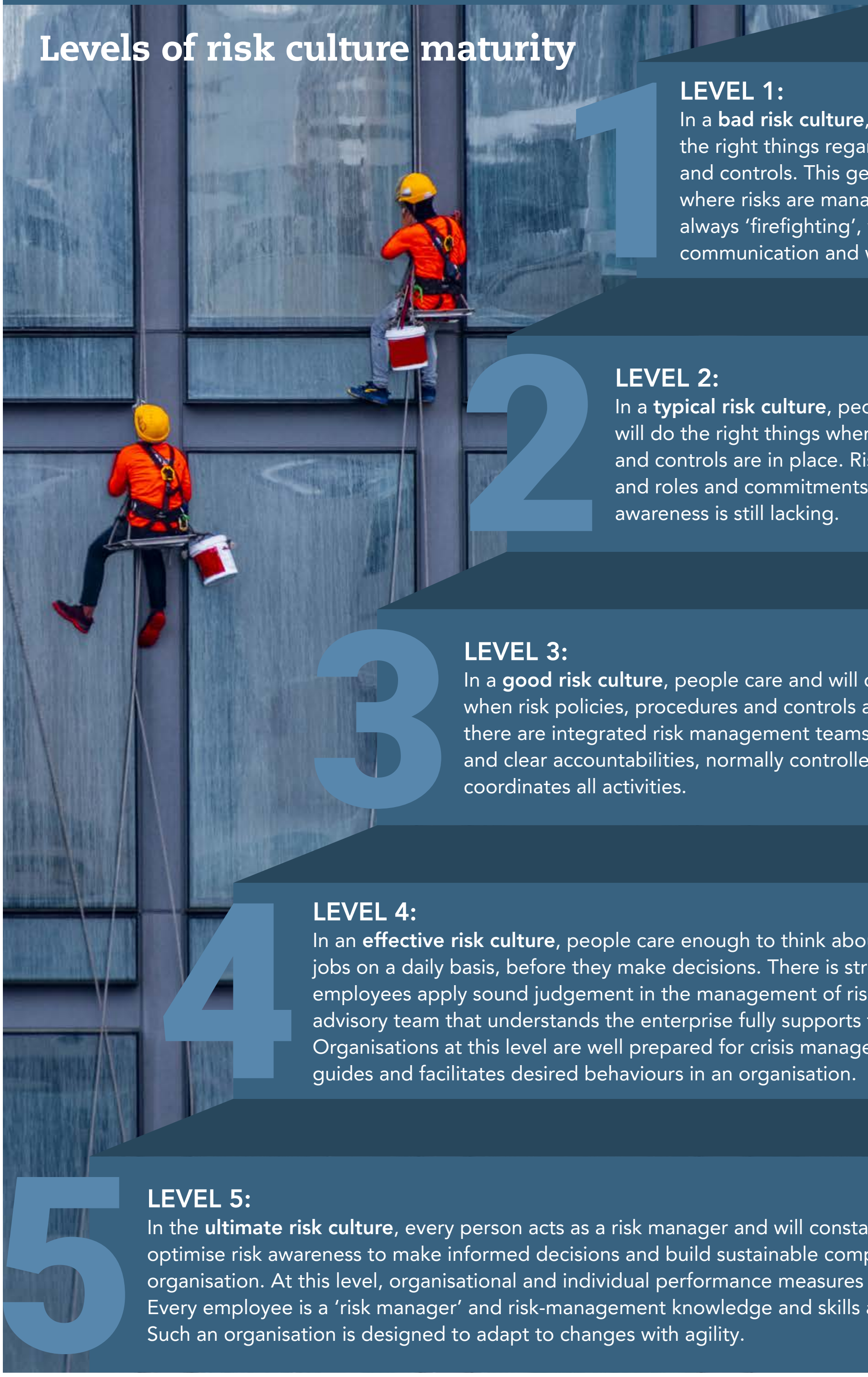
DOS AND DON'TS in measuring risk culture maturity

by **Horst Simon**, Risk Culture Builder

Building an effective risk culture starts with an accurate evaluation of the level of maturity in the organisation, and there is no 'one size fits all' model for measuring that. There are various methods for executing such assessments; some of these are commercially available.

In general, these models use five levels of maturity with descriptors, and measure specific elements. These 'levels' are my own assessments, based on my experience with the measurement of risk culture in the financial services, engineering, healthcare, and energy industries.

Levels of risk culture maturity



1 LEVEL 1:
In a **bad risk culture**, people do not care and will not do the right things regardless of risk policies, procedures and controls. This generally reflects an environment where risks are managed in silos, and people are always 'firefighting', with no clear risk owners, no real communication and weak accountability.

2 LEVEL 2:
In a **typical risk culture**, people tend to care more and will do the right things when risk policies, procedures and controls are in place. Risk owners are clearly defined, and roles and commitments are understood, but effective awareness is still lacking.

3 LEVEL 3:
In a **good risk culture**, people care and will do the right things even when risk policies, procedures and controls are not in place. At this level, there are integrated risk management teams with standardised roles and clear accountabilities, normally controlled by a central function that coordinates all activities.

4 LEVEL 4:
In an **effective risk culture**, people care enough to think about the risks associated with their jobs on a daily basis, before they make decisions. There is strong cross-functional teamwork and employees apply sound judgement in the management of risk. A small central risk-management advisory team that understands the enterprise fully supports the business at all levels. Organisations at this level are well prepared for crisis management. An effective risk culture guides and facilitates desired behaviours in an organisation.

5 LEVEL 5:
In the **ultimate risk culture**, every person acts as a risk manager and will constantly evaluate, control, and optimise risk awareness to make informed decisions and build sustainable competitive advantage for the organisation. At this level, organisational and individual performance measures are fully aligned and risk sensitive. Every employee is a 'risk manager' and risk-management knowledge and skills are upgraded continuously. Such an organisation is designed to adapt to changes with agility.

DOS AND DON'TS in measuring risk culture maturity

by **Horst Simon**, Risk Culture Builder

Boards and executives always want to know how they're doing versus their peers, and they generally rely on third-party consultants to produce a report to tell them that. Assessments are normally conducted through one or a combination of: surveys/questionnaires; staff interviews; focus groups; external stakeholder interviews; social media reviews; and reviews of operational processes.

Owing to the underlying human factors and behaviours of employees, the subjective responses to these tools and activities are often not accurate. Just as no two people will respond the same way to a specific situation of risk, the way a person responds to the questions and ratings is influenced by several factors, such as nationality and culture; work ethics, trust and honesty; religion and other spiritual thinking; and unconscious biases.

Risk culture maturity surveys attempt to assess the attitudes and perceptions of their employees towards risk, but they are prone to many inefficiencies. Reasons for the limitations and ineffectiveness of surveys and risk culture maturity assessment interviews can be found in the appendix.

Through my work experiences in Africa, the Middle East, Canada, and Australia, I found that using an online assessment tool is much more accurate and cost-effective than days of consulting time spent through human intervention with interviews, questionnaires, and 1-to-5 ratings. There are various psychological assessment tools such as AS200 and DISC that measure human behaviour, but do not have links back to risk perception. There are also many risk-management measuring tools based on ISO31000 and COSO standards that focus merely on control assessments and compliance with processes; with no link to the human factors and behaviours involved.

The Risk Culture Maturity Monitor[3] that my company uses provides outcomes-based reporting on the level of maturity in six categories of risk-management operations: policies; processes; people and organisational design; reporting; management and control; and systems and data.

The assessments are delivered through a unique IT platform; therefore, no infrastructure investment is required by the organisation. Users are required only to have access to the Internet and each user is supplied with a unique user ID and password to complete their assessment online. The underlying mathematical model is not visible to users and all questions and answers are structured in such a way that it is impossible for any user to manipulate or predict the outcome.

Organisations need to use tools that can effectively measure the level of maturity of risk-management systems, processes, organisational design, and related human factors in a consolidated and accurate manner. The outcomes of such an assessment must clearly drive a combination of strategies, such as training, communication, and leadership, to formulate targeted actions and so build an effective risk culture. Additionally, building such a culture also requires continuous monitoring and improvement.

It is thus important to understand that building an effective risk culture is a continuous process that requires commitment and effort from all levels of the organisation. Executives and their teams manage risks successfully in their jobs, every day. This will ultimately lead to improved performance and much better outcomes.

[3] The Risk Culture Maturity Monitor, by Genius Methods Ltd; is an effective software tool that accurately measures the level of maturity of embedding an effective risk culture in any organisation.

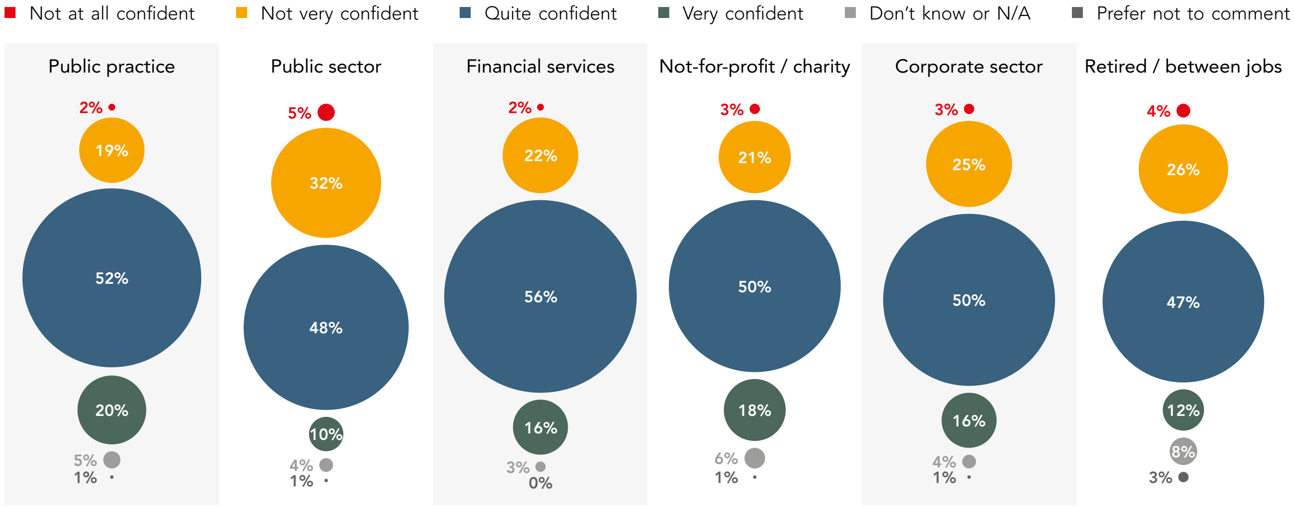
How well does risk culture detect misconduct?

Improvements in risk culture are also aimed at anticipating and detecting unexpected behavioural or misconduct issues. We asked respondents whether they were confident that their organisation's risk culture could do this, and our data reveals a mixed picture of success, with the dominant response being only 'quite confident detection will happen' (Figure 2.21). Overall, respondents seemed uncertain about whether risk culture enables detection of risky behaviours and misconduct. However, respondents from mainland China were generally more confident in their organisations' risk culture compared to other countries.

The public sector notably scores highest for 'not very confident that detection will happen'. Interestingly, the public sector also placed misconduct/fraud/reputational damage higher than other sectors as a risk priority – with only not-for-profit/charity organisations placing it higher. This perhaps indicates an awareness of the issue.

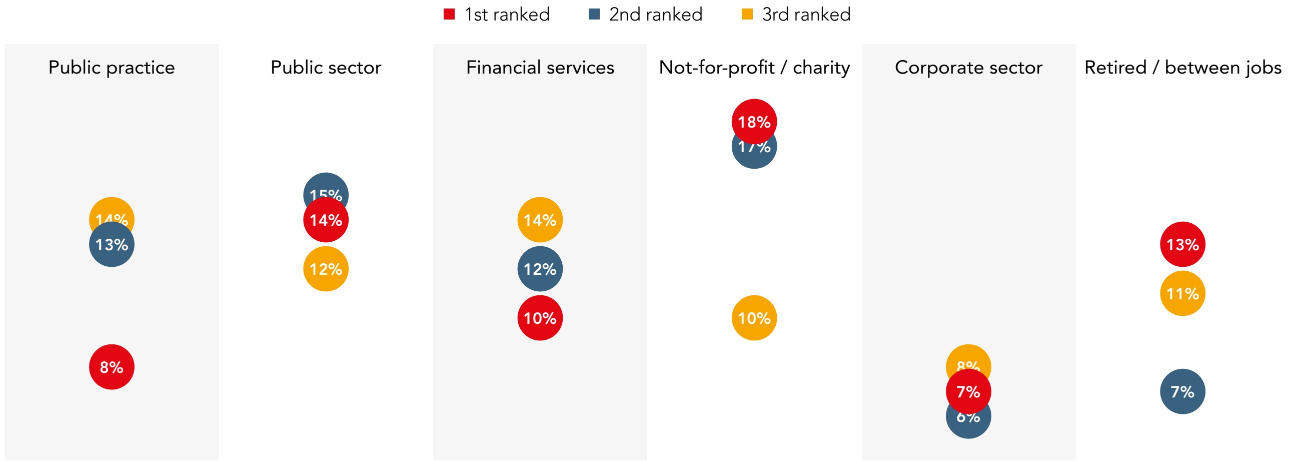
The corporate sector stood out on the other end of the spectrum, ranking misconduct/fraud/reputational damage significantly lower than others (Figure 2.22). This sparked much discussion with our special interest group, given the news headlines about numerous fraud indictments across the corporate world at the time we analysed the results, and with most cases being characterised by prosecutors as 'accounting-related misstatements and errors'.

FIGURE 2.21: Respondents overall seemed uncertain about whether risk culture enables detection of misconduct



(Data rounded to nearest whole number)

FIGURE 2.22: Public sector most concerned about misconduct, fraud and reputational damage, while corporate sector significantly less worried



The paper, 'How Pervasive is Corporate Fraud?' by Alexander Dyck and colleagues was also mentioned in our discussions. Published in January 2023 in the *Review of Accounting Studies*, it reveals that only one-third of frauds in public companies actually come to light, suggesting just how common and widespread corporate fraud really is. Dyck et al. estimated that 'in normal times only one-third of corporate frauds are detected… on average 10% of large publicly traded firms are committing securities fraud every year… Combining fraud pervasiveness with existing estimates of the costs of detected and undetected fraud… corporate fraud destroys 1.6% of equity value each year, equal to $830 billion in 2021'(Dyck et al. 2023).

The public sector most frequently agreed that: 'I am aware of wrongdoing in my workplace that has not been investigated'. Respondents from China, in particular, emphasised how state-owned enterprises (SoEs) there have been working on enhancing transparency of their risk governance, as an increasing number of them look abroad to raise capital.

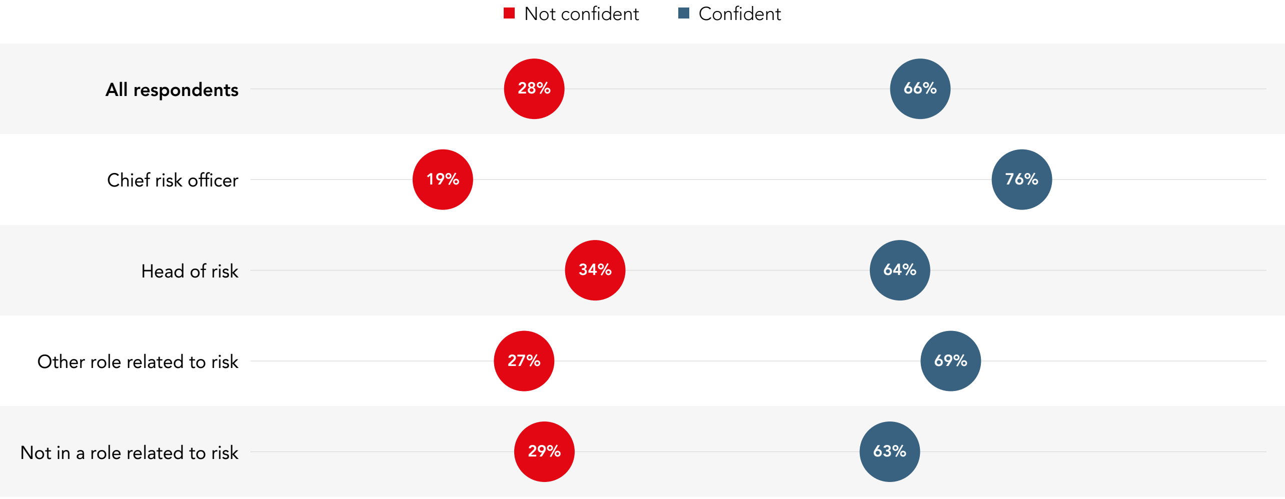
> **ONLY ONE-THIRD OF FRAUDS IN PUBLIC COMPANIES ACTUALLY COME TO LIGHT.**
> DYCK ET AL (2023)

> *'SoEs have placed greater emphasis on risk management in the past couple years, with some revising their risk management systems and processes. For example, one SOE has put forward the concept of risk control as the standard, internal control as the basis, and compliance as the foundation.'*
> **Chair of venture capital fund focusing on SOEs in China**

> *'SoEs are the biggest group of companies in China, so there's naturally great interest about them from a global standpoint and often the concern from a risk perspective is about government inference. As part of China's 2018 corporate governance code all listed companies must have a Party Committee, and for SoEs it is important to remember that many of their leaders are also government officials who were appointed by the SASAC [State-owned Assets Supervision and Administration Commission of the State Council] so the risk management and risk culture is very much be driven by the government.'*
> **Lyndsey Zhang, author of Corporate Governance in China Seen Through a Practitioner's Lens (Zhang 2021) and member of the special interest group**

While CROs have more faith than others in the ability of their risk culture to detect misconduct, this could be an indication that CROs are less in touch with attitudes on the frontline where misconduct issues are perhaps not being dealt with thoroughly (Figure 2.23).

FIGURE 2.23: Faith in the ability of their risk culture to detect misconduct across different roles



(Data rounded to nearest whole number)
('Don't knows' remain the balancing figure for each role)

Of those in a risk role, the CROs also ranked highest on 'not aware of any wrongdoing' and ranked notably higher in confidence than the heads of risk that there were no wrongdoings in their organisations (Figure 2.24). Most likely these heads of risk (or directors of risk) are in companies without a CRO and therefore are the 'one' overseeing all risk or they are responsible for managing a certain category of risk, such as operational. Either in large or small firms, the data shows that heads of risk appear much more aware than CROs about what is happening down the structure.

CROs and heads of risk both showed stronger confidence than those in the non-risk roles when asked about comfort in using a whistleblowing platform, perhaps biased because they share some responsibility for its operation even though it typically sits under legal or compliance. (Figure 2.25).

> *'The response that 37% of CROs are unaware of wrongdoing suggests a possible lack of engagement with whistleblowing or wrongdoing management processes, cases, and outcomes.'*
> **Jane Walde, enterprise risk consultant, who is also a member of the special interest group and ACCA's Global Forum for Governance, Risk and Performance**

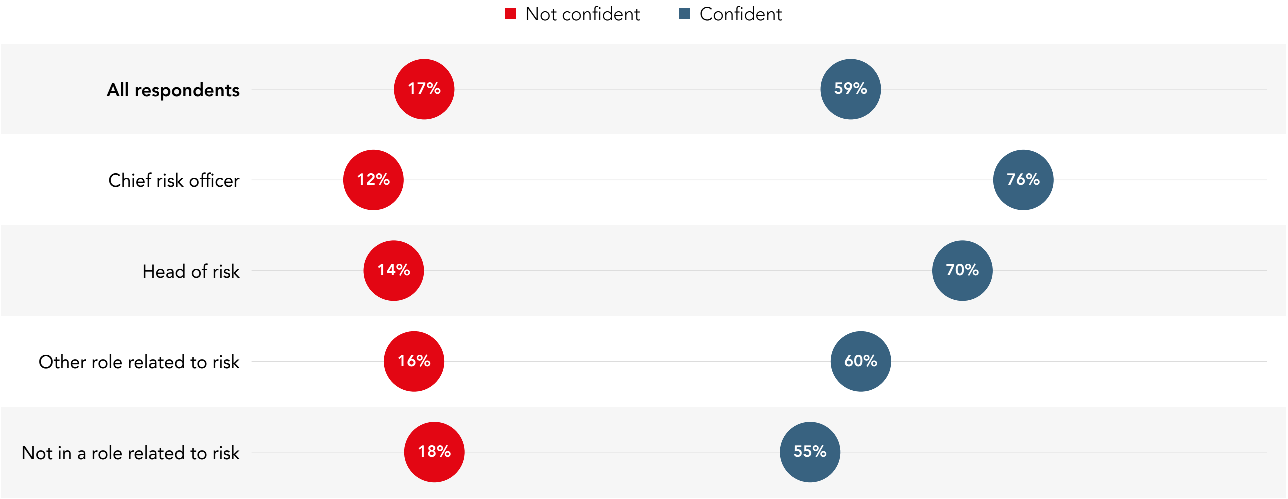
The responses raise concerns about possible disconnections between the managers or guardians of whistleblowing channels and the risk leaders. Questions were also asked about how whistleblowing outcomes are reported and to whom and whether our research shows that risk leaders need to be pushing for more engagement in channels for whistleblowing and suspicions of wrongdoings.

FIGURE 2.24: Awareness of wrongdoing, by role

	CHIEF RISK OFFICER	HEAD OF RISK	OTHER ROLE RELATED TO RISK	NOT IN A ROLE RELATED TO RISK
I am not aware of any wrongdoing in my workplace	37%	22%	34%	51%
I am aware of a wrongdoing that has been investigated and resolved	37%	42%	33%	22%
I am aware of a wrongdoing that has been investigated, but not resolved	16%	27%	20%	15%
I am aware of a wrongdoing that has not been investigated	10%	8%	14%	13%

(Data rounded to nearest whole number)

FIGURE 2.25: Risk bosses show most confidence in the whistleblowing platform



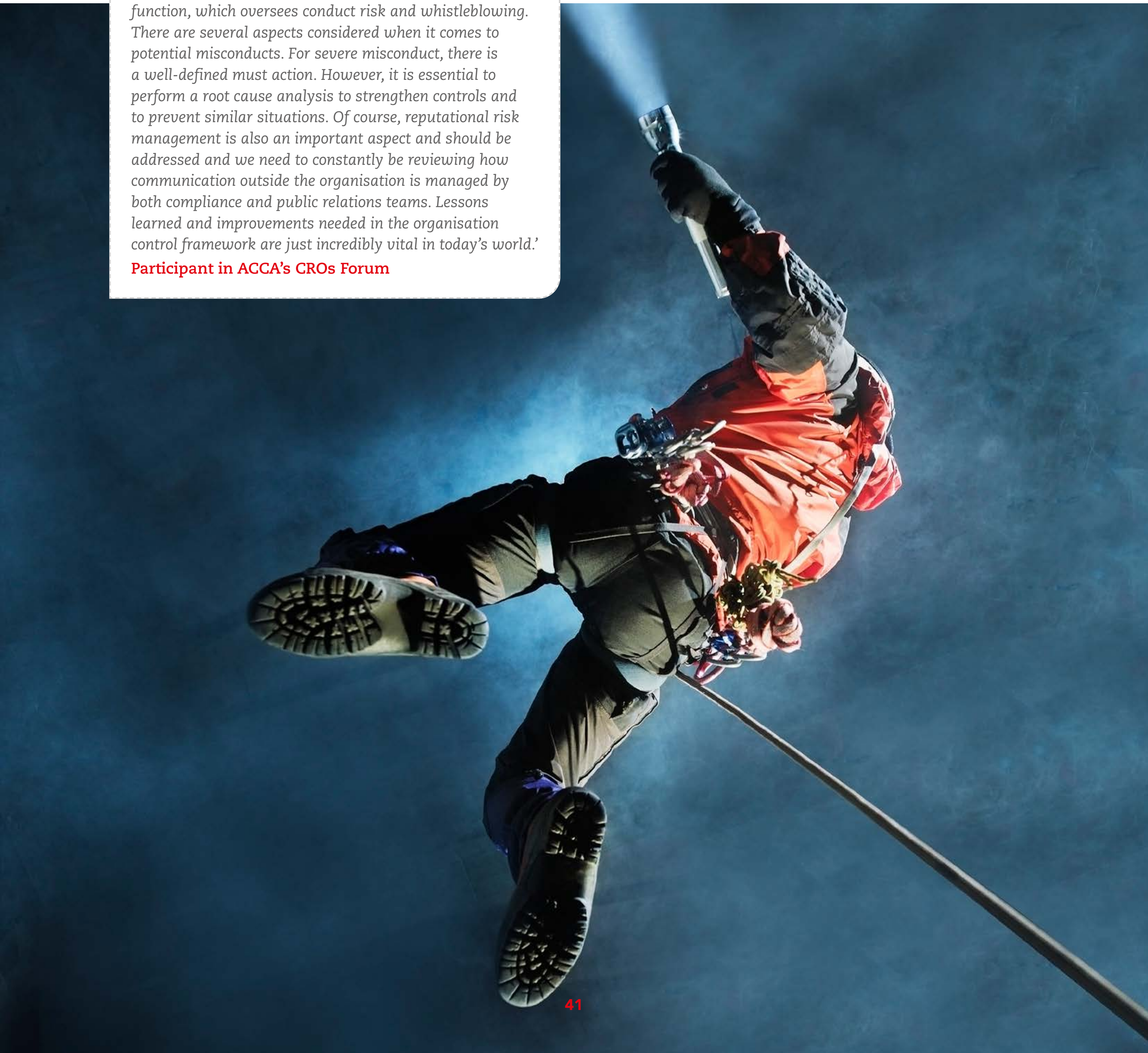
(Data rounded to nearest whole number)
('Don't knows' remain the balancing figure for each role)

The findings show how a measure of caution is often required in investigations, but nonetheless there is never a good outcome if the CRO is in the dark. We could see that while CROs shone a light on the various roles and responsibilities, different levels of information and visibility of issues inside the organisation mean that much can be missed, and that depends highly on the organisational structure of the company as we explain further in the sections below.

> *'I sit on our board with full membership and voting rights, so my opinions are valued and considered for business decisions and strategy setting. The head of risk reports to me so I work very closely with my risk department to understand what's happening in the first line. My head of risk, who by the way oversees fraud risk, is very close to what's happening in the first line and so is the compliance function, which oversees conduct risk and whistleblowing. There are several aspects considered when it comes to potential misconducts. For severe misconduct, there is a well-defined must action. However, it is essential to perform a root cause analysis to strengthen controls and to prevent similar situations. Of course, reputational risk management is also an important aspect and should be addressed and we need to constantly be reviewing how communication outside the organisation is managed by both compliance and public relations teams. Lessons learned and improvements needed in the organisation control framework are just incredibly vital in today's world.'*
>
> **Participant in ACCA's CROs Forum**

Another possible reason for CROs' greater confidence about misconduct may be their direct access to board members. They may believe that they can report issues more easily, as one CRO from a bank in Africa commented on the survey findings.

> *'With these findings, you can see that CROs, and heads of risk often point in different directions. I think it is important to note that most CROs are likely to report to the board and board committees, as opposed to the heads of risk who report to executive management. This difference gives the CRO more authority and makes it difficult for those with less authority to easily report wrongdoing or whistleblowing.'*
>
> **CRO at bank in Africa**

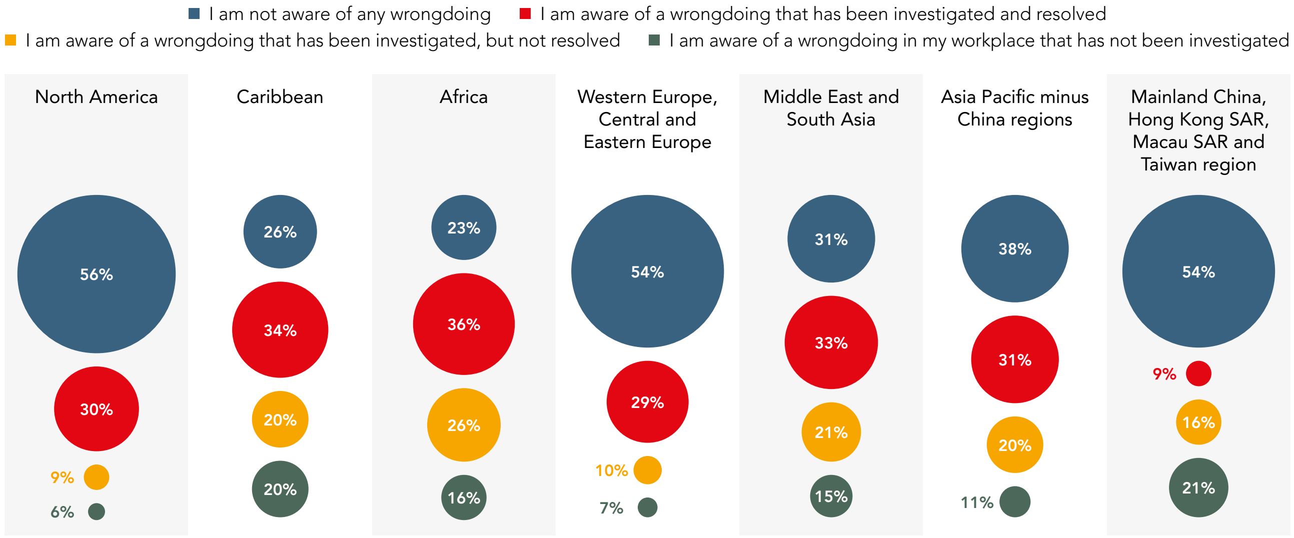


Regional differences in comfort with whistleblowing

The data on a regional and country level for awareness of wrongdoing and resolution provides interesting food for thought (Figure 2.26). For example, Africa ranks highest for stating 'I am aware of wrongdoing that has been investigated, but not resolved' and China highest for stating 'I am aware of a wrongdoing that has not been investigated'.

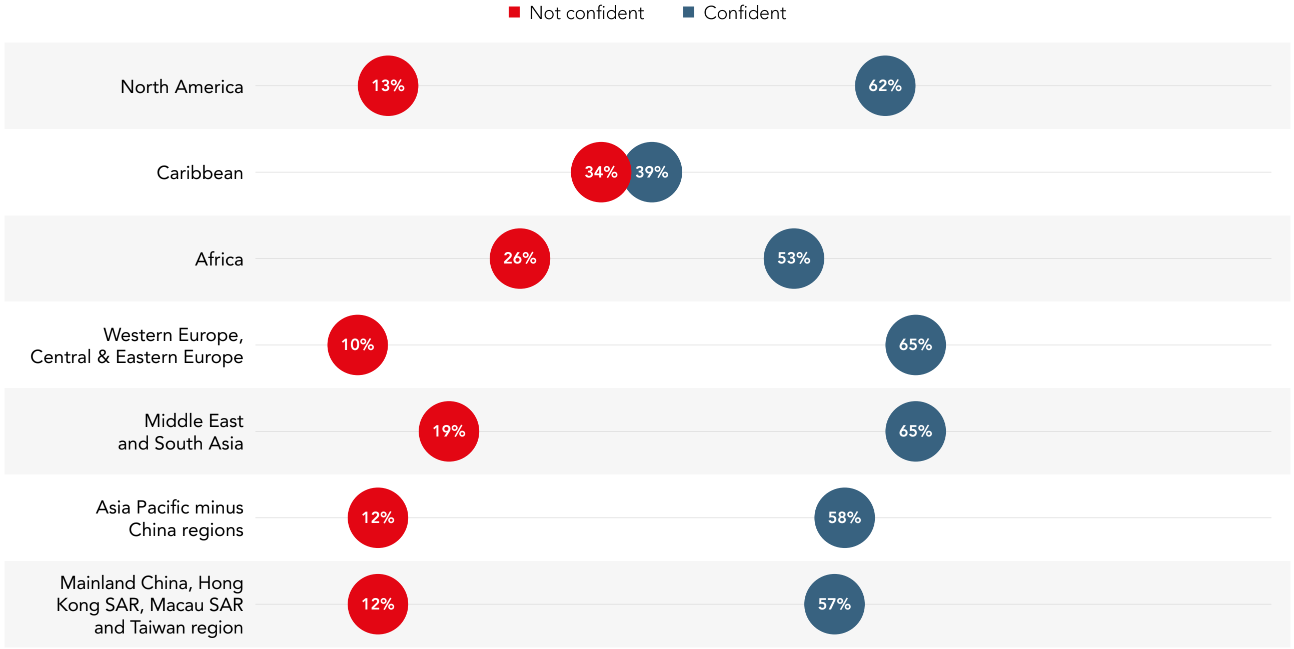
We also asked specifically about 'comfort with using a whistleblowing platform' not just whether respondents were aware of a wrongdoing, and if so whether it had been investigated and resolved. And here the Caribbean scored lowest (Figure 5.27).

FIGURE 2.26: Awareness of wrongdoing



(Data rounded to nearest whole number)

FIGURE 2.27: Comfort in using whistleblowing platform, by region



(Data rounded to nearest whole number)
('Don't knows' remain the balancing figure for each region)

> *'In developed countries, where systems are more mature, whistleblowing is higher [than in] less developed countries, where bribery and corruption up and down the ladder is just business as usual, and systems are less developed. In other words, confidence levels are lower where systems are less mature.'*
>
> **A former head of risk at a telecom in Africa**

There were many anecdotal comments from respondents, for example, one from a listed company in Vietnam who said that as they expand abroad "managing personnel in North America has been the most challenging culture issue". However, the question of safety, irrespective of a country's cultural tendencies, was raised as something that ultimately trumps any regional comparisons, which led us to discuss the differences in whistleblowing protection across jurisdictions and how people in those countries are influenced by them.

Regulations covering this vary around the world, adding to the challenges for multinational companies and putting into context some of our findings across borders. For example, we found that while the UK is considered to have one of the best protections under the Public Interest Disclosures Act, evidence from our roundtable discussions around the world indicated that overall trust in how whistleblowing platforms are managed seems strongest in North America-based companies. Furthermore, the US Securities Exchange Commission compensates whistleblowers for timely information that leads to successful enforcement action, but that is not done in the UK and differs significantly from the European Union's Directive on Whistleblowing Protection of 2019 (European Commission n.d.) which, although comprehensive, was not yet adopted by all member states' parliaments when the survey was conducted (Terracol and Nowars 2022).

As cases of retaliation and intimidation tactics continue to come to light, regulators are only increasing efforts to progress the protections and rights offered to whistleblowers. For example, in January 2023, the Australian Securities and Investments Commission (ASIC) reissued its whistleblower protections guide, spelling out the laws administered and enforced by ASIC.[4]

Regarding the US, there have been significant cases that have been featured in the headlines. The Wells Fargo whistleblowing fall-out post the '8 is great' cross-selling scandal, that came to light in 2016, is a prime example. Employees were given the target of opening 8 accounts per customer, which resulted in some employees opening fake accounts [see Smagalla 2022]. The whistleblowers stated that they lost their jobs, or were demoted, because of speaking up.

> *'I was surprised by the confidence coming from European respondents since (at the time of the survey) the new EU directive was not fully transposed into law by member states and there have been some very high-profile European cases that have featured in the press – most notably the German cases of Wirecard and DWS. Perhaps the fact that the German whistleblower cases resulted, eventually, into good outcomes for the whistleblowers is reflected in the results. To illustrate, the Wirecard whistleblower has a new job and is also on the speaker circuit, and the DWS[5] ESG funds whistleblower has been appointed onto the UK FCA's ESG Advisory panel.'*
>
> *Perhaps the reference in the survey question to using a whistleblowing "platform" rather than escalating it to a "manager" also resulted in higher levels of confidence. The reference to a platform may have implied to respondents a process that supported greater anonymity?'*
>
> **Emma Parry, senior advisor, conduct, culture and risk, and member of the special interest group**

> *'I've implemented whistleblowing policies as the chair of the board and as chair of the audit committee at other publicly listed corporations both in North America and the rest of the world. Unsurprisingly, there are countries in which the process is less mature and by design discourages people to report. In places like North America, the narrative is positive, but I can tell you that it is still not safe for the big majority of the people to report because the processes despite the infrastructure are designed to support the more powerful.'*
>
> **Participant in North America roundtable held in January 2023**

> *'Senior leaders must find a way to make junior people feel "safe" when communicating what may be perceived as "bad news".'*
>
> *'I wonder what the responses would look like if the question was: I feel confident that I will not be victimised, but protected if I blow the whistle in my organisation? I think therefore a strictly confidential, discreet, and separately managed channel is essential for whistleblowing, albeit that this may in turn hinder transparency of data around usage and outcomes.'*
>
> **Comments from online community pop-up**

[4] <https://asic.gov.au/about-asic/news-centre/find-a-media-release/2023-releases/23-046mr-asic-publishes-report-on-good-practices-for-handling-whistleblower-disclosures/>

[5] See Chapter 4.

Others pointed out that even a perception of being 'safe' would not be enough to increase comfort levels. In other words, how do organisations ensure someone can benefit for doing the right thing? The common theme in our analysis is that being safe is not a benefit, it's a basic right.

'Although I'm strongly in favour of robust legal structures for whistleblower protection, sadly the research record of "what actually happens" to whistleblowers is pretty dismal. I have yet to meet, or to read about, any whistleblower whose life was improved following the event of their blowing the whistle. Despite rewards and legal protection, no whistleblower ever quite recovers their pre-incident sense of identity and self-worth, which is a terrible thing. Those who aren't moved into distant 'witness protection' are unfortunately prey to ostracism from former colleagues, awkwardly often including people who weren't "in on" the misconduct that the whistle-blower had called out.'

Online community pop-up platform

'I think that in North America, comfort with whistleblowing could get much better if the media situation changed. I feel that the media is making it more difficult for people to come out and utilise a whistleblowing platform because of how they cover what comes out. People would be more willing if they believed it was anonymous. They maybe think that if they must provide specific information, the next thing they know it's all over the media and different media is going to portray things very differently. People don't want to take that risk.'

CFO at large retail chain in North America

The chair of the board at a municipal entity in Canada told us that the secretive nature of whistleblowing makes it difficult to interpret survey data. This respondent pointed out that one of the first rules of whistleblowing is that the information does not go to people who are not affected or who are not close to the situation, meaning only a handful of people might ever know about larger wrongdoings that affect the organisation. Many respondents therefore may not be qualified to comment on whether an issue has been resolved.

Additionally, we appreciate that the trust between employees and their managers will influence responses and have concluded that the conversation about 'trust' at organisations often concentrates on the consumer and external view of a brand, particularly during times of crisis, rather than on the trust within the organisation.

'We must somehow emphasise how vital trust is. The three lines of defence – now the three lines – do not work if those on the different lines do not trust one another. Teams underperform when there is a dearth of trust among members. This is true in any industry and it's not something even the regulators truly appreciate. At present, the closest proxy is a focus on psychological safety and whether an organisation promotes, or fails to promote, a "speak-up" culture.'

Participant in special interest group discussion

'Whistleblowing protection is an important piece of regulation in North America that contains relevant aspects, for example, of anonymity and non-retaliation. We do not see similar laws in Asia, but from what I've seen with my clients the geographical nuances are more cultural. For example, in Asian countries, such as China or Korea, calling and reporting on your boss is not something that employees feel comfortable with because of the power gap in their culture. They're not as confident and think it's inappropriate to report on their bosses. So, there's a cultural aspect beyond the legislation and whistleblower protection that they may get in their respective countries that is driving our survey responses. We see US multinational companies with a presence in Asia driving the culture down, telling staff they should feel comfortable speaking up if they see something that's not right. Yet, on the other hand, if it's a Chinese-based company, that would not always be the clear message.'

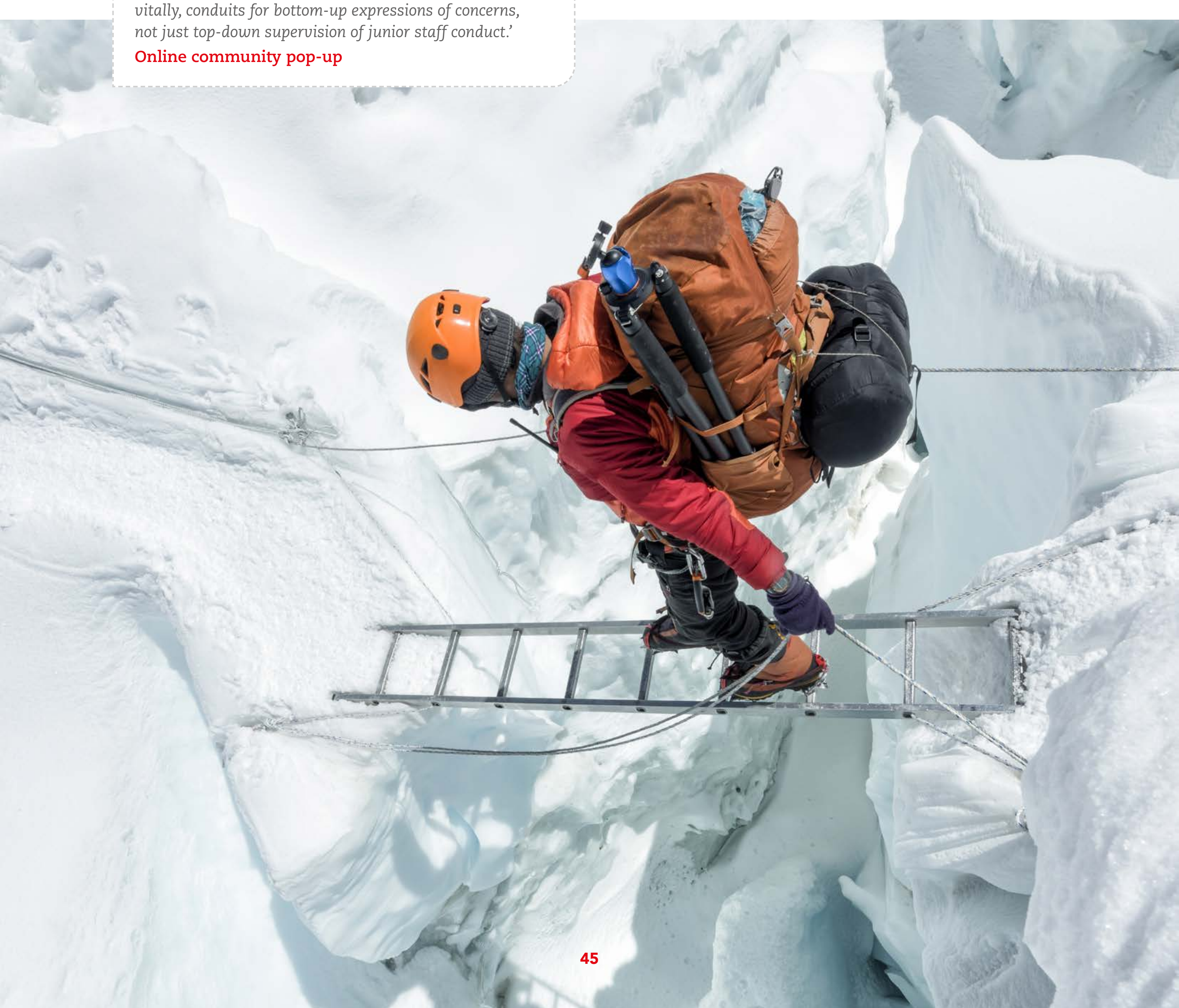
Monica Young, director of risk and compliance at KMPG LLP in Chicago, and a member of our special interest group

Our research also reveals several limitations with whistleblowing for the broader question of combating misconduct that transcend regional boundaries. Unfortunately, the outcomes for whistleblowers are often unhappy ones and their experiences more regretful than rewarding. It is rare for them to see their career progress to higher places and, as mentioned before, their reputations became stained, so the incentives are difficult to facilitate. Whistleblowing as a concept is quite reactive and doesn't necessarily stop someone from being tempted to carry out fraud or other misconduct.

> *'Although it's a hugely important safety valve and control on senior management abuses, whistleblowing is one of the least effective risk-management levers. This is because it operates 'ex-post' – i.e., after the event – rather than as a 'prophylactic' crisis-preventative risk control. Far better to detect early, and so prevent growth of misconduct by having in place a healthy conversation about "what we do around here" at all levels in the organisation; including, vitally, conduits for bottom-up expressions of concerns, not just top-down supervision of junior staff conduct.'*
>
> **Online community pop-up**

> *'Very transparent policies on whistleblower protection should be implemented but I also think it is best of all to create a work environment that makes fraud and criminal activity less attractive, such as competitive salaries, attractive bonuses, benefits and other recognition packages. Happier employees are less likely to risk their jobs with fraudulent or illegal behaviours and so it should make it easier to weed out the ones involved.'*
>
> **Online community pop-up**

While having a facility for whistleblowing is a necessity, respondents overwhelmingly agreed in the interviews and discussions that it is not a 'culture management mechanism' and therefore has limited impact on the broader questions of tackling risks in a holistic and sustainable way. As one ACCA member in the UK said, 'whistleblowing is really about justice, not prevention'.



Sector differences in comfort with whistleblowing

Those in the public sector showed the lowest confidence in using a whistleblowing platform. Only 48% said they were comfortable, 25% said they were not comfortable at all, while the rest opted to be neutral and would not say either way (Figure 2.28).

When we showed the results to our special interest group and members' roundtables, the conversations tilted towards more idiosyncratic issues inherent in specific industries rather than general sectorial trends, for instance, in the healthcare and aviation industries, and what drives behaviours in them, given the nature of the business.

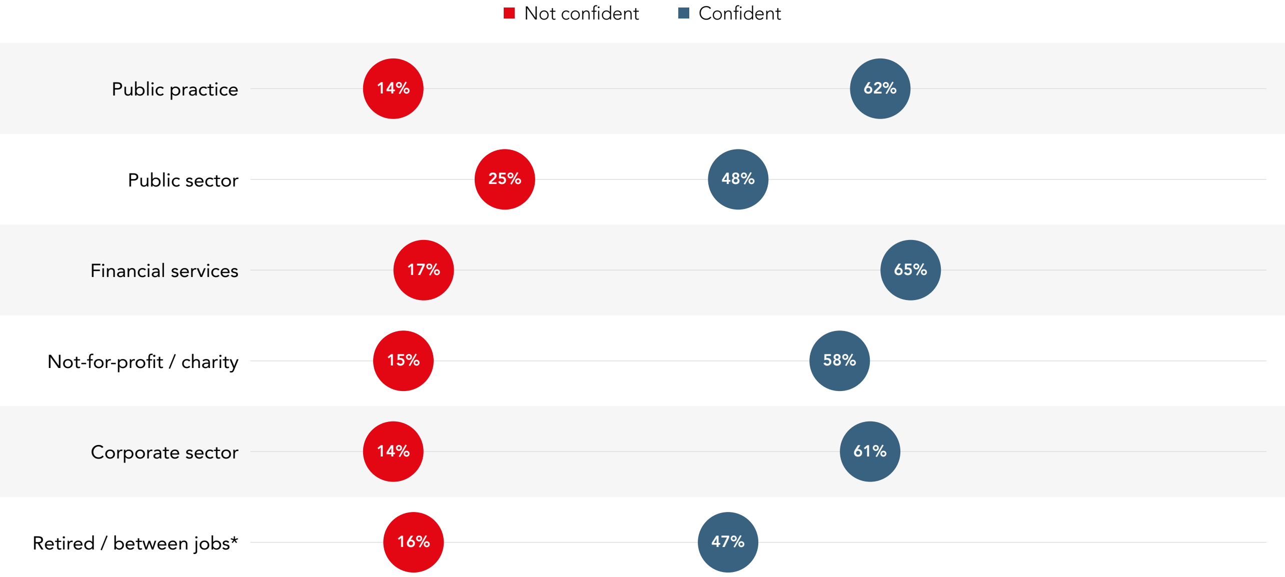
> *'If you say something is wrong and then get knocked down, no one is ever going to feel safe speaking up, and this is the culture we see in medicine, which is why in the US more people die from preventable medical errors because of the fear of malpractice lawsuits. It would be like two jumbo jets blowing out of the sky, but the aviation industry created an open, non-blame culture 30 years ago with an element of amnesty. So, when something goes wrong, they investigate it and share it with everybody. But there is an example of one hospital in the US that completely shifted from being the worst performing hospital in the country to the best. It wins awards because it took away that fear factor by actually saying "we will reward you to inform us for the greater good when things go wrong".'*
>
> **Special interest group discussion**

When speaking at an ACCA webinar for European members, Christian Hunt, author of *Humanizing Rules: Bringing Behavioural Science to Ethics and Compliance,* also pointed out the aviation industry's focus on eliminating human risk where consequences are critical. Of course, airlines are generally successful at making sure what happens in the sky is safe, but these companies have other challenges on the ground that were heightened during the pandemic, for example, data leaks and customer services issues (Hunt 2023).

> *'The biggest challenge here is making sure the organisation understands what it is in its environment, in [its] culture that's driving human behaviour, because if you have a situation where something has gone wrong – a human has made a bad decision, perhaps because of the incentive programme or the culture that encourages that sort of action – getting rid of that individual does not actually solve the problem.'*
>
> **Christian Hunt, member of the special interest group, presenting to ACCA European forum on risk culture, June 2022 (ACCA 2022)**

> *'Look at the NHS crisis in the UK, it's not that there is no money. It is that the funding model is unsustainable. There's a lot of waste and difficult questions that become hugely political about what improves the quality of patients' care and how to plan winter resilience better, for example, but they don't want to talk about risk. They talk about safety and clinical governance, and the moment you put enterprise risk into the equation all the waste and bad decision making is exposed because you are now adding in accountability and that leads to more transparency and responsibility. This is the problem.'*
>
> **Former risk manager at the NHS and a building society in the UK, now works as risk consultant**

FIGURE 2.28: Respondents' comfort with using whistleblowing platforms



*Based responses on previous place of work
(Data rounded to nearest whole number)
('Don't knows' remain the balancing figure for each sector)

WE FOUND PLENTY OF THOSE FINANCIAL PROFESSIONALS FROM OUTSIDE THE RISK TEAM AGITATING TO BE HEARD WHEN WE ASKED TWO OPEN ENDED-QUESTIONS AND IN THE ONLINE COMMUNITY POP-UP.

See the supplementary document *Risk Culture Conversations* for the two open-ended questions in the survey and discussions from our online community pop-up.

3. **What's next?**

Can **regulatory forces build trust** through **purpose** and **accountability**?

Greater accountability, not only for firms but also for individuals

We can see how regulators across jurisdictions are cooperating in their investigations and putting firms under greater scrutiny to identify the root causes of misconduct and risk governance failures.

From the new Consumer Duty imposed by the UK's Financial Conduct Authority (FCA) – where failure to prevent fraud is now a criminal offence (see FCA 2022) – to the Reference Checking Scheme run by the Hong Kong Monetary Authority (HKMA), the consequences of misconduct are becoming much more material for both financial institutions and the individuals who work for and with them (Au 2022).

> *'The HKMA's "rolling bad apples" scheme basically means we are obligated to call out the staff who are a risk so any financial practitioners who have a record of misconduct or unsatisfactory behaviour cannot move somewhere else and do it.'*
>
> **CRO at a Chinese bank in Hong Kong SAR**

Board directors are prime examples of those targeted by the evolving focus on personal liability and breach of statutory duties, including the duty to prevent wrongdoing. The idea of a board's collective responsibility is eroding, and, in some countries, there have been prosecutions of experts on boards, on the grounds that they should have known better and steered the board's decisions in a different way. Currently, the 11 board directors of oil multinational Shell are personally being sued by environmental lawyers, ClientEarth, who are accusing them of failing to prepare the company properly for its net-zero-transition strategy.

A report by the UK's Prudential Regulatory Authority (PRA) in late 2020 to assess progress of its Senior Managers and Certification Regime (SM&CR) (PRA 2020) reinforced the rationale for homing in on accountability for individual directors, alongside their board's collective responsibilities. It said that a large majority (around 95%) of the firms surveyed said the SM&CR was having a positive effect on individual behaviour. 'Furthermore, while individual accountability is crucial to good decision-making, and is the focus of this report, it does not substitute for the responsibility a firm's board has for overseeing the firm'.

What should individuals be accountable for inside their organisations?

Where precisely an individual's accountability should begin and end compared with that of a colleague inside the same organisation is also not always clear. There are choices, and those choices can cause tension when trying to decide who should be held accountable. The question is: How do leaders oversee conduct and consider the consequences of their decisions?

> *'Regulators are looking to hold senior executives more accountable, but many financial firms are saying that it should be the first line CROs, COOs, sometimes legal and even HR. It's like a game of hot potato. Ultimately, it reflects an unwillingness to accept responsibility perhaps because no one is quite sure what to do to meet such responsibility. This is something auditors may in future be asked to test, so it's another area where accountancy can take a lead.'*
>
> **Special interest group discussion**

> *'Having corporate values that are lived out through behaviours is critical to building an effective risk culture. In essence it also comes down to whether a person has basic business ethics; the knowledge of what is "right" and "wrong" and the choice he/she will make.'*
>
> **Horst Simon, a member of the special interest group, on conduct being the outcome of how good or bad you manage people**

Respondents also told us how, in an organisational context, this should come from corporate values and communicating the organisation's appetite for risk through its policies, processes and practices. One emphasised that staff need to be well motivated to do the 'right thing' and that external forces such as fines cannot do this alone: it must come from an internal desire if it is to be sustained (Figures 3.1 and 3.2).

FIGURE 3.1: Behaviours associated with a good risk culture

- Demonstrating a positive attitude towards the management of risk
- Considering risk in every business decision that is made, *before* the decision is made
- A good risk 'nervous system': strong and open communication channels where bad news travels faster than good news and escalation happens as soon as a problem or issue arises
- Taking responsibility for risks and controls, honesty, and clear ownership of risk
- Encouraging and educating others in the management of risk

FIGURE 3.2: Risks associated with bad conduct

Financial

- Profiting from dishonesty
  (withholding material information; 'greenwash' trades)
- Market disorder
  (rate-fixing)
- Excessive risk taking
- Customer detriment
  (ignoring 'duty of care'; mis-selling; trapping)
- Abuse of 'privilege'
  (conflict of interest; info sharing)

Non-financial

- Discrimination
  (favouritism; exclusion; ostracising)
- Abusive behaviour
  (harassment; 'culture of fear'; bullying; intimidating)
- Dishonesty
  (not transparent with the regulator, or mis-reporting – eg 'greenwash' marketing comms)
- Not talking *(or caring)* about Conduct or Culture

Source: adapted from Dr Roger Miles

Role clarity and bringing the G in ESG up to speed

Governance is an impactful aspect of everything above that nonetheless continues to lag and lack resources. Governance affects everything – in ESG, the 'S' needs the 'G', the 'E' needs the 'G'. Those three letters have never really been equal, which is why so many people in our professions have told us that although highly interconnected, the E, S, and G have been bound together in one confusing acronym that means different things to different people.

In theory, governance starts with role clarity and hence knowing who is responsible for what. When German authorities raided Deutsche Bank and its asset manager DWS in May 2022 for alleged greenwashing, our member engagement for this research turned to how the accountancy and audit professions should be re-assessing their own roles and responsibilities. Respondents overwhelmingly concluded that the G in ESG needed upgrading if their organisations' objectives for the E and the S are to be achieved. A wise first step would also be to reflect on their risk-reporting culture by asking themselves how they would describe it. For example, does it consist of ticking the box or 'gaming the system', or is it helping to shape strategy? And would it make sense to audit the audit culture too?

> *'Climate, biodiversity, equitability, [employee] diversity, and inclusion, these are all serious matters that we rightly need to address and act on, but we also see in case after case how the numbers [being disclosed] are not always reflecting what is really happening behind the scenes. You need to have the governance and you need to have the risk culture to drive ESG and achieve what you have set out to do.'*
>
> **Non-executive director of an investment management firm in the US**

The power of good governance lies in its ability to influence behaviours both at a firm level and a team level. This involves spelling out subtle differences between responsibilities, aligning what one person or function might be doing with another, or deciding what might be most appropriate for each area to own and ensuring that those responsibilities are fulfilled.

Presenting to ACCA's Chief Risk Officers in January 2023, Dr Roger Miles introduced his *'12-year-old test'*, meaning *'how do you explain your job to your 12-year-old?'* with the trick being *'to frame the question in a way that's more engaging than the regulator's'*.

> *'Building a strong understanding that risk is not internal audit and for internal audit not to cover risk scope. Embedding risk management into strategy, performance, and human behaviours.'*
>
> *'Internal audit driving their own agendas and expect risk management to play a supporting role. Governance has been captured.'*
>
> **CRO survey answers to: 'what is your biggest challenge today?'**

> *'Finance team members also have a natural risk sensitivity and might be more direct in the detection and identification of risks. Meanwhile, through auditing, accountants can more easily identify both subjective and objective risks, to play a very important role in the enterprise risk management process. They must, however, be involved at the beginning of any process to be effective in helping the business monitor risks.'*
>
> **ACCA member at a Chinese corporation**

Pleading ignorance is no longer acceptable

As there are ever fewer hiding places or excuses, because someone will be found responsible, regulators and prosecutors are becoming intolerant of an 'I don't want to know what I don't know' attitude or any argument that 'absence of evidence is evidence of absence'. When things go awry, firms that adopt a PR-driven exercise rather than conducting a meaningful operational assessment of what went wrong will find themselves facing intense scrutiny.

The US Department of Justice requires companies to demonstrate an ability to get to the root cause of misconduct and the US attorney general has advised federal prosecutors that, when sentencing a firm found guilty of misconduct, the verdict should not merely reflect the incident at hand but also the firm's history of dealing with such issues.

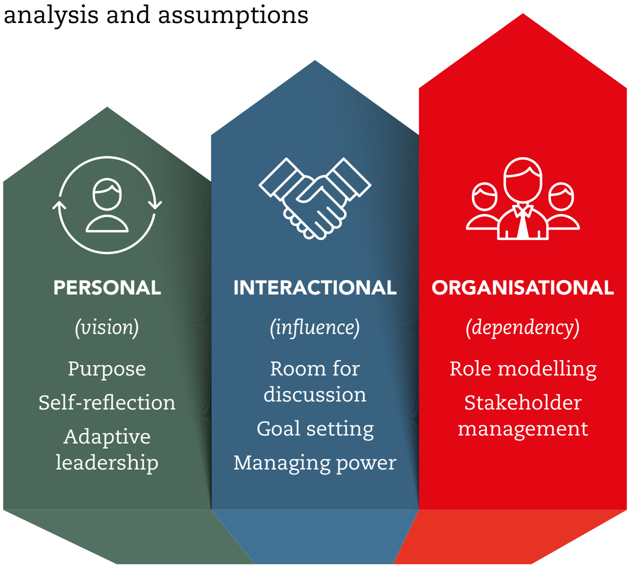
This is leading to additional disclosure requirements affecting both internal and external audit functions. Firing someone for making a mistake or wrongdoing is no longer an answer. Firms will need to understand what drove that employee to do what he or she did in the environment they occupied. In other words, what did the culture have to do with it and would the wrongdoing have happened in a different setting? The prevalent approach to tackling fraud and misconduct in the banking sector has been 'detect and correct', yet despite mounting costs through fines, the problems are yet to be resolved. What is really required is proof of action taken to 'predict and prevent'.

Rising regulatory expectations have become a major force in the evolution of what risk culture as a concept entails (Figure 3.3). Given that it is still unclear where this process will end, our respondents often referred to 'risk culture' as 'culture as an ongoing concern' – and by that they meant 'if no one is thinking about risk culture then that is a significant, perhaps unacceptable, risk'. We see an increasing willingness to think and worry about behaviours, and deciding how to applaud and recognise those who are 'doing the right thing' inside their organisations has become a priority.

And it is also fair to point out that ACCA, Airmic and PRMIA members agreed that governance and the rules that must be followed are key to providing stability and security, as the comment below from a non-executive director in Pakistan – about governance being an 'inconvenient truth' for family offices and family-run businesses in the Middle East and South Asia – shows in the starkest of ways.

> *'I've worked in banking and the manufacturing sector in the C-suite and on boards for decades, and now more recently with family offices, because there are a lot of opportunities to help them build governance in line with the corporate governance code [see SECP n.d.]. There is no risk culture, there is no governance. When the father of one family-run flagship company, which at the time owned six companies in the Middle East, asked me to come in as CEO he knew I understood the bottom line much better than other people, however, there was a lot of resistance from his children in high positions. They were not making decisions based on valid information and not interested in attending formal board meetings. They also were putting all their eggs in one basket and not thinking things through. The risk governance learning curve is a steep one but one that I think you will see is becoming much more of a focus in this region now.'*
>
> **Non-executive director, Pakistan**

FIGURE 3.3: Levels of leadership: analysis and assumptions



Source: adapted from DNB

Board and management must agree on how purpose is understood and put into practice

The Social Licence for Financial Markets: Reaching for the End and Why It Counts by David Rouch makes the point that once purpose is clear it can help financial professionals make the mindset shift away from pure profit maximisation to how they maintain loyal customers and attract innovative talent, not just in the short-term but for the long-run (Rouch 2020).

This is also something in which regulators are taking a stronger interest. The Federal Reserve Bank of New York leads roundtables, inviting other supervisory bodies and risk professionals from around the world to discuss aspects of risk culture, and its series of blogs and podcasts were mentioned many times for raising awareness of the value of managing human capital. The point is that under-investment in human capital has caused a long-term erosion of service and quality in the financial services sector (Rosenberg 2022).

But, as we have seen in our research, putting all this into practice is easier said than done. One of our interviewees referred to *Too Big to Jail* by Chris Blackhurst, a book about HSBC and the drug cartels' money laundering scandal in Mexico, which exemplifies vividly how tough values-based change can be (Blackhurst 2022).

> *'Every time a big case comes out everyone gets that feeling of, "we need to uplift our controls". Yet, despite the regulatory pressures, there is still reluctance to accept the need for behavioural change. Some business leaders talk about well-being and others focus on doing the right thing, but a lot of financial firms become complacent and think some people will make mistakes whether they do it deliberately or not and that getting caught every now and again is just a cost of doing business.'*
>
> **Former chief operating officer of a global bank**

The conflict between profits and ethical behaviour is at the heart of the fight for a singular definition of purpose in many organisations.

> *'I understand purpose but at the end of the day a public company is still scrutinised by its share price and what we are doing if the EPS [electronic point of sale system] goes down. Without profit nothing exists and that includes people's jobs. It has become a cut-throat market for retailers in North America. This is where accountants come in to work out where and what drives profit. That involves knowing the stakeholders and what makes them happy and here's my soundbite: making sure we do that ethically, morally and legally.'*
>
> **Director of financial planning at retail chain in North America**

In one roundtable discussion, respondents discussed the challenge of changing mentality from a 'profit-oriented shareholder approach' to a 'stakeholder-led purposeful corporation' given the complex priorities leaders face today. Another interviewee referred to Colin Mayer, professor and former dean of the University of Oxford's Said Business School, who says the solution is simple: 'enshrine airy mission statements in articles of association'.[6]

> *'If the purpose of the corporation does not align with your competitive advantage, and your numbers, balance sheet, income statement, do not resonate with the things that you want to do, then you have a huge consideration. You need to be a consensus builder at the highest level to change that mentality from a profit-oriented shareholder approach to a more holistic stakeholder-led purposeful corporation. It is a very difficult topic to sell, and I would advise those sitting on boards to be smart about understanding where the organisation is on that spectrum. You need to identify win-win relationships and as the stakeholder pool is only expanding, it is a challenge to find the value that everyone wants to see. And it is very important for accountancy professionals to use the right words when speaking with the different stakeholders if we want to progress our roles and make real change at the organisations we serve.'*
>
> **Chair of board in public sector and non-executive director at publicly traded companies**

There is also recognition that it is perhaps easier to see how culture is contingent on purpose in some sectors than others.

> *'In my sector we are always interacting with our stakeholders to fulfil our goals of providing education and creating new knowledge. Yes, we must be financially sustainable, and that has been difficult in recent years, but our outreach needs to be active to maintain that. For example, providing libraries and fitness centres to the community through alumni interaction and sponsors from the government.'*
>
> **Head of audit and risk management at a Canadian university**

We see that there is still no standard practice for aligning purpose and culture, which is why we include a deeper dive on this later in this chapter, and that there are often tensions between company purpose, business purpose, team purpose and individual purpose, so what comes first? As a couple of members of the special interest group suggested, the military offers useful examples of how this can be managed by emphasising an understanding of 'commander's intent' for a successful mission (Pavilion n.d.).

The quote below from a chief financial officer in North America also gives a good insider's view of what purpose working in lockstep with risk culture looks like and why: it's not just that employees should understand correct behaviour – they must believe it.

> *'In North America, we see purpose statements well-documented and all over websites but over the past couple of years we can see that this is not really happening down the food chain given all the changes in how we work and consume. It is becoming more important to push purpose at the middle and cascade down the organisation – on the ground, where it counts. Each associate in the organisation needs to be connected to purpose because the workers need to believe they add value and understand what their output is, what are they working for. When you get this connection, you solve a lot of risk problems, and you can see how their roles and output shapes up. Are we there yet? No, but we are moving in this direction.'*
>
> **CFO, North America**

[6] Mayer is a leading figure in the global discussion about the purpose and role of companies. In his book, *Prosperity: Better Business Makes the Greater Good* (2018), Mayer defines corporate purpose as 'producing profitable solutions for the problems of the people and planet, and not from profiting from creating problems', adding that proving that purpose can lead to profit is only useful if maximising financial returns is the prime objective (Mayer 2018).

Why aligning purpose, culture and risk appetite makes a difference

by **Julia Graham**, CEO, Airmic

Clarity of purpose informs an organisation's brand, values, and desired behaviours, and should act as a beacon to inspire and signpost everything an organisation does. There are two key elements of an organisation's purpose – the 'why' and the 'who'. The 'why' explains the organisation's reason for being. The 'who' highlights which stakeholders an organisation exists to serve. Once the purpose – the 'why' and the 'who' – are embedded in the culture of an organisation they become part of it, like a corporate DNA, informing everything that the organisation does (Figure 3.4).

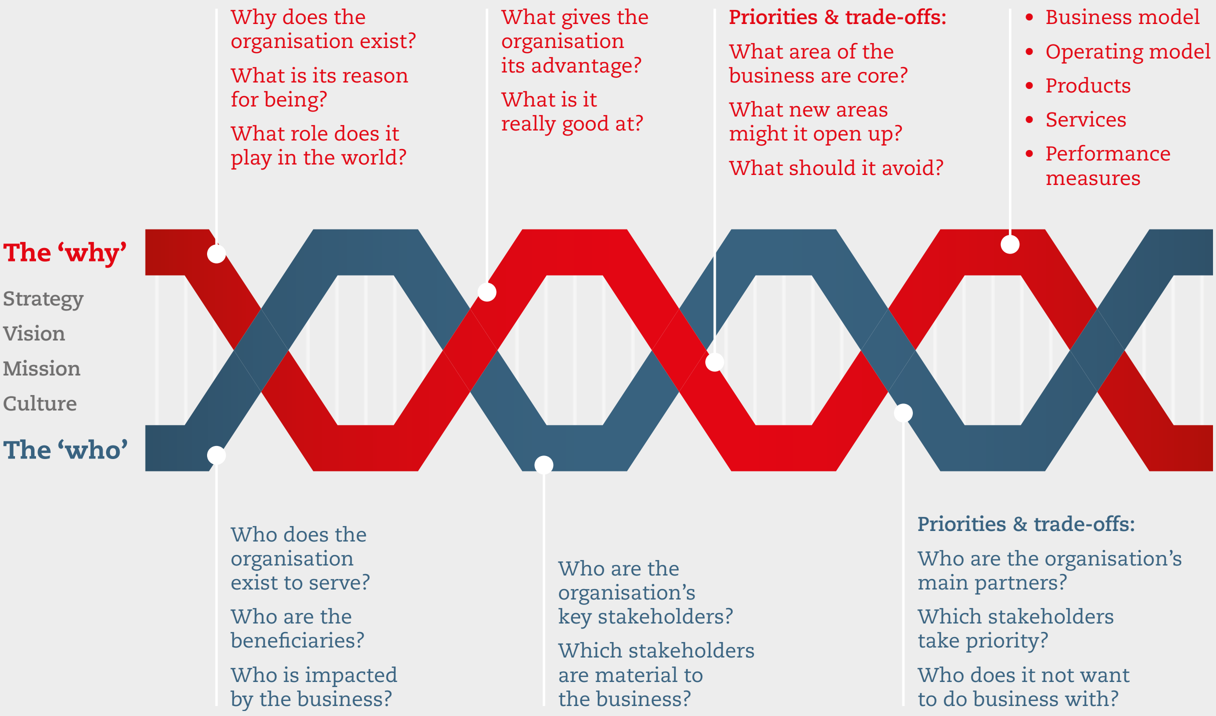
The relationship between risk appetite and risk culture is mutually supportive. A risk appetite sets expectations for consistency of approach and, as such, is the foundation for the risk culture. A strong risk culture should increase the chances of success in applying risk appetite, because effective leadership, communications and governance systems will be aligned (see Figure 1.1 on p16).

Even so, while risk culture might be consistent across an organisation, setting out what 'we do or don't do here', risk appetite may not be homogeneous. The business streams and stages of maturity of an organisation and where and how it trades will influence risk appetite – there is unlikely to be one 'risk appetite size that fits all'. It is the framework within which risk appetite operates that is key and where the overall risk cultural tone and the application of this across an organisation is set (see Figure 2.13 on p34).

In an increasingly complex, fast-changing, challenging, and at times confusing, world, the beacon of purpose will help to ensure that all stakeholders of an organisation receive a stream of consistent messages. If messages are unclear or inconsistent, and purpose, risk culture and risk appetite lose synchronisation, organisations may not only fail to manage risk effectively, but may also fail to grasp opportunities that come their way effectively: risk has two sides – a downside and an upside – and we should not overlook this.

As we discuss in this report, a strong risk culture will help integrate risk appetite throughout core processes and prevent it from being viewed as a stand-alone initiative. Risk appetite may be addressed through operational and governance controls established in assurance layers – as defined in the 'Three Lines Model' (see Figure 2.10 on p30).

FIGURE 3.4: The DNA of purpose



Why does the organisation exist?

What is its reason for being?

What role does it play in the world?

What gives the organisation its advantage?

What is it really good at?

Priorities & trade-offs:

What area of the business are core?

What new areas might it open up?

What should it avoid?

- Business model
- Operating model
- Products
- Services
- Performance measures

The 'why'

Strategy

Vision

Mission

Culture

The 'who'

Who does the organisation exist to serve?

Who are the beneficiaries?

Who is impacted by the business?

Who are the organisation's key stakeholders?

Which stakeholders are material to the business?

Priorities & trade-offs:

Who are the organisation's main partners?

Which stakeholders take priority?

Who does it not want to do business with?

Source: adapted from the Airmic-ACCA–Crawford–Lockton-University of Oxford Saïd Business School Report, *Roads to Repurposing*, 2021

Supervisory oversight efforts to force cultural change

DeNederlandsche Bank (DNB), the Dutch central bank, is widely regarded as the pioneer in supervisory oversight of behaviours and culture in financial services. Since 2011, it has focused on behavioural economics and decision-making biases, showing how organisations that embrace this approach are better equipped for detecting emerging risks and building a purposeful culture that truly combines psychological safety and cognitive diversity.

In January 2023, DNB released a report documenting the progress of its initiatives over the past decade. 'Banks and other institutions have set up entire departments for this purpose and there are boardroom evaluations and prominent culture agendas during meetings'. It points to how making the change is hard and that 'doing this right can be a lengthy process. You can't just press a button and expect everything to be perfect. Moreover, things are certainly not going well everywhere. Too often managers still revert to what we call the short-term action reflex' (DNB 2023).

Continuous monitoring is also highlighted by the UK's FCA, through its 'five conduct questions' introduced in 2015 for getting wholesale banks to develop their own definition of conduct risk and what it means to them as a first step in fully understanding their own risk culture. Over subsequent years the exercise allowed banks to gain a sense of what their purpose is. By 2017, it had extended the programme to other sub-sectors of the financial markets, and found that regularly walking the floors, asking employees what they think their purpose is and how it affects the way they work and act, produced the results that were intended (FCA 2017).

> *'The best of these banks went to their staff and asked what they thought the company's purpose should be. They asked them how this should be articulated, and they involved them all in the process. It was electrifying to see, and those that did it saw how much it paid off.'*
>
> *'The staff said that purpose helped them figure out what to do. They said purpose helped them whenever there were grey areas. They said, "if we think somebody could get in the way of purpose, trip us up or be a risk, purpose is what clarified the situation because we don't want to do something that gets in the way of achieving our purpose". So, risk management gradually became a function of how a bank could be split up to deliver its purpose to different customers, stakeholders and society at large.'*
>
> **Conduct and behaviour at risk advisor**

Benchmarking and the all-important MI

The management information (MI) that is being collated in some national banking systems allows for useful benchmarking. Driven by an incessant desire for evidence that their policies are working, various supervisory and other standards bodies continue to gather comparative data to see what is happening across the horizon. The value of these databases is immense, allowing regulators and firms alike to dig into demographic intersectionality and paint a bigger picture of trends and characteristics. The UK has been a leader on this front, namely with the Financial Services Culture Board and the Financial Markets Standard Board.

> *'One thing some of these agencies are doing well is providing horizontal reviews. When we talk about the question of introspection, it's really hard to try to define one's culture. But when these regulators go from firm to firm assessing their governance and culture and ask[ing] where they believe their strengths lie, and then compare that to the firm's competitors, you can often see where your weak spots may be. It's an outstanding bit of feedback that the supervisors can provide banks.'*
>
> **Non-executive director at Europe-based bank**

The Monetary Authority of Singapore (MAS) is also a good example of how some central authorities are extending their reach by collaborating with local banking associations to acquire new information. MAS managing director, Ravi Menon, says the mission has always been to make the global financial community 'safer and more purposeful'.

But our research also yields a note of caution about riding on the back of regulatory tailwinds. Some of these supervisory bodies have their own challenges in adopting more granular approaches, when they often lack resources and depend on the banks to report truthfully. Regulatory forces may therefore, inadvertently, continue to push organisations into more box ticking and by doing so encourage the reverse of what is needed and stated in the quotes below: that is, a careful examination of what's behind the more obvious numbers.

> *'I got to know the CEO and the CRO at Wells Fargo during meetings with large banks, and I was always impressed, but you learn that you must look beyond the numbers to see culture. I was surprised at what was unveiled. It was not just an idiosyncratic, one-off thing. It was one thing after another and I thought "wow I misread that organisation", so there are knowledge asymmetries that need to be carefully considered.'*
>
> **Respondent formerly at the BIS**

> *'Preoccupation with regulatory risk is concerning. It feels like the tail wagging the dog and raises the risk that scarce and precious risk-management resources may be misdirected away from the highest priority risks facing the firm. Risk culture helps to capture the unique context of the enterprise whereas regulation pulls attention more towards standardisation, which can sometimes disguise the problem.'*
>
> **Dr David Cooper, specialist on leadership risk and member of our special interest group**
>
> *'The moment you set up a behavioural indicator, don't be surprised if people game it by modifying their behaviour to fit what it says while ignoring the principle behind it.'*
>
> **Participant in special interest group discussion**

Nevertheless, when done right, as another business leader in China implies, an easier way of establishing a culture of risk management for employees is to tailor what the regulator has imposed to your own organisation's needs. This ACCA member described risk culture as 'an early warning system for not only detecting threats but also unmissable opportunities' (Figure 3.5).

> *'We have established a conceptual culture of risk management for employees. This awareness is built up from the general risk management requirements of State-owned Assets Supervision and Administration Commission of the State Council (SASAC) on the one hand and includes the basic business logics of our company in the process of business development on the other. This is to ensure the long-term development of the company in a safe and stable internal and external environment and to achieve its business objectives and vision.'*
>
> **Deputy general of an SoE in China**

FIGURE 3.5: The evolution of conduct and culture reporting expectations

FROM:	TO:
defining Conduct **infractions** *punish misconduct; manage 'enforcement risk'*	defining **Purposeful** Culture *coaching; elevate 'exemplary conduct'; 'social-licence'-aware*
history-based: **pro forma** reporting *economic MI; value-at-risk; 'detect-and-correct'*	'live view': **dynamic**; sentient; human MI *behaviour-at-risk; Six Qs; social goods; 'predict-and-prevent'*
local regulator values and assumptions *market- and jurisdiction-specific*	**globally** agreed 'Conduct and Purpose' values *informed by treaties and MOUs between regulators*
Command-and-control *structured MI, internally generated by the firm (eg sentiment surveys)*	**What actually happens** *unstructured, real-world external data; many informal sources (live observation; aggregators – public ratings; record of violations*
'Tone at the top' SMCR (and local equivalents)	**BAU** embeddedness *motivation in the mid-levels; all staff engagement*

Source: adapted from Dr Roger Miles

WHEN THINGS GO AWRY, FIRMS THAT ADOPT A PR-DRIVEN EXERCISE RATHER THAN CONDUCTING A MEANINGFUL OPERATIONAL ASSESSMENT OF WHAT WENT WRONG WILL FIND THEMSELVES FACING INTENSE SCRUTINY.

4. Closing remarks from Stephen Scott, Starling

starlinginsights

Jeffrey E. Garten, Dean Emeritus of the Yale School of Management, has described the financial sector as 'the circulatory system of any country, as well as of the global economy'. A former US Treasury official, Garten emphasised that 'a smoothly functioning system is central to national growth and prosperity, to international trade, international economic growth and development, and to fewer global crashes than otherwise would take place (Garten 2018). It is therefore in keeping with the metaphor that some have described the Global Financial Crisis of 2007–8 as the equivalent of an economic heart attack (Coburn 2014).

But however apt the metaphor, the crisis represented more than a shock to physical health – it also did deep damage to our collective civic 'spiritual health'. Stephen Green, then-chairman of HSBC, captured this compellingly in his 2009 book, *Reflections on Money, Morality, and an Uncertain World*. 'There has been a massive breakdown of trust', Green wrote, 'trust in the financial system, trust in bankers, trust in business, trust in business leaders, trust in politicians, trust in the media, trust in the whole process of globalization – all have been severely damaged, in rich countries and in poor countries alike' (Green 2009).

Shocked by the near collapse of trust in the global financial system, the decade following the crisis saw a spate of macroprudential policy initiatives aimed at correcting the 'Too Big to Fail' problem (Tarullo 2009). Our experience throughout the Covid pandemic suggests that these initiatives served their intended purpose well (FSB 2020). But the crisis was about more than failures in financial risk management – it also reflected deep-seated *non-financial* risk management challenges that remain with us today (Khan 2016).

Too big to manage

If the crisis caused affliction to our economic body and spirit, then we have treated the former without a commensurate focus on the latter. Trust matters (Cook and Scott 2019). A series of misconduct scandals in the financial sector since the crisis have eroded our faith in the industry, and in government more broadly. To redress this, after the LIBOR-fixing scandal of 2012 (McBride 2016), banking sector overseers began to focus on the *culture* of the industry (Deloitte 2013). Bill Dudley, president of the Federal Reserve Bank of New York (2009–18), gave lasting momentum to this initiative in a 2014 speech and workshop calling for 'Enhancing Financial Stability by Improving Culture in the Financial Services Industry' (Dudley 2014).

The Federal Reserve has continued to play a leading role in convening a relevant global dialogue, joined by many global peers (Starling Insights n.d.a). This initiative, Dudley argued, was important for financial stability reasons, but also 'to ensure the public trust in our financial system'. Suggestions from academic researchers, that the culture in banking may in fact *prime* people to cheat, heightened interest in culture as a potentially systemic risk issue warranting supervisory attention (Smith 2014).

Bank regulators and supervisors across the world have heeded Dudley's 2014 call to action (Group of Thirty 2018). In June 2022, vice-chair of the European Central Bank's Supervisory Board, Frank Elderson, equated concern for bank culture with a broader interest in good governance. 'A bank can have all the risk controls in place, avail itself of the most advanced tools to manage risks, and rely on data of the highest quality, but still become mired in a scandal it has brought upon itself, owing to weaknesses in its internal culture' (Elderson 2022). In a January 2023 speech, the US acting comptroller of the currency, Michael Hsu warned of a 'Too Big to Manage' problem, which may warrant the breaking up of banks that seem irremediably unwieldy (Hsu 2023).

Auditing audit culture

If the banking sector is akin to an economy's circulatory system, the audit sector serves as its kidneys.[7] Regrettably, in recent years we have seen a rash of culture concerns and misconduct scandals across the audit industry, in every major market, and involving all the most significant audit firms. Some have faced fines for misconduct, such as exam cheating (Starling Insights n.d.b), and lying to regulators (Starling Insights n.d.c). But, just as in the banking sector, punitive fines do not appear to be effective in prompting changed behaviour (Black 2015).

Audit industry overseers and professional bodies are therefore looking pointedly at the experience of banking sector peers (Scott 2022). 'There is a clear consensus on the importance of a purpose-led culture and how an audit firm's purpose should have audit quality and maintaining trust in capital markets at its core', the UK Financial Reporting Council argued in a December 2021 paper, *Audit Firm Culture: Challenge. Trust. Transformation* (FRC 2021). In March 2022, the Chartered Institute of Internal Auditors issued a paper on cultivating a healthy culture, subtitled 'Why internal audit and boards must take corporate culture more seriously in a post-Covid world' (Chartered Institute of Internal Auditors 2022).

[7] Starling will be issuing a white paper to expand on this argument, which will be available at <www.insights.starlingtrust.com>.

The audit industry plays a unique and essential role in helping to assure the trustworthiness of markets and the firms that they comprise. 'With trust being lost in the audit industry, people are not only losing trust in the accountancy firms themselves, but in our ability to trust any business to act correctly and to be held accountable', a 2019 article in *Accountancy Age* argues (Jewars 2019).

This has implications for those in internal (Deloitte 2017) and external (Munter 2022) audit roles. Hence, audit industry regulators have begun making efforts to ensure that audit firms maintain a sound culture and reliable non-financial risk-management practices. In banking, these efforts have involved both punishing firms – and their leaders – when perpetual culture and conduct issues suggest broad resistant to remediation (Monaco 2022). But regulators are also introducing requirements that firms report on their culture and on the steps they are taking to remediate any known or potential cultural issues, as seen in the UK (FCA 2017), Australia (APRA 2022), Hong Kong (HKMA 2020) and the US (Office of the Comptroller of the Currency 2018).

'The implications of the public losing trust in audit extends further than the audit industry, to society as a whole', *Accountancy Age* rightly argues (Jewars 2019). Culture is thus central to the perceived trustworthiness of audit firms, the audit industry, and auditors more generally. Audit sector overseers have taken note and have begun to focus on culture as a driver of conduct and audit quality (Jung and Meyer 2021).

'We expect audit firms to understand the importance of culture and to have in place a culture programme that identifies the critical behaviours that correlate to high-quality audit with initiatives to embed these behaviours within the audit firm', writes Sarah Rapson, UK Financial Reporting Council executive director of supervision, in Starling's 2022 *Compendium*. 'The most innovative firms are using a variety of techniques to measure the success of their culture frameworks', Rapson notes, adding, 'The FRC [Financial Reporting Council] is monitoring their individual approaches with a view to identifying good practice' (Rapson 2022).

And it isn't just regulators who are emphasising concern for culture and the conduct it promotes. Again, as in banking, audit firms are also being held to account for improving culture by their employees, and particularly those who are younger (Weber Shandwick 2019). A feature of what may be considered a new era of accountability is employee readiness to 'speak out' externally when 'speaking up' internally is considered unwelcome or untenable (Starling Insights n.d.d). This puts a premium on assuring that workplace culture promotes an atmosphere of 'psychological safety' (Lightle et al. 2017).

As a recent research paper concludes, 'A number of studies find that positive ethical tone (e.g., emphasis on audit quality during brainstorming, maintaining a psychologically safe environment, emphasizing interests of users, and support for whistleblowing or ethical behaviour) influences audit quality and/or work attitudes' (Alberti et al. 2020). Audit sector regulators are therefore beginning to emphasise and test for the existence of psychologically safe workplace cultures.

What comes next?

Many trained in audit operate in risk-management roles. Increasingly, they are tasked with evidencing to the satisfaction of clients, boards, regulators, employees and the investing public that the firms in which they work are not only alive to culture as a critical risk-governance concern, but that they are adept in the proactive management of culture concerns. Note that this does not equate to assuring compliance in some tick-box manner. Rather, it emphasises working purposefully to create and maintain workplace operating norms that allow for the early detection of conduct and other non-financial risk concerns (Reader and Scott n.d.).

As this report reveals, many respondents across sectors and regions say they understand the risk appetite of their companies, but few can provide evidence that employees are working within it. Risk governance is fragmented across systems and functions, collaboration is wanting, and an understanding of culture as a driver of risk is not readily seen, top-down or bottom-up. There is thus broad misalignment in risk perceptions and risk priorities across organisations, compounded by the absence of a common language with which risk-related imperatives could be discussed.

Beyond setting an obligatory 'tone from the top' with appeal to pious assertions and virtue signalling, many CEOs relegate concern for culture to those in subordinate functions: human resources, compliance, risk, legal, employee relations, etc. If the experience of the banking sector is mirrored in the audit profession, this will not stand. Bank regulators show increasing concern for good outcomes, rather than good intentions, and are insisting that firms possess an ability to demonstrate, reliably, that desired outcomes can be expected. A failure to meet these new standards implies individual accountability.

This report does the audit profession a great service by calling attention to many of the questions and challenges that continue to bedevil those in banking and other industries. By raising awareness and seeking to promote new thinking that supports improved practices, it reflects a healthy readiness to lead on these issues. By taking lessons from those who have gone before, audit professionals can side-step many of the pratfalls experienced by peers in other industries. And by viewing proactive culture management as a powerful means by which to promote outcomes that reflect company purpose and values, the audit function serves as a creator of value, as well as its guardian.

This is a cause worth taking up, and this report points us in helpful directions.

Stephen Scott, Founder & CEO, Starling

MANY RESPONDENTS ACROSS SECTORS AND REGIONS SAY THEY UNDERSTAND THE RISK APPETITE OF THEIR COMPANIES, BUT FEW CAN PROVIDE EVIDENCE THAT EMPLOYEES ARE WORKING WITHIN IT.

Special interest group

Alastair Goddin, head of risk at Asta in London, as well as a member of ACCA's Global Forum for Governance, Risk and Performance and ACCA's CROs Forum

Alexander Larsen, enterprise risk consultant, *Risk Manager of the Year Award for Middle East Africa* (the MEA and Insurance Excellence Awards)

Christian Hunt, author of *Humanizing Rules: Bringing Behavioural Science to Ethics and Compliance*

Dr David Cooper, leadership specialist at Cooper Limon

Dr Roger Miles, author of *Culture Audit in Financial Services: Reporting on Behaviour to Conduct Regulators*, a specialist in behavioural science and UK Finance faculty lead – conduct leaders academy

Emma Parry, senior advisor, conduct, culture and risk

Horst Simon, risk culture builder consultant and Africa Risk Management Award 2019, Institute of Risk Management South Africa

Jane Walde, enterprise risk consultant, member of ACCA's Global Forum for Governance, Risk and Performance

Julia Graham, CEO of Airmic, member of ACCA's Global Forum for Governance, Risk and Performance

Justin McCarthy, CEO of PRMIA

Lyndsey Zhang, author of *Corporate Governance in China Seen Through a Practitioner's Lens*

Martin Massey, chair of Institute of Risk Management's climate change special interest group and author of *Climate Change Enterprise Risk Management: A practical guide to reaching net zero goals*

Monica Young, director of risk and compliance at KMPG LLP in Chicago, and a member of our special interest group

Patrick Butler, board chair, Net Zero Labs and adviser on culture and conduct management

Stephen Scott, founder and CEO, Starling

Appendix

Inefficiencies of risk culture maturity surveys

by **Horst Simon**, Risk Culture Builder

- **Lack of employee engagement:** for a risk culture survey to be effective, it's important that employees are engaged and willing to participate. If they don't see the value in the survey or don't trust that their responses will be taken seriously, they may not be forthcoming with their answers.
- **Inaccurate or incomplete data:** surveys are often subject to biases and inaccuracies, particularly if respondents are not being truthful or are not fully aware of the risks within their organisation.
- **Difficulty interpreting survey results:** even if the data collected from a risk culture survey is considered acceptable, it can be difficult to interpret the results and understand what they mean for an organisation. This is particularly true if the survey questions are not well-crafted or if the results are not analysed by experts.
- **Limited ability to change culture:** ultimately, surveying does not change the culture. Even if an organisation identifies issues with its risk culture through a survey, it can be difficult to change the culture of the organisation and to ensure that employees are acting in line with the values and behaviours that the organisation wishes to promote.
- **Complexity of risk culture:** measuring the maturity of an organisation's risk culture can be challenging because risk culture is a complex and multi-dimensional concept that can be affected by a variety of factors, such as organisational structure, leadership, and employee attitudes.
- **Limited ability to measure continuous improvement:** surveys can be considered a snapshot in time, so one survey cannot be used to measure whether an organisation is continuously improving its culture.

Risk culture maturity assessment interviews are sometimes used to try to assess the level of maturity of an organisation's risk culture, but they also have their limits. Issues to consider include the following.

- **Limited sample size:** risk culture maturity interviews typically involve a relatively small number of participants, so the findings may not be representative of the entire organisation. Additionally, interviews may be biased by the selection of participants, or be influenced by the interviewer's perspective or interpretation.
- **Limited objectivity:** risk culture maturity interviews are often conducted by internal staff or consultants who may have biases or vested interests. They may also lack the necessary expertise or training to conduct effective interviews, which can limit the objectivity of the findings.
- **Limited scalability:** interviews can be time-consuming and resource-intensive, which may make it difficult for an organisation to conduct a large-scale assessment of its risk culture in this way.
- **Limited depth and accuracy:** interviews are often conducted by using a set of predefined questions that may not capture all aspects of the organisation's risk culture. They may also not be able to provide an in-depth understanding of the underlying reasons for the current culture.

Demographic breakdown of respondents

The comprehensive nature of our coverage of sectors can be seen in Figures A1, A2 and A3, with those working as accountancy practitioners identified as part of our scope. It should be noted that retired / in-between job respondents were asked to base their answers on their most recent work. Across those sectors, the survey covered over 20 different types of industry (Figure A4). And in financial services we broke down responses into sub-types such as retail banking vs asset management (Figure A5).

FIGURE A.1: Respondents by region

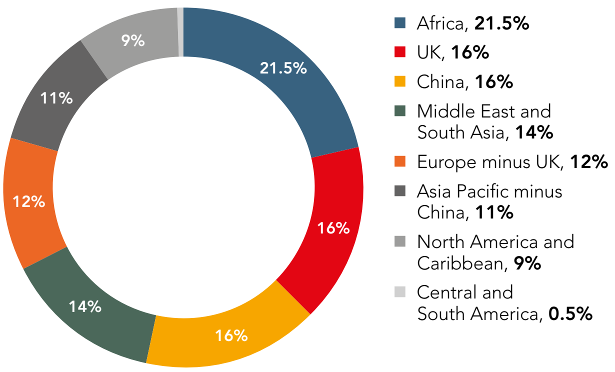


FIGURE A2: The size of respondents' organisations

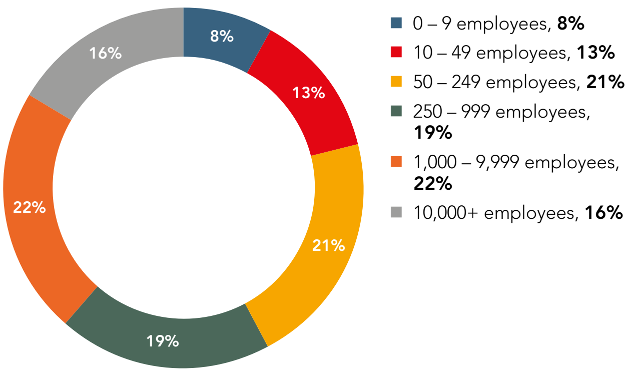


FIGURE A3: The sectors in which respondent work

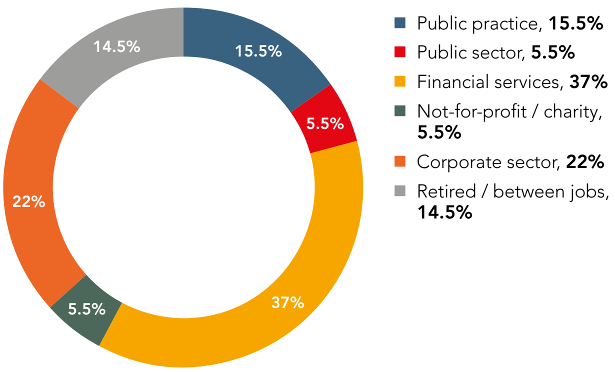


FIGURE A4: The types of industry

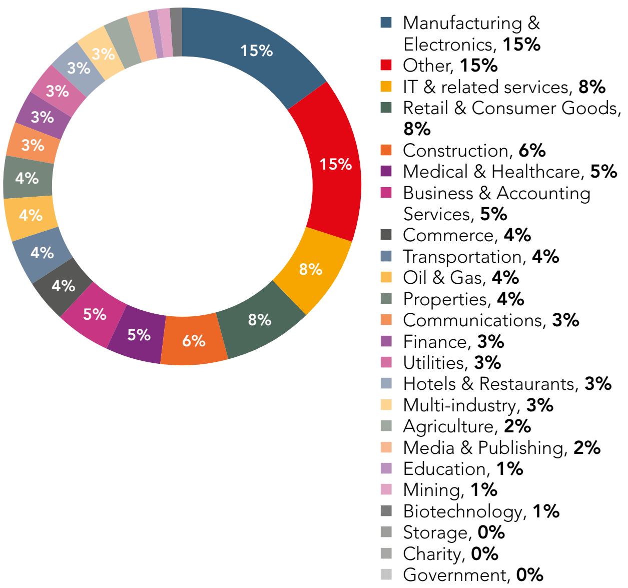
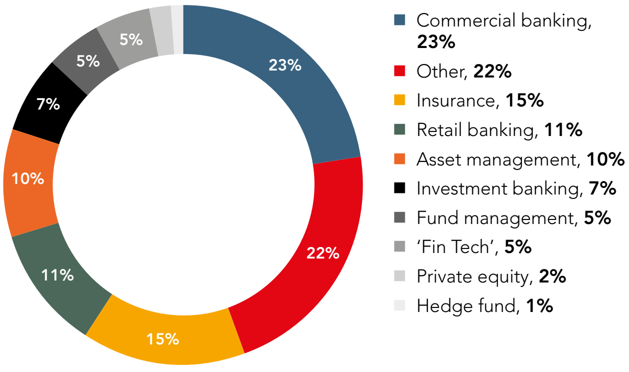


FIGURE A5: The subsectors of financial services in which respondents worked



References

ACCA (2021), *Rethinking Risk for the Future*. Downloadable from <https://www.accaglobal.com/hk/en/professional-insights/risk/rethinking-risk.html>, accessed 15 March 2023.

ACCA (2022). 'Risk Culture Building Webinar for ACCA Members in Europe' [webinar]. Available via: <https://event.on24.com/wcc/r/3796805/FB9DCEC9E6F10471FE2EDDBC531920D9>, source page accessed 16 March 2023.

Alberti, C.T., Bedard, J.C., Bik, O. and Vanstraelen, A. (2020), 'Audit Firm Culture: Recent Developments and Trends in the Literature' [online article], *European Accounting Review*, 31 (1): 59–109 <https://www.tandfonline.com/doi/full/10.1080/09638180.2020.1846574>, accessed 17 March 2023.

APRA (2022), 'No Room for Complacency on Bank Risk Culture' [website report], 10 November <https://www.apra.gov.au/news-and-publications/no-room-for-complacency-on-bank-risk-culture/>, accessed 14 March 2023.

Au, A. (2022), 'Sound Bank Culture: The Fundamental Key to Managing Conduct Risk', Regulatory keynote address at XLoD Global 2022 [speech] <https://www.hkma.gov.hk/eng/news-and-media/speeches/2022/11/20221116-1/#>, accessed 16 March 2023.

Baunsgaard, V.V. (2022), 'What is Psychological Safety and How to Create It?' [online article], *Manage Magazine*, 1 September <https://managemagazine.com/article-bank/leadership/what-is-psychological-safety-and-how-to-create-it/>, accessed 14 March 2023.

BCBS (Basel Committee on Banking Supervision)/BIS (Bank for International Settlements) (2014), *Corporate Governance Principles for Banks*, <https://www.bis.org/publ/bcbs294.pdf>, accessed 14 March 2023.

Black, W.K. (2015), 'Are Financial Penalties Enough to Deter Banks' Bad Behaviour?' [online article], *Knowledge at Wharton*, 21 May <https://knowledge.wharton.upenn.edu/article/are-financial-penalties-enough-to-deter-banks-bad-behavior/>, accessed 17 March 2023.

Blackhurst, C. (2022), *Too Big to Jail ...*

Chartered Institute of Internal Auditors (2022), *Cultivating a Healthy Culture: Why Internal Audit and Boards Must Take Corporate Culture more Seriously in a Post-Covid World*, <https://www.iia.org.uk/policy-and-research/research-reports/cultivating-a-healthy-culture/>, accessed 17 March 2023.

Coburn, A. (2014), 'The Circulatory System of Finance' [website article], Centre for Risk Studies Viewpoints, <https://risk-studies-viewpoint.blog.jbs.cam.ac.uk/2014/10/16/the-circulatory-system-of-finance/>, accessed 17 March 2023.

Conmy, S. (2023), 'Have You Heard of a Shadow Board?' [website article], Corporate Governance Institute, 1 January <https://www.thecorporategovernanceinstitute.com/insights/guides/a-shadow-board-of-younger-employees-could-save-your-company/#:~:text=The%20CEO%20usually%20sponsors%20the,company%2C%20representing%20their%20generation's%20perspective>, accessed 14 March 2023.

Cook, K. and Scott, S. (2019), *Trust Matters*, <https://starlingtrust.com/couch/uploads/file/trust-matters-starling.pdf>, accessed 17 March 2023.

Deloitte (2013), *Culture in Banking: Under the Microscope*, <https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/financial-services/deloitte-uk-culture-in-banking.pdf>, accessed 14 March 2023.

Deloitte (2017), 'Culture and Conduct Risk: Elevating Internal Audit's Role' [online article], *Wall Street Journal* (sponsored content) <https://deloitte.wsj.com/articles/culture-and-conduct-risk-elevating-internal-audits-role-1496116938>, accessed 17 March 2023.

DNB (20**), ...

DNB (2023), *Moving from Reflex to Reflection*, Downloadable from <https://www.dnb.nl/en/sector-news/supervision-2023/from-reflex-to-reflection>, accessed 16 March 2023.

Dudley, W.C. (2014), 'Enhancing Financial Stability by Improving Culture in the Financial Services Industry' [website: speech], 20 October <https://www.newyorkfed.org/newsevents/speeches/2014/dud141020a.html>, accessed 16 March 2023.

Dyck, A., Morse, A. and Zingales, L. (2023),'How Pervasive is Corporate Fraud?', *Review of Accounting Studies*, 5 January <https://link.springer.com/article/10.1007/s11142-022-09738-5#:~:text=Combining%20fraud%20pervasiveness%20with%20existing,to%20%24830%20billion%20in%202021>, accessed 15 March 2023.

Elderson, F. (2022), 'Supervising Banks' Governance: Structure, Behaviour and Culture' [website: speech] <https://www.ecb.europa.eu/press/key/date/2022/html/ecb.sp220611~01ae4a6b1c.en.html>, accessed 17 March 2023

European Commission (n.d.), 'Protection for Whisleblowers' [website page] <https://commission.europa.eu/aid-development-cooperation-fundamental-rights/your-rights-eu/protection-whistleblowers_en>, accessed 16 March 2023.

FCA (Financial Conduct Authority) (2017), '5 Conduct Questions Programme' [website page], 12 April <https://www.fca.org.uk/firms/5-conduct-questions-programme>, accessed 14 March 2023.

FCA (Financial Conduct Authority) (2022), 'The FCA's Consumer Duty will lead to a major shift in financial services' [website press release], 27 July <https://www.fca.org.uk/news/press-releases/fca-consumer-duty-major-shift-financial-services>, accessed 16 March 2023.

FRC (Financial Reporting Council) (2021), *Audit Firm Culture: Challenge. Trust. Transformation*, <https://www.frc.org.uk/getattachment/fe2b0d35-aeb0-4d3c-8c96-cb04ac0f449d/FRC-Audit-Firm-Culture-Collection-of-Perspectives_December-2021.pdf>, accessed 17 March 2023.

FSB (Financial Stability Board) (2014) *Guidance on Supervisory Interaction with Financial Institutions on Risk Culture*, <https://www.fsb.org/wp-content/uploads/140407.pdf>, accessed 14 March 2023.

FSB (Financial Stability Board) (2020), 'Evaluation of Too-Big-to-Fail Reforms: Lessons for the Covid-19 Pandemic' (website report], 28 September <https://www.fsb.org/2020/09/evaluation-of-too-big-to-fail-reforms-lessons-for-the-covid-19-pandemic/>, accessed 17 March 2023.

Garten, J.E. (2018), *From Silk to Silicon: The Story of Globalization Through Ten Extraordinary Lives* (Amberley Publishing).

Green, S. (2009), *Reflections on Money, Morality, and an Uncertain World* (London: Penguin Group).

Group of Thirty (2018), *Banking Conduct and Culture: A Permanent Mindset Change*, <https://group30.org/images/uploads/publications/aaG30_Culture2018.pdf>, accessed 17 March 2023

Harwood, P. (2022), 'Book Review: Culture Audit in Financial Services' [online article], *The Actuary*, 5 October <https://www.theactuary.com/opinion/2022/10/06/book-review-culture-audit-financial-services>, accessed 14 March 2023.

HKMA (Hong Kong Monetary Authority) (2020), *Report on Review of Self-assessments on Bank Culture*, <https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2020/20200522e1.pdf>, accessed 14 March 2023.

Hsu, M.J. (2023), *Detecting, Preventing and Addressing 'Too Big to Manage'*, Remarks at Brookings 17 January <https://www.occ.gov/news-issuances/speeches/2023/pub-speech-2023-7.pdf>, accessed 14 March 2023.

James Lam & Associates (2023) 'Risk Insights' [website] <https://jameslam.com/risk-insights/>, accessed 14 March 2023.

Jewars, C. (2019), 'The Social Impact of Losing Trust in Audit' [online article], *Accountancy Age*, 25 October <https://www.accountancyage.com/2019/10/25/comment-social-impact-of-losing-trust-in-audit/>, accessed 17 March 2023.

Jung, C. and Meyer, M. (2021), *Remaking Audit: A Plan for Culture Change and Regulatory Reform: Briefing 2*, <https://www.ippr.org/files/2021-05/remaking-audit-may21.pdf>, accessed 17 March 2023.

Kelley, R. (1992), *The Power of Followership: How to Create Leaders People Want to Follow and Followers Who Lead Themselves* (New York: Ban tam Dell Publishing Group).

Khan, A. (2016), *Central Bank Governance and the Role of Nonfinancial Risk Management*, <https://www.imf.org/external/pubs/ft/wp/2016/wp1634.pdf>, accessed 17 March 2023.

Lam, J. (2003/2014), *Enterprise Risk Management: From Incentives to Controls* (New Jersey: Wiley Finance).

Lightle, S., Castellano, J.F. and Baker, B. (2017), 'Why Audit Teams Need the Confidence to Speak Up' [online article], *Journal of Accountancy*, 1 January <https://www.journalofaccountancy.com/issues/2017/jan/psychological-safety-for-audit-teams.html>, accessed 17 March 2023.

Mayer, C. (2018), *Prosperity: Better Business Makes the Greater Good* (Oxford: Oxford University Press).

McBride, J. (2016), 'Understanding the Libor Scandal' [website article] <https://www.cfr.org/backgrounder/understanding-libor-scandal>, accessed 17 March 2023.

Miles, R. (20**), ...

Milkau, U. (2017), *Risk Culture During the Last 2000 Years – From an Aleatory Society to the Illusion of Risk Control*. Downloadable from <https://www.mdpi.com/2227-7072/5/4/31>, accessed 14 March 2023.

Monaco, L.O. (2022), 'Deputy Attorney General Lisa O. Monaco Delivers Remarks on Corporate Criminal Enforcement' [website article], 15 September <https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-delivers-remarks-corporate-criminal-enforcement>, accessed 17 March 2023.

Munter, P. (2022), 'The Critical Importance of the General Standard of Auditor Independence and an Ethical Culture for the Accounting Profession' [SEC website statement], 8 June <https://www.sec.gov/news/statement/munter-20220608>, accessed 17 March 2023.

Office of the Comptroller of the Currency (2018), *Comptroller's Handbook: Large Bank Supervision*. Version 1.0, June <https://www.occ.gov/publications-and-resources/publications/comptrollers-handbook/files/large-bank-supervision/pub-ch-large-bank-supervision.pdf>, accessed 17 March 2023.

Pavilion (n.d.), 'The Elements of Commander's Intent' [website article] <https://pavilion.dinfos.edu/Article/Article/2163950/the-elements-of-commanders-intent/>, accessed 16 March 2023.

Pound, J. (2023), 'Silicon Valley Bank is Shut Down by Regulators in Biggest Bank Failure since Global Financial Crisis' [website article], CNBN, 10 March <https://www.cnbc.com/2023/03/10/silicon-valley-bank-is-shut-down-by-regulators-fdic-to-protect-insured-deposits.html>, accessed 14 March 2023.

Power, M., Ashby, S. and Palermo, T. (n.d.), *Risk Culture in Financial Organisations*, <https://www.lse.ac.uk/accounting/assets/CARR/documents/Risk-Culture-in-Financial-Organisations/Final-Risk-Culture-Report.pdf>, accessed 14 March 2023.

PRA (Bank of England's Prudential Regulation Authority) (2020), *Evaluation of the Senior Managers and Certification Regime*. <https://www.bankofengland.co.uk/prudential-regulation/publication/2020/evaluation-of-the-senior-managers-and-certification-regime>, accessed 16 March 2023.

Primeau, M. (2021), 'Your Powerful, Changeable Mindset' [website report], *Stanford Report*, 15 September <https://news.stanford.edu/report/2021/09/15/mindsets-clearing-lens-life/>, accessed 14 March 2023.

Rapson, S. (2022), 'Regulating a Cultural Shift in Audit' [website article – restricted access] <https://insights.starlingtrust.com/content/compendium/regulating-a-cultural-shift-in-audit>, source page accessed 17 March 2023.

Reader, T. and Scott, S. (n.d.), 'Culture & Conduct Risk in Banking: Achieving a Better Standard of Care' [website article – restricted access] <https://insights.starlingtrust.com/content/compendium/culture-and-conduct-risk-in-banking-achieving-a-better-standard-of-care-1>, accessed 17 March 2023.

Rosenberg, J. (2022), 'Things that Have Never Happened before Happen all the Time' [website: speech] <https://www.newyorkfed.org/newsevents/speeches/2022/ros221027>, accessed 16 March 2023.

Rouch, D. (2020), *The Social Licence for Financial Markets: Reaching for the End and Why It Counts.*

Scott, S. (2022), *Like Banks, Audit Firms will Face Culture Scrutiny and Conduct Risk Assessments*. Downloadable from <https://www.jdsupra.com/post/fileServer.aspx?fName=f712b5b2-07cc-458f-bfa9-5d75a4fb8165.pdf>, accessed 17 March 2023.

SECP (Securities and Exchange Commission of Pakistan) (n.d.), *Principles of Corporate Governance for Non-Listed Companies* Downloadable from <https://www.secp.gov.pk/corporate-governance/corporate-governance/>, accessed 16 March 2023.

Smagalla, D. (2022), 'Wells Fargo Fined $22 Million for Alleged Whistleblower Retaliation' [online article, restricted access], *Wall Street Journal*, 2 September <https://www.wsj.com/articles/wells-fargo-fined-22-million-for-alleged-whistleblower-retaliation-11662148588>, source page accessed 16 March 2023.

Smith, K. (2014), 'Banking Culture Primes People to Cheat' [online article], *Nature*, 19 November <https://www.nature.com/articles/nature.2014.16380>, accessed 17 March 2023

Starling Insights (2018), 'Concluding Remarks to the 2018 Compendium' [website report, restricted access] <https://insights.starlingtrust.com/content/compendium/concluding-remarks-to-the-2018-compendium>, source page accessed 14 March 2023.

Starling Insights (n.d.b), 'UK FRC Scrutinizes Audit Firms Over Exam Cheating' [website article – restricted access] <https://insights.starlingtrust.com/content/observations/uk-frc-scrutinizes-audit-firms-over-exam-cheating>, source page accessed 17 March 2023.

Starling Insights (n.d.c), 'KPMG Fined for Misleading UK FRC' [website article – restricted access] <https://insights.starlingtrust.com/content/observations/kpmg-fined-for-misleading-uk-frc>, accessed 17 March 2023.

Starling Insights (n.d.d), Deeper Dive: The Era of Accountability [website article – restricted access] <https://insights.starlingtrust.com/content/thoughts/deeper-dive-the-era-of-accountability>, source page accessed 17 March 2023.

Tarullo, D.K. (2009), 'Confronting Too Big to Fail' [Speech; website], Board of Governors of the Federal Reserve System, 21 October <https://www.federalreserve.gov/newsevents/speech/tarullo20091021a.htm>, accessed 17 March 2023.

Terracol, M. and Nowars, I. (2022), 'EU Countries Continue to Fail Whisleblowers' [blog article], 19 December <https://www.transparency.org/en/blog/eu-countries-continue-to-fail-whistleblowers>, accessed 16 March 2023.

UK Finance (20**), ...

Weber Shandwick (2019), 'Half of Millennial Employees Have Spoken Out about Employer Actions on Hot-Button Issues' [website article], <https://www.prnewswire.com/news-releases/half-of-millennial-employees-have-spoken-out-about-employer-actions-on-hot-button-issues-300857881.html>, accessed 17 March 2023.

Wucker, M. (2021), 'You Are What You Risk: The New Art and Science of Navigating an Uncertain World' [website article] <https://www.wucker.com/writing/you-are-what-you-risk/>, accessed 14 March 2023.

PI-RISK-CULTURE-BUILDING-RESILIENCE

ACCA The Adelphi 1/11 John Adam Street London WC2N 6AU United Kingdom / +44 (0)20 7059 5000 / **www.accaglobal.com**