Risk and the strategic role of leadership

Think Ahead

About ACCA

ACCA (the Association of Chartered Certified Accountants) is the global body for professional accountants, offering business-relevant, first-choice qualifications to people of application, ability and ambition around the world who seek a rewarding career in accountancy, finance and management.

ACCA supports its **200,000** members and **486,000** students in **180** countries, helping them to develop successful careers in accounting and business, with the skills required by employers. ACCA works through a network of **101** offices and centres and more than **7,200** Approved Employers worldwide, who provide high standards of employee learning and development. Through its public interest remit, ACCA promotes appropriate regulation of accounting and conducts relevant research to ensure accountancy continues to grow in reputation and influence.

ACCA is currently introducing major innovations to its flagship qualification to ensure its members and future members continue to be the most valued, up to date and sought-after accountancy professionals globally.

Founded in 1904, ACCA has consistently held unique core values: opportunity, diversity, innovation, integrity and accountability.

More information is here: www.accaglobal.com

About this report

This report illustrates the current practice of board oversight of risk management, based on in-depth interviews with executive and non-executive directors. It highlights good practices but also challenges that leaders face and considers way forward.

February 2018

Risk and the strategic role of leadership

Dr Simon Ashby University of Plymouth
Dr Cormac Bryce University of Nottingham
Dr Patrick Ring Glasgow Caledonian University

Foreword

How often, as we glance through the news headlines, do we see another corporate failure and wonder – where was the board?

Risk and risk management have always been at the heart of concerns about leadership. In this report, we explore the role of boards in the risk management of the organisations they lead.

Following the global financial crisis in 2007-8 the focus on risk and risk management has intensified. Today there is an abundance of literature as well as legislative and regulatory requirements. Risk and risk management regularly features on the board agenda, irrespective of sector.

Yet remarkably less is known of the reality of day to day practices among executives and board members. We know little about how boards are truly integrating risk discussions into strategic decision making, as well as the skills and experience they have in managing risks to deliver business goals, and where there may be gaps.

This report suggests there are different approaches to risk management in practice each with their own respective strengths and weaknesses. It also suggests that there is some way to go to integrating strategy and risk decisions effectively and many conversations on risk appear to focus on the downside rather than upside. Perhaps we should ask a different question– how can boards better exploit the opportunity implicit in risk and uncertainty to drive better business outcomes?

We hope that this report provides useful insights for both boards and executives to reflect on emerging good practice. Policy makers too may also benefit by reflecting on these findings in the light of recent developments. The next phase of our work on risk will go on to consider how organisations embed effective risk management across the business.

Maggie McGhee
Director of Professional Insights
ACCA

Executive summary

Boards have always been involved in the management of risk. Without appropriate risk taking, organisations cannot exploit the full range of strategic opportunities that are available to them, nor can they hope to protect themselves from less positive outcomes.

Equally, the governance and internal control roles of boards are closely connected with risk management. Effective risk assessment, reporting and control help to enhance a board's governance and internal control activities, reducing the probability that an organisation may deviate from its stated objectives and so fail to meet the needs of its stakeholders.

What is less clear is how board-level risk management discussions and practices are changing and developing, especially in relation to the complex and dynamic world that characterises the early 21st century. Changing technology, such as the growth of cloud computing and social media, creates opportunities for returns as well as losses as do the major political and economic changes associated with events such as Brexit, the election of President Trump in America, or the global financial crisis of 2007–8.

The purpose of this ACCA research project was to discover what boards are talking about and doing about risk management, and the challenges that they face in ensuring the effectiveness of these activities. In particular, this project explored how boards are integrating their discussions about strategy and risk, along with how their risk-management skills and experience are developing. The project also investigated the challenges that boards face in performing their risk-management roles and how the roles of the executive and non-executive director are evolving: even on an Anglo-Saxon style unitary board it is possible that differences may emerge.

The intention is to shed light on, and learn from, current practice, and to share examples of good practice where possible. It is for organisations and their boards to decide which of these practices are relevant to them, as part of their efforts to ensure that board level risk-management conversations and practices are as 'future-proof' as possible.

The project is based on:

- 30 interviews with practising executive and non-executive directors (NEDs) from a broad cross-section of organisations;
- two focus groups consisting of a number of risk-management professionals; and
- ACCA's Global Forums, with particular thanks to the Global Forum on Governance, Risk and Performance.

The research shows that board-level conversations and practices are varied and that this variation does not necessarily reflect the nature, scale and complexity of an organisation's activities. It shows, however, a wide range of good practice across both larger and smaller organisations in a range of for-profit and not-for-profit sectors.

> Risk may bring with it the potential for losses, but it also offers the potential for opportunity.

Key findings include the following.

- Board-level conversations and practices in relation to strategy and risk management take place along a spectrum, with those of many boards being nearer to one end of the spectrum or the other (although a few display features from across the spectrum). The extremes of the spectrum can be characterised as:
  - the *Principled* approach, where discussions about risk are more likely to focus on the exploitation of upside opportunities, and connect strategy and risk in an implicit and unstructured way, potentially leading to inconsistent risk-management decisions, and
  - the *Prescriptive* approach, where risk-management activities are much more formalised and consistent, but with a high degree of focus on internal control which may mean that strategic opportunities are missed.
- Boards are still finding it hard to understand and address softer factors, such as culture and risk appetite. Often, this is because of a lack of clear information and difficulties in connecting them to organisational performance.
- Regulation and compliance remain key drivers for board-level involvement in risk management. Nonetheless, some organisations are increasingly aware of the strategic benefits of risk management in helping them to exploit opportunities and so exceed their stated objectives.
- A high level of diversity in boards' risk skills, knowledge, experience, education and training helps to develop a collective consciousness that allows a board to identify changes in risk exposures and respond appropriately.
- Factors such as lengthy risk reports and insufficient time devoted to risk management at board meetings create significant challenges for board-level risk-management activities.
- NEDs walk a delicate line between participation (ensuring that tasks are performed) and oversight (providing assurance that tasks have been performed within the agreed parameters). NEDs need to understand the organisations that they are a part of and participate in strategic decision making, but their ability to step back from day-to-day pressures and their experience in other organisations allows them to perform a 'critical friend' role, helping to restrain over-confident executives or encourage overly cautious ones. A unitary board should not mean that all board members need a single perspective.

The report also makes a series of recommendations for organisations, their boards and for policymakers. In particular, the report reflects interview participants (hereafter 'participants')' concern that risk and risk management are not always viewed in a positive way. Risk may bring with it the potential for losses, but it also offers the potential for opportunity. Today's board has a key role to play here, helping its organisation identify and exploit opportunities, which is as much a part of maximising the long term sustainable performance of the organisation as well as overseeing the mitigation of threats.

Disclaimer

Though funded by ACCA, this research project was conducted by independent university academics. The findings from this project reflect the views of the participants and are not necessarily those of ACCA or its staff and members.

Contents

1. Introduction

1.1 UNCERTAINTY AND CHANGE: HOW ARE BOARDS RESPONDING TO RISK-MANAGEMENT CHALLENGES?

Organisations in the 21st century are facing high levels of complexity and uncertainty. Whether it is from the effects of global warming, developments in cloud computing, social media or political change and the potential for less liberal trading environments, the number of ways in which organisations can trip up only ever seems to increase.

In the face of this increased complexity and uncertainty, the temptation for boards is to become more conservative and risk averse in an attempt to create certainty. In practice, boards that choose to do this risk missing out on significant potential opportunities for their organisations and stakeholders. Worse still, they risk losing ground to entities with more innovative and entrepreneurial boards that are better able to steer their organisations towards the opportunities on offer. Choosing the 'safe' option can be a risky strategy in itself, as illustrated by companies such as IBM, which failed to capitalise on the personal computer, and Kodak, which, despite developing the digital camera, chose not to market it.

Corporate governance codes and standards are also changing. In the US a major revision of the COSO Enterprise Risk Management (ERM) Guidance was completed in 2017 (COSO 2017). In the UK, revisions to the Corporate Governance Code were released for consultation in December 2017 (FRC 2017). In both cases, a closer relationship between the strategic-management and risk-management roles of the board has been proposed. In addition, there is a greater emphasis on 'softer' considerations, such as the culture of an organisation.

External events such as technological developments, regulatory change or public scandals are easy to observe. It is, however, much more difficult to see is how boards are responding to the risk-management challenges presented by these events.

The purpose of this research project was to investigate how boards understand their role in relation to risk management today. Specifically, the aim was to explore how boards satisfy their oversight responsibilities and evaluate their effectiveness and whether boards view risk management simply as a tool for reducing risk and increasing certainty, or whether risk management and strategic management are integrated to support innovation and the pursuit of opportunities.

Another concern is how boards understand concepts such as culture (including risk culture) and risk appetite. Further, the research explored what, if any, barriers exist to prevent boards from having effective risk-management conversations, as well as board members' perceptions of the roles of executives and non-executive directors in relation to risk management.

The intention is not to find fault with or criticise current risk-management practices. The researchers know personally the challenges that board directors can face in navigating a path that both creates value for stakeholders and ensures that an organisation can remain viable into the long term. By learning from the current practice of boards, and the views of executive and non-executive directors, the intention here is to highlight where boards have got to in the 'journey' to evermore successful value creation.

Finally, this report highlights areas of good board-level risk-management practices, and provides insights that boards can use to enhance their practice further. The report also provides recommendations for policymakers, to assist in the spreading and adoption of good practice as well as highlighting areas that call for more guidance.

1.2 CONNECTING THE DOTS: STRATEGY, GOVERNANCE, PERFORMANCE AND RISK MANAGEMENT

> *'One of the greatest benefits the board can bring to its management is to declare itself open to the discussion and the possibility of risk'* (consultant).

Risk management is often viewed as an internal control activity, protecting organisations from harmful events such as fires, employee misconduct or reputation-damaging scandals. From this perspective, risk is a bad thing for organisations, something to be assessed and limited as much as possible. To the extent that risk is tolerated, it is done so only because it is an inescapable part of 'core' activities such as manufacturing processes, marketing or service delivery.

This report does not challenge this perspective or existing corporate governance frameworks in this regard. Organisational scandals from Enron to Barings, Barclays and VW have all highlighted the significant damage that

Risk comes with the opportunity for returns, and even seemingly adverse events such as regulatory change or political uncertainty can create opportunities that may be exploited.

can be associated with weak governance, culture and control. Risk management provides tools that organisations can use to help identify and reduce the probability and impact of such damage.

On the other hand, neither does this report endorse one particular perspective or another. While risk management can help a board to control risks that may threaten the achievement of the organisation's strategic objectives, it is also important to recognise the speculative dimension of managing risk, especially when dealing with the strategic-level risks that may occupy the attention of a board. As participants discussed, risk comes with the opportunity for returns, and even seemingly adverse events such as regulatory change or political uncertainty can create opportunities that may be exploited.

Equally, highly strategic risks, such as the development of a new product or market, or an acquisition or merger, very clearly combine a range of positive and negative outcomes. In such situations, some boards and organisations may prefer to use terms other than 'risk', such as 'volatility' or 'opportunities and threats' or 'managing opportunity'. Nonetheless, the fact remains that exploiting opportunities is as much part of risk management as controlling downside outcomes, as participants consistently pointed out.

1.3 RESEARCH AIMS, OBJECTIVES AND APPROACH

The aim of the project was to explore current practice in board-level risk-related activities and to make recommendations to help improve the readiness of boards for the strategy, risk and governance challenges.

The specific objectives were as follows.

1. To explore how boards have developed and perform the following roles in practice:
   a. strategic risk management and decision making (seizing opportunities, avoiding inappropriate strategies, managing risks to strategic objectives, as well as enabling boards to prepare for disruptive, non-routine and reputational issues, such as 'black swan' type risks)
   b. oversight of risk-management effectiveness (formal aspects of internal control)
   c. communicating their approach to risk management, and
   d. managing and embedding appropriate culture (including risk culture).
2. To understand the factors (eg regulation, stakeholder pressure, improvements to strategic decision making) that have encouraged boards to perform the above roles.
3. To determine whether boards have the skills, experience and training necessary to fulfil their risk-management roles, in increasingly complex risk environments.
4. To investigate other barriers that may prevent boards from performing their risk-management roles (eg lack of skills within the risk function, silo-based risk management, complex organisational structures, lack of data).
5. To examine whether there are areas of convergence and divergence in the roles of NEDs, executives and risk specialists in relation to the above.

In exploring board-level risk-management activities and in providing recommendations for good practice, the intention is not to complicate the role of boards. What works for one board and organisation may not for another. Trying to fit every board and organisation into a specific theoretical approach can be a thankless task; best practice can vary according to the nature, scale and complexity of an organisation's activities, as well as its culture, competencies and resources. Consequently, this report does not intend to replace existing theoretical frameworks by proposing any new frameworks or risk-management tools.

Instead, the aim was to conduct the interviews objectively without a specific theoretical or conceptual agenda. This report intends to find out how board members understand their risk-management role and make use of risk-management concepts and tools, and how they perceive the challenges that they face in performing their risk-management duties.

Resulting suggestions for practice (Chapter 4) are based upon what the participants said about things that they have done that have worked and those that have not worked. It is for the readers of this report to select the ideas and activities that may work for them or their organisation.

2. Findings

The next five subsections present the findings for each of the research objectives. The first of these was to explore the various roles that boards may perform in relation to risk management.

2.1 THE ROLE OF THE BOARD IN RISK MANAGEMENT

> *'The role of the board is oversight of the company's strategy and performance, in general and, therefore, the question of risk is a key element of strategy. So, assessing the risk implications of strategy, discussing risk appetite, understanding the elements of risk and where they sit in the organisation, and overseeing the process by which risks are monitored and managed and mitigated through the organisation'* (non-executive director).

2.1.1 Strategy governance, performance and risk

The above quote reflects the prevailing view of the participants as to the role of the board in risk management. All the participants emphasised the oversight role that boards have, a role highlighted in the UK Corporate Governance Code and many other governance codes worldwide.

The quote also highlights that although strategy and risk are connected, the relationship may sometimes be a linear one: the desired strategy is determined first, and then the risks that may arise from this strategy and its implementation are considered. In this context, strategy is the mechanism for creating value and risk management exists to help protect the value-creation process from negative events. This linear approach is reflected in the quote below from an executive director of a large listed company:

> *'I think strategy is decided at some point... And once you've agreed that, then you say right, okay, for us to get there, that is not going to be easy, and yes, there are risks associated with that, and that each of those risks, here is the impact, and here is where the impact is going to be. And then it's a question of "how do you manage it?"'* (executive director).

The quote highlights a potential issue with an overly linear approach to strategy and risk. In taking this approach, risk is generally viewed in terms of the probability and impact of loss, so the focus is on the minimisation of risk associated with downside possibilities. Viewing risk as 'bad' means that the potential for better-than-expected outcomes may be overlooked. It may also foster high levels of risk aversion in boards, a problem that was identified by a number of the participants in both large and SME organisations. The consequence of this approach is that innovations may be missed.

> *'In some areas there should be a willingness to proactively take risk and indeed that to take no risk is potentially the biggest risk of all because there's a possibility that people innovate around you, you're left standing, and as time goes by you become the dinosaur in comparison to the rest of the sector'* (non-executive director).

Even where risk is viewed more positively, there remains a danger that its significance is underestimated or that strategic-level risks are not viewed as risks:

> *'...it's very easy to say, "yes, we're doing this... but we don't need to consider risk because it is just a strategic direction and we know there will be risk in that". Actually you do need to take that step back of formally considering the risk in order to get the benefits of the risk management in there.*
>
> *...quite often people think, actually, yes, we deal with risk every day, and, therefore, we don't actually need to focus on specific risk management; and that's a bit dangerous'* (executive director).

In a small number of organisations strategy setting and risk were integrated to a much greater extent. The directors of these organisations indicated that their boards considered the risks associated with choosing or not choosing specific strategic options at the strategy setting phase, as well as the organisation's risk-management competencies and capabilities.

Such discussions were not necessarily structured in a formal way, nor did they tend to use terms such as 'risk' or 'risk management'. Despite the relatively unstructured nature of their approach, these boards were more likely to exploit opportunities even when faced with seemingly adverse events, such as the economic consequences of the EU referendum, the election of President Trump and his America First agenda or government welfare changes.

Each approach has strengths and weaknesses, especially in organisations whose boards are close to one of the ends of the spectrum.

Case studies: Turning adversity into opportunity

An SME component manufacturer was concerned about the election of Donald Trump as president and the potential for increased tariffs on goods imported to the US. As a result, the firm created a US subsidiary to manufacture components for its American customers.

A Housing Association was concerned about the implications of the UK government's Welfare Reform Act 2016 on its financial sustainability. In response, the board created a strategic planning forum led by NEDs with executive input. The revised strategy led to a major restructuring and the development of new housing products and markets, all with the aim of meeting the needs of both existing and future tenants.

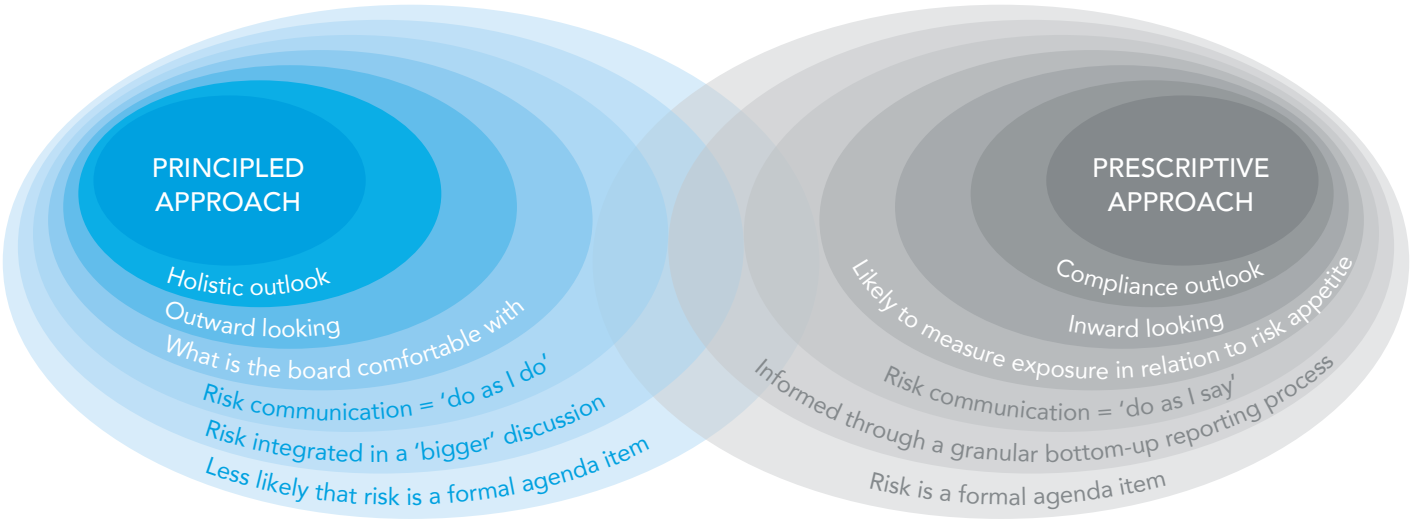
2.1.2 The principled–prescriptive spectrum

There is a spectrum of practice as to how structured or unstructured a board's approach is to risk management. This spectrum also goes beyond the structural nature of a board's approach, and includes factors like: how risk is perceived (as an opportunity or a compliance matter); board level and organisational cultures in relation to risk; and the board's approach to communication. Figure 2.1 explains the two extremes of this spectrum.

A number of the participants discussed elements of the two approaches. It is important to stress that one approach is not necessarily better than the other. The appropriate approach may be influenced by industry sector, the level of regulation and the size or purpose of an organisation. For example, all the boards of the financial services organisations in the sample tended to be prescriptive in their approach, primarily because of high levels of regulation. In contrast, the SME boards tended to be more principled in approach.

Each approach has strengths and weaknesses, especially in organisations whose boards are close to one of the ends of the spectrum. For example, there were claims that an extremely prescriptive risk-management approach may cause board-level risk-management activities to become static and reactive, with board members getting lost in operational detail (a potential problem made worse by lengthy risk registers) and taking an overly negative view of risk.

FIGURE 2.1: Principled–Prescriptive spectrum[1]



1 The terms 'principled approach' and 'prescriptive approach' came from the study participants. At its extreme, the prescriptive approach is intended to capture an approach focused exclusively on risk compliance and procedures. On the other hand, the principled approach is intended to reflect an approach that, at its extreme, focuses on the 'in-principle' business objectives of a board to the exclusion of explicit risk-management compliance and procedures.

An organisation's culture can have a significant effect on how people within the organisation behave and communicate with each other.

In contrast, participants warned that boards following an extremely principled approach may make inconsistent decisions and may pursue upside opportunities at any cost, exposing an organisation to excessive amounts of risk. There is also the danger that boards that appear to adopt a principled approach are not actually discussing risk and risk management in a sufficiently explicit way. It suggests that an appropriate balance must be struck.

> *'When you start to scratch away from the surface, you hear, "actually, no, that did go wrong", or "actually, yes, we didn't consider how these risks link together"… there's almost like a sort of bravado that you often hear about: "of course, we do this stuff". But it's the question of when should you have more explicit and formal consideration of risk: at what junctures will that add value?'* (Focus group member).

It should be emphasised that while boards following a principled approach were more likely to make connections between strategy and risk, this does not guarantee that they will make successful connections. Equally boards following a prescriptive approach may be just as capable of connecting strategy and risk and when they do so are likely to make more considered and consistent decisions. Each type of organisation has to work to overcome its own limitations in this regard. 'Principled approach' boards should guard against excessive opportunism and inconsistent risk-management decisions, and find ways to anchor their discussions, linking back to the organisation's risk appetite statement, for example. In contrast, prescriptive approach boards should avoid focusing too closely on internal controls, as this may cause excessive risk aversion and a failure to exploit value-enhancing strategic opportunities.

2.1.3 Risk appetite and setting parameters

One concept that can help to improve the decision-making consistency of more principle-oriented boards, and help to overcome the negativity associated with the prescriptive approach, is risk appetite. Most of the participants used the concept in their organisations to some degree, although it appeared that there was little agreement on how to express this in a quantitative way. Often risk appetite might be expressed qualitatively in terms of risks that organisations might want to take or avoid, or less explicitly in terms of organisational values and ethics (eg attitudes towards compliance breaches, misconduct).

Participants said that a key benefit of thinking about risk appetite was to help boards set the parameters within which the executive directors and wider senior management team could operate on a day-to-day basis. This approach provides clarity about the risks that may be taken and those that should be treated with caution, as well as how risk-management activities and processes should be conducted across the organisation. Setting parameters is hard if there are no clearly defined quantitative limits: but the following comment indicates that there is readily available information to support the process.

> *'So the classic thing, zero harm – we've got no appetite for something – it's a complete misunderstanding of what risk appetite is. There is a wealth of metrics and information out there that you can tap into to articulate statements in a way which will actually add practical guidance to a business, and you'd be able to measure whether you're operating within those parameters. But a lot of companies are just nowhere… they're still doing the sort of high, medium and low, hungry-averse-type scales, which are just worthless'* (Focus group).

2.1.4 Culture, communication and risk

An organisation's culture can have a significant effect on how people within the organisation behave and communicate with each other. This can influence the tendency for misconduct as well as how risk and risk management are perceived (eg whether risk management is seen as a business enabler or bureaucratic red-tape) and reported. Events such as the Barclays LIBOR scandal clearly illustrate such connections (Salz 2013).

On organisational culture and the specific aspects of culture related to risk taking and control (so called 'risk culture'), participants claimed that culture was not discussed in an explicit way by most of the boards in the sample, and risk culture was hardly ever discussed or understood as a discrete concept. Outside financial services, only two boards regularly discussed culture in relation to risk and this was because one was in a people-focused business and the other had a risk director responsible for focusing on culture, and risk culture in particular.

Those with a top-down approach put a greater emphasis on maintaining board independence and the avoidance of it becoming overly operational.

Other non-financial services organisations only discussed culture at board level on an ad hoc basis, for example in relation to major change projects, or the appointment of a new CEO or chair. Risk culture was not generally discussed by non-financial organisation. In contrast the boards of all the financial services organisations in the sample looked at culture and explicitly at risk culture. Regulation was cited as the main reason for this.

Outside financial services, attempts to assess culture formally may have been rare, but the value of doing so was recognised by some of the participants:

> *'…you've got to have a definition of what you think the culture is. And then you've got to have metrics which help you determine whether that culture, in fact, exists. And those…might involve employees' feedback surveys, discussions with focus groups of employees... There are practical steps that boards and management take to determine whether … the culture they aspire to is, in fact, the culture that is operating in the business.'* (Non-executive director)

On the subject of communication many of the participants did make links between this and culture, and in particular the importance of an appropriate 'tone from the top' in relation to risk taking and control. Several of the participants also emphasised the importance of the board's 'talking the talk' and 'walking the walk' to ensure that people within the organisation would believe that the board took the management of risk seriously.

Opinion was split on how communication between the board and the wider business should be achieved. In some organisations, boards communicated via the executive team and communication tended to be top-down. In others, non-executive members of the board communicated directly with a range of people, not just the executive, and communication was more integrated. Those with a top-down approach put a greater emphasis on maintaining board independence and the avoidance of it becoming overly operational.

An SME Perspective

Investigating the role of the board in strategy governance, performance and risk identified some findings specific to SMEs that are worth highlighting.

A number of participants had executive and non-executive director experience with SMEs. These directors commented that SME boards tend to be more innovation-focused and will get involved in entrepreneurial activities. They said that this is driven in part by the need for SMEs to innovate to survive in highly competitive marketplaces (as they often have less financial security or brand reputation to fall back on than larger organisations), but it was also a consequence of increased agility and the closer proximity of the board to the wider business. SME boards appeared to be able to make strategic decisions to exploit new opportunities that could be implemented quickly.

Nonetheless, it was also observed that SME boards can be more short-term and reactive in their approach, primarily because of their higher risk of failure. Formal risk management conversations were comparatively rare in participant SMEs, suggesting a more principled approach (in the sense used in section 2.1.2 above). In general, risk management was considered formally only once or twice a year, in relation to topics of regulatory significance such as health and safety.

SME board members were also much more likely to have closer communication with the wider business, and some of the SME participants with risk-management expertise were helping their organisations to drive significant improvements in practice. Participants explained that the smaller size of SMEs made it easier for board members to get to know the wider management team of their organisation. In addition, board members may possess skills that are not present anywhere else in the organisation (eg specialist knowledge of risk management) and that enable the business to be driven forward.

> Significantly, there appeared to be an increasing recognition of the importance of board-level risk discussions.

2.2 DRIVERS FOR BOARD INVOLVEMENT IN RISK MANAGEMENT

This section is concerned with key drivers that participants believed were prompting risk discussions and activities in boardrooms. The responses may be, to some degree, regarded as reflecting the spectrum identified in section 2.1.2. On the one hand, a number of the motivations identified could be considered to fall within a strategic, or value creation, perspective. On the other hand, another set of motivations might be regarded as inclining more towards a regulatory governance, or value preservation, perspective. Significantly, there appeared to be an increasing recognition of the importance of board-level risk discussions.

The themes presented below are ordered according to the importance assigned to them by the participants. Regulatory drivers were by far the most cited reasons for board-level risk discussions and activities.

2.2.1 Regulation and compliance – requirements and influences

The direct impact of regulation

Legislation, regulatory requirements, corporate codes and professional codes of conduct were regarded by many participants as having a direct effect on attitudes and practices in relation to risk management. There was an acceptance that sometimes this might lead to a 'tick box' approach:

> *'..I do think there are times when you do need to tick some boxes, by the way, because you have lists of compliance matrices that you have to follow, and you have to show that you've followed them, and the best way of doing that is to tick a box to say that you've done it.'* (non-executive director)

Nonetheless, some also recognised that adopting a 'compliance mind-set' reflected the more prescriptive approach to risk management outlined in section 2.1.2, a situation that may foster excessive risk aversion: 'it's the mind-set of actually, rather than helping us take risks better it's about not taking risks at all' (executive director). It was also clear that many saw the influence of regulation and regulators at work directly in day-to-day risk-management practice in areas of risk such as governance, culture and strategy. Specific examples are set out in Table 2.1.

TABLE 2.1: Examples of regulatory influence on boardroom decision making

AREA OF REGULATORY INFLUENCE	EXAMPLE
Risk appetite Boards are more conscious of their role in risk oversight	*'The risk-appetite framework and risk-appetite statements are very much something that the board seems to feed into. We are seeing,… through regulatory pressure, to evidence more what the board are actually doing in the oversight piece'* (executive director)
Committee structure Board members may not be clear as to the responsibilities of the committee versus the board	*'If the regulator wants the board to be more collectively involved in everything,.. why make us have separate committees?'* (executive director)
Board member responsibility The role of chairman in setting the culture is clear in the current regulatory framework	*'There's a prescribed responsibility for culture within the organisation that resides with the chairman. And our chairman is fairly conscious of ensuring that he can fulfil that...'* (executive director)
Horizon scanning and scenario planning Some boards are actively using horizon scanning and scenario planning in fulfilling their oversight responsibilities. This may include the use of internally generated scans and external resources, such as risk reports by regulators.	*'There's some really good external publications that are put out by the regulator…they'll do a review themselves of all of the concerns and risks that they've identified through the course of the year…[and]…more broadly looking forward as well and thinking, what are the things that are keeping the regulator awake at night?…that's a key document really for any kind of … audit and risk committee to be poring through and saying, right, here are the 10 risks the regulator has identified as being really key and on its mind.* *'Where do we sit against these 10 risks? What are we doing in relation to these 10 risks? Are these risks we're aware of? We do that exercise proactively…cross-check or cross-reference to say…these are the key risks, these are the ones that appear on our register, these are the ones that don't appear on our strategic risk register, and these are the reasons why. This is one that… we didn't have previously as a risk. We've rated it here. It's not on a strategic, [but] it's on an operational risk register'* (executive director)

> Non-executives need to be assured that executives have ensured there is an appropriate risk-management framework that is operating effectively.

Regulatory requirements and statements influence the strategy, structures, practices and behaviours of organisations in more or less subtle ways. This is also having an effect on risk-management practices among organisations operating within less-regulated sectors. Firstly, board members who have worked in regulated environments appear to see the benefit of transposing these regulation-driven, risk-management practice into other organisations.

> *'I joined the board…and we also had a new chairman at the same time and we both come from working in a highly regulated environment…and we were a little surprised at the lack of risk expertise and focus on risk that we found when we joined the business so I think it's probably fair to say that the impetus [for changing things] was driven by the chairman and then myself with the recognition that really we have to get the organisation up to speed … around risk'* (consultant).

Secondly, there is also recognition that even in less regulated environments boards are nevertheless being held more accountable for their decisions by stakeholders.

> *'In a non-regulated organisation the risk has always been there, but … I'm seeing in some of the stuff I've done more of a move towards, not the level of stuff that's expected by the FCA from a regulated body, but it's a move towards that direction, a greater scrutiny, a greater… assessment. … The concept of holding to account of directors by shareholders is out there and it's coming with a bit of a force'* (non-executive director).

Embedding regulatory impact within organisations

Participants spoke of the increasing recognition and importance of risk, and risk management practices, at board level. This attitude, and the pervasiveness of the influence of regulation discussed above, was reflected by a number of the participants in discussing the relevance of risk culture, or their role in embedding risk awareness, in their organisation.

> *'One of the things that… is generally accepted [is] that boards need to be involved in…agreeing … what the overall risk appetite of the business is. How can you do that if you don't understand the concepts of the culture in which risk appetite is articulated and agreed, because they're entwined with each other. They're part of the same thing'* (non-executive director).

From a board perspective, this is important for two reasons. Firstly, and as has been a key theme of financial regulators (FSB 2014), if the 'right' risk culture is embedded in an organisation then this provides additional assurance to a board about the effective operation of the organisation's risk framework. Secondly, it explains the importance that many of the participants placed upon 'tone at the top' and the non-executive board members' understanding of what was happening on the ground and checking this against their experience at board level.

> *'First of all, the tone has to come from the top so if your…board thinks about risk management in terms of…a compliance exercise, it will always remain a parallel process. It will never be embedded in the day-to-day work, in the day-to-day operating model of the company. And therefore it will never be part of discussion at board level'* (executive director).

The report will further discuss the importance of the board's understanding of what is happening on the ground in the wider organisation in section 2.3.

2.2.2 Oversight: reputation and emerging risks

Governance and oversight of their organisations was often mentioned by participants when discussing the importance of risk at board level. This was often associated with compliance. Non-executives need to be assured that executives have ensured there is an appropriate risk-management framework that is operating effectively. In this context of governance and oversight, two specific drivers were mentioned consistently: reputation and emerging risks.

Board role in protecting and enhancing reputation

> *'Reputation is kind of an interesting one, because it tends to be an underestimated risk by management, I think, and yet you can point to examples in the public domain where people have suffered quite badly from reputational risk or having a bad reputation for something…'* (non-executive director).

What was stressed by a number of participants was the need for discussion of risk at a strategic level ... in order to be able to take advantage of opportunities.

This was emphasised particularly by organisations that were customer facing, focused on ensuring they had the trust and confidence of their customers. For example, the significance of this issue for oversight and governance is apparent in the experience of the financial services sector and its efforts to gain or regain the trust of the general public after the financial crisis of 2007–8.

While discussions about reputation often took place in the context of protecting value – perhaps the more customary 'defensive' risk governance perspective – it was also recognised that effective management of risks to reputation could also enhance reputation:

> *'And we've seen some of that in the last five years, I would suggest in some of the cyberattacks that have happened to major organisations. Some have handled them very badly and have upset their customers and had their reputation damaged. Others have managed it really well, really transparently and have done a great deal to enhance reputation, and in fact their share price'* (consultant).

Emerging risks and incidents

A wide range of external events (eg sectoral risk events, political and socio-economic events, media reports) were reported as common drivers for board-level discussions about risk:

> *'Boards don't know what they don't know. So, if something happens outside that you believe will have a substantial impact on the business, the board then has to have a conversation about it'* (non-executive director).

In turn, this echoed participants' discussion of the importance of the diversity of the board in bringing a range of ('outside') expertise and experience to risk discussions (see section 2.3.1 for further discussion of board diversity); of scenario planning as a tool for anticipating new or developing risks (such as cyber risk); and of horizon scanning in actively researching and examining the implications of what is happening to competitors and similar organisations, as well as in the socio-economic environment in which the business is operating.

2.2.3 Strategy – value creation, risk appetite and the pursuit of opportunities

In addition to regulation and compliance as a driver of board-level risk discussions, participants also emphasised strategic drivers. This echoes again the prescriptive-principled spectrum discussed in section 2.1.2.

What was stressed by a number of participants was the need for discussion of risk at a strategic level – not at a level of governance and oversight that dwells on risk registers and frameworks – in order to be able to take advantage of opportunities.

> *'What really could unseat the strategic objectives of the business? What really are those opportunities that the business might be missing because it's too conservative in its risk appetite. And then real discussions are not so much risks, but they are issues that affect the risk and the environment in which the organisation is trading. And it's absolutely vital that the board has the opportunity and the education to allow them to have those kinds of discussions'* (non-executive director).

In having these discussions, participants emphasised how important it is that a clear understanding of the organisation's risk appetite is embedded in strategic decision making. It was also suggested by some participants that this is key to acting strategically in a fast-moving environment:

> *'in order for the board to achieve their strategy, people needed to be doing things differently, faster and making different decisions. So that was actually key about making sure that the risk appetite in the business or the definition of risk in the business underpins the strategy. They couldn't do the strategy without that right risk appetite'* (executive director).

This reflects back to the discussion in section 2.1.1 concerning the relevance of risk in strategy setting.

> Throughout the interviews and subsequent focus groups, it became apparent that diversity was central to a board's ability to manage risk.

2.3 BOARD SKILLS AND EXPERIENCE

This section considers the skills and experience that are brought to bear on strategic decision making within the boardroom in relation to risk management.

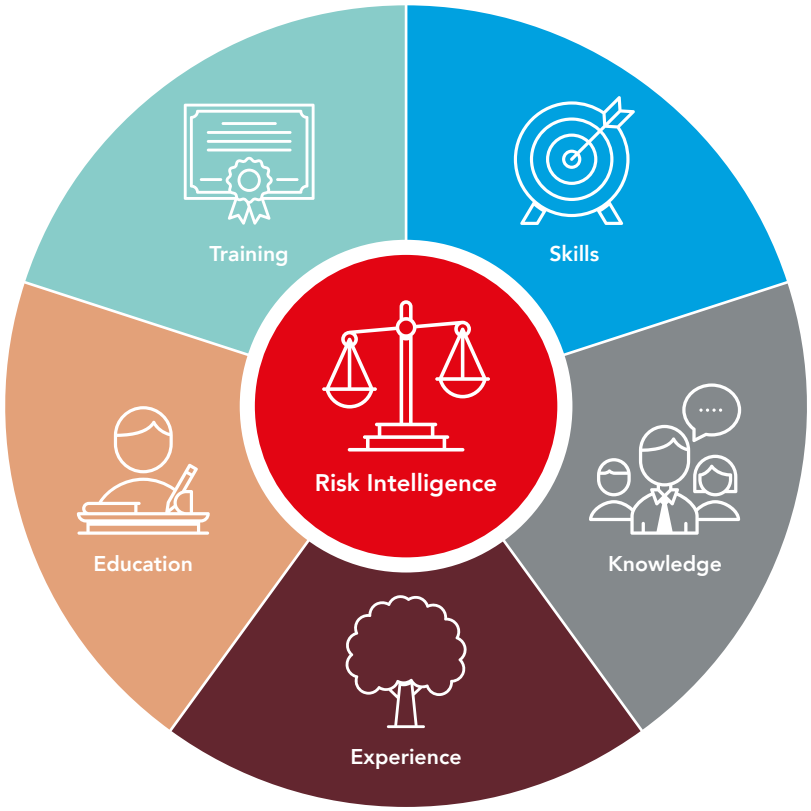
> *'Understanding risk management, the risk–reward equation, is fundamental to the role of the board'* (non-executive director).

2.3.1 Board diversity – Risk skills, knowledge, experience, education and training (RI-SKeet)

Throughout the interviews and subsequent focus groups, it became apparent that diversity was central to a board's ability to manage risk. This concept of diversity (in its broadest sense) was especially pronounced when discussing the composition of NEDs required to enable the board to understand the 'risk-reward equation'. This diversity came in various guises throughout the interviews, summarised here as **R**isk **I**ntelligence, **S**kills, **K**nowledge, **E**xperience, **E**ducation, and **T**raining (**RI-SKeet**, Figure 2.2). The enrichment and enhancement of strategic decision making brought about through RI-SKeet ensures a collective board intelligence that is balanced, allowing it to understand fully the dynamics of the risk–reward equation.

Diversity was also seen by some participants as a way of 'de-risking' the board, broadening opinion and enabling non-executives to pool their RI-SKeet. In addition, RI-SKeet was regarded as a source of competitive advantage for organisations.

FIGURE 2.2: RI-SKeet



> *'If you have an organisation, for example, that's had a board composed of people who've come up through the ranks, understand the culture of the organisation and understand what really makes it tick and how things, how politics work, and how communication really works in practice, and you have non-execs who all come from the same industry, then you have a board that is very good at understanding what I would describe as internal risk…[But] if they lack true exec and non-exec members who have come from outside of the organisation and ideally outside the industry, then they will lack that external perspective and there will be a lens around the board room table that is missing'* (consultant).

> The ability of a board to anticipate risk and identify opportunities underlines how strategic decisions may be enhanced by a diverse RI-Skeet board.

The ability of a board to anticipate risk and identify opportunities underlines how strategic decisions may be enhanced by a diverse RI-Skeet board. Such opportunities may not be as apparent to executives owing to their involvement in the day-to-day workings of the organisation. A highly functioning board with good RI-SKeet can provide an accelerator and a brake when considering the risk-reward equation as part of its strategic decision making.

Ensuring boards remain risk-relevant

Organisations within the study have, through a number of mechanisms, actively sought to increase RI-SKeet within their boardrooms in an attempt to ensure that consideration of risk is embedded in strategic decision making.

A large proportion of organisations in the sample employed board skills matrices and audits to evaluate areas of perceived overlap or insufficiency on their board. As one participant stated:

> *'one of the things we do is a skills audit, or skills review every now and again, to say what are we missing, what skills are we missing. We type [sic.] that into our strategy as well' (non-executive director).*

The organisation referred to in the above quote was a relatively small SME operating in the third sector, yet it still recognised the importance of aligning the board's RI-SKeet to the organisation's mission and business model. Matrices and subsequent audits of board skills in RI-SKeet become particularly important when bringing non-executives on to the board, as this is seen as an opportunity for ensuring that the board remains risk-relevant while 'future proofing' against the ever-changing business environment in which the organisation finds itself.

Board transition arrangements are not the only means of ensuring that a board remains diverse in RI-SKeet. A number of participants, both executive directors and NEDs, highlighted the importance of ensuring that the board knows the business, is aware of its idiosyncrasies, and understands the culture of the business on the shop floor, as outlined in section 2.1 below. This process of 'kicking the tyres' by getting out of the boardroom and into the business itself was seen by some as a process that allows the board to ensure they are risk-relevant, getting a sense of the 'qualitative' that is so often lost in risk registers.

> *'I know the chairman of one company… they [sic] always have their lunch with the employees, they never go and sit in a separate dining room. And when they say you can come and have a chat with me and tell me what you think they mean it…I think it's something that a lot more boards are doing now than they ever did before. They cannot hide away in an ivory tower, they need to actually understand the business. If you're going to govern something you must have a decent level of understanding, otherwise how on earth can you govern?'* (non-executive director).

Case study: RI-SKeet in the boardroom

An SME third-sector investment company with credit risk ratings higher than would be found among commercial lenders was required to develop a risk register and robust business strategy as part of its funder's conditions of business. In order to do so, the board went on an away day to determine the principal risks to the business and discuss how they fitted within the company's strategy and mission. In doing so, the board was then able to use its RI-SKeet matrix to determine the most appropriate director to take ownership of that risk on the risk register, thus providing accountability and leadership of those risks from within the boardroom.

A qualitative understanding of the business also allows NEDs to obtain assurances about what they are hearing within the boardroom.

> *'What you don't want to happen is that the chief executive is telling you everything's rosy in the garden, but when you go out in the field, you find that all the things that you've been told are rosy aren't really happening'* (non-executive director).

The presence of gaps in board RI-SKeet was not uncommon throughout the study, with a particular emphasis on emerging areas of potential exposure. For example, the effects of merger and acquisition on the risk-relevance of the board and the prevalence of cyber risk in organisations were seen as particularly pertinent by

Risk specialists also enhance the risk-relevance of a board through facilitating the explicit discussion of risk at away-days, in which time is dedicated to strategic 'deep dives' of risk issues.

some participants, with the latter being related on multiple occasions to a well-known large-scale hacking event in a telecommunications company.

This event provided boards with a near-miss scenario that placed cyber risk as a focal point of discussions within the boardroom. It was apparent that potential near misses (proactive) and actual losses (reactive) were extremely important in prompting explicit and strategic risk discussions in the boardroom. This emphasises the significance of such events as a driver for risk discussion (as outlined in section 2.2).

It was also clear that boards use the expertise of external and internal risk specialists in an attempt to provide RI-SKeet in areas in which they have a particular lack of expertise. While this is especially common in relation to financial misstatement risk, via the use of external auditors (the risk specialists for financial misstatement risks), it was suggested that the use of other types of risk specialists (eg cyber risk or health and safety specialists) was just as relevant for other areas.

> *'Having finances misstated is a risk, and therefore [external] auditing is well known [as a means of mitigating financial misstatement risk] and everybody assumes it's there. But doing the same on health and safety or on IT is also, to me, a logical step, if that's one of your risks'* (non-executive director).

Risk specialists also enhance the risk-relevance of a board through facilitating the explicit discussion of risk at away-days, in which time is dedicated to strategic 'deep dives' of risk issues.

Case study: using external specialists to enhance RI-SKeet

In the aftermath of two publicly reported hacking incidents it was acknowledged by a manufacturing company that its board's RI-SKeet regarding the cyber domain was weak. The board supplemented the relevant RI-SKeet by bringing in an external specialist to advise the members; during this audit, the company actually came under attack by a foreign entity attempting to steal intellectual property. It was acknowledged that had the board not been proactive in obtaining this expertise it would have been a 'disaster' for the company as its products could have been made available on the grey market.

These discussions are further supported through the use of scenario exercises that allow the board to understand its members' strengths and weaknesses in prevention of and responsiveness to risk, as well as the pressure points around RI-SKeet, risk ownership, and risk appetite that require attention.

In order to ensure that boards remain risk-relevant, and taking into account the findings of skills matrices, audits and scenarios, there was an understanding from participants that training is beneficial, particularly for 'killer issues'. Even so, this attitude was not unanimous, especially among participants in the SME sector, where risk training (whether in-house or external) at board level is less prevalent. This was articulated by one executive director, who stated that the reason there was not enough board training was because it is generally assumed that risk management is something anyone can do, because they do it unconsciously every day.

2.4 BARRIERS TO BOARD INVOLVEMENT IN RISK MANAGEMENT

This section examines the barriers that prevent a board from managing risk effectively. The research objective was to identify common barriers that can impede the functioning of a risk-sensitive board.

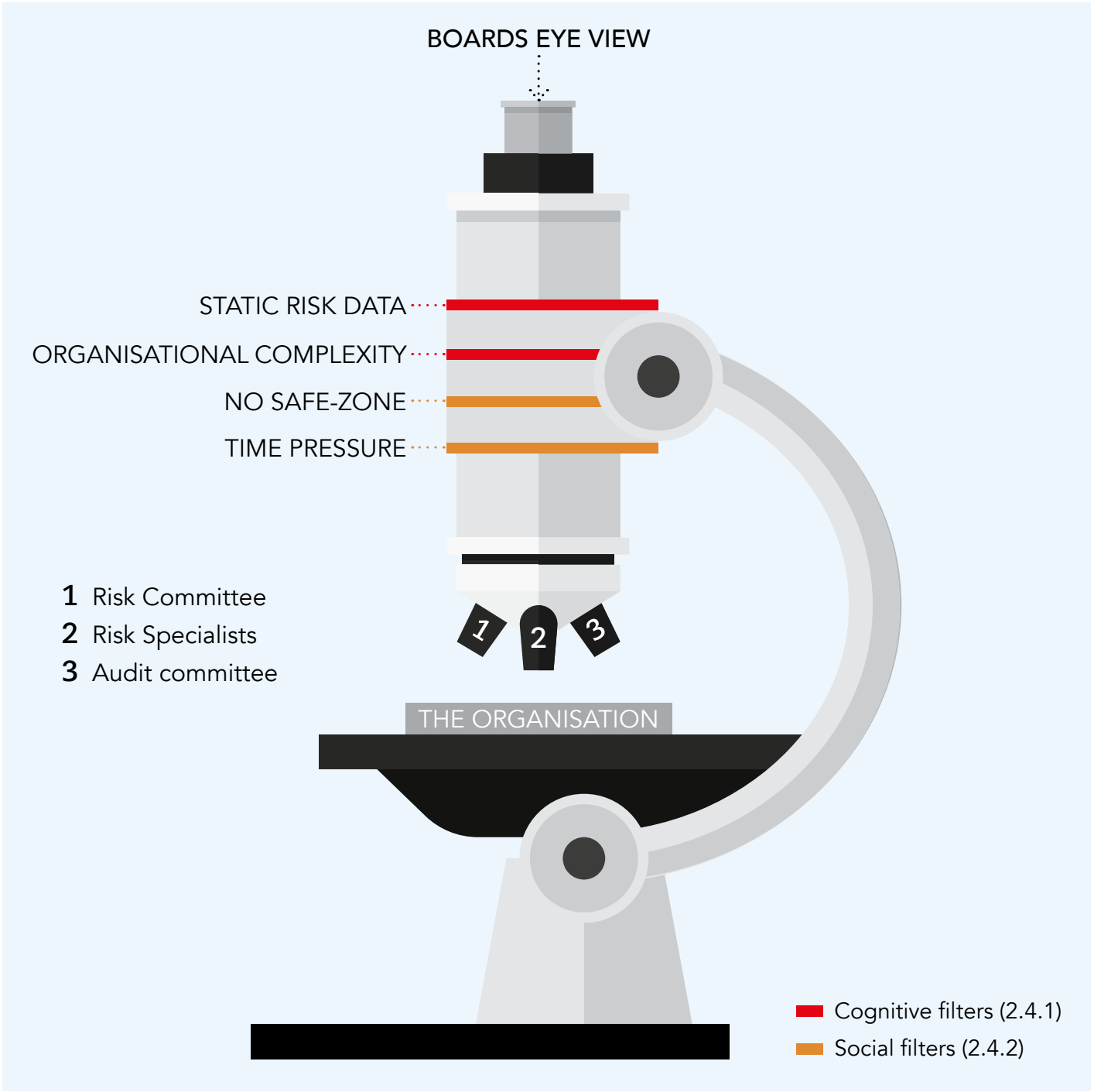
> *'The problem with risk is that if you don't keep it alive it will die'* (executive director).

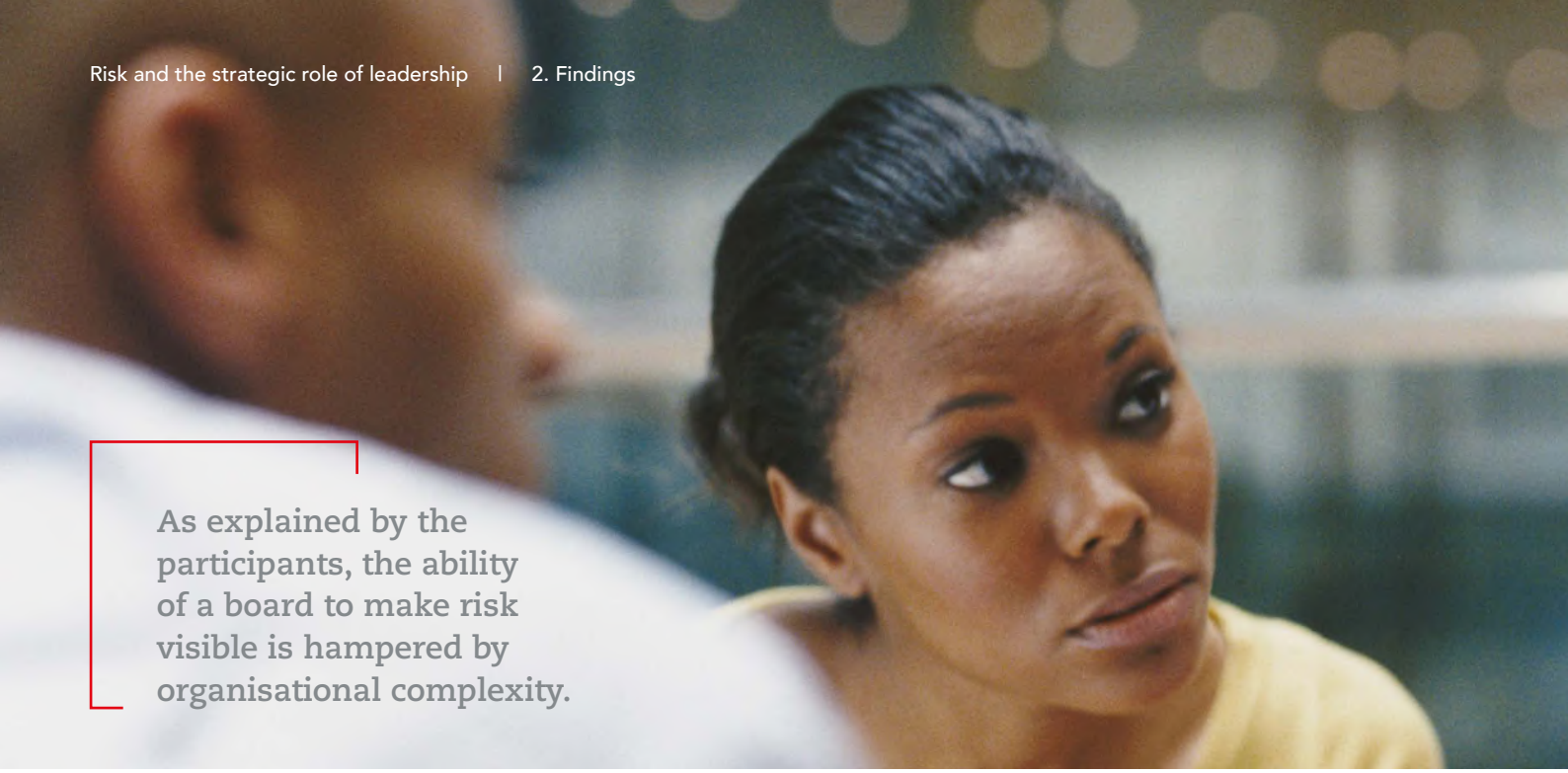
Many participants made it clear throughout the interviews that, in order to be able to consider risk strategically, boards need to be aware of, and understand, how risk 'lives' in their organisation. Risk needs to be alive and visible at board level to enable meaningful discussion. Yet, the process of making risk more visible to the board is fraught with difficulties as there are multiple barriers that inhibit this from occurring.

It is evident from the interviews that the majority of these barriers fall within two categories; these are '**cognitive impediments**', which reduce a board's ability to make risk-sensitive strategic decisions, and '**social obstructions**', which suppress risk-relevant dialogue in the boardroom. As shown in Figure 2.3, the board's-eye view of the organisation becomes blurred because these barriers filter out a holistic view of the organisation. It is also important to note

> To bring risk back into focus, the board may make use of various committees and specialists as lenses through which to see the organisation closely.

FIGURE 2.3: A boards eye view of the organisation





As explained by the participants, the ability of a board to make risk visible is hampered by organisational complexity.

that the presence of 'social obstruction' may facilitate the creation of a 'cognitive impediment' and vice versa.

To bring risk back into focus, the board may make use of various committees and specialists as lenses through which to see the organisation closely. However, our participants observed that the existence of these risk focal-lenses does not sufficiently compensate the loss of vision caused by these barriers. Therefore, participants considered it important to reduce the internal barriers to increase the ability of the board to obtain a holistic view of the organisation that is grounded in knowledge and understanding.

2.4.1 Cognitive impediments

Cognitive impediment 1: Static risk data

The majority of respondents, regardless of industry or scale of operations, emphasised that the single largest impediment to a functioning, risk-sensitive board is the inability to obtain an adequate view of the health of the company through the board papers. The ability to move away from vast static risk registers that are essentially backward looking, towards a dynamic view of the real-world impact of risks on the activities of the organisation, was something that many have aspired to, but few have actually achieved, in their board's approach to risk registers. All too often, and much to the disappointment of some participants, the use of risk registers was seen as a 'tick-box' exercise characterised as compliance, as opposed to one of many sources of information pertinent to strategic decision making.

In an attempt to ensure that standing items on risk registers do not lead to complacency, some participants highlighted the importance of focusing on 'emerging' and 'moving' risks. This approach has three benefits. Firstly, it ensures that information going to the board remains relevant and forward-looking. Secondly, it ensures that the board does not become overly involved in operational issues arising from the risk register, as highlighted by one executive director: *'If they start talking about the 99th risk on the register, they're getting too much into the operational'*. Thirdly, providing information on developing risk situations enables risk conversations that help to mitigate potential losses and exploit strategic opportunities.

The ability to provide a bottom-up synthesis of information that makes the invisible visible, while reducing the overburdening amount of risk information the board receives, can improve general enquiry and strategic decision-making within the boardroom.

Cognitive impediment 2: Organisational complexity

As explained by the participants, the ability of a board to make risk visible is hampered by organisational complexity. This complexity makes the setting of decision-making parameters difficult for boards. This is further accentuated by static risk data that is backward looking and potentially irrelevant to challenges the business currently faces internally and within its environment. As outlined by one participant:

> *'the big complex ERM systems, which take an enormous amount of time to gather [information on], and information is providing a picture of what was, as opposed to…what is currently pulsing around you in the organisation'* (executive director).

Case study: when static data (*unfortunately*) becomes reality

A company was considering a large-scale IT reconfiguration project throughout its business operations. During this process, a crucial strategic decision on whether to proceed with the project was brought to the board for consideration. Given the time it had taken to implement the project, by the time the end-to-end system was fully implemented the business had changed its strategic direction and the system was no longer fit for purpose.

It turned out subsequently that the report presented to the board contained many technological terms, and detailed a combination of risks associated with the functionality that was being designed and their relevance to the changes of business strategy. When an investigation as to the cause of delay had been completed, it turned out that the board had found the report difficult to understand owing to the volume of technical terms contained. As a result, the board had been unable to consider the issues effectively and efficiently when considering the viability of the project.

Further, in the context of the 'prescriptive' and 'principled' approaches to making decisions on strategic risks outlined in section 2.1.2, it was suggested that more complex 'principled' organisations should have visible anchors to ensure that business critical issues are not missed, for example risk metrics and currently significant risks from the risk register.

Participants also noted that the time made available for effective risk-management discussions may not be adequate.

'If somebody is doing a good job…they are smartly and honestly saying 'here are the three things we are most worried about at the moment' (executive director).

By contrast, more complex 'prescriptive' organisations may get lost in the detail and become overly risk averse in their approach to strategic decision making. Given the effect of static risk data and organisational complexity on decision making within the boardroom, participants emphasised that audit and/or risk committees create a vital conduit through which to ensure the timely flow and filtering of relevant information to the board. It was unfortunate in the above static data case study that this practice was not conducted sufficiently thoroughly, and the consequences of this were sizeable for the organisation in question. The ability of these committees, along with the support of risk specialists, to reduce the cognitive burden on board members allows the board to focus its RI-SKeet on making better decisions on strategic risks.

2.4.2 Social obstructions

Social obstruction 1: Risk safe zone

'The fact that challenge is there makes the executive work harder' (non-executive director).

Turning to the social obstructions to board involvement in risk management, participants noted the difficulties associated with enabling debate and challenge in the boardroom, especially when discussing sensitive risk-management issues (for example, 'bad news' events such as major fraud or reputational damage). To help facilitate debate and challenge, a number of participants recommended creating a 'safe-zone' atmosphere for risk-management discussions, where constructive dissent and disagreement is encouraged within a non-judgemental and supportive environment.

This creation of a safe-zone in which concerns around risk at board level can be expressed freely and without discrimination allows RI-SKeet to be used more resourcefully. This resourcefulness arises from improved transparency and increased trust within the board because it allows non-executives to speak 'truth to power' (executive director), while respecting the insights of the executive (see also section 2.5.2). This ability to create an open and transparent arena for discussion alleviates the psychological burden of challenge:

'in a really deep personal level it's really tiring to consistently put yourself in the way of asking the difficult questions' (executive director).

It was acknowledged by one of the participants that the creation of a 'safe zone' can be taken a step further by holding separate non-executive 'in-camera' sessions. The specific function of these is to allow for the candid and transparent discussion of risk without the presence of the executive team. This is particularly effective in mitigating the effect of dominant executive personalities, when a 'command and control' dictatorial approach to strategic risk in the boardroom may run contrary to the board's effective performance of its assurance function.

Social obstruction 2: Board sensitivity to time pressure

'I think time is a big factor; do they spend enough time specifically talking about risk [rather] than talking about strategy? I think that's an issue' (executive director).

Irrespective of the development of a safe zone, the nature of the risk data, or the complexity of the business, if a board does not have adequate resources and time to undertake risk-management activities it will struggle to carry out its role satisfactorily. Participants noted that, without the time to employ RI-SKeet effectively within the boardroom, the natural tendency would be to focus on the downside while supressing upside considerations. This places more emphasis on the importance of away-days, for example, to allow the board to give undivided time and attention to focus on risk, as outlined in section 2.3.

Participants also noted that the time made available for effective risk-management discussions may not be adequate. One of the key reasons why this is so, is that it can be perceived as a bureaucratic hindrance, getting in the way of what are perceived to be more immediate board-level concerns. Among the participants' firms, this was particularly common in environments that are dynamic and fast-paced, especially where boards are reacting to events rather than taking more proactive control. This bureaucratic hindrance perspective was explained as follows: *'I think risk gets a bad press, a bad name, because it's seen as a box ticking, very routine, that doesn't add value'* (non-executive director).

Some participants argued that executives are the risk owners, with the board setting the parameters and assessing the risk controls.

2.5 EXECUTIVE AND NON-EXECUTIVE CONVERGENCE AND DIVERGENCE

The participants generally accepted the importance of risk management in board deliberations. This section considers divergence and convergence in the roles of executive and non-executive directors when managing risk at board level, as well as the role of other risk specialists in supporting them.

2.5.1 The role of the board

There is no distinction in law between the executive and non-executive directors on the board of a company (although there can be a distinction in not-for-profit and charity organisations). When describing the role of the board in relation to risk, unity of purpose was reflected by various participants, and centred on the issue of (risk) governance.

> *'So absolutely, there's a very important role for the board to play, but they are not the executive. They are the governance. And I do think sometimes people get a bit mixed up about what the role is. And the role is not to manage the company. The role is to govern the organisation…*
>
> *'If you have a crisis, it is not the role of the board to jump in and manage the crisis, that's an executive role. The board's role is to make sure that the business has a crisis team, that they're properly resourced, properly rehearsed, and can give comfort to the board that if something goes wrong, they know that the organisation is prepared and will cope with it'* (non-executive director).

Nevertheless, some participants argued that executives are the risk owners, with the board setting the parameters and assessing the risk controls. On this role of the board, participants emphasised the importance of non-executives, and the following statement is typical:

> *'the big difference is that they… [are] able to take that more independent, strategic view as a non-executive, that's harder to do as an executive. And I think the lines should be very clearly drawn between the two, because if it starts, that blurring of lines then that can be difficult for the executive. But also when non-executives do have to take that step back and exercise some independent judgement, that can be very hard, if [they are] too involved in the day-to-day or too close to the day-to-day management of the business'* (non-executive director).

The blurring of responsibilities may arise where non-executives have been brought onto the board specifically because of their expertise:

> *'what you find happening is that non-executives are brought in because of a specific area of expertise and they spend their life second guessing the executives, which of course leads to enormous frustration'* (executive director).

Participants indicated that smaller, particularly owner/manager, organisations can experience particular problems in maintaining this divide:

> *'one of the things that is really difficult… is that there are no distinguishing elements between direction and management… So that distinguishing between what is strategy and what is operational is quite blurred…and always the operational imperative will trump the strategic perspective'* (non-executive director).

2.5.2 The 'critical friend'

When discussing governance and the management of risk, some participants did so in the context of a board's relationship to the managers in the business.

> *'But I think the board can step aside and see the bigger picture and identify more global risks, maybe, that could have an impact on the business that the executives at the lower level [non-board senior management] wouldn't be able to see'* (executive director).

Nonetheless, the majority of participants discussed this supportive and inquisitive relationship in the context of the relationship between executives and non-executives at board level. Thus participants variously referred to non-executives bringing to the board:

- an external perspective (non-executive director)
- positive challenge and holding to account (non-executive director)
- objectivity (executive director)
- an 'additive' input (non-executive director)

> Participants were also clear about the effect that different personalities can have on board dynamics and resultant risk-management outcomes.

- support and the right parameters (non-executive director)
- oversight (executive director)
- influence (non-executive director)
- critical friend (non-executive director).

The 'critical friend' concept captures both the support and the rigorous examination that participants expected NEDs to bring to an organisation and to the executive directors in their running of that organisation, to ensure the effectiveness of the board.

2.5.3 Different perspectives and board dynamics

The participants drew attention to the different perspectives that executives and non-executives bring to the operation and decisions of the board.

> *'… the execs bring experience, detail, track record, you name it from the business. The non-executives bring dispassion … without emotional investment … the execs bring depth, then the non-executives should bring breadth and bring … to bear their experience they had from other areas'* (non-executive director).

Participants went on to suggest that the NED's job is to provide support through constructive input and suggestions for optimising risk-management decisions, while it is the executive's job to think of the practical solutions for the implementation of these decisions. Participants were also clear about the effect that different personalities can have on board dynamics and resultant risk-management outcomes:

> *'if you've got some people that are really passionate about it and have the trust of the board then [they] can revolutionise the way a board looks at risk. If you haven't got somebody [who is] passionate and [who] doesn't really get it, then it becomes fairly piecemeal and fairly, sort of, part of what happens'* (non-executive director).

It was also noted that the stability of a particular business or industry can have an effect on the board's approach to risk. A key concern expressed by some participants was that 'cosy club' type cultures can emerge in benign risk environments, leading to complacency and a lack of challenge in the board room.

> *'In some businesses, where things tend to be very, very stable, the non-execs tend to be a little club, they just come in and they meet, and they go through the motions, but because the environment is stable, then they tend to be fairly tame at meetings. We've got completely the opposite, where they come in, they aren't aggressive, but very challenging, simply because they recognise transformation puts the business at enormous risk'* (executive director).

Overall, participants observed that managing the mix of characters, in what one participant referred to as the 'theatre of the board' (executive director) was regarded as key in enabling the discussion of risk at board level. The same participant also noted how this extended to the management of board meetings themselves, especially when agendas are large, limiting discussion and challenge (see also section 2.4).

2.5.4 Risk discussion at board level – the critical space

A theme emphasised by a number of participants was the distinction between 'ensurance' and assurance – where the role of the executive directors is to ensure that the organisation's strategy is implemented, and NEDs assure that the implementation is performed effectively and is consistent with the agreed strategy.

> *'We very often think about the role of the board being fundamentally about the assurance in terms of safety of the overall organisation – reputation, cost of return on capital, all of those issues; and the executive is responsible for the "ensurance" of the way in which assets are deployed in the organisation, and how you have as a board a sensible, meaningful conversation about that interrelationship seems to me to be absolutely critical – it's a critical space …'* (executive director).

The risk and/or audit committee was seen to act as a filter for the board, with a more succinct discussion taking place at board level.

A distinction was also made between executives and non-executives' roles in the management of risk. Outside the board, executives were responsible for day-to-day risk taking across the organisation, while the board itself, and in particular NEDs, kept a degree of separation from this activity:

> *'there's a dichotomy that exists between the board table and the executives, because the executives actually are taking the risk [whereas] the board very rarely takes the risk; it's the executives themselves who are taking that risk'* (non-executive director).

The reason for this separation was to allow the board to operate as a 'critical space' within which both executives and non-executives can debate and challenge at a strategic level. The 'critical' nature of the 'critical space' arises because the interactions between board members are crucial for effective risk governance. In turn, it is this space that encourages and nurtures a relationship where each non-executive can be both a 'critical' and a 'supportive' friend.

> *'Their main role is to hold [me] and the group chief executive to account, and to make sure that we have got the processes and procedures in place to manage the risks that we…as the executive, …think we face. And to challenge us on our assessment of those risks'* (executive director).

Within this critical space, the importance of the safe-zone atmosphere discussed in section 2.4.2 becomes even more obvious.

2.5.5 Committees and risk managers

The discussion by participants of the relationship between the board and audit committee, risk committee, or audit and risk committee, as well as risk managers, reflected the issues already mentioned above. Participants noted the difficulty of drilling down into detailed risk issues within time-pressured board meetings, and the important role of the audit and/or risk committee:

> *'the Board meeting was three hours … he [the risk manager] should really have had an hour out of that three hours, in my view, to really get to the bottom of some of these [risk] areas, [but] he was granted 10 minutes or so...So that bit there said, okay, so things aren't happening correctly at [the] board, where should they then happen? So the audit committee, in my view, is the place where scrutiny of the [risk] areas takes place'* (non-executive director).

The risk and/or audit committee was seen to act as a filter for the board, with a more succinct discussion taking place at board level.

> *'It's a very fine filter, if you like, in that the discussions that take place in the committees, it's really down to the chair of that committee then to distil the key points from the committee discussion to the board'* (executive director).

Nonetheless, participants noted the possibility of duplication, especially if there is both a risk committee and an audit committee and reporting lines are not clear. Outside formal reporting, established lines of communication between executive and non-executive board members, as well as between board members and sub-committees, were therefore regarded as important in enhancing the risk discussion at board level. Key one-to-one relationships that were identified included the board chair and CEO and the audit committee chair and CFO.

Participants also mentioned the importance of the board's, especially non-executives', relationship with senior risk managers in the organisation. These relationships helped ensure that discussions at board level were supported with all necessary data, as well as allowing NEDs to metaphorically 'kick the tyres' (executive director) of the organisation in relation to its risk policies.

3. Suggestions for practice

This section provides some suggestions that boards and policymakers may wish to consider so as to improve their practice. All the suggestions have come from the participants and reflect practices that they have put into place and which have been proved to work.

3.1 SUGGESTIONS FOR BOARDS

3.1.1 Integrating risk and strategy

1. Place risk in a positive context. Consider the potential for outcomes to be better, as well as worse, than expected, making it clear when you are talking about opportunities and risks. If necessary, avoid using words such as risk if they have a negative meaning in your organisation; eg consider alternatives such as 'volatility' and 'uncertainty'.

2. Integrate your strategy and risk decisions. When setting your strategy and business objectives, consider the potential for better or worse-than-expected outcomes from the outset.

3. Boards should adopt the 75:25 rule. Spend 75% of board meetings looking outwards and forwards. This will help the board to identify external and future threats and opportunities. Spend the remaining 25% of board meetings looking inwards and backwards. This will help the board to understand the organisation's capabilities and competencies in areas such as finance and risk management.

4. It may be instructive for boards to reflect on the relationship between risk appetite and strategy when reaching decisions about both. Section 2.2 indicated that it is often unclear whether risk appetite should come before or after strategy (a 'chicken and egg' situation). Consider whether the board's risk appetite determines strategy, or whether decisions about strategy lead to how the organisation frames its risk appetite.

3.1.2 Deriving value from risk management

1. Compliance and a 'tick box' approach may be the correct approach to take to certain elements of risk governance. Nonetheless, boards should be aware of the limitations that a 'compliance mind-set' may place upon their ability to exploit opportunities by taking risks.

2. Boards should be mindful of the interrelationship between the embeddedness of risk in the discussions and decisions of the board, and its embeddedness in the organisation itself. This emphasises the importance of the 'tone at the top' set by the board and of efforts of board members to 'test the temperature' of what is happening in practice in the organisation.

3. Boards should recognise that, in managing significant risk events, it is possible to enhance, not just preserve, the value of the organisation, for example in managing reputational risk. Significant events, mishaps and failures can also be used as prompts for testing the risk appetite, and the resilience of the risk framework and governance structures, of an organisation.

4. Boards are being held more accountable by a wider range of stakeholders than in the recent past. Being clear and transparent about how the board manages risk, and communicating this externally, is important for every organisation, including those in less-regulated sectors.

3.1.3 Delivering RI-SKEET

1. Identify gaps in RI-SKeet by employing board reviews that align strategic risks with the output of those reviews, and where necessary include annual training that ensures that members of the board remain risk-relevant with bespoke training for each of the members of the board.

2. 'Kick the tyres'. All NEDs should get out into the business to understand it. Think about spending time in social environments within the business – the tea room, the canteen – where much more can be picked up qualitatively than is presented to boards in their meeting packs.

3. Use awaydays in order to improve RI-Skeet. They should be an impetus within the boardroom for the development and improvement of understanding of organisational risk exposure. The use of scenarios that are facilitated independently from the board, and executed with the business strategy and current strategic exposures in mind, will focus attention on exposures much more than a monthly RAG (Red, Amber, and Green) traffic-light rating.

4. The owner-manager, as the 'Swiss army knife of risk' within their SME business, should identify the 'killer issues' to their business and ensure that they actively acquire appropriate RI-SKeet to address these issues. This may include using external risk specialists to support them.

3.1.4 Managing and enhancing board risk discussions

1. NEDs should consider the adoption of an 'in camera' session before and/or after board meetings. These sessions allow NEDs to meet without the presence and influence of the executive team to create a safe zone for the candid discussion of risk. This can be enhanced further by allowing NEDs to meet with representatives of the risk and independent oversight functions during 'in camera' sessions, to ensure that the tone at the top reflects the tune on the shop floor.

2. All papers going to the board should have a dedicated risk section within the executive summary, highlighting their risk implications for the strategic objectives of the business. This provides visible anchor points for discussion of the strategic risk-reward equation.

3. In the process of horizon scanning, the board should consider requesting a 'deep dive' analysis of a number of the key strategic risks for scrutiny during away days with a dedicated risk focus. This will reduce the information burden on the board while ensuring that the reporting of information is tailored to the needs of the decision makers. 'Deep-dive' analysis can also be performed through audit and/or risk committees.

3.1.5 Executive and non-executive dynamics

1. Create a critical space for risk debate by encouraging constructive challenge. Boards should be aware of the possibility of apparently benign risk environments leading to complacency in the boardroom.

2. Unified responsibility does not necessarily mean unified roles at board level. NEDs should maintain a degree of separation from day-to-day risk taking activities, enabling them to carry out their role as 'critical friends' to the executive and senior management.

3. Boards should ensure they structure, and make use of, their committees (eg risk, audit) in a way that best supports the board's decision making on strategic risks while not delegating their accountability. Established lines of communication between the board, its committees, and the risk specialists supporting those committees, should be clear and transparent.

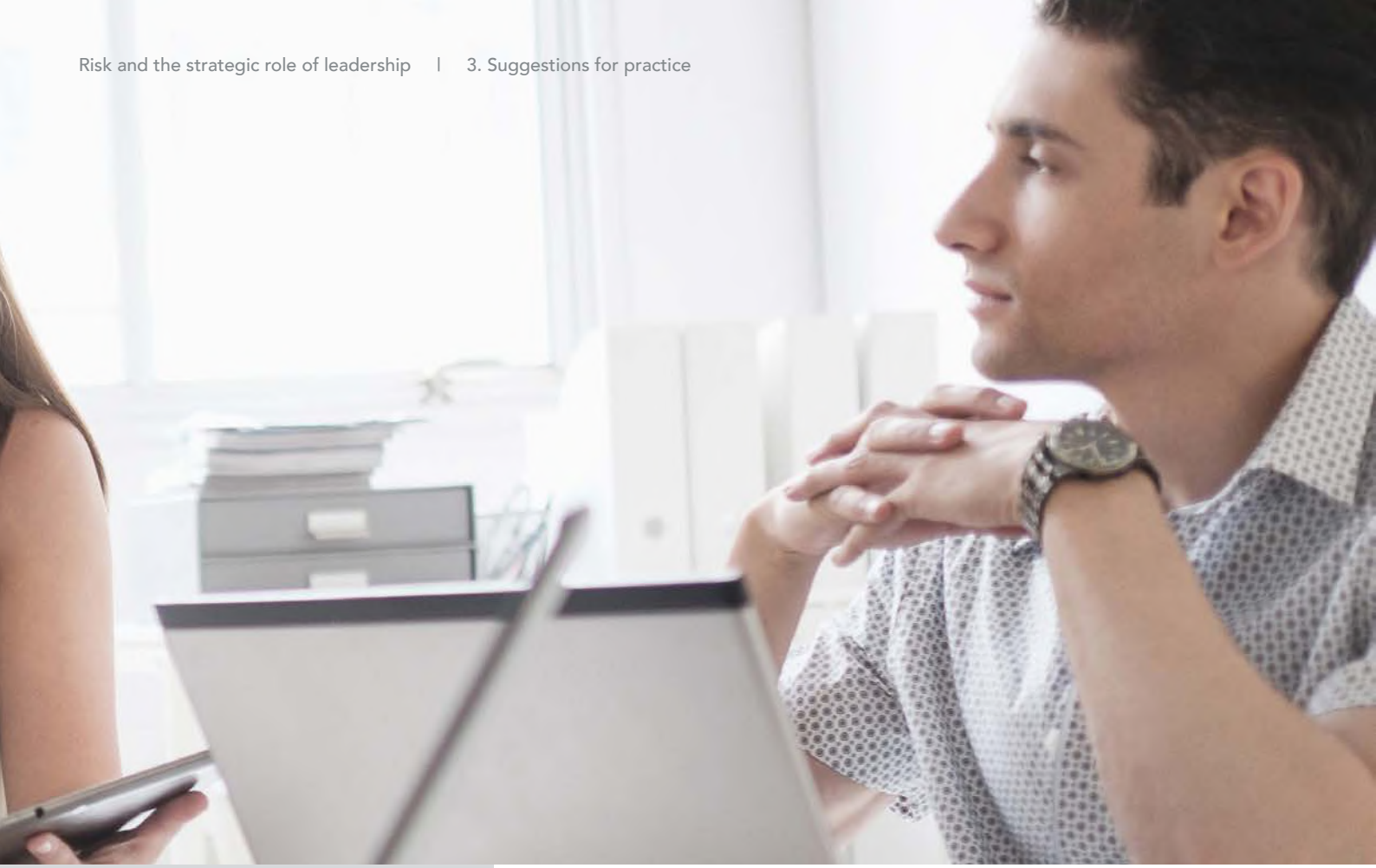
3.2 SUGGESTIONS FOR POLICYMAKERS

The participants showed that policymakers can have a significant influence on board-level risk-management conversations and practices. Often this influence is positive, but care is needed to move board activities in the right direction.

1. Policymakers should revisit their risk mind-set: risk is not bad in itself and opportunities are never certain. Rather than considering risk management as a device for increasing certainty, it should be considered as a means for achieving ever more positive outcomes. Risk management should help an organisation to create value, as well as to protect it.

2. Always encourage boards to make links between strategy and risk. Potential risk exposures, along with the ability of an organisation to manage these exposures, should be considered as part of strategy setting. Risk management should not be a bolt-on activity after the strategy has been determined.

3. Recognise the difference between separation and segregation. Boards, and especially non-executives, need to maintain a degree of independence, but that does not mean they should be kept apart from the people within the organisation. Boards should understand



and steer the culture of an organisation so that it promotes an appropriate balance between risk and control.

4. Culture, including risk culture, is still an ambiguous concept for many. Policymakers may wish to facilitate best practice sharing as well as provide more guidance on what culture means in the context of risk management and how boards may lead in setting the right risk culture.

5. Policymakers should be mindful of the effect (and potential benefits) that the work they do in more regulated sectors can have on (and for) the behaviour of boards in less regulated sectors.

6. Use failures as feedback. Help organisations to learn the lessons from past failures. Use this information as feedback to assist organisations in improving their approach to understanding and dealing with risk.

Questions for reflection

Organisations and their boards may wish to reflect on the following questions, which may help benchmark their board-level risk-management activities.

1. How often does your board review and enhance its risk-management activities?
2. Does your board consider, from the outset, the risk implications of different strategic options, ie as a key component of strategy creation? How are these options and their associated risks presented to the board?
3. Where is your board on the principled–prescriptive spectrum? What are the strengths and weaknesses associated with your board's position and do you need to consider becoming either more principled or more prescriptive?
4. How do you review the diversity of risk intelligence, skills, knowledge, experience, education and training (RI-SKeet) across the board? How do you address any gaps in RI-SKeet?
5. How often do you consider the composition of the board, and its RI-Skeet? Do you review composition and RI-SKeet when changes, or proposed changes, to the strategic direction of the organisation are being considered?
6. Do you create a safe-zone atmosphere for the discussion of risk-management issues? Are board members encouraged to challenge the status quo?
7. Are board members, and NEDs in particular, encouraged to get out into the organisation and to understand its people and culture?
8. Do NEDs act as critical friends to the executive and wider senior management team – helping them to exploit opportunities and avoid losses?
9. How much time do you devote to risk management at board meetings? Are opportunities to discuss risk management provided outside formal board meetings?
10. How effective are the board's subcommittees in enabling the board to focus on strategic risk-management issues?

4. Conclusion

'Boards are responsible for setting strategy and fundamental to that is this understanding of risk versus reward. So, if we sit in this direction, what are the potential risks? What's the reward? Obviously in formulating that kind of cohesive strategy you need to have a really good grasp of that. So, to me it's kind of fundamental to the core function of a board for it to have… a good appreciation and understanding of risk management. That's kind of response number one' (executive director).

The effective governance of organisations requires boards to fulfil a wide range of responsibilities and it is often hard to balance these during time-limited board meetings. One solution is to recognise the fact that many of these responsibilities are connected, especially those related to strategy and risk, as indicated by the above participant.

The research shows that while many boards are taking steps to connect their strategic and risk-management responsibilities, there does not appear to be one best way to achieve this. Rather, a diversity of practices exists, each with different strengths and weaknesses. It is possible, however, to situate these practices, to a degree, via what is termed above the 'principled–prescriptive spectrum' (see section 2.1.2 above)

- Organisations and boards that adopt a more principled approach are likely to make more connections between strategy and risk, but these connections may not be very explicit and are often unstructured. Failure to make such connections can lead to inconsistent decision making and the pursuit of opportunities without the proper consideration of downside outcomes.

- Organisations and boards that adopt a more prescriptive approach tend to view risk management as a device for internal control and, to the extent that connections are made between strategy and risk, their focus is on risks to objectives. This can make it harder to exploit opportunities, but risk-management activity is more structured, meaning that 'downside' outcomes may be better controlled.

Whichever approach is adopted between the two extremes, effective strategic-level leadership is not necessarily about achieving greater levels of certainty; it is about being able to exploit any uncertainty that may exist to the advantage of the organisation and its stakeholders. Risk-management tools such as risk reports, risk appetite statements and managing the cultural aspects of risk taking can be used to help support this, as much as they can be used to mitigate losses.

Perhaps unsurprisingly, this research also shows that the primary driver for much board-level risk-management activity is compliance. Legislation, regulatory requirements, corporate codes and professional codes of conduct were regarded by many participants as having a direct effect on attitudes and practices in relation to risk management. This may be a doubled-edged sword; on the one hand ensuring that boards are engaged in risk management, but on the other promoting a tick-box approach. What may help here is a greater emphasis on the other benefits of risk management, for example in mitigating reputational effects, improving efficiency or the exploitation of opportunities.

As regards the mix and composition of board skills, having board members who are risk-management professionals can be helpful, as are internal and external

From this research it is clear that there is already much good risk-management practice, but this practice needs to be shared more widely and in an open-minded way.

risk management specialists who support boards. Nonetheless, it would seem that even more important is fostering a diverse range of risk intelligence, skills, knowledge, experience, education and training (RI-SKeet) across the board. Boards operate as a collective intelligence: no one board member can possibly know everything there is to know about risk management or the various risks and opportunities that may affect the strategy and governance of an organisation. The more diverse the types of RI-SKeet among the board members, the better prepared organisations will be both to avoid and mitigate the downside of risk events and to exploit potential opportunities.

It is therefore important to ensure that a board maximises its RI-SKeet potential. Backward looking, static and/or lengthy risk reports do not help here, but equally significant is the creation of a safe-zone atmosphere where boards are free to discuss risk issues in an open and constructive way. This may include encouraging board members to ask 'dumb' questions, challenging the status quo by playing devil's advocate or considering extreme risk events or control failures.

Finding ways to explore risk-management issues outside time-pressured board meetings can also be important, for example by organising board away days.

Finally, it was plain that, while boards may have shared responsibilities, this does not mean that board members all share the same roles. Participants explained that the role of the executive is to ensure that the organisation's strategy is implemented and that the board, and NEDs in particular, assure that the implementation is effective and consistent with the agreed strategy. In this context, the board provides a critical space for discussions about strategy and risk, with the NEDs acting as critical friends to the executive and wider senior management team. In performing this critical friend role, NEDs are able to step back and see a bigger picture. As a result, they are better able to use their RI-SKeet to 'horizon scan' for emerging opportunities or losses and so guide executives/management in the most appropriate way. They may also help to constrain both over-exuberant and too-timid risk taking.

Are boards ready for the challenges of today, as the strategic environment becomes ever more complex and interconnected and regulation only ever seems to increase? Can they exploit the opportunities that come with change, while at the same time mitigating any associated potential loss events? From this research it is clear that there is already much good risk-management practice, but this practice needs to be shared more widely and in an open-minded way. It is for organisations to select the practices that best suit their needs. It is hoped that this report will help boards to learn from the experiences of a wide range of organisations to enable them to continue to future-proof their activities.

Project methodology

The findings from this report were drawn from 30 semi-structured interviews conducted with non-executive and executive board members from a wide range of organisations.

Table 2.1 provides an overview of the 14 executive and 14 non-executive participants in this project, plus two board-level consultants. Participants came from both large quoted (eg FTSE 100 and 250) companies and SMEs and included people from both for-profit and not-for-profit organisations, including charities and social enterprises. A significant number of the participants, especially the non-executives, had current experience of multiple organisations, so in fact information on experience of board-level risk-management activities in approximately 60 different organisations was collected.

All interviews were conducted on the phone via conference call facilities and were recorded, allowing for each interview to be transcribed for subsequent analysis. In most cases interviews were conducted by two, occasionally three, of the researchers to help control for interviewer bias and to ensure that each interview was as complete as possible.

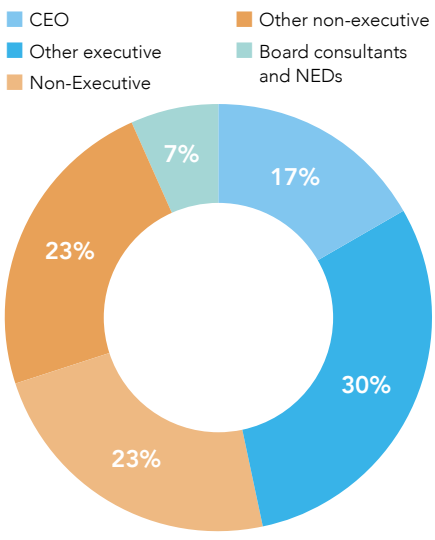
To improve robustness further, the draft findings from the interviews were presented to two focus groups in November and December 2017. These focus groups consisted of risk-management experts and industry association representatives.

Data limitations, especially for private companies, make the precise calculation of the split between SME and larger organisations complex. A search based on publicly available information indicated that the participants have been involved in, approximately, a total of 7 FTSE 100 and 10 other quoted (eg FSE 250, 350 and AIM) companies. In addition a total of 17 private, 8 partnership and 15 not-for-profit entities were represented. The remainder were a variety of other organisational forms (eg networks, members' associations and employee-owned firms).

To manage the effects of cross-cultural biases and different regimes for corporate governance and risk-management regulation, the research focused on UK-based organisations (though a number were multinational in focus). The researchers would encourage organisations, boards and researchers in other countries to build on this research and explore the risk-management activities of boards based in their countries. The expansion of this research would create further opportunities for sharing good practice.

TABLE 2.1: Overview of participants

ROLE	NUMBER	SECTORS	LARGE/SME SPLIT *(Approximate)*
CEO	5	Banking; Consulting; Housing; Investment; Trade Association	40%/60%
Other executive	9	Consulting; Financial services; Hotel; IT; Manufacturing; Property; Public services; Retail	70%/30%
Non-Executive (including one or more appointments as board chair)	7	Aerospace; Charity and voluntary; Commercial property; Government advisory; Hospital; Investment; IT; Housing; Insurance; Legal services; Manufacturing; Pensions; Religious; Retail; Social Enterprise; Telecommunication; Transport	60%/40%
Other non-executive (including one trustee)	7		
Board consultants and NEDs	2	Board advisory services; Education; Insurance	0%/100%



References

COSO (Committee of Sponsoring Organizations of the Treadway Commission) (2017), *Enterprise Risk Management: Integrating with Strategy and Performance*, Committee of Sponsoring Organisations of the Treadway Commission, <https://www.coso.org/Pages/erm.aspx>, accessed 19 January 2018.

FRC (Financial Reporting Council) (2017), *Consulting on a Revised UK Corporate Governance Code*, Financial Reporting Council, <https://www.frc.org.uk/consultation-list/2017/consulting-on-a-revised-uk-corporate-governance-co>, accessed 19 January 2018.

FSB (Financial Stability Board) (2014), *Guidance on Supervisory Interaction with Financial Institutions on Risk Culture: A Framework for Assessing Risk Culture* <http://www.fsb.org/wp-content/uploads/140407.pdf>, accessed 19January 2018.

Salz, A. (2013), *Salz Review: An Independent Review of Barclays Business Practices* <https://online.wsj.com/public/resources/documents/SalzReview04032013.pdf>, accessed 19 January 2018.

Author biographies

Dr Simon Ashby is Associate Professor of Financial Services at the Plymouth Business School (www.plymouth.ac.uk/schools/plymouth-business-school). Prior to this he worked as a financial regulator for the UK Financial Services Authority (writing policy on risk management) and a senior risk manager in a number of UK financial institutions (covering both credit and operational risk).

Simon has a PhD in corporate risk management and has published many academic papers and industry reports in the discipline. His current research interests include board-level risk management and risk governance; cyber risk management; risk culture; and the reputational effects of operational risk events.

Simon is a fellow and former chairman of the Institute of Operational Risk (www.ior-institute.org) and a non-executive director and audit and risk committee chair of Plymouth Community Homes (www.plymouthcommunityhomes.co.uk).

Dr Cormac Bryce is an assistant professor of risk at the University of Nottingham within its Business School, and is a member of the Centre for Risk, Banking, and Financial Services. His multi-method research spans from human behaviour in financial organisations to the effect of regulation on organisational behaviour within the aviation and financial services industry.

Cormac's recent research focus has been grounded in the areas of error-reporting climate and the effects of risk events on the market sentiment of financial services organisations.

Dr Patrick Ring is a qualified solicitor who, before entering academia, worked in the corporate area of private practice, later working as a lawyer with a large life assurer for a number of years. He is currently a senior lecturer in financial services in the Glasgow School for Business and Society at Glasgow Caledonian University. Patrick is a member of both the Chartered Institute of Securities and Investment and the Chartered Insurance Institute, as well as an associate of the Pensions Management Institute.

Patrick's teaching and research interests include financial regulation and compliance; operational risk management and culture in financial services; trust in financial services; pension policy and reform; and the retail financial advice sector.

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