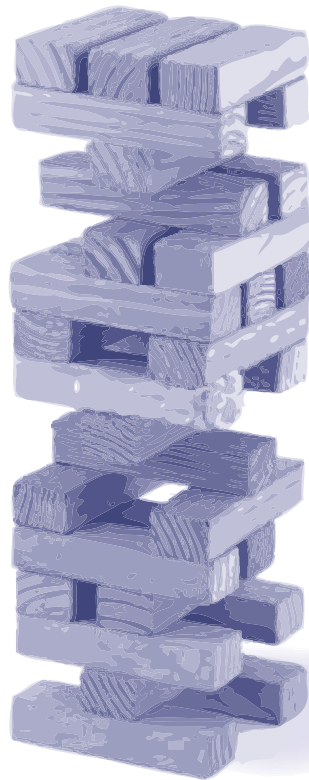


Tomorrow's Corporate Governance

Tomorrow's Risk Leadership:
delivering risk resilience and business performance



tomorrow's
good governance forum

tomorrow's
company

About Tomorrow's Good Governance Forum

The Forum was formed in March 2010 in response to questions raised about the effectiveness of corporate governance as a result of the financial crisis and the subsequent reviews by Sir David Walker and the Financial Reporting Council (FRC).

The Forum brings together a number of key businesses, organisations and individuals to explore what good governance means, to make practical recommendations to company boards and policy makers.

The purpose of the Forum is:

- to develop specific ways forward following the recommendations arising from Tomorrow's Innovation Risk and Governance, in particular those where input may be most valued by the FRC, the Department for Business Innovation and Skills (BIS) and the participating companies, individuals and organisations
- to consider in detail the deeper set of issues which are strategically critical to the well-being of companies over the longer-term. These include:
 - risk, innovation and governance, and how best to develop and implement good practice within boards in relation to these linked issues at a strategic level
 - the relationship between companies, their boards, and major shareholders and how that relationship can be strengthened through greater transparency
 - how in practice to define, differentiate and reward effective 'stewardship' by boards of all stakeholder interests.

The key outcomes arise from two distinct forms of engagement:

- engaging with and influencing boards, with a particular focus on the strategic effectiveness of board behaviours and procedures, in part through the membership of the Forum
- engaging with government and other relevant bodies to influence reforms of corporate governance in the light of the Forum's findings and recommendations.

This publication is the fourth in a series of guides and tool-kits from the Tomorrow's Good Governance Forum for use by chairmen, boards and advisors, to help achieve practical change. The first in the series was 'The case for the Board Mandate' which advocated the creation of a formal mandate by boards as a useful framework for internal strategic decision-making and subsequent communication. This was followed by 'Improving the quality of boardroom conversations' which focuses on the importance of, and how to get the right level of engagement in board conversations to get the very best from the skills and abilities around the board table. The third focused on 'Boardroom and Risk' aimed at helping boards achieve a more risk resilient organisation.

Further publications in this series will focus on key roles and development, board composition and board evaluation.

Other useful information can also be found on www.tomorrowscorporategovernance.com

"Tomorrow's Company is to be congratulated on its timely initiative in creating the Tomorrow's Good Governance Forum. We need a place where the natural leaders from companies and investment can come together and create the stewardship and governance solutions to the problems which my report identified. New rules and codes can only get you so far – what we now need is innovation and leadership and through its work Tomorrow's Company is ideally placed to maintain the momentum."

Sir David Walker

tomorrow's
good governance forum

Foreword



Sir Richard Olver

It is a real pleasure for me to contribute once more to a Tomorrow's Company publication that tackles the crucial governance issues facing boards and directors in an increasingly fast-paced and complex operating environment.

Recent, and recurring, failures of corporate leadership have highlighted the scope for improvement in the understanding of good corporate governance. Simply observing the rules, regulations and compliance procedures alone will not deliver the kind of well run, ethical, companies we are looking for. To produce these companies, boards need to take a lead in creating and embedding the right culture.

A deep, integrated, understanding of risk is a central part of this. Risk is present in every decision a company makes and cannot, nor should it, be eliminated. However, making the link between risk, reward and strategy in the context of a forward-looking and external understanding of all aspects of the business is crucial in enabling high quality decision-making at board level.

The process for achieving this is, however, not static and it is never complete. The best boards are self-critical and challenging and I see parallels between the risk leader recommended in this guide and the role played by Lord Gold as independent corporate monitor during the culture change we undertook at BAE Systems. Lord Gold, through his gravitas, seniority, energy, integrity, intellect and commitment ensured that we had our very own 'continuous improvement machine' within BAE Systems.

However, there is no one-size-fits-all solution to risk leadership. And what works well in one organisation may not be appropriate in another. I would urge board members, and in particular chairmen, to read this publication and consider its recommendations in the light of the following simple question: is the existing risk leadership within your company sufficient?



Sir Richard Olver

At a glance...

The complexity of the business environment and risk landscape demands a deep appreciation of the link between risk, reward and strategy. Leading this agenda well is fundamental to building the resilience that companies need to achieve business success in the short, medium and long term.

Recent research has demonstrated that not all boards are navigating the uncertainties inherent in this changing risk landscape effectively, resulting in significant loss of value. There is a danger that different risks are still being dealt with in silos. Yet risks are interdependent and do not respect functional boundaries.

An integrated approach to risk is vital. In particular, defining the appropriate risk appetite for the organisation and creating the supporting culture and behaviours required – the ‘risk culture’.

In line with the changes in corporate governance set out by the Financial Reporting Council, this publication puts forward the case for all organisations to rethink their risk leadership and consider the value of a dedicated executive risk leadership role, taking into account how risk is structured in the organisation and its risk maturity.

Tomorrow's risk leadership



Transformation of the...



The role is not about removing the responsibility for risk from members of the board. It is to help support them in managing today's and tomorrow's risk agenda.

Having in place an executive voice of risk in the organisation that leads the risk agenda helps deliver the business model and drive business performance.

This leadership is achieved through being a voice of challenge as well as a business educator and enabler, fully empowered to help the business gain a deeper appreciation of the relationship between risk, reward and strategy to enable better and more informed decisions to be taken.

It involves embedding a risk culture to help the organisation proactively deal with risk issues and inherent dilemmas, across and beyond the enterprise.

To be successful they must be able to see, and integrate, the whole risk agenda for the business, aligned to its business model, and navigate this agenda over immediate and longer-term horizons, with independence and assuredness. This involves having a strong forward-looking and external focus, scanning the business environment for risks and opportunities that can impact business performance.

“A risk leader in an organisation should no longer be discretionary; it should be the norm for good management practice. That senior risk professional, bringing an objective and authoritative perspective on the risk side of managing a business and demonstrably adding to the success of an organisation is something every management should embrace. Equally there is a real opportunity for the risk management community to step up and act as a business partner bringing a forward looking perspective and real solutions to management.”

Arnout Van der Veer, former chief risk officer, Reed Elsevier and board member and chair of audit committee, AIRMIC

“We are currently strengthening our risk structure and I think this report is spot on. Thanks to regulation and today’s environment one voice for risk, separate but still closely aligned to audit, is the sensible way forward. In our business there isn’t the need for the individual to report directly into the board but it now makes sense to have one person leading risk in a commercial manner. We need to step away from risk managers who block and obfuscate new initiatives, to a leader who helps a business manage and mitigate in a strategic way. This paper really hits the mark and I look forward to sharing it with my colleagues to help shape our thoughts on the way forward.”

Andrew Blowers OBE, chair of risk, AA PLC

“Risk leadership is not only about ensuring that the right people in the organisation have the skills, information and systems to assess and manage the company’s risks. It also means enabling the board to have a strategic review of the risks that may affect the longer-term viability and reputation of the company, and communicating the results clearly throughout the organisation so that everyone understands the risks it is prepared to take and the context in which they are being taken.”

Richard Shoylekov, company secretary, Wolseley

“The core themes of this report resonate very strongly with me. Regulation and reputational risk, a more complex environment with a changing stakeholder mix and an evolving customer dynamic is driving a rethink of how to manage risk. I am, like many CEO’s, wary of Risk Management because of its reputation for being a box-ticking function which adds more checking and/or review into processes. However, I also believe that companies are now trying to find the right route for their business to hold the leadership to account to values and strategy. I fundamentally believe that all of the leadership are responsible for managing risk in a way that is forward thinking and commercial but also considers the needs of stakeholders. I believe this report brings to life the challenges and balances that need to be considered and makes a strong case for the way forward.”

Andrew Miller, CEO, Guardian Media Group

Introduction and background

The risk landscape and risk agenda are constantly evolving and becoming more complex and remain the subject of much discussion and concern at board level.

Achieving resilience by mitigating uncertainty and managing the risks of what is now essentially one heavily interconnected and integrated world is a priority for all organisations. It is a priority not just because of the need to avert crisis but also to ensure the opportunities for value creation are identified and leveraged.

What is becoming clear from the research undertaken and published by Airmic and other members of the Good Governance Forum is the need for a transformation in the risk function to match the transformation in the risks organisations are facing.

This guide explores the case for a distinct and more specialist role, particularly within non-financial services organisations, to support the board in their risk leadership role, recognising there will be differences in how risk is managed and roles are structured across organisations and sectors.

It draws on the previous research undertaken (see opposite) and also the experience of those who are actively leading an evolution of the risk function in their organisations. As part of the research 58 CEOs, CFOs, chief risk officers and others have been consulted.

At the back of this guide is a 'tool-kit' aimed at helping boards review the effectiveness of their current risk leadership and whether such a role may be needed.

Tomorrow's Corporate Governance: The case for the 'Board Mandate' published in 2010 by the 'Good Governance Forum' convened by Tomorrow's Company, champions the concept of a 'mandate' which sets out the 'essence' of the 'character' and distinctiveness of the company including the company's appetite for risk. This 'working charter' can help boards navigate their way through increasingly choppy waters by facilitating more effective strategic engagement: primarily between executive directors and NEDs to improve board effectiveness.¹

Roads to Ruin: A Study of Major Risk Events: Their Origins, Impacts and Implications was produced by Cass for Airmic in 2011. It investigated the impact of 18 high profile corporate crises over the period 2000-2007 and identified seven key underlying risks that make companies especially prone both to crises and to the escalation of a crisis into a disaster.²

In 2013, building on the research undertaken for Airmic above, the Good Governance forum publication **Tomorrow's Corporate Governance: The boardroom and risk** focused on the changing nature of the risk landscape and aims to help boards have conversations that dig deeper into their own actions, and into the organisation, to illuminate the range of risks they may be facing and consider how to more effectively govern risk.³

The report **Roads to Ruin** was followed up by research to establish why some companies are more resilient than others. **Roads to Resilience: Building dynamic approaches to risk to achieve future success**, published in 2014, identified that resilient organisations have cultural and behavioural traits, backed by systematic planning and risk management that encourage companies to be flexible, customer-focused and alert to danger. In these organisations boards and risk professionals have complementary roles.⁴

Transformation of the risk landscape

Ask most boards what is worrying them most about the changing context for their business and economic, societal and environmental concerns will continue to dominate; for example, shifts in economic power, the impact of the misuse of technologies, rapid urbanisation, social instability and environmental degradation.⁵

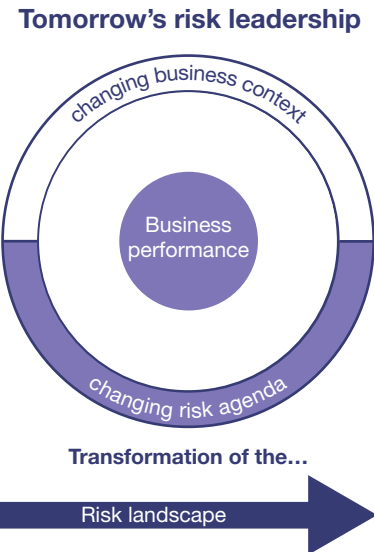
And it is not only these trends in isolation that are of concern but the interconnected systemic nature of their impact, the potential for disruptive change and the incredible speed at which this is all happening, which is unlikely to slow in the future.

The nature of the risk landscape is therefore such that being able to identify and 'manage' all the risks to an organisation is no longer possible. The discussion has now turned to how to make the organisation more resilient – being able to anticipate change, adapt and recover from a wide range of risk events including unforeseen ones; and how to ensure that risks are turned into value-creating opportunities wherever possible.

Value creation relies on relationships and reputation is key. Yet stakeholder expectations are often viewed only as risks, especially as these expectations grow and become more demanding – exacerbated by every corporate crisis or indiscretion that occurs.

But the same stakeholders provide a key route to resilience. Building effective relationships which are reciprocal and mutually beneficial helps provide a stream of intelligence from customers, employees and others that can provide early warnings of looming risks and prevent boards becoming blind to risks because of inadequate information. These relationships can also give businesses room to manoeuvre and recover during and after a crisis.

The heart of understanding the changing risk landscape is to recognise that not only are the risks interconnected but the way to resilience is also through greater connectivity inside and outside the organisation.



“The defining characteristic of our age is increasing connectivity... Increasing connectivity means growing complexity. This complexity is leading to increasing systemic risk...”

Following the collapse of Lehman brothers, the world continues to struggle with the consequences of the first systemic crisis of the twenty-first century. Yet larger and potentially more harmful risks are lurking. These include climate change and pandemics. We see fragility in global supply chains and the interdependent physical infrastructure on which they rely. Latent systemic risks are prevalent in many domains...

Systemic risk is not simply financial, environmental, or biological. Nor can it be confined to infrastructure or social risks. It extends across all these domains and must be dealt with in an integrative manner.”

From The Butterfly Defect: How Globalization Creates Systemic Risks, and What to Do about It by Ian Goldin and Mike Mariathan⁶

What this means for boards

In September 2014, the UK Financial Reporting Council (FRC) revised its guidance setting out the board's revised responsibilities for risk management and internal control.

The UK Corporate Governance Code emphasises that the long-term survival of a company depends on its ability to develop and implement a robust business model and strategy, and the identification of the nature and extent of the principal risks materialising in the short and longer term that they are willing to take to achieve the company's strategic objectives.⁷

Board agendas are already being stretched but boards cannot delegate their ultimate responsibility for risk management and internal control.

The determination of risk appetite and consideration of risk must take place in the context of the organisation's strategy and is therefore an integral part of the board's strategic debate. Neither can boards delegate their responsibility for ensuring that an appropriate risk culture has been embedded throughout the organisation – the tone has to start at the top.

However, the degree of connectivity required across and within the organisation to enable them to fulfil their responsibilities and achieve resilience in a context characterised by volatility, uncertainty, complexity and ambiguity is challenging. It involves a transformation of the risk function:

- moving from a reactive, often compliance-driven, approach to one that is more proactive and focused on building collaboration and creating integration across functional silos; and
- embedding an appropriate risk culture at every level of the organisation and ensuring that the right roles, responsibilities and controls are in place.

Given the importance of this to the success of the business model and strategy – how can this best be achieved?

Tomorrow's risk leadership





Richard Sykes

Crises and the changing board agenda

Richard Sykes, partner, PwC

Not all crises are the same. So a 'one size fits all' approach to prepare and respond for a crisis fails to address the wide range of causation and form that any event might take.

Most organisations have a **classic rapid onset crisis** (such as a physical hazard) in mind when they put together their risk/resilience/crisis approach. These are plainly obvious and easier to deal with; something big has happened, or is about to, and a significant senior response is going to be necessary. More challenging are the **operational disruptions** that bubble along at a regular pace with supply-chain failures or IT outages. The crisis can be masked by this constant flow of noise and weak signals and as a result one of those outages could tick-upwards to cause a major crisis that would arrive with very little warning. Other events such as serious frauds or ethical breaches tend to have a similar path to major physical events but their arrival is **hidden**, either because of their nature or because they are contained within parts of the organisation before emerging as a serious crisis. And finally there's the long-term **strategic crisis** which is so slow in its build up, such as the financial crisis, that the squeeze is felt over time but not considered a crisis event itself, until the very operating model of the organisation is challenged and tipped over the edge.

All of these events form different crises and require senior leadership and, often, a non-routine response. However, they are thoroughly challenged by two factors of the modern operating environment. The first is the cyber threat which can encompass all of the above crisis models at once and impact across an organisation in a way that most 'traditional' risks cannot. The second is the collective impact of social media and a 24/7 news cycle which can turn a very small event into a rolling national and international story.

As a result, boards, and their executive teams, need to find a way to look forwards, balancing opportunity and risk as strategy is converted into action. This also means looking for indicators and signals of other forms of crisis as a form of early warning. This more rounded approach is much more likely to both be effective and drive resilience within the organisation.

Transforming the risk function – tomorrow’s risk leadership

We believe the transformation required to the risk function to reflect the changes in the risk landscape requires a strong executive voice of risk to help drive the success of the business.

The role holder must be able to see, and integrate, the whole risk agenda for the business, within the context of its business model and strategy, and navigate this agenda over immediate and longer-term horizons, with independence and assuredness. This involves having a strong forward-looking and external focus, scanning the business environment for risks and opportunities that can impact business performance.

At its heart, the role is about leading the risk agenda by being a voice of challenge as well as a business educator and enabler, fully empowered to help the business gain a deeper appreciation of the relationship between risk, reward and strategy to take better and more informed decisions. It is therefore about helping build risk capability at all levels of the organisation so that everyone can identify and manage risk more effectively rather than building a large risk ‘empire’.

The relationship of this role to others in the organisation also depends on where responsibilities for risk leadership and strategic activities sit in the organisation. For example, in the UK, the Chief Risk Officer role provides such a focus within the financial services sector.

While different organisations have different structures and relative roles and responsibilities for risk, we suggest that to be fully effective the risk leadership role needs to be close to the board or at board level. At the very least it is important that they have senior NED engagement and support to ensure that they have both the express and implied authority to act.

What is also clear is that it takes time to embed such a role and that success is heavily dependent on the experience, skills, credibility, integrity and professionalism of the role holder.

Tomorrow’s risk leadership





John Hurrell

The role of tomorrow's risk leader

John Hurrell, chief executive, Airmic

Board level responsibility for risk oversight and governance has been clearly established over many years and now the FRC code makes this requirement more explicit than ever before.

However, the risk management challenge for most organisations is becoming ever more complex and more demanding. There are three reasons for this:

- 1 Businesses are becoming more global, often trading in parts of the world outside of the previous experience of the board and senior management. Even if the company itself is not established outside of the UK, it will be exposed to risks from global markets (e.g. through its supply chain or sales networks).
- 2 Companies are outsourcing or subcontracting more and more of the process work in their business and focusing on soft assets such as brand, reputation, IP, R&D, people and technology. However, this does not outsource the risk as the automotive and food retailers have found to their cost over the last year or two. But the management of these risks may well be beyond the current oversight of the board.
- 3 Many organisations are extending their dependencies on technology, often dramatically, over a short timeframe. Board members, understandably, may well have only a limited understanding of the specific technological threats (which may well include external threats from very well resourced outside agencies).

If board members were to receive detailed reports on these threats, they would be even more overloaded with paper than ever before! We, therefore, support the proposal in this guide that boards need to consider the appointment of dedicated resources to act as an adviser to the board on risk issues by developing close partner relationships with the critical functions and operating divisions and to provide to the board prioritised risk information and recommendations for board actions.

Tomorrow's Risk Leadership

John Ludlow, SVP and head of global risk management, IHG

A strong business aligns behind a core purpose, a code of behaviour and business model. It is also trusted and valued by shareholders, economic stakeholders and those in wider society.

Risk leaders work with the board, its committees and other senior leadership teams to reduce levels of risk and respond to uncertainty. They also work in partnership with the business to strengthen resilience and to facilitate the balancing of risk with reward and of opportunities with consequences.

Risk leaders have a deep understanding of their stakeholders and business models as well as the inherent internal and external vulnerabilities and threats. Their approach is business based and intelligence led, focusing on performance and how it fits into the shifting competitive, economic, political, technological, regulatory and societal landscape. Context and insight help identify a compelling and relevant risk agenda at a strategic, tactical and operational level that proactively engages a workforce.

Risk leaders influence behaviours and decisions at all levels, overseeing programmes to identify major risks, develop risk strategies, implement change and monitor controls. This results in robust and dynamic risk management control capability and communications between teams, functions and departments within a business.

In conclusion, risk leaders champion a proactive risk culture that recognises the need for broad stakeholder support and mature ethical values and helps to ensure that the thousands of decisions made each day build valuable trust, even in times of crisis.



John Ludlow

The changing importance of the risk function

The Federation of European Risk Management Associations undertook a survey from April to June 2014, published in October 2014. From the 850 responses it found:

- 84% of risk management functions report to top management level/board. However this practice is declining compared to 2012 (93%) and 2010 (85%). The main reporting lines of risk managers are respectively CFO (22%), board of directors/supervisory board (18%) and CEO level (17%)
- 66% state that risk management is generally formally addressed by the board at least on an annual basis, with 48% of risk managers formally presenting risk management activities to the board/top management several times a year.⁸

A global survey conducted by the ERM Initiative in the Poole College of Management at North Carolina State University on behalf of the Chartered Institute of Management Accountants (CIMA) asked respondents if their organisation has formally designated an individual to serve as chief risk officer (CRO) or senior risk executive equivalent.⁹ For the full global survey of 481 respondents, just under half of the organisations around the globe (46%) have taken that step, which is similar to what was found for the subset of 158 UK-based organisations. Larger organisations are more likely (58%) to designate an executive to serve as CRO or equivalent. But, such appointments are most common for financial services organisations where 80% indicate that they have made such designations. Overall, the global findings are much higher than what is observed by U.S. organisations.¹⁰

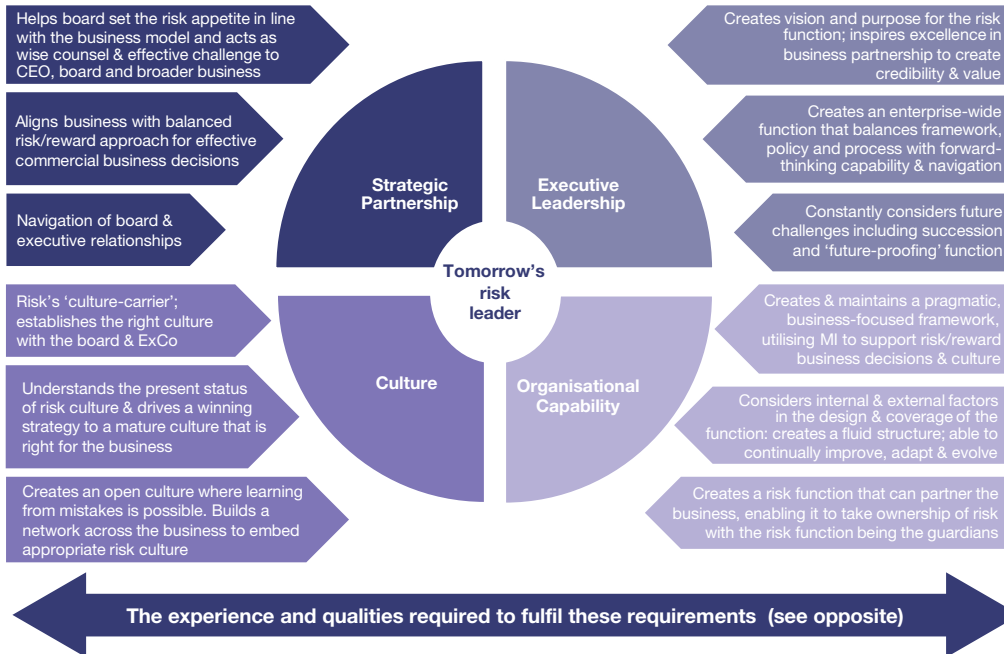
When organisations designate an individual to serve as CRO or equivalent, their lines of formal reporting are generally split between reporting directly to the board of directors (35% of the time for global organisations) or to the CEO (35% of the time for global organisations). Interestingly, the likelihood of reporting to the board or CEO is higher for financial services organisations. These global results differ from the U.S. only results which show a higher likelihood of reporting directly to the CEO (versus the board of directors).

Tomorrow's risk leader

We have identified 4 key components to such a role:

- strategic partnership
- executive leadership
- culture
- organisational capability.

Tomorrow's risk leader – the brief



© 2015 Korn Ferry. ALL RIGHTS RESERVED

... and five key qualities:

- organisational and stakeholder navigation
- courage
- communication
- integrity, ethics and values
- credibility.

Tomorrow's risk leader – qualities



© 2015 Korn Ferry. ALL RIGHTS RESERVED

The CFO-CRO partnership

Gillian Lees, head of research & development, CIMA

The very nature of the roles means that the CFO and CRO share many qualities in common. Both must build on their skills to create and protect value within the context of the connected business environment. In particular, they must understand the dynamics of the business model and how digitisation and other disruptive technologies are changing the rules of the game. The power of big data and predictive analytics are revolutionising the insights available to both the CFO and CRO, enabling them to support better decision-making as well as enhanced performance and risk management.

There are differing views on the appropriate levels of integration between risk and finance. But what matters is that there should be effective collaboration between the CFO and CRO while each retains professional independence and objectivity.

Key synergies are around data, systems and processes to avoid unproductive disagreements about the facts. It is better to share common platforms, built on data integrity, to facilitate constructive dialogue. Recent research suggests that effective coordination can be achieved through sharing and joint development of data warehouses and modelling competences as well as through mechanisms for coordinating risk and finance input to strategic discussions.¹²

This shared platform enables more productive conversations built on each function's strengths. For example, the CFO and CRO should review strategy, implementation risks and performance and consider whether additional mitigation or contingency actions need to be recommended to keep the strategy on track – and whether there are emerging opportunities that could be seized. A further useful conversation is about understanding the extent to which the board and executive team is aligned and how this impacts on the organisation's risk profile and performance.



Gillian Lees

Perspectives from other functions

“Public affairs, with its focus on issues management from the late 1970s, has been involved in scanning and monitoring organisations’ external environments to look for signals of emerging issues and to plan for appropriate action. Bound up with this work are assessments of threats, vulnerability and risk, and preparations for crises that may ensue from failure to manage issues. In recent years, public relations practice has also come to recognise the importance of similar intelligence on internal relationships and developments.”

Jon White, visiting professor, Henley Business School, research and development unit, Chartered Institute of Public Relations

“The oversight, understanding and mitigation of risk in a volatile, uncertain, complex and ambiguous world has never been more important. This report rightly calls attention to this and promotes a stronger level of risk governance, and also highlights the cultural and behavioural aspects of risk that are so fundamental. Building the right skills and capabilities in the workforce, understanding and aligning the behaviours, developing leadership capabilities, and understanding and evolving corporate cultures are all vital parts of HRs role in an organisation. But HR needs to be more aware and engaged on the risk agenda, and closer collaboration with the risk function is essential to build more risk resilient enterprises for the future.”

Peter Cheese, chief executive, Chartered Institute of Personnel and Development

Finding tomorrow's risk leader

Amelia Stubbs. senior client partner, head of audit and risk EMEA, Korn Ferry

An executive risk leader can be a tough appointment to make. Risk does not respect functional boundaries and responsibility can be divided amongst a number of senior executives; appointing one may offend or alienate a number of others. Dividing responsibility can provide multiple commercial perspectives, but can deprioritise the importance of risk and allow for issues to fall between individual accountabilities.

Risk has a historic reputation for being 'box-ticking and a business blocker'. There is now clear evidence that risk is evolving and risk leaders are developing to take up broader and more influential roles. Whilst many will not want to make, or be capable of making, the shift from technical guru to executive leader, a small group of individuals is now emerging. Risk is also attracting individuals from the business or other functional leadership roles enticed by the opportunity to make a difference through changing the approach and view of risk.

We are seeing an increasing demand for and appointment of risk leaders, such as Chief Risk Officers at divisional and at group level, or Enterprise Risk Leaders. Responsibilities range from being the portal for risk information and provider of education (often as a first step to a more integrated approach to risk) to an empowered risk leadership role tasked with enhancing risk and resilience across an organisation.

Few organisations will find the perfect candidate. The board and CEO should agree on what the company needs; where are they today and what role do they want Risk to perform. Answering these and other questions will determine the key skills required enabling the review of internal and external candidates. Any search will look for candidates from various sectors and role types, but success is often dependant on prioritising requirements (rather than expecting one candidate to have everything) and considering supporting a leader with the technical expertise whilst they come up the curve.



Amelia Stubbs

The financial services view of tomorrow's risk leader



John Scott

John Scott, chief risk officer, Zurich Global Corporate

It is humbling to look back at the lessons of the financial crisis of 2008 and to acknowledge the impact on business, economies and societies. In this context it is worth remembering that, despite some excellent analytical advances in the understanding of financial risk in the decade preceding the crisis, risk management largely failed in the financial services sector.

The lessons have been well understood and have practical implications for all industries.

First, it is important to understand what risks an enterprise faces and how these link with an overall risk appetite. This is not a simple task and requires a deep knowledge of the value drivers and their link with measurable outcomes of a successful strategy. These will be different for different companies, but it is critical for sustained business success that these are measured, monitored and acted upon. It is difficult for executives running the business to achieve this in an objective way, without a risk leader to provide this challenge at Board level.

Secondly, it is important to recognise that not all risks are amenable to analysis using the same tools. Operational risks may need statistical analysis, business and strategic risks may need other tools such as scenario analysis, but the key is to have risk leadership that can help the board identify, prioritise and mitigate risk at all levels in the organisation.

Thirdly, none of this is effective unless it is built into 'the way we do business around here' i.e. the culture of the organisation. It needs a robust individual with wide business experience to effectively challenge an executive or board team, when the attractions of continuing to 'dance while the music plays' are obvious, but the risks unpalatable.

Risk leadership in practice

Enclosed in this guide is a ‘tool-kit’ to help boards think more deeply about establishing a dedicated risk leadership role.

It has two elements:

1. A roadmap to risk leadership

This roadmap is designed as an aid to boards to help them make an assessment of how mature the organisation’s approach is to risk and the need for a dedicated risk leadership role.

It shows four stages of maturity in terms of achieving risk leadership so that boards can review where the organisation is now and determine where they want to be. Each board will prioritise differently.

The stages and their indicators are drawn from our research and should be used as a stimulus for discussion. It is likely that boards will assess their organisation as currently operating across the levels in terms of specific approaches.

The final stage is not intended to be a description of the end of a journey. Instead it should be seen as an indication that the organisation is well advanced in building effective risk leadership capability. Inevitably, further improvements will be identified.

2. An agenda for boards

This agenda for the board’s discussion suggests some key questions boards can ask of themselves to help them identify the need to enhance their risk leadership, find the right risk leader and help set them up for success. It also outlines some common pitfalls when selecting candidates.

Tomorrow's Risk Leadership: delivering risk resilience and business performance

This 'tool-kit' supports the publication: *Tomorrow's Corporate Governance: Tomorrow's Risk Leadership: delivering risk resilience and business performance*

It is designed to help boards think more deeply about establishing a dedicated risk leadership role.

There is no one-size-fits-all solution to risk leadership and this 'tool-kit' cannot be full comprehensive given the differences in how risk is structured in organisations. However we hope it provides a good starting point for a deep discussion at board level as to whether the existing risk leadership within your organisation is sufficient.

The 'tool-kit' consists of two elements

1. A roadmap to risk leadership

This is designed as an aid to boards to help them make an assessment of how mature the organisation's approach is to risk and the need for a dedicated risk leadership role. It shows four stages of maturity in terms of achieving risk leadership so that boards can review where the organisation is now and determine where they want to be. Each board will prioritise differently.

The stages and their indicators are drawn from our research and should be used as a stimulus for discussion. It is likely that boards will assess their organisation as currently operating across the levels in terms of specific approaches.

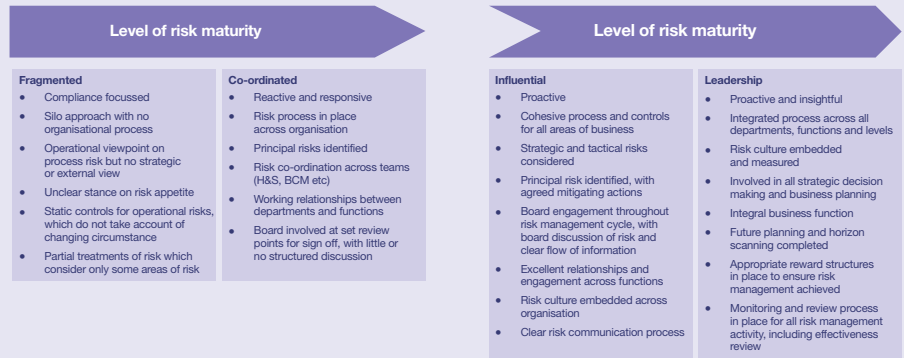
The final stage is not intended to be a description of the end of a journey. Instead it should be seen as an indication that the organisation is well advanced in building effective risk leadership capability. Inevitably, further improvements will be identified.

2. An agenda for boards

This suggests some key questions boards can ask of themselves to help them identify the need to enhance their risk leadership, find the right risk leader and help set them up for success. It also outlines some common pitfalls when selecting candidates.

tomorrow's
good governance forum

A roadmap to risk leadership



tomorrow's
company

Tomorrow's Risk Leadership: delivering risk resilience and business performance

An agenda for boards

Key questions

- How aligned is your business model, strategy and risk agenda?** Consideration of risk and opportunity must take place in the context of the organisation's strategy and is therefore an integral part of the board's strategic debate
- How well aligned are the board, chair and CEO in terms of their vision for the risk function and its leadership?** This is an essential first step. Misalignment will lead to unnecessary challenges if the risk leader is appointed without clarification
- How advanced is the firm's approach to risk?** Understanding where you are on the spectrum of risk maturity is also essential for defining the leader you require. (see the 'tool-kit' 'Roadmap to risk leadership')
- How well are you 'plugged in' to the external environment and all those that can give early warning of risks and identify opportunities?** Building effective relationships is a key part of the 'radar' needed to navigate a fast changing environment
- How well will your culture support a specialist risk leadership role?** Risk leaders who cannot operate in your culture will struggle to get traction on shared agendas and difficult issues, let alone influence the culture
- What is the risk culture today and where do you want it to be?** This should form the foundation for the risk leader's mandate. A proactive risk culture is needed where risk leadership operates at all levels of the organisation.

Common pitfalls when selecting candidates:

- Different views** on what is needed from the individual and the function
- Expecting to get all skills in one individual.** Risk appointments are challenging and require realistic prioritisation
- Technical over Leadership:** Influencers can hire technical specialists.

tomorrow's
good governance forum

Measuring the effectiveness of relationships

Notes/Additional Questions

For information

Extract from 'Guidance on Risk Management, Internal Control and Related Financial and Business Reporting' issued by the Financial Reporting Council
SECTION 2: Board Responsibilities for Risk Management and Internal Control

24. The board has responsibility for an organisation's overall approach to risk management and internal control. The board's responsibilities are:

- ensuring the design and implementation of appropriate risk management and internal control systems that identify the risks facing the company and enable the board to make a robust assessment of the principal risks;
- determining the nature and extent of the principal risks faced and those risks which the organisation is willing to take in achieving its strategic objectives (determining its 'risk appetite');
- ensuring that appropriate culture and reward systems have been embedded throughout the organisation;
- agreeing how the principal risks should be managed or mitigated to reduce the likelihood of their incidence or their impact;
- monitoring and reviewing the risk management and internal control systems, and the management's process of monitoring and reviewing, and satisfying itself that they are functioning effectively and that corrective action is being taken where necessary; and ensuring sound internal and external information and communication processes and taking responsibility for external communication on risk management and internal control.

See: Guidance on Risk Management, Internal Control and Related Financial and Business Reporting, Financial Reporting Council, September 2014. Available at: <https://www.frc.org.uk/Our-Work/Publications/Corporate-Governance/Guidance-on-Risk-Management-Internal-Control-and.pdf>

tomorrow's
company

Appendix

Extract from ‘The UK Corporate Governance Code’ issued by the Financial Reporting Council¹³

Main Principle

Every company should be headed by an effective board which is collectively responsible for the long-term success of the company.

Supporting Principles

The board’s role is to provide entrepreneurial leadership of the company within a framework of prudent and effective controls which enables risk to be assessed and managed. The board should set the company’s strategic aims, ensure that the necessary financial and human resources are in place for the company to meet its objectives and review management performance. The board should set the company’s values and standards and ensure that its obligations to its shareholders and others are understood and met.

All directors must act in what they consider to be the best interests of the company, consistent with their statutory duties.¹⁴

Section C: Accountability

The board should present a fair, balanced and understandable assessment of the company’s position and prospects.

The board is responsible for determining the nature and extent of the principal risks it is willing to take in achieving its strategic objectives. The board should maintain sound risk management and internal control systems.

The board should establish formal and transparent arrangements for considering how they should apply the corporate reporting, risk management and internal control principles and for maintaining an appropriate relationship with the company’s auditors.

Extract from Guidance on Risk Management, Internal Control and Related Financial and Business Reporting issued by the Financial Reporting Council ¹⁵

SECTION 2: Board Responsibilities for Risk Management and Internal Control

24. The board has responsibility for an organisation's overall approach to risk management and internal control. The board's responsibilities are:

- ensuring the design and implementation of appropriate risk management and internal control systems that identify the risks facing the company and enable the board to make a robust assessment of the principal risks;
- determining the nature and extent of the principal risks faced and those risks which the organisation is willing to take in achieving its strategic objectives (determining its "risk appetite");
- ensuring that appropriate culture and reward systems have been embedded throughout the organisation;
- agreeing how the principal risks should be managed or mitigated to reduce the likelihood of their incidence or their impact;
- monitoring and reviewing the risk management and internal control systems, and the management's process of monitoring and reviewing, and satisfying itself that they are functioning effectively and that corrective action is being taken where necessary; and ensuring sound internal and external information and communication processes and taking responsibility for external communication on risk management and internal control.

Sources and notes

- ¹ Tomorrow's Company and the Tomorrow's Good Governance Forum. *Tomorrow's Corporate Governance: The case for the 'Board Mandate'*, London: The Centre for Tomorrow's Company, September 2010.
- ² Cass Business School on behalf of Airmic, sponsored by Crawford and Lockton. *Roads to Ruin: A Study of Major Risk Events: Their Origins, Impacts and Implications*, London: Airmic, 2012.
- ³ Tomorrow's Company and the Tomorrow's Good Governance Forum. *Tomorrow's Corporate Governance: The boardroom and risk*, London: The Centre for Tomorrow's Company, May 2013.
- ⁴ Cranfield University on behalf of Airmic. *Roads to Resilience: Building dynamic approaches to risk to achieve future success*, London: Airmic, January 2014.
- ⁵ See for example Global Risks 2015, 10th Edition, World Economic Forum, <http://www.weforum.org/reports/global-risks-report-2015> ; and PwC 17th Annual Global CEO Survey: Fit for the future, <http://www.pwc.com/gx/en/ceo-survey/index.jhtml>
- ⁶ Ian Goldin and Mike Mariathasan. *The Butterfly Defect: How Globalization Creates Systemic Risks, and What to Do about It*, New Jersey: Princeton University Press, May 2014.
- ⁷ The Financial Reporting Council. *Guidance on Risk Management, Internal Control and Related Financial and Business Reporting*, The Financial Reporting Council, September 2014. Available at: <https://www.frc.org.uk/Our-Work/Publications/Corporate-Governance/Guidance-on-Risk-Management,-Internal-Control-and.pdf> [accessed April 2015].
- ⁸ FERMA. *European Risk and Insurance Full Report of the FERMA Risk Management Benchmarking Survey 2014*, FERMA, 2014. Available at <http://www.ferma.eu/app/uploads/2014/10/ERI-Full-Report-v4.pdf> [accessed April 2015].
- ⁹ For more information about the ERM Initiative, please see www.erm.ncsu.edu. The results of the global survey will be published with comparisons with the separate US survey (footnote 10) in a forthcoming CGMA report by the AICPA and CIMA.
- ¹⁰ A separate US survey was conducted on behalf of the American Institute of Certified Public Accountants (AICPA) and the results have been published in the 2015 Report on the Current State of Enterprise Risk Oversight: update on trends and opportunities, 6th edition, February 2015.
- ¹¹ CGMA. *Big Data – readying business for the big data revolution*, CGMA briefing, November, 2014. Available at <http://www.cgma.org/Resources/Reports/DownloadableDocuments/CGMA-briefing-big-data.pdf> [accessed April 2015].

- ¹² Accenture and Oxford Economics. *Rethinking risk in financial institutions: making the CFO-CRO partnership work*, Accenture, 2012. Available at <http://www.accenture.com/SiteCollectionDocuments/us-en/Accenture-Rethinking-Risk-Financial-Institutions-CFO-CRO.pdf> [accessed April 2015]
- ¹³ The Financial Reporting Council. *The UK Corporate Governance Code*, The Financial Reporting Council, September 2014. Available at <https://www.frc.org.uk/Our-Work/Publications/Corporate-Governance/UK-Corporate-Governance-Code-2014.pdf> [accessed April 2015].
- ¹⁴ For directors of UK incorporated companies, these duties are set out in the Sections 170 to 177 of the Companies Act 2006.
- ¹⁵ The Financial Reporting Council. *Guidance on Risk Management, Internal Control and Related Financial and Business Reporting*, The Financial Reporting Council, September 2014. Available at: <https://www.frc.org.uk/Our-Work/Publications/Corporate-Governance/Guidance-on-Risk-Management,-Internal-Control-and.pdf> [accessed April 2015].

We as Forum members welcome this document as an important contribution to improving the effectiveness of corporate governance.

This guide is the fourth in a series of publications, proposing instruments and practical tools for consideration by chairs, chief executives, company secretaries and other key figures responsible for the quality of corporate governance. Together these publications will provide an essential guide to good governance.

Tomorrow's Company thanks and acknowledges the support and expertise of members of the Good Governance Forum.

As well as the corporate members shown, we are immensely grateful to a number of individuals: Dick Olver for his endorsement, John Hurrell, Paul Hopkin and Katie Moore (Airmic), Gillian Lees (CIMA), Amelia Stubbs (Korn Ferry), Richard Sykes (PwC) for their leadership and support in creating this guide and 'tool-kits'. Also to Arnout Van Der Veer (Airmic Board), John Ludlow (IHG), John Scott (Zurich) and James Maxwell for their insight and contributions.

We also want to express our deep appreciation to BIS (The UK Department for Business, Innovation and Skills) and the FRC (Financial Reporting Council) for their support and active engagement with the work of the Forum.



Help us strengthen organisations through enhanced risk leadership

tomorrowscorporategovernance.com

tomorrow's company

shaping the future of business
success to build lasting value

Centre for Tomorrow's Company
Charity registration number 1055908.
Registered office: Samuel House
6 St Alban's Street, London SW1Y 4SQ



The paper used in this publication is from mixed responsible sources and certified in accordance with FSC® (Forest Stewardship Council), reducing the impact of landfill and energy consumption



© Centre for Tomorrow's Company, May 2015

3768 Designed and produced by  studio401

£20 Institutions/Organisations
£5 Individuals/Members/Reduced
(including p&p)