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 fully 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 their 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.

A roadmap to risk leadership

Level of risk maturity

Fragmented

- Compliance focussed
- Silo approach with no organisational process
- Operational viewpoint on process risk but no strategic or external view
- Unclear stance on risk appetite
- Static controls for operational risks, which do not take account of changing circumstance
- Partial treatments of risk which consider only some areas of risk

Co-ordinated

- Reactive and responsive
- Risk process in place across organisation
- Principal risks identified
- Risk co-ordination across teams (H&S, BCM etc)
- Working relationships between departments and functions
- Board involved at set review points for sign off, with little or no structured discussion

Level of risk maturity

Influential

- Proactive
- Cohesive process and controls for all areas of business
- Strategic and tactical risks considered
- Principal risk identified, with agreed mitigating actions
- Board engagement throughout risk management cycle, with board discussion of risk and clear flow of information
- Excellent relationships and engagement across functions
- Risk culture embedded across organisation
- Clear risk communication process

Leadership

- Proactive and insightful
- Integrated process across all departments, functions and levels
- Risk culture embedded and measured
- Involved in all strategic decision making and business planning
- Integral business function
- Future planning and horizon scanning completed
- Appropriate reward structures in place to ensure risk management achieved
- Monitoring and review process in place for all risk management activity, including effectiveness review

tomorrow's good governance forum

tomorrow's company

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