airmic

2014 Update to the UK Corporate Governance Code

Implications of the FRC guidance on risk management, internal control and related financial and business reporting for risk managers and the board

Guide 2015

Contents

"the new guidance presents a clear explanation of board responsibilities with regards to risk management.."

The Financial Reporting Council (FRC) published revised guidance entitled 'Risk Management, Internal Control and Related Financial and Business Reporting' in September 2014. It is referred to by the FRC as the 'risk guidance' and should be followed by all companies that are required to comply with the UK Corporate Governance Code. The guidance is effective from 1 October 2014 and reports of compliance with the guidance will be required for reporting periods ending 1 October 2015 and later.

Airmic was involved throughout the consultation and believes that the new guidance presents a clear explanation of board responsibilities with regards to risk management. Although the guidance directly relates to listed companies, the FRC believes that the guidance describes an appropriate approach for all types of companies with regard to risk management and internal control.

The risk guidance states that economic developments and some high-profile failures of risk management in recent years have reminded boards of the need to ensure that the company's approach to risk has been properly considered in setting strategy. The guidance emphasises that the board's responsibility for the organisation's culture is essential to the way in which risk is considered and addressed. The assessment of risks should:

- be part of the normal business planning process
- support better decision-taking
- ensure the board and management respond promptly to risks when they arise
- ensure shareholders and other stakeholders are well informed about the principal risks and prospects of the company.

The guidance replaces the 'Turnbull Report' (2005) and states that ultimate responsibility for risk management and internal control rests with the board. The guidance also states that risk management should support better decision-making, rather than inhibit sensible risk-taking, in line with growth strategies and operations.

While risk managers may have day-to-day responsibility for implementation of risk management processes, it is up to the board to ensure that the appropriate systems and policies are in place. The board needs to ensure that understanding of risk is high, that risks are maintained within tolerable levels and that risk mitigation is appropriate.

The UK Corporate Governance Code (2014 edition) sets out the following principles in relation to the accountability provisions of the code:

- Financial and Business Reporting – the board should present a fair, balanced and understandable assessment of the company's position and prospects
- Risk Management and Internal Control – the board is responsible for determining the nature and extent of the risks it is willing to take in achieving its strategic objectives and should maintain sound risk management and internal control.

In summary, the board has ultimate responsibility for risk management and internal control, including for the determination of the nature and extent of the principal risks it is willing to take to achieve its strategic objectives. It is also responsible for ensuring that an appropriate culture has been embedded throughout the organisation. This commentary outlines some of the factors that boards should consider in relation to the design, implementation, monitoring and review of the risk management and internal control systems. As stated by the FRC, risk management systems and processes cannot eliminate all risks, but it is the role of the board to ensure that they are robust and effective, and take account of such risks.

The FRC guidance lists six board responsibilities for risk management and internal control, and these six responsibilities are used to structure this commentary. These responsibilities are described in more detail in Table 1 in the next section. In summary, they relate to:

1. Risk management processes – the design and implementation of appropriate risk management and internal control systems.

2. Principal risks and risk appetite – the assessment of the nature and extent of the principal risks and the risks the organisation is willing to take.

3. Risk culture and risk assurance – the development of appropriate culture and reward systems that have been embedded throughout the organisation.

4. Risk profile and risk mitigation – the means by which the principal risks are managed or mitigated to reduce their likelihood and/or impact.

5. Monitoring and review activities – the monitoring and review of risk management systems to ensure they are functioning effectively.

6. Risk communication and reporting – the implementation of internal and external information and communication processes.

Section 2: Summary of FRC guidance

The FRC risk guidance outlines the responsibilities of the board and identifies the factors they must consider when taking risk management decisions. It emphasises that the board should be satisfied that day-to-day management of risk is appropriate and that it receives timely and accurate information on risks. These responsibilities form the basis and of the guidance and are described in Table 1.

Table 1:
Risk management responsibilities of the board

1.	**Risk management processes** • design and implementation of appropriate risk management and internal control systems that identify the risks facing the company • ensure that risk management is incorporated within the company's normal management and governance processes, and is not treated as a separate exercise
2	**Principal risks and risk appetite** • establish robust assessment of the principal risks to the company's business model and ability to deliver its strategy, including solvency and liquidity risks • identify the nature and extent of the principal risks that the organisation is willing to take in achieving its strategic objectives (determining its 'risk appetite')
3	**Risk culture and risk assurance** • ensure that an appropriate culture embedded throughout the organisation, including embedding risk considerations into reward systems • facilitate adequate risk management discussion at the board, including the assurance the board requires and how this is to be obtained
4	**Risk profile and risk mitigation** • ensure that management's systems include appropriate delegation and controls, and the company's risk profile is kept under review • implement measures to manage or mitigate the principal risks to reduce the likelihood of their incidence and/or their impact
5	**Monitoring and review activities** • ensure that management's process of monitoring and reviewing risk management systems, and ensuring that they are functioning effectively • check that monitoring and review of the associated systems are carried out as an ongoing process and not as an annual one-off exercise
6	**Risk communication and reporting** • introduce sound internal and external risk management and internal control information and communication processes • ensure adequate quality of the risk information communicated to and from the board and the process for producing the risk disclosures in the annual report

It is the responsibility of management to ensure that processes are in place to achieve appropriate understanding of risks at all levels, as well as a culture in which employees understand their responsibilities and behave accordingly. It is also the role of management to implement and take day-to-day responsibility for board policies on risk management. Additionally, management should ensure internal responsibilities and accountabilities are clearly established, understood and embedded at all levels of the organisation. Employees should understand their responsibility for behaving according to the culture.

Although management and employees have responsibilities, it is ultimately the board that needs to satisfy itself that management has understood the risks, implemented and monitored appropriate policies and controls, and is providing the board with timely information so that it can discharge its own responsibilities. Appendix A contains a series of questions for a board's consideration to assist it in measuring the effectiveness of its risk management.

2.1 Risk management processes

Boards are required to establish systems of risk management and internal control. This includes policies, culture, organisation, behaviours, processes, systems and any other activities to assess risk, manage risk, ensure compliance or ensure quality of risk information. This will include details of how risks are identified and managed on a day-to-day basis, as well as defining what constitutes a principal risk.

Risk management expertise will be required to design, implement, monitor and enhance controls, and this may necessitate the employment of a chief risk officer. This is often the case, because the range of a company's risk management and internal control systems and processes will be very broad and may include:

- risk assessment to identify principal risks
- statement of the risk appetite of the organisation
- risk culture and risk assurance arrangements
- management or mitigation of risks
- use of control activities and processes
- information, communication and reporting
- monitoring and review of control effectiveness.

These systems should not be seen as a periodic compliance exercise, but instead as an integral part of the company's day-to-day business processes. The risk management and internal control systems should be embedded in the operations of the company and be capable of responding quickly to evolving business risks, whether they arise from factors within the company or from changes in the business environment. The purpose of the risk management processes will include:

- assess current and emerging risks, respond appropriately to risks and significant control failures, and safeguard assets

- help to reduce the likelihood and impact of poor judgement in decision-making and risk-taking that exceeds the levels agreed by the board
- minimise the chances of control processes being deliberately circumvented or defeated by human error
- help ensure the quality of internal and external risk information, communication and risk reporting
- help ensure compliance with applicable laws and regulations and internal policies with respect to the conduct of business.

2.2 Principal risks and risk appetite

The design of a robust assessment process to determine the principal risks and consider their implications for the company should be appropriate to the size, nature, complexity and circumstances of the company. It is a matter for the judgement of the board, with the support of management and specialist risk management expertise. Circumstances may vary over time due to changes in the business model, performance, strategy, operational processes and the stage of development the company has reached in its own business cycles, as well as changes in the external environment.

When determining the principal risks, the board should focus on those risks that, given the company's current position, could threaten the company's business model, future performance, solvency or liquidity, irrespective of how they are classified or from where they arise. The board should treat such risks as principal risks and establish clearly the extent to which they are to be managed or mitigated. Risks will differ between companies but may include financial, operational, reputational, behavioural, organisational, third-party or external risks, such as market or regulatory risk, over which the board may have little or no direct control. These risks will include emerging, cyber and supply chain risks, as well as other operational risks.

When considering risk, the board should pay regard to the following aspects:

- the nature and extent of the risks, including the principal risks that it regards as desirable or acceptable for the company to take
- the likelihood of the risks concerned materialising and the impact of related risks materialising as a result or at the same time
- the company's ability to reduce the likelihood and the impact / consequences of the risks materialising and affecting the business
- the exposure to risks and level of risk before and after risks are managed or mitigated, as appropriate
- the operation of the relevant controls, as well as the effectiveness and relative costs and benefits of particular controls
- the impact of the culture of the company and the way that teams and individuals are incentivised, on the effectiveness of the systems.

2.3 Risk culture and risk assurance

As part of the risk management systems and processes, the board should also consider the corporate culture and how communication and training can affect this, ensuring that the culture supports the company's risk management strategy. The board should challenge the risk management processes and its own abilities to understand the principal risks. Risk culture is so important that Appendix B sets out the indicators that point to an inadequate risk culture and that should be noted by the board.

The board should establish the tone for risk management and internal control, and put in place appropriate systems to enable it to meet its responsibilities effectively. These depend on factors such as the size and composition of the board; the scale, nature and complexity of the company's operations; and the nature of the principal risks the company faces. In deciding what risk management systems are appropriate, the board should consider the factors that influence the risk culture, including:

1. Embedded culture – the board needs to ensure that values are communicated by management, incentivise the desired behaviours, sanction inappropriate behaviour and assess whether the desired behaviours are embedded.
2. Board discussion – the board needs to ensure that it engages in informed debate and constructive challenge, and keeps under review the effectiveness of its decision-making processes.
3. Capabilities and experience – the board should consider whether it, and any committee or management group to which it delegates activities, has the necessary skills, knowledge, experience, authority and support to assess risks.
4. Information and communication – the board should specify the nature, source, format and frequency of the information that it requires and ensure that the assumptions are understood and, if necessary, challenged.
5. Accountability and delegation – the board should determine to what extent it wishes to delegate some activity to committees or management groups, and the appropriate division of responsibilities and accountabilities.
6. Advice and assurance – the board should identify what assurance it requires and satisfy itself that sources of assurance have sufficient authority, independence and expertise to enable them to provide objective advice and information.

2.4 Risk profile and risk mitigation

A robust assessment of risks is an essential component of the risk management systems and processes. The board needs to be aware of the relationship and interdependencies between the principal risks, as well as the circumstances where risks can accumulate or cause other risks to materialise. A clear understanding of the risk profile of the company is required and this will include careful consideration of emerging, developing and changing risks, such as cyber, political and supply chain risks, including other operational and strategic risks.

The descriptions of the principal risks and uncertainties should be sufficiently specific that a shareholder or other stakeholder can understand why they are important to the company. The report might include a description of the likelihood of the risk, an indication of the circumstances under which the risk might be most relevant to the company and its possible impact and consequences. Significant changes in principal risks such as a change in the likelihood or possible impact, or the inclusion of new risks, should be highlighted and explained. A high-level explanation of how the principal risks and uncertainties are being managed or mitigated should also be included.

Effective controls are an important element of the systems of risk management and internal control, and can cover many aspects of a business, including strategic, financial, operational and compliance issues. Also, risks to the business model need to receive structured analysis and evaluation. The board should agree how the principal risks will be managed or mitigated and which controls will be put in place. In agreeing the controls, the board should determine what constitutes a significant control failing.

2.5 Monitoring and review activities

The board should define the processes to be adopted for its ongoing monitoring and review, including specifying the requirements, scope and frequency for reporting and assurance. Regular reports to the board should provide a balanced assessment of the risks and the effectiveness of the systems of risk management and internal control in managing those risks. The board should form its own view on effectiveness, based on the evidence it obtains, exercising the standard of care generally applicable to directors in the exercise of their duties.

When reviewing reports during the year, the board should consider:

- how effectively the risks have been assessed and the principal risks determined, and how they have been managed or mitigated
- whether necessary actions are being taken promptly to remedy any significant failings or weaknesses
- whether the causes of the failing or weakness indicate poor decision-taking, a need for more extensive monitoring or a reassessment of the effectiveness of management's ongoing processes.

In addition to its ongoing monitoring and review, the board should undertake an annual review of the effectiveness of the systems to ensure that it has considered all significant aspects of risk management and internal control for the company for the period under review and up to the date of approval of the annual report and accounts. The annual review of effectiveness should, in particular, consider:

- the company's willingness to take risk or its 'risk appetite'
- the desired culture and whether it has been embedded
- the operation of the risk management and internal control systems
- the integration of risk management with strategy and business model
- the changes in the nature, likelihood and impact of principal risks
- the extent, frequency and quality of the risk communications
- the state of control and the effectiveness of risk mitigation
- the incidence of significant control failings or weaknesses
- the effectiveness of the company's public reporting processes.

2.6 Risk communication and reporting

Training and communication assist in embedding the desired culture and behaviours in the company. In considering communication systems, the board should also consider the company's whistle-blowing procedures. The assessment and processes described in this commentary should be used coherently to inform a number of distinct but related disclosures in the annual report and accounts of listed companies.

The purpose of risk reporting is to provide information about the company's current position and prospects, and the principal risks it faces. It helps to demonstrate the board's stewardship and governance, and encourages shareholders to perform their own stewardship role by engaging in appropriate dialogue with the board and holding the directors to account as necessary.

The board should summarise the process it has applied in reviewing the effectiveness of the system of risk management and internal control. The board should explain what actions have been or are being taken to remedy any significant failings or weaknesses. Where this information has been disclosed elsewhere in the annual report and accounts, for example in the audit committee report, a cross-reference to where that information can be found would suffice. In reporting on these actions, the board would not be expected to disclose information which, in its opinion, would be prejudicial to its interests, perhaps because it is commercially confidential.

Section 3: Risk management responsibilities of the board

The UK Corporate Governance Code (2014) sets out the responsibilities of the board for accountability of the organisation to shareholders. In relation to risk management and internal control, 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. In particular, the board should:

- confirm in the annual report that it has carried out a robust assessment of the principal risks facing the company, including those that would threaten its business model, future performance, solvency or liquidity, and describe those risks and explain how they are being managed or mitigated
- explain in the annual report how they have assessed the prospects of the company, over what period they have done so and why they consider that period to be appropriate, and state whether they have a reasonable expectation that the company will be able to continue in operation and meet its liabilities as they fall due
- monitor the company's risk management and internal control systems and, at least annually, carry out a review of their effectiveness and report on that review in the annual report. The monitoring and review should cover all material controls, including financial, operational and compliance controls
- receive the report of the audit committee regarding the review of the company's internal financial controls and review of the company's internal control and risk management systems, and determine whether necessary actions are being taken promptly to manage or mitigate principal risks.

The board must make a statement that "the annual report and accounts, taken as a whole, is fair, balanced and understandable, and provides the information necessary for shareholders to assess the company's performance, business model and strategy". Also, the directors should include in the annual report an explanation of the basis on which the company generates or preserves value over the longer term (the business model) and the strategy for delivering the objectives of the company. Appendix A contains a series of questions for a board's consideration to assist it in measuring the effectiveness of its risk management.

Section 4: Role of the risk manager

The risk guidance published by the Financial Reporting Council (2014) to replace the Turnbull Guidance (2005) represents a significant development in the risk management and internal control obligations placed on the boards of companies. In fulfilling these more onerous risk responsibilities, boards will require the help and support of risk management professionals. There is a clear and developing need for in-house risk management expertise to help boards and management to fulfil the obligations set out in Table 1 in this commentary and represented in more detail by the questions set out in Appendix A.

The next step for risk managers is to consider the questions in Appendix A and assist boards in measuring the effectiveness of their risk management. Risk managers should find it useful to work through these questions as a means of assessing the current risk management performance of their company. Table 2 has the same structure as Appendix A and it provides a checklist of actions to be taken by the risk manager. The FRC risk guidance could also be used as a tool to aid discussion with boards and internal stakeholders on their responsibilities, or to highlight the strengths and weaknesses of the current risk management systems and processes.

The importance of risk culture is emphasised in the FRC risk guidance and the indicators of inadequate risk culture are presented in Appendix B. An important part of achieving an adequate risk management culture is to ensure that the company has sufficient risk management capabilities and expertise. An objective of Airmic is to support the work of in-house risk managers and a number of ongoing technical projects will be influenced by the approach set out in this commentary, including work with the Chartered Institute of Management Accountants (CIMA) to consider the ways that risk management can be integrated with the business model and work with Tomorrow's Company to define the developing role of the in-house risk leaders.

The role of the risk manager in helping their board achieve compliance with their risk management responsibilities is extensive. In relation to the six risk management responsibilities outlined in an earlier section, the risk manager needs to make the contribution set out in Table 2.

Table 1:
Risk management responsibilities of the board

	Board responsibility	Board requirements	Risk manager contribution
1.	Risk management processes	• risk management and internal control systems that identify the risks facing the company	• responsibility for planning, designing and facilitating the implementation of the overall risk management process for the company • se risk management systems and procedures that ensure that the approach to risk is co-ordinated and not fragmented • record the risk management roles and responsibilities, as part of the risk management systems and procedures • develop the risk management manual for the company, including the statement of risk management
		• risk management is incorporated within the normal management and governance processes	• devise risk management systems and procedures that are aligned with the corporate calendar • ensure that the impact of risks is understood and the company is able to withstand the risks that do materialise • develop response plans that reflect the responsibilities of the board and senior management for crisis management • make recommendations to the board that update the risk management strategy and framework, as necessary
2.	Principal risks and risk appetite	• assessment of the principal risks to the company's business model and ability to deliver its strategy	• develop the schedule of risk assessments to facilitate the evaluation of each principal risk and the controls in place • facilitate the assessment of the risks to the assets, earning capacity, success, business model and company strategy • take account of the impact of related risks materialising at the same time, including catastrophic risk combinations • ensure the robust analysis of identified risks and evaluation of risks compared with the established risk criteria
		• statement of the nature and extent of principal risks the organisation is willing to take (risk appetite)	• develop a clear risk appetite statement that identifies the risks the company is willing to take and have it agreed by the board • ensure that the risk appetite statement takes account of the risks associated with joint ventures and third parties • structure the risk appetite statement(s) so that it takes account of the level of organisational complexity of the company • include details of how the principal risks should be described, so that they are linked to the risk appetite of the company

3.	Risk culture and risk assurance	• appropriate culture embedded throughout the organisation, including into reward systems	• evaluate the risk culture in the company by using a structured approach, such as the indicators in Appendix B • establish mechanisms for monitoring the influence of the risk culture to ensure that it is achieved in practice • confirm the implementation of appropriate remuneration policies and procedures that take account of risk • design and implement self-assessment and self-certification procedures that include questions on risk culture
		• adequate risk management discussion at the board, including necessary risk assurance	• analyse the board skills and report situations where the skills and experience do not align with and/or support the risk culture • lead a staff risk engagement programme to develop a risk culture that increases the risk knowledge of management • ensure that arrangements are in place to facilitate whistleblowing and guarantee an appropriate response • support managers in the production of their risk registers to ensure that risk culture considerations are included
4.	Risk profile and risk mitigation	• appropriate delegation and controls are in place and the company's risk profile is kept under review	• review the delegation of authority arrangements and confirm that they are in line with the risk appetite statement • establish the triggers for notifying the board that a significant risk has materialised or a crisis has arisen • plan and facilitate appropriate test scenarios to challenge the preparedness of the company to deal with a crisis • evaluate the procedures for assessing and responding to emerging risks, including the need for reports to the board
		• measures to manage or mitigate the principal risks to reduce the likelihood and/or their impact	• introduce a means for the board to consider the cost-benefit aspects of different control options for principal risks • establish risk assessment methodologies that require the collection of risk-related data from internal or external resources • create procedures to ensure that a risk assessment is part of any board discussion of changes in strategy and/or business model • ensure that a risk assessment becomes part of the approval processes for new projects, products or significant commitments

5.	Monitoring and review activities	• process of monitoring and reviewing risk management systems functions operates effectively	• establish processes for senior management to monitor the systems of risk management and evaluate risk performance • facilitate the establishment of the mechanisms for the board to engage in horizon scanning for emerging risks • devise the approach to ensure that the company anticipates possible severe market events and the impact of new legislation • support the development of contingency and continuity plans to deal with disruptive emergencies and other crises
		• monitoring and review of risk systems is carried out on an ongoing process and not as a one-off	• identify the available sources of assurance for the board and evaluate the extent and reliability of each source • design and implement a risk and control self-assessment process, including reporting on material control weaknesses or failures • Support senior management and assist with the investigation of emergencies, crises and/or compliance incidents • Provide proactive support, advice and guidance on incidents with the potential to cause reputational damage
6.	Risk communication and reporting	• internal and external risk information and communication processes are in place	• establish the information needs of the board and ensure that the board risk information is timely and fit for purpose • design a suitable means for reporting risk information to employees and to external and other stakeholders • provide support, education and training to staff to build awareness of the importance of internal risk communication • establish suitable ‘risk radar’ arrangements to provide early warning of changes in the internal and external risk environment
		• quality risk information is communicated to and from the board and used for producing the risk disclosures in the annual report	• evaluate the means for compiling the risk information for the annual report, including training for persons involved • introduce the means for the risk information to be challenged, including the creation of a disclosures committee, if necessary • create the means for the board to review that the risk information in the annual report is fair, balanced and understandable • finally, ensure that the annual report gives a fair and balanced overview of the position and prospects of the company

Appendix A: Questions for the board to consider

Questions that the board may wish to consider and discuss with management and others such as the risk or internal audit functions are set out below and are based on the questions in the FRC risk guidance. If the answers to the questions pose concern for the board, it may wish to consider whether action is needed to address possible failings. The questions are not intended to be exhaustive and not all will be appropriate in all circumstances, but should be tailored to the company.

Risk management processes

- How does the board ensure that it has sufficient time to consider risk and how is that integrated with discussion on other matters?
- Have the board and management reviewed the ability of the company to manage the risks that it faces and withstand any risks that do materialise?
- Are authority, responsibility and accountability for risk management and internal control clearly defined and appropriately co-ordinated?
- How does senior management monitor the application of risk management policies, systems and activities, and how is effectiveness assessed?
- How has the board satisfied itself that the risk management systems are designed in such a way as to ensure that risk is not managed in silos?
- What are the responsibilities of the board and senior management for crisis management and have the plans been tested?

Principal risks and risk appetite

- What risks is the board willing to take and what risks will it not take, and how has the board agreed the company's risk appetite?
- What are the inherent risks in the company's business model and strategy, and what are the factors on which successful delivery of the strategy depends?
- To what extent do the risk management and internal control systems underpin and relate to the company's business model?
- How has the board assessed the interrelationship between different risks and the impact of them materialising at the same time?
- To what extent has the company identified risks from joint ventures, third parties and the way the company's business is organised?
- How effectively is the company able to withstand risks, and risk combinations, including risks with 'low probability' but a very severe impact?

Risk culture and risk assurance

- Do the board and its committees have the skills, knowledge, experience and support necessary to understand the risks facing the company?
- Have the board and management assessed whether employees have the knowledge, skills and tools to support objectives and manage risks effectively?
- Has the board assessed the company's culture and satisfied itself that the company has a 'speak-up' culture to learn from past mistakes?
- How do the company's culture, code of conduct and reward systems support the business objectives and risk management?
- Has the board considered whether senior management promotes the desired culture and demonstrates the commitment to risk management?
- How is inappropriate behaviour dealt with and does dealing with such behaviour create the potential for consequential risks?

Risk profile and risk mitigation

- How does the board ensure it understands the company's exposure to each principal risk and whether controls are operating as expected?
- How does the board consider risk when discussing changes in strategy or approving new transactions, projects, products or significant commitments?
- To what extent has the board considered the cost-benefit aspects of different control options for principal risks?
- How often are the company's principal internal and external risks assessed, and has the company considered scenarios in which risks might become realities?
- How effectively does the company capture emerging risks and determine which emerging risks should be considered to be principal risks?
- What triggers the decision to notify the board that a significant risk has materialised and/or a serious crisis has arisen?

Monitoring and review activities

- What are the processes by which senior management monitors the effective application of the systems of risk management?
- In what way do the monitoring and review processes take into account the company's ability to re-evaluate the risks and adjust controls?
- To what extent does the board engage in horizon scanning for emerging risks and respond to changes in the external environment?
- How are processes and controls adjusted to reflect new or changing risks, or operational deficiencies?

- What sources of assurance does the board rely on and how does the board assess the reliability of each source?
- How are material control weaknesses or failures dealt with and what follow-up procedures are in place to ensure that appropriate action is taken?

Risk communication and reporting

- How are the board's information needs reassessed as objectives and related risks change or as reporting deficiencies are identified?
- Is the board satisfied that the information being received from management and others is timely and fit for purpose?
- How does the company communicate to its employees what risks are not acceptable and how does the board assess whether this has been understood?
- What are the channels of communication that enable individuals to report unacceptable behaviour and how does the board and management respond?
- How does the board satisfy itself that the disclosures on risk management included in the annual report are fair, balanced and understandable?
- How does the board satisfy itself that reporting on a going concern basis gives a fair and balanced overview of the company's position and prospects?

Appendix B: Indicators of inadequate risk culture

This Appendix is intended to assist boards in assessing whether the culture of the company is what they would wish it to be; and whether the risk management and internal control system is operating effectively. Boards should identify indicators that might suggest failures or weaknesses in one or more of these areas, which would prompt them to consider whether action is needed to address the issue. The indicators are not intended to be exhaustive and may not be appropriate in all circumstances.

Embedded culture

- Lack of clarity about which board committee is responsible for ensuring that any reward schemes reflect the company's approach to risk
- Company culture where people are reluctant to admit risk management mistakes and do not welcome challenge
- Senior management does not give a clear lead on risk management or visibly support the risk and internal audit functions
- Culture and performance reward systems that do not support the business objectives and risk management systems

Board discussion

- Board papers and processes that fail to allow risk management discussion and cause time to be used unproductively
- Insufficient breadth of risk management experience and expertise on the board and/or board committees
- Non-executive directors lacking understanding of the risks inherent in the company's business model
- Risks associated with major transactions or projects not adequately assessed or discussed at board level

Capabilities and experience

- Inability to assess whether employees are listening to, understanding and/or implementing what the board is saying
- Misaligned incentives that encourage either inappropriate risk-taking or excessive risk aversion
- Documented procedures for whistle-blowing, so that inappropriate behaviours can be reported, do not exist
- Lack of access to necessary risk management and internal control expertise, and no CRO in senior position

Information and communication

- Senior management does not communicate the desired culture and fails to demonstrate the necessary commitment to risk management
- Failure to communicate to its employees what risks are not acceptable and what is expected of them
- Lack of mechanisms for the board to assess whether employees have understood their risk management obligations
- Failure to communicate a consistent attitude to risk and mitigation, and defective internal risk communication

Accountability and delegation

- Too much responsibility is delegated to board committees so that some directors are not involved
- An inability to stop failing projects once they have gathered momentum, perhaps because of a risk information glass ceiling
- Unclear lines of responsibility and accountability often combined with excessive organisational complexity
- Existence of a 'blame culture' where people are reluctant to admit mistakes and do not welcome challenge

Advice and assurance

- Risk managers are prevented from addressing risks emanating from the upper echelons of the company
- Existence of significant regulatory problems, possibly including poor relationships with regulators
- Managers who do not accept the need for the more formal risk control and information processes
- Failure to acknowledge emerging risks, and inability to acknowledge and analyse the causes of failure

6 Lloyds Avenue
London
EC3N 3AX
Ph. +44 207 680 3088
Fax. +44 20 7702 3752
email: enquiries@airmic.com
www.airmic.com