Deloitte.

Governance *in focus*
Risk management: getting your house in order

A Deloitte Academy publication
February 2015

Contents

What do the updates to the UK Corporate Governance Code mean for the corporate sector?

Introduction

Significant changes have been made to the requirements to managing and reporting of risk which apply to listed companies for accounting periods beginning on or after 1 October 2014. The extent of the changes is only just beginning to be understood. All readers are now in this new regime, but can you say you have reviewed your processes to ensure your company is ready? This edition of Governance in focus provides a practical perspective on the impact and required actions.

There has never been more focus on how organisations identify and manage risk: from regulators, to investors to senior executive management; companies are under pressure to be able to articulate clearly how they identify risks to their business and how they ensure these are being managed within an agreed risk appetite. This will also have implications for how the corporate sector thinks about its risk assessment, measurement and aggregation approaches.

Effective governance is a critical aspect of a successful business: it supports management in executing strategy, managing costs, responding to risk, attracting investment, achieving regulatory compliance and making better, and faster decisions. But as an organisation's risk profile changes, with new risks emerging and the speed and impact with which risks can materialise accelerating, internal control systems that support good governance need to adapt to be more agile and flexible.

The FRC has replaced its existing 'Internal control: Guidance for Directors' (2005) and 'Going Concern and Liquidity Risk: Guidance for Directors' (2009) with one set of integrated guidance which also reflects their 2012 'Boards and Risk' paper. This implements the Sharman principles on going concern, taking on board feedback from the FRC's three consultations on the subject.

Boards are now required to have one comprehensive and ongoing process to consider risk identification and management, including the assessment of solvency and liquidity risks. In addition, the board will need to determine whether the company is able to adopt the going concern basis of accounting, provide a statement of longer term viability, and provide enhanced reporting on risk management and internal control systems.

The Code changes

The changes to the UK Corporate Governance Code introduce two new board statements and a requirement for monitoring of risk management and internal controls. As with all Code provisions, these apply on a 'comply or explain' basis. In its January 2015 report 'Developments in Corporate Governance and Stewardship 2014', the FRC reminds companies and investors that simply complying with the Code without giving due consideration to what is appropriate and relevant reduces the flexibility that the 'comply or explain' approach aims to achieve. We expect that a good number of companies will be explaining a journey of implementation of these requirements during the course of at least one year.

New board statement 1 – Robust assessment of principal risks

The directors should confirm in the annual report that they have 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 – describe those risks and explain how they are being managed or mitigated. (Code Provision C.2.1)

New board statement 2 – Longer term viability statement

Taking account of the company's current position and principal risks, the directors should 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. The directors should 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 over the period of their assessment, drawing attention to any qualifications or assumptions as necessary. (Code Provision C.2.2)

New board requirement – Monitoring risk management and internal controls

The board should **monitor the company's risk management and internal controls and**, at least annually, carry out a review of their effectiveness, and report to shareholders that they have done so. The **monitoring and** review should cover all material controls, including financial, operational and compliance controls. (Code Provision C.2.3)

Highlighted text denotes new wording in the Code

What is the status of the new, integrated guidance compared to the 'comply or explain' Code provisions? The FRC issues guidance to assist boards and board committees in considering how to apply the UK Corporate Governance Code to their particular circumstances. The guidance is intended to bring together elements of best practice for risk management; prompt boards to consider how to discharge their responsibilities in relation to the existing and emerging principal risks faced by the company; reflect sound business practice, whereby risk management and internal control are embedded in the business process by which a company pursues its objectives; and highlight related reporting responsibilities.

The role of non-executive directors and board committees

Non-executive directors and board level committees play a critical role in ensuring that management is robustly challenged as to how principal risks are being identified, managed and monitored. This publication includes a number of questions which we believe non-executive directors should be asking management. This increased level of challenge will continue to contribute to organisations focussing more time and resource on how risk is managed. It is important to remember that, under the Code (Provision C.3.2), it is the audit committee's responsibility to review the company's internal control and risk management systems unless expressly addressed by a separate board risk committee comprised of independent directors, or by the board itself.

Key challenges

In our view the FRC's updates to the UK Corporate Governance Code and the content of the Guidance summarises the practice we see in operation in leading organisations at the present time (although few organisations have implemented all the dimensions that are being promulgated as best practice and now need to be addressed). For the majority of businesses, especially those in less regulated industries, we believe that the adoption of these changes will likely represent a significant challenge.

We have highlighted some of the challenges below:

Key challenges of the new guidance	
Robust assessment of principal risks	• Agreeing the level of risk the organisation is willing to take to achieve its strategic objectives (determining its "risk appetite"). • Organisations will have to ensure that they are operating a robust mechanism to identify their 'principal' risks – in addition, organisations will need to assess and disclose both the likelihood and impact of the individual principal risks identified and the aggregate impact of those risks. • For many companies this will involve a significant evolution of their risk management processes; especially in the consideration of strategic risks and how these risks are identified and managed; and in the processes in place to assess and quantify the potential impact of principal risks both individually and in aggregate. • To effectively and efficiently identify and manage risk we believe organisations should consider and challenge how integrated their governance framework is, and how effectively the constituent parts link together.
Longer term viability statement	• Organisations will have to prepare a 'viability statement'; stating that they have a reasonable expectation that their company will remain viable for a period they need to define. This will require the board to be closely involved in the risk process throughout the period and to consider carefully how to provide a meaningful statement. • Boards will have to decide early on how much work or assurance is required to support making this statement. In some cases the assessment may be relatively qualitative, for others, more complex modelling solutions may be appropriate.
Monitoring risk management and internal controls	• An increased focus on monitoring an organisation's system of risk management and internal control will encourage companies to challenge themselves as to how effective their current monitoring processes are. • Management should consider a number of aspects of their risk management and internal controls monitoring processes: from the management information they collate, to the effectiveness and co-ordination of the various assurance functions within their business, to the opportunities improved technology can bring in real-time understanding of the control environment. • There will need to be agreement of how 'material controls' and 'significant failings and weaknesses' are to be defined in the context of the organisation from the outset of the financial year. The Guidance does not define these terms and makes it clear that this is an area for board judgement. • Governance responsibilities in this area will need to be clearly defined.
Reporting and disclosure	• External reporting of the principal risks identified will need to become increasingly specific to the particular organisation and circumstances. Disclosure will increasingly focus on how the risks identified are mitigated, since there is now a need to assess and report likelihood and impact. • In addition, companies will need to explain in the annual report what actions they are, or have taken to mitigate significant failings or weaknesses in material controls identified in the period. As with the viability statement this will require the board to carefully consider what 'significant' means in their context and the level of detail to disclose.

In the following sections we look in more detail at the three new requirements: the robust assessment of principal risks; the longer term viability statement; and monitoring risk management and internal controls. Plus we set out the key considerations for reporting on risk and provide a summary checklist for boards to assist with meeting all the new requirements. Effective boards will welcome the opportunity to improve their business practices and how risks are managed and mitigated.

Robust assessment of principal risks

The FRC guidance states that the board should:

- identify the principal risks facing the company and evaluate the likelihood of their incidence and their impact if they were to materialise;
- assess the availability and likely effectiveness of actions that they would consider undertaking, either in advance or when a trigger event occurs, to avoid or reduce the impact of the underlying risks; and
- be aware of those risks (or combination of risks) that could seriously affect the future performance, solvency or liquidity of the company.

The FRC Guidance on the Strategic Report (2014) defines a principal risk as: **A principal risk is a risk or combination of risks that can seriously affect the future prospects or reputation of the entity. These should include those risks that would threaten its business model, future performance, solvency or liquidity.** This will include strategic, financial, operational, reputational, behavioural, organisational, third party and external risks.

Some organisations have, over the past few years, perhaps directly as a result of the financial crisis, taken steps to address this challenge already. We have seen increasingly senior levels of management closely involved in the risk process; more consideration of strategic risks, emerging risks and "black swan events" together with increased focus on how they are being managed and whether more can be done to increase the organisational resilience. This increased level of focus on principal risks will, when done well and embedded in business processes, support organisations to deliver their strategic objectives and focus on what really matters rather than risk assessment being a worthless annual paperchase.

In order to undertake a robust assessment of principal risks, boards will need to have awareness of and confidence in the effective operation of the following processes:

Risk appetite	• The board must have defined a clear risk appetite and set appropriate, quantified thresholds. Most importantly, the board must be comfortable that principal risks are being appropriately managed to a net acceptable level which falls within the agreed risk appetite. Developing a risk appetite framework requires director input and understanding, driven by both top down board leadership and bottom up management involvement. • An effective risk appetite framework will help directors to identify and determine the relative positions of its risk capacity, risk profile and risk appetite when evaluating and pursuing strategy and to take recommended corrective action where necessary. The key is achieving an appropriate balance between risk and reward such that returns are optimised.
Assessment & identification	• Many organisations do not yet have a risk process in place that goes sufficiently beyond the identification of risks: the detailed work required to really understand these risks and to distil *principal* risks from the risk register, their probability of occurrence and their potential gross impact, how they are being mitigated and monitored and whether the risk profile is changing is often either absent, or happening in an uncoordinated way with limited transparency to senior management. • Principal risks should be the risks that are being discussed at board level. If they are not, there is a need to decide where changes should be made either to the register or to the focus of board discussions! It is also important to ensure that a sufficiently wide group of stakeholders and subject matter experts have been allowed to provide their inputs and perspectives.
Impact & residual risks	• The board must be clear about the extent to which there are residual risks even where risk management processes, internal controls and contingency plans are operating effectively. Integration and ongoing management and monitoring is what reduces risk to a net residual which should be within the organisation's risk tolerance threshold for that item.
Scenario testing and integration into business planning	• In order to assess the company's resilience to particular situations and its adaptability, the board should consider undertaking stress tests and reverse stress tests to assess different scenarios. To be effective, risk management needs to be truly embedded into how an organisation operates, in other words there needs to be integration with key business planning and decision-making processes. Risk management needs to be dynamic, particularly in the current environment. If embedded, the board is much better placed to respond rapidly when the risk profile changes.

Longer term viability statement

New Code provisions (C2.1 and C2.2) require the company directors to 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 over the period of their assessment, drawing attention to any qualifications or assumptions as necessary'.**

Boards are encouraged to assess what processes they need to follow to allow them to have a 'reasonable expectation' and to decide what is an appropriate period of assessment? Of course, there is a significant level of judgement involved in both decisions and the outcome will vary by business and by industry.

We believe there are a number of options to consider in assessing whether there is a 'reasonable expectation'. These include performing:

- A qualitative assessment of the principal risks in aggregate; considering both the potential impact and likelihood;
- Scenario analysis including the principal risks identified (i.e. developing a number of scenarios where one or more of the principal risks identified occur and assessing the overall impact on the business); and
- Modelling of the principal risks both individually and in aggregate to assess the potential impact on longer term viability over the period identified.

	Qualitative	Scenario	Modelling
Complexity	Low	Medium	High
Data requirements	Low	Medium	High
Outputs	Qualitative Assessment	Directional	'At risk' measures individual risks & combinations of risk

The FRC has worked hard to develop wording which will allow boards the flexibility to provide disclosure tailored to the specific circumstances of the company. In the *Guidance on Risk Management, Internal Control and Related Financial and Business Reporting* the following comment is made about reasonable expectation and period covered for the new viability statement required by provision C.2.2:

> "Reasonable expectation does not mean certainty. It does mean that the assessment can be justified. The longer the period considered, the more the degree of certainty can be expected to reduce.
>
> That does not mean that the period chosen should be short. Except in rare circumstances it should be significantly longer than 12 months from the approval of the financial statements. The length of the period should be determined, taking account of a number of factors, including without limitation: the board's stewardship responsibilities; previous statements they have made, especially in raising capital; the nature of the business and its stage of development and its investment and planning periods."

In relation to the qualifications or assumptions referred to in the board statement, the Guidance states:

"Any qualifications or assumptions to which the directors consider it necessary to draw attention in their statement should be specific to the company's circumstances, rather than so generic that they could apply to any predictions about the future. They should be relevant to an understanding of the directors' rationale for making the statement. They should only include matters that are significant to the company's prospects and should not include matters that are highly unlikely either to arise or to have a significant impact on the company. Where relevant, they should cross-refer to, rather than repeat, disclosures given elsewhere".

Organisations will therefore need to assess their current process for aggregating the potential impact of the risks identified and in some cases develop new or additional processes to allow them to make the statement.

The Guidance also makes the point that there may be a degree of overlap both with the disclosures on principal risks and with disclosures over any material uncertainties relating to the going concern basis of accounting, and that companies should consider how best to link these disclosures.

It is important to remember that the statement is about longer term viability and not a statement of maintainable earnings. It should be a statement that directors do not feel too uncomfortable about as they have choice around the lookout period and the level of detail provided – they can use their own words.

Monitoring risk management and internal controls

The updates to the UK Corporate Governance Code also include some significant changes to the Code's wording on risk management and internal control systems. We believe that the changes are designed to emphasise the importance of the board monitoring the company's risk management and internal control systems throughout the year, rather than undertaking a one-off, annual review as required by the 2012 code provision. As stated in the Guidance: "Effective and ongoing monitoring and review are essential components of sound systems of risk management and internal control".

The board should monitor the company's risk management and internal control and, at least annually, carry out a review of their effectiveness, and report to shareholders that they have done so. The monitoring and review should cover all material controls, including financial, operational and compliance controls (Code Principle C.2.2).

The board should explain what actions have been or are being taken to remedy any signficant failings or weaknesses (Guidance on Risk management, internal control and related financial and business reporting para 58).

In order to monitor risk management and internal controls effectively, boards will need to ensure that processes and information are in place to be able to answer the following key questions at regular intervals throughout the year:

- How effectively have risks been assessed and the principal risks determined?
- How have the principal risks been managed or mitigated?
- Have all material controls been identified?
- Do monitoring processes and risk indicators cover all principal risks and material controls?
- Have necessary actions been taken promptly to remedy any significant control 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?

Definitions

A key issue to address at the earliest opportunity will be agreement of how 'material controls' and 'significant failings and weaknesses' are to be defined in the context of the organisation. The Guidance does not define these terms and makes it clear that this is an area for board judgement. It is important that there is clarity of these definitions from the outset of the financial year if an effective monitoring system is to be established. The board should be satisfied that, having made a decision, they would be able to provide a robust defence of the definition if challenged by shareholders, regulators or other stakeholders.

The external auditor will need to be involved in these discussions of definition as there have been corresponding changes to auditing standards which will require the auditor to state if they have anything material to add to the disclosures the board makes about the principal risks and monitoring of risk management. Reporting on internal controls, and in particular reporting on significant failings or weaknesses identified in the system of internal control, is covered by the auditors overall requirement to consider whether the annual report, taken as a whole, is fair, balanced and understandable.

Establishing an effective monitoring process

There are a number of ways an organisation can monitor the effectiveness of its system of risk management and internal control: from timely and insightful management information, through to assessing the output from the organisation's embedded control structures which provide assurance (not just internal audit).

To ensure an organisation's monitoring is effective, efficient and sustainable it is important to focus on a number of areas such as:

- Establish **clear roles and responsibilities** across board committees such that each committee is aware of their responsibilities and those of others committees to avoid overlap or gaps.
- Carry out a comprehensive **mapping exercise** to establish what processes exist and where there are gaps.

- **Have a clear view of value drivers** – which activities really create significant value for the organisation, or, conversely, could destroy significant value if not managed effectively?

- Ensure that the organisation has **timely and good quality management information** that links clearly to the risk areas identified and how these are managed. Many organisations generate a huge amount of data but have not effectively linked these data points to high value activities or defined thresholds for the metrics that may indicate additional/less mitigating activity is required.

- **Consider the use of technology in risk systems** – technology can both improve the monitoring of the system of internal control and deliver efficiencies to the organisation. The range and quality of 'GRC' (Governance, risk and compliance) tools available has increased significantly in recent years.

- **Understand sources of assurance and their activities** – taking a broader view on assurance than just internal audit and building a picture of the 'three lines of defence' against each key activity will allow organisations to ensure there are no unnecessary overlaps or significant gaps in assurance plans.

- Consider and challenge **the remit and effectiveness of the internal audit function**: is internal audit providing the appropriate depth of assurance across the broad range of risks facing the organisation? Does internal audit have the requisite remit, capability and experience to deliver robust assurance? Internal Audit departments play a key role testing and reporting on the effectiveness of the system of internal control. It is therefore critical that these functions are 'fit for purpose'.

There is no 'right answer' when it comes to how an organisation can, most effectively, monitor its system of internal control: it will depend on the types of activities that are key to creating or destroying value at the company; the technology infrastructure in place to provide accurate and timely information; the scope and quality of assurance functions and the organisational structure and size of the business.

However, directors should develop a clear view on the framework in place for monitoring the system of internal control; challenge this framework on a regular basis and ensure that it is proportionate to the risks facing the organisation. We believe that the FRC changes will prompt most organisations to review their existing processes in light of the above questions, both to better understand their current position and to identify areas of enhancement more effectively, both to achieve benefits of this as a goal in itself and to comply with the latest guidance.

Compatibility with the COSO Framework

In our view the FRC guidance includes principles which are wholly compatible with the latest edition of the US Committee of Sponsoring Organisations of the Treadway Commission's (COSO) framework on internal control issued in May 2013. The updated COSO framework contains 17 principles across five key internal control components – control environment, risk assessment, control activities, information and communication and monitoring activities.

COSO is a useful guide in implementing aspects of the FRC guidance, particularly in the area of ongoing monitoring of controls. It shouldn't be in any way incompatible with the FRC guidance.

Risk reporting and disclosure

The FRC is also looking to improve the quality and level of detail around risk disclosures. The Guidance states:

> The board should provide clear and concise information that is tailored to the specific circumstances material to the company, and should avoid using standardised language which may be long on detail but short on insight.
>
> Organisations should focus on six main aspects of risk disclosure:
>
> • sufficient specific detail that a shareholder can understand why they are important to the company;
>
> • details of any significant changes in principal risks, such as a change in the likelihood or possible impact or new risks included;
>
> • a description of the likelihood of the risk;
>
> • a high-level explanation of how the principal risks and uncertainties are being managed or mitigated;
>
> • an indication of the circumstances under which the risk might be most relevant to the company and its possible impact; and
>
> • for a more generic risk or uncertainty, a description of how that risk or uncertainty might affect the company specifically.

The FRC has made it clear that these disclosures should be included in the Strategic Report so that the directors are covered by the safe harbour provision in the Companies Act 2006.

We support the FRC's attempts to improve the quality of risk reporting. While much progress has been made in recent years, more details along the lines suggested will provide much better quality information for investors. In addition to clear risk descriptions specific to the circumstances of the company, we believe it is important to link the strategy and business model disclosures with the principal risks and uncertainties. The proposed new disclosures acknowledge that drawing out both an explanation of the possible impact and timing of risk as well as mitigation being undertaken provides much more meaningful information and will facilitate better investor engagement on this topic.

In addition to the above there is also a significant new recommendation included in the Guidance:

> **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.**

This is a significantly higher level of disclosure than that included in the previous guidance which required a board to confirm that necessary actions have been or are being taken (without explaining what those actions are).

The board will have to assess what a 'significant' failing or weakness is and how much information to report on the actions taken. Note that the guidance does add that 'any disclosure which would be prejudicial to business interests does not have to be made'. Boards will wish to consider this definition early so they receive scored reports on failings and weaknesses during the year, for example from internal audit, within this new context.

Summary

In our view the changes to the UK Corporate Governance Code and the FRC Guidance are very much aligned with where multiple stakeholder groups are heading: all want to see organisations develop and improve their mechanisms for identifying, assessing, measuring and managing risks to their business. Focusing on these important areas will deliver real business benefits, not just compliance with the UK Corporate Governance Code: more highly developed governance systems will improve business decision making and provide greater confidence to boards, investors and wider stakeholder groups.

However, for many organisations these new requirements will represent a significant challenge. Management will need to challenge their existing risk management and internal control systems, and, where necessary, invest appropriately in developing these to meet the challenges outlined in this paper.

Key mobilisation steps

We believe the following are the key steps you need to take to get your organisation in a position to start meeting these new requirements:

- review your organisation's risk and control governance structure in light of new guidance to produce a gap analysis;
- agree a framework for articulating your risk appetite if not already in place;
- revisit and reassess those risks deemed to be principal risks and consider the likelihood of those principal risks and the quantification of likely impact, both individually and in aggregate;
- ensure "ongoing monitoring" is built in to the board/committee process and agendas from the start of the year;
- many organisations are developing a risk dashboard to track how the organisation is managing key risks identified;
- agree definitions for identifying and reporting significant failings or weaknesses in the risk management and internal control systems. Also, consider whether there is a need to revisit internal audit/risk reporting methodology;
- consider viability statement decisions: how long will the lookout period be and what level of work to support the statement will be required, including modelling and risk/impact scenario planning;
- agree a clear accountability structure and timetabled action plan; and
- engage in discussions with your auditor, who will have expectations from you, and their own reporting responsibilities, to fulfil.

Contacts

Contact us – corporategovernance@deloitte.co.uk or

Risk management

Hans-Kristian Bryn
+44 20 7007 2054
hbryn@deloitte.co.uk

Internal audit

David Noon
+44 20 7007 3660
dnoon@deloitte.co.uk

Corporate Governance

William Touche
+44 20 7007 3352
wtouche@deloitte.co.uk

The Deloitte Academy

The Deloitte Academy has been designed for main board directors of listed companies. The Deloitte Academy provides support and guidance to boards, individual directors and company secretaries of listed companies through a programme of briefings and update sessions. Bespoke training for the whole board or individual directors is also available.

If you would like further details about the Deloitte Academy, including membership enquiries, please email enquiries@deloitteacademy.co.uk.

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 2 New Street Square, London EC4A 3BZ, United Kingdom. Tel: +44 (0) 20 7936 3000 Fax: +44 (0) 20 7583 1198.

Designed and produced by The Creative Studio at Deloitte, London. 41303A