UK Corporate Governance Code: Raising the bar on risk management

Why this is not business as usual and what you need to do to comply

September 2014

"The FRC's amendments to the UK Corporate Governance Code and Directors Guidance (the Code) are intended to raise the bar on the way organisations think about, manage and report on their principal risks and culture."

Simon Perry, *partner, PwC*

pwc

What's on your mind?

The revised Code will intensify the spotlight on effective risk management. Do you fully understand its requirements and are you confident that your current system will satisfy them?

The revised Code is intended to drive a step-change in the way risk is managed and improve the insight that can be derived from related disclosures in annual reports and accounts. The FRC is clear that this is not business-as-usual; however, our conversations tell us many organisations may have misinterpreted this, underestimating the extent of the change that may be required to satisfy the intent. Are you one of them?

The revised Code remains high level, documenting principles-based guidance specifically requiring you to:

- confirm that a robust system of risk management has been developed and is fully integrated into normal management and governance processes (e.g. business strategy and planning)
- define and articulate your appetite for risk in key areas
- describe your principal risks and how they are being managed
- confirm the identification and assessment e.g., via techniques such as stress and reverse stress testing, of all principal risks
- review and confirm the ongoing effectiveness of key operational, financial and compliance controls
- communicate, incentivise, embed and measure behaviours that create a strong risk and control environment and confirm the existence of an appropriate culture
- consider how much assurance you need over the risk management process, how it will be objectively obtained and what should be communicated externally

The revised Code inevitably increases the focus on risk management and also includes a recommendation that group auditors provide external assurance over the completeness and material accuracy of the statements you make.

Most large organisations have some kind of system for managing risk, although many do not meet the criteria to be described as enterprise risk management (ERM), i.e., providing a consistent view of risk that is aligned and integrated with strategic decision making and reflecting a defined risk appetite.

Our point of view

"Good risk management is not a compliance activity, but a fundamental driver of value and competitive advantage"

For you to confidently provide the required risk information and assurances, you need to be sure that your ERM system is fit for purpose and provides a complete and accurate view of your risk profile; if it does not, you risk being exposed by increased scrutiny from your stakeholders. How confident are you?

To comply with the proposed amendments, boards will need to consider a number of questions, including:

- How can we practically define and articulate our risk appetite?
- What does a robust ERM system look like and how do we compare with our peers?
- Have we identified and assessed all of our principal risks?
- How do we promote the necessary behaviours and measure whether the right culture is in place?
- What form should the required disclosures take?

It's important to understand the difference between risk disclosure and risk management. You need to do both well. For audit committees, the revised Code means deriving certainty that ERM has been sufficiently developed and embedded; that they 'can walk the talk'. The following key ERM components will likely receive scrutiny and require enhancement.

Risk appetite – are you biting off more than you can chew?

Even in financial services, where risk appetite has been well defined for some risk categories for years, this is an area which is relatively immature. While a lot of business activity and theory has been touted, organisations generally struggle to practically define and articulate their risk appetite in a way that adds value. Some executives will argue that risk appetite does not need to be formally defined, being inherently considered as part of the decision making process; to an extent this is true, but this view is often biased by factors such as a reluctance to address conflicting opinions of executives and NEDS or to invest the time required to achieve success. With the right guidance, you can define clear, measurable parameters aligned to your purpose, vision and values, that provide the necessary basis for driving enhanced, more consistent risk decision making.

Effective monitoring – managing crises is missing the point!

The FRC guidance reflects the reality that effective risk monitoring is a prerequisite to ensuring continuous business operation in line with desired appetite levels. In the absence of a reliable monitoring system, any breaches of defined appetite may be identified too late. While a strong capability to react to crises is admirable, this is not the point of risk management; organisations need to focus on avoiding them in the first place and better capitalising on opportunities. The Code requirement to not only monitor risk, but also derive ongoing satisfaction that key controls are functioning effectively is a big ask and one that you need to respond to. Indeed, some forward-looking organisations are starting to explore and capitalise on technology-driven opportunities, harnessing the exploding data environment to generate genuine, leading risk awareness and insight.

The right culture – have you forgotten something?

The importance of promoting a strong culture aligned to organisational values in order to successfully embed risk management is often overlooked, but is one of the key reasons why ERM fails to deliver on expectations. Embedding an appropriate culture demands more than undertaking employee surveys and tracking resulting scores, it means defining and embedding the required behaviours and monitoring their drivers to provide insight on their effectiveness. For example, helping to understand and answer questions such as, 'how do we know that an apparent one-off issue is not a deeper, systemic cultural problem due to a reluctance to challenge?' Such an understanding will also provide a basis for reporting what is being done to instil the required behaviours and measure performance.

Providing assurance – do you have the required confidence?

The FRC clearly wants to discourage the use of 'boilerplate' language that can make it impossible to tell how good an organisation is at managing risk. With an expectation of more specific and detailed disclosures, eg, around continuing control effectiveness, directors will want to have confidence in the accuracy of their statements. In support of this, we expect many will seek out external assurance to provide comfort similar to that derived from the financial audit.

When to act

The revised Code applies to accounting periods beginning on or after 1 October 2014. Companies should take appropriate actions, where required, to improve their systems prior to the start of the financial year for which they need to comply.

Here are some examples of when to act:

- You are not confident about the quality or robustness of your ERM system.
- You have been susceptible to undesirable surprises or are continuously firefighting.
- You are uncertain how your risk appetite can be practically articulated and add value.
- Conduct and behavioural failures have occurred in your organisation and their root causes are unclear.

What good looks like

While there is no one-size-fits-all approach, the following principles will help you ensure the right building blocks are in place:

- The board visibly promotes and supports, both in word and spirit, the importance of effective risk management.
- Risk management is wholly integrated into group business planning and strategic decision making.
- A formal definition and articulation of your risk appetite for all major risk areas exists, providing practical guidance on acceptable risk and reward.
- Robust analysis of risk information, focusing challenge and resource on critical risk areas is undertaken.
- An embedded early warning system provides timely awareness of changes in control effectiveness and material areas of risk.
- An understanding exists of the drivers of desired behaviours and the alignment of performance and incentivisation structures.
- Transparent risk disclosures that balance stakeholder insight with protecting competitive advantage are undertaken.

How we can help

Drawing on our experience with some of the world's leading organisations of developing and embedding numerous ERM systems, and our innovative approach to measuring and strengthening culture, we can help you satisfy both the word and spirit of the Code. Typical areas of support include:

- Conducting maturity and effectiveness reviews of your current ERM system and peer group benchmarking to identify areas of good practice and those requiring development
- Developing practical, principles-based ERM frameworks or enhancing specific risk management components such as quantification and stress testing
- Facilitating definition of risk appetite to practically articulate your desired risk taking approach
- Crafting informative disclosures that balance evidencing the required assurances with protecting competitive positioning
- Defining robust key risk indicators (KRIs) and deploying technology-based early warning risk monitoring solutions that address the common resourcing and cost challenges
- Bringing behaviours to life, understanding what drives them, and facilitating their measurement to help organisations successfully cultivate and embed the desired risk culture and mindset

What you gain

In addition to compliance with the Code, you can expect to realise the following benefits from investing in development of your ERM capability.

Enhanced insight
Early and more accurate visibility of changes in the risk landscape in areas that could materially impact corporate objectives, facilitating more timely and informed management intervention.

Better decisions
Increased awareness and understanding of the board's desired risk and reward trade-offs, driving decision making consistency throughout the organisation.

Superior performance
Identifying and embedding the behaviours that generate competitive advantage, and the agility and flexibility needed to anticipate change and capitalise on opportunities.

Increased stakeholder trust and confidence
Reduced performance volatility and increased consistency in delivering objectives, which, combined with greater levels of transparency, engenders stakeholder confidence and potentially enhanced valuations.

Changing your perspective

The revised Code does not create onerous new compliance requirements; rather, it provides a platform for leading organisations to differentiate themselves.

History consistently shows that organisations that fail to effectively manage risk, often themselves fail.

What sort of case study do you want to be?

Delivering value

Our deep technical expertise developing practical systems of risk management, a track record of successful project delivery with leading organisations, and experience shaping corporate disclosures, allow us to provide invaluable support in helping clients derive real value from their risk management activities, as well as satisfying Code requirements.

Case study: risk appetite definition

Our client was decentralising its decision making authority and the board wanted to ensure its business units consistently took the right risks for the right returns. Having determined the organisation's key objectives, stakeholders and risk profile, we identified core decision points where risk-taking guidance would be valuable. Building on existing articulations where possible, we drafted a group level appetite statement, incorporating metrics to promote measurability. The engagement challenged management and the board to explicitly consider their appetite for specific risks and promoted the awareness and value of risk management throughout the organisation.

Case study: embedding appropriate culture and behaviours

We have developed comprehensive cultural assessment and measurement approaches to enable banks to effectively monitor their behaviours. One of our clients had recently conducted a major behavioural change programme and we were engaged to review its design and operational effectiveness; providing comfort to management and the regulator that the required change was occurring. Our work included testing key controls to ensure that the right people are recruited, promoted and trained, and that consistent values and behaviours are embedded across the business.

Contact:

Simon Perry
simon.perry@uk.pwc.com
+44(0)20 7213 4242

Matt Elkington
matt.elkington@uk.pwc.com
+44(0)20 7804 1417

Richard Sykes
richard.sykes@uk.pwc.com
+44(0)20 7804 5466

www.pwc.co.uk

140929-173752-AJ-OS