Deloitte.

The Deloitte Academy
November 2019

Internal control and the board: What is all the fuss about?

Headlines

- The UK Corporate Governance Code already establishes a clear responsibility on the whole board to establish a framework of prudent and effective controls—however, underlying the calls for a US style internal control attestation are very real questions as to whether that responsibility goes far enough and whether there is sufficient guidance for boards, together with sufficiently detailed information from management, to execute this responsibility effectively.
- In particular boards may not be obtaining sufficient assurance around the effectiveness of IT controls given the complexity and interdependency of the IT infrastructure which exists in many companies today.
- The extent of work performed by external auditors is not well understood—careful questioning of auditors in relation to their audit scope and approach could reveal much about the control environment.
- Boards should not wait for further announcements from the Government or FRC/ARGA before taking action in this area, particularly if they are not able to answer the questions which we raise throughout this publication.

A reminder of the current UK Corporate Governance Code requirements

- **Overarching board responsibility from Code Principle C**: The board should establish a framework of **prudent** and **effective** controls, which enable risk to be assessed and managed.
- **Secondary board responsibility from Code Principle O**: The board should establish procedures to manage risk, **oversee the internal control framework**, and determine the nature and extent of the principal risks the company is willing to take in order to achieve its long-term strategic objectives.
- **Board activity prescribed by Code Provision 29**: The board should **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.
- **Audit committee responsibilities prescribed by Code Provision 25**: **Reviewing** the company's internal financial controls and internal control and risk management systems, unless expressly addressed by a separate board risk committee composed of independent non-executive directors, or by the board itself.

So what does this mean in practice?

The FRC's Guidance on Risk Management, Internal Control and Related Financial and Business Reporting states that "effective and on-going monitoring and review are essential components of sound systems of risk management and internal control". It recommends the following disclosure:

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.

So in putting together a robust process, the Guidance recommends that, on an ongoing basis, the board should consider:

- how effectively the risks have been assessed and the principal risks determined;
- how the principal risks have been managed or mitigated;
- whether necessary actions are being taken promptly to remedy any significant failings or weaknesses; and
- 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 on-going processes.

In addition, the annual review of effectiveness should consider:

- the company's willingness to take on risk (its "risk appetite"), the desired culture within the company and whether this culture has been embedded;
- the operation of the risk management and internal control systems, covering the design, implementation, monitoring and review and identification of risks and determination of those which are principal to the company;
- the integration of risk management and internal controls with considerations of strategy and business model, and with business planning processes;
- the changes in the nature, likelihood and impact of principal risks, and the company's ability to respond to changes in its business and the external environment;
- the extent, frequency and quality of the communication of the results of management's monitoring to the board which enables it to build up a cumulative assessment of the state of control in the company and the effectiveness with which risk is being managed or mitigated;
- issues dealt with in reports reviewed by the board during the year, in particular the incidence of significant control failings or weaknesses that have been identified at any time during the period and the extent to which they have, or could have, resulted in unforeseen impact; and
- the effectiveness of the company's public reporting processes.

The FRC Guidance makes clear that the assessment and processes described above should be used coherently to inform a number of distinct but related disclosures in the annual report and accounts including the statements on longer term viability and the going concern basis of accounting. The purpose of such 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. In putting together these disclosures there is a balance to be struck between compliance and also taking the opportunity to provide a more forward-looking and proactive dialogue which can reinforce the robustness of the board's oversight activity and highlight any potential issues which are being actively managed, e.g. in relation to a major IT systems change programme.

The case for change in the UK—why are we talking about a UK Sarbanes-Oxley?

Recommendation 51 of Sir John Kingman's Independent Review of the Financial Reporting Council: BEIS should give serious consideration to the case for a strengthened framework around internal controls in the UK, learning any relevant lessons from operation of the Sarbanes-Oxley regime in the USA. The pros and cons of options for change should be analysed and consulted upon, giving special consideration to the importance of proportionality in relation to the size of the company.

A number of respondents to Sir John's review suggested that there was a serious case for considering the introduction of stronger regulation in respect of companies' internal controls, similar to that applying in the USA under the Sarbanes-Oxley Act. In particular, there was support for this from members of audit committees on the grounds that, based on their experiences with US registrants, the legilsation is seen as having led to better financial reporting, fewer significant accounting restatements and a higher focus on greater clarity on the robustness of internal controls within an entity.

BEIS has welcomed this recommendation acknowledging that it is a "detailed and complex issue" and that options need to be explored. A consultation on those options is expected in Q1 2020.

What requirements does the Sarbanes-Oxley Act place on the various parts of the US governance ecosysytem?

In terms of reporting, under the current UK Corporate Governance Code, boards are only required to explain the process for their review of the effectiveness of the risk management and internal control systems rather than comment on the outcome of the review. The Sarbanes-Oxley Act is a much more demanding piece of legislation. Here is a summary of the requirements:

Management	Audit Committees	Auditors
Annually assess and report on the effectiveness of the internal controls over financial reporting	The audit committee must be made up of board members independent from management	Provide a report on the effectiveness of the internal controls over financial reporting (a tiering structure exists so not all entities have this requirement but all large equity listed entities would be covered)
Annually assess and report on the effectiveness of disclosure controls and procedures	The independent audit committee is directly responsible for the appointment, compensation and oversight of the external auditor and the services provided	Communications with the audit committee must include a discussion of critical accounting policies and key judgements & estimates used by the company, all alternative accounting treatments that have been discussed with management and the impact of alternative accounting treatments and disclosures
Disclosure of any material weaknesses in controls that would not prevent or detect a material misstatement in the financial statements	Companies must disclose whether there is at least one 'financial expert' on the audit committee	The lead engagement partner must rotate every five years
CEO and CFO must certify that they have reviewed the annual or quarterly reports; the financial information included is fairly presented; the report does not contain any untrue statement of material fact or omission that would make the financial statements misleading		Strict rules on the provision of non-audit services
CEO and CFO must acknowledge their responsibility for establishing, maintaining and evaluating internal controls over financial reporting plus disclosure controls and procedures		
CEO and CFO must certify that each periodic report containing financial statements complies with the US securities laws and fairly presents, in all material respects, the financial condition and results of operations		

The following types of controls need to be considered as part of the attestation provided by management:

Entity-level controls—e.g. the Code of conduct, HR recruitment policies, period-end financial reporting processes.

Process-level controls—these can be either manual (e.g. bank reconciliations, inventory counts, review of aged debtors) or automated (e.g. three way match of purchase orders, to invoice, to goods received note).

General IT controls—e.g. access controls that restrict the ability of unauthorised users to amend certain records or documents.

IT controls—why are they so critical and so challenging to get right?

Your IT environment and the controls over this are the fundamental building block upon which your internal control environment is built. Businesses are ever more reliant upon their IT systems to operate the business, interact with customers and suppliers and produce financial statements.

Effective IT controls are critical in ensuring:

Security
Ensuring that your systems and data are secure and appropriately protected from the risk of unauthorised access

Integrity
Ensuring that your systems are functioning as intended and you can rely on the accuracy and completeness of processing

Availability
Ensuring the resilience and redundancy of your environment to support ongoing operation and organisational viability

There are multiple challenges associated with implementing an effective IT control environment:

Complexity of the IT environment—is there a good understanding of the IT environment, particularly those systems critical to operations and financial reporting? This can be further complicated by the use of "shadow IT" (systems acquired and supported outside of the core IT function) and outsourcing to third parties, to support and operate your environment.

Multiple layers of IT—controls need to be implemented and operated across the multiple layers of the environment, including: the application; the relevant database; and, the underlying operating system.

Interdependency of controls—multiple layers of IT controls, operating in tandem, need to be deployed across the environment. For example, the controls to manage a change are only as good as the controls that restrict who can develop that change.

Questions for boards and audit committees to consider:

- How do you get assurance over the effectiveness of your IT controls?
- How integrated are your IT controls into your overarching internal control framework?
- How effective is your cyber security system?
- Have you a clear understanding of critical finance and operational systems, including data storage?
- Do you understand how management control "shadow IT" and controls operated by third parties?

What should boards be assessing the effectiveness of controls against?

To help build up a clear picture of 'what good looks like', boards could refer to a specific framework. A well-established and well-recognised internal control framework, against which to judge the effectiveness of internal controls, is the COSO framework. COSO is the acronym given to the framework which was developed by the Committee of Sponsoring Organisations of the Treadway Commission and received a considerable overhaul in 2013. Use of the COSO framework is not mandated by the Sarbanes-Oxley Act but the vast majority of companies reporting in the USA do report against the COSO framework. So what is it?

The framework recognises five components of internal control that need to be present and operating for a control environment to be considered effective. These components are further broken down into 17 principles (see below) and the framework provides specific points of focus as a guide to help with each of those principles

Control environment

01. Demonstrates commitment to integrity and ethical values.
02. Exercises oersight responsibilities.
03. Establishes structure, authority, and responsibilty.
04. Demonstrates commitment to competence.
05. Enforces accountability.

Risk assessment

06. Specifies suitable objectives.
07. Identifies and analyzes risk.
08. Assesses fraud risk.
09. Identifies and analyzed significant change.

Control activities

10. Selects and develops control activities.
11. Selects and develops general controls over technology.
12. Deploys through policies and procedures.

Information & Communication

13. Uses relevant information.
14. Communicates internally.
15. Communicates externally.

Monitoring activities

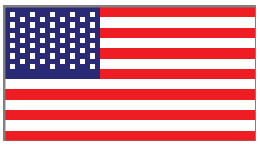
16. Conducts ongoing and/or seperate evaluations.
17. Evaluates and communicates deficiencies.

Questions for boards to consider:

- Is there benefit in a generally recognised framework to help define what good looks like?
- Should you have a conversation about the application of COSO or a similar framework?

How different are the UK and US approaches?

- Requirements set out in the UK Corporate Governance Code—accountability to shareholders
- Covers all material controls, including financial, operational and compliance controls
- Responsibility of and reporting by the whole board
- Disclosures explain the process of review undertaken, no requirement to confirm the effectiveness or otherwise of the controls
- Guidance also recommends that the board explains actions being taken to remedy and significant failings or weaknesses



- Requirements set out in legislation with associated sanctions
- Covers internal controls over financial reporting
- CEO and CFO responsibility for the effectiveness of those internal controls over financial reporting
- Disclosure on the effectiveness of controls over financial reporting—supported by documented evidence—plus auditors' attestation
- Disclosure of any material weaknesses in controls that would not prevent or detect a material misstatement in the financial statements

As set out above, there are substantive differences between the two approaches. In principle, there is alignment between the COSO framework and the FRC's Guidance yet some would argue that, within the UK, there is not a sufficiently clear vision of a framework which UK boards can use to meet their responsibilities under the Code to establish a "a framework of **prudent** and **effective** controls" and which can then be used to hold management to account through the board and audit committee's oversight roles.

What is the role of auditors in the UK?

It is possible that boards are under the impression that the auditors play a significant role in reviewing and/or assessing the effectiveness of internal controls—the reality is potentially very different.

International Standards on Auditing ("ISAs") require the auditor to evaluate design and determine implementation of controls over the significant risks they identify plus any other controls judged to be relevant by the auditor. Not all controls that relate to financial reporting may be relevant to the audit, any incremental testing is a matter for the auditor to determine using their judgement.

Under auditing standards the auditor must tell you about any significant deficiencies they have found in the course of their work but the scope of that work, in relation to controls specifically, may in fact be very limited. But it should be recognised that because there is very limited UK guidance on what constitutes effective controls there is also little guidance on how to interpret a significant deficiency.

Questions for audit committees to ask the auditors to clarify their position on controls:

- Are you adopting a controls reliance or a substantive approach in your audit?
- Why can you not adopt a controls approach?
- Which of our controls do you consider to be relevant to your audit, by process and by function?
- Do we have controls which you elect not to test because you believe they are not operating effectively?
- How does the narrative in our Annual Report on controls compare to best practice?
- What do you plan to publically report this year end as your observations on internal control?

What should boards be doing now?

Notwithstanding the ongoing Government activity which could take the UK in a more prescriptive direction around the board's responsibilities for internal controls, there remains today a responsibility, under the UK Corporate Governance Code, to establish a framework of prudent and effective controls, to oversee that framework and to perform an annual review of effectiveness.

To meet this responsibility we believe boards and audit committees should take the opportunity now to look carefully at the control frameworks within their organisations. In our opinion boards who confirm they have reviewed the effectiveness of their internal controls must as a minimum have done the following activities:

- have a documented financial risk assessment
- have a documented fraud risk assessment
- have identified and documented all material controls, based on their risk assessment, and have tested and be monitoring their operation
- have clearly defined entity level controls
- have decent transaction process and control documentation, with clear process and control owners, and testing of controls design and operating effectiveness with clear linkage to risk
- be clear which IT systems are critical, and have defined their general IT controls, again with clear risk linkage, ownership, documentation and testing
- ensure all material controls are signed off by management as operating effectively on a regular basis
- operate a clear hierarchy of delegated authorities from the board

Areas some more sophisticated organisations are addressing also include consideration of the appropriate mix of controls—for example, over-reliance on management review controls can lead both to lack of precision and controls really should be supporting business processes. In addition, organisations need to consider what information is used in operating a control, to ensure that information is appropriate. The classic example is the debtor ageing report—is this aged from invoice date or due date—and how free from "re-aging" is it? Another common area is outsourced services—where organisations need to ensure that the controls around these are operating effectively.

Boards that believe they have a way to go on this journey may wish to start with the following questions:

- Are the risk management and internal control systems appropriate for the company's business model?
- How are authority, responsibility and accountability for risk management and internal control defined, co-ordinated and documented throughout the organisation?
- Has a financial risk assessment been undertaken? What does it tell us?
- Have "material controls" been defined for the business? Where are material risks apparent and decisions taken?
- Can management provide an analysis of material controls by process and central function and provide details around how they are assured?
- Is the company clear about which IT systems are material to financial reporting, operating or compliance controls and have the IT controls been tested?
- At an entity level, has the board considered how the company's culture, code of conduct, human resource policies and performance reward systems support the business objectives and risk management and internal control systems?
- Has management undertaken a fraud risk analysis, including the risk of fraud in financial reporting?
- What are the channels of communication that enable individuals, including third parties, to report concerns, suspected breaches of law or regulations, other improprieties or challenging perspectives?
- How does the board satisfy itself that the information it receives is timely, of good quality, reflects numerous information sources and is fit for purpose?
- Are the papers supporting the board's annual review of effectiveness of internal controls sufficiently comprehensive to support the conclusions, or are the papers more of an "exception report"?
- If the annual review of effectiveness has revealed areas where more needs to be done to enhance material operational, financial or compliance controls, are these areas appropriately disclosed in the annual report?

For further information:

The UK Corporate Governance Code

The FRC Guidance on Risk Management, Internal Control and Related Financial and Business Reporting

COSO Framework—Executive Summary

ICAEW publication: Internal control effectiveness: who needs to know?

The Deloitte Academy

The Deloitte Academy provides support and guidance to boards, committees and individual directors, principally of the FTSE 350, through a series of briefings and bespoke training. Membership of the Deloitte Academy is available to board directors of listed companies, and includes access to the Deloitte Academy business centre between Covent Garden and the City.

Members receive copies of our regular publications on Corporate Governance and a newsletter. There is also a dedicated members' website www.deloitteacademy.co.uk which members can use to register for briefings and access additional relevant resources.

For further details about the Deloitte Academy, including membership, please email enquiries@deloitteacademy.co.uk.

Contacts—Accounting Operations Assurance Leader

Sonya Butters—0117 984 1074 or sobutters@deloitte.co.uk

Contacts—Centre for Corporate Governance

Tracy Gordon—020 7007 3812 or trgordon@deloitte.co.uk

Corinne Sheriff—020 7007 8368 or csheriff@deloitte.co.uk

William Touche—020 7007 3352 or wtouche@deloitte.co.uk

This publication has been written in general terms and we recommend that you obtain professional advice before acting or refraining from action on any of the contents of this publication. Deloitte LLP accepts no liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 1 New Street Square, London EC4A 3HQ, United Kingdom.

Deloitte LLP is the United Kingdom affiliate of Deloitte NWE LLP, a member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"). DTTL and each of its member firms are legally separate and independent entities. DTTL and Deloitte NWE LLP do not provide services to clients. Please see www.deloitte.com/about to learn more about our global network of member firms.

© 2019 Deloitte LLP. All rights reserved.