Deloitte.

The Deloitte Academy
June 2021

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, behind the UK proposals for a US style internal control attestation are very real questions as to whether responsibilities go far enough and whether there is sufficient guidance for boards, together with sufficiently detailed information from management, to meet these responsibilities effectively.
- In particular the guidance does not address the pervasiveness of technology in detail, and boards may not be obtaining sufficient assurance over 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 also not well understood - careful questioning of auditors in relation to their audit scope and approach could reveal much about the control environment.
- In summary, 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?

A number of respondents to Sir John Kingman's Independent Review of the Financial Reporting Council 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 legislation is seen as having led to better financial reporting, fewer significant accounting restatements and to a higher focus on and greater clarity over the robustness of internal controls within an entity. This recommendation was further endorsed in Sir Donald Brydon's review into the quality and effectiveness of audit.

In March, the Government published a White Paper 'Restoring trust in audit and corporate governance' which sets out options for strengthening the UK's internal controls regime. The aim is to achieve a proportionate strengthening of the internal control regime which builds on and develops the UK's existing provisions. The Government's initial preferred option is as follows:

Directors' responsibility statement

Directors should be required to acknowledge their responsibility for establishing and maintaining an adequate internal control structure and procedures for financial reporting.

Annual review of internal control effectiveness and new disclosures

Directors should be required to:

- Carry out an annual review of the effectiveness of the company's internal controls over financial reporting;
- Explain – as part of the annual report and accounts – the outcome of the annual review, and make a statement as to whether they consider the systems to have operated effectively;
- Disclose the benchmark system that has been used to make the assessment;
- Explain how they have assured themselves that it is appropriate to make the statement.

If deficiencies have been identified, these should be disclosed and the directors should set out the remedial action that is being taken and over what timeframe.

External audit and assurance

Decisions about whether the internal control effectiveness statement should be subject to external audit and assurance should usually be a matter for audit committees and shareholders. Decisions should be based on judgements about the strength of companies' systems and controls and whether extra assurance would be proportionate. This should be considered as part of the proposed Audit and Assurance Policy.

Companies should be required to have their internal controls assured by an external auditor in limited circumstances (e.g. where there has been a serious and demonstrable failure of internal controls or where material control weaknesses have persisted over several years).

Connected to the effectiveness of internal controls over financial reporting, the White Paper also proposes that directors should report on the steps they have taken to prevent and detect material fraud.

What should boards be assessing the effectiveness of controls against?

In order to provide the attestation described above as part of the Government's initial preferred option, a board would need to decide on the benchmark or standard of effectiveness against which the internal controls were being assessed.

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

1. Demonstrates commitment to integrity and ethical values.
2. Exercises oversight responsibilities.
3. Establishes structure, authority, and responsibilty.
4. Demonstrates commitment to competence.
5. Enforces accountability.

Risk assessment

6. Specifies suitable objectives.
7. Identifies and analyzes risk.
8. Assesses fraud risk.
9. Identifies and analyzes 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.

Question for boards to consider:

- What framework are we going to apply? COSO is an internationally recognised framework and is widely adopted.

Which types of controls should be considered?

The following types of controls should be considered as part of the attestation:

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. 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 blocks 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 operational 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?

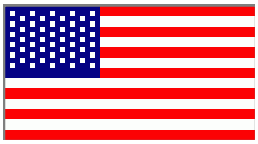
How different are the UK's current and proposed and US approaches?

Current Approach

- 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 any significant failings or weaknesses

Preferred Option Additions

- Requirements set out in legislation with enforcement
- Covers internal controls over financial reporting
- Responsibility of and reporting by the whole board
- Disclosures explain the outcome of the annual review, the benchmark system used, whether the system has operated effectively and identify any deficiencies together with an action plan
- Audit and assurance considered as part of the Audit & Assurance Policy, not mandatory



- 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 approaches in the UK and USA. In principle, there is alignment between the COSO framework and the FRC's Guidance yet some would argue that, within the UK, there is currently 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 by the board and audit committee's oversight.

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 the design and determine the 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, and any incremental testing is a matter for the auditor to determine using their judgement.

Under auditing standards the auditor must tell those charged with governance 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.

For entities applying the UK Corporate Governance Code the audit report includes a statement whether the section of the annual report that describes the review of the effectiveness of an entity's risk management and internal control systems, covering all material controls, including financial, operational and compliance controls is materially consistent with the financial statements and the auditor's knowledge obtained in the audit.

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?

In order to ensure well documented compliance with the UK Corporate Governance Code, boards should consider whether the following is in place and this should enable them to get ahead for a future attestation of the effectiveness of internal controls over financial reporting. A strong team, including finance leadership, should be engaged in this process and there should be clarity on the assurance strategy which sits with it (connecting with the proposed Audit and Assurance Policy).

STEP 1 – initial assessments and entity level controls

- Start with a detailed understanding of the business model
- Undertake a financial risk assessment and fraud risk assessment
- Establish clear and robust entity level controls to ensure the right "tone from the top"
- Define a hierarchy of delegated authorities from the board

STEP 2 – confirmation of in scope systems and identification of material controls

- Obtain clarity over in scope systems and related general IT controls
- Generate robust process documentation for material business cycles, with clear process owners
- Identify the material controls

STEP 3 – establish robust monitoring and review processes

- Define and evidence a robust process for on-going monitoring of the design and operating effectiveness of material controls
- Define and evidence a robust process for a year-end assessment of the design and operating effectiveness of material controls

STEP 4 – establish clear reporting protocols and accountability for action

- Define a significant control failure or weakness that would require detailed consideration and disclosure of remediating actions
- Define reporting processes including remedial action tracking

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 to lack of precision, and controls really should be embedded in and 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:

STEP 1 - initial assessments and entity level controls

- 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?
- 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?

STEP 2 - confirmation of in scope systems and identification of material controls

- Have "material controls" been defined for the business? Where are material risks apparent and where are material 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?

STEP 3 - establish robust monitoring and review processes

- 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"?

STEP 4 - establish clear reporting protocols and accountability for action

- If the annual review of effectiveness has revealed areas where more needs to be done to enhance material operational, financial or compliance controls, is there a clearly defined action plan and are these areas of weakness 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?

BEIS White Paper 'Restoring trust in audit and corporate governance'

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