Understanding the BEIS consultation

‘Restoring trust in audit and corporate governance’

A series of frequently asked questions on the key proposals

A strengthened internal controls regime

Introduction

On 18 March 2021, the Government (BEIS) published its long-awaited consultation on reforms aimed at ‘Restoring trust in audit and corporate governance’ (the Consultation). It’s a significant Consultation with 98 questions covering almost all 155 recommendations from the Kingman, CMA and Brydon reviews, and sets out a broad programme of reform for auditors, companies, directors, audit committees, investors, other stakeholders and the regulator. The deadline for responses to the Consultation was 8 July 2021. See our summary briefing document for more details of the key proposals.

These ‘frequently asked questions’ are part of a series intended to help you understand the implications of these proposals in more detail.

This is not an exhaustive list, and we’re sure there will be plenty of questions we’ve not yet considered. Our answers are based on our interpretation of the Government’s proposals. There’s also still a lot of uncertainty about what will be implemented, and the details of any new regime; the thoughts we’ve set out below are designed to help you consider the implications for your organisation, but please do remember that the final rules could well result in a different outcome.

One of the proposals in the Consultation seeks to strengthen the UK’s internal controls regime through emphasising the responsibility and accountability of board members for the effectiveness of internal controls; sometimes, informally, this is referred to as ‘UK SOx’. This proposal could have a significant impact on companies and their boards. Here we’ve answered questions over what this new regime could look like and some of the potential challenges around implementation and operation.

If you would like to discuss any of these points further, please ask your usual PwC contact, or alternatively you can contact:

Sotiris Kroustis
PwC UK Head of Public Policy
sotiris.kroustis@pwc.com

Simon Perry
Partner, Head of Markets and Services – Risk
simon.perry@pwc.com

Gilly Lord
Global Leader, Public Policy & Regulation
gillian.lord@pwc.com

Jayne Kerr
Director, Audit Strategy and Public Policy
jayne.l.kerr@pwc.com

pwc

Background

1 What responsibilities do UK companies currently have around internal controls?

UK law and regulation already includes various responsibilities in respect of internal control for companies and their directors. Key elements include:

- The **Companies Act** requires all companies to keep adequate accounting records (although there is no recent guidance on what this means in practice).
- The **Listing Rules** require premium listed companies to report against the UK Corporate Governance Code (the Code), which itself requires boards to establish a framework of prudent and effective controls, which enable risk to be assessed and managed.
- To address these responsibilities under the **Code**, boards must also 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, although there is no actual requirement for Boards to make a positive statement on the conclusion of the review. Guidance on performing the review is set out in the FRC's Guidance on risk management, internal control and financial and business reporting (which superseded the well-known 'Turnbull Guidance'). This recommends that companies applying the Code 'explain what actions have been taken or are being taken to remedy any significant failings or weaknesses'.
- Directors of a company that is seeking a premium listing of its shares on the Main Market of the London Stock Exchange, have to be satisfied that there are established procedures that provide a reasonable basis for them to make proper judgements on an ongoing basis as to the financial position and prospects (**FPP**) of the applicant and its group (Listing Rule 8.4.2(4)). There is guidance from the ICAEW on what these procedures should entail, which includes assessing the IT environment, although there is little mention of transactional level controls.
- Most existing listed public interest entities (PIEs) must, under the **FCA Disclosure Guidance and Transparency Rules**, provide a description of the main features of their systems of internal control and risk management specifically in relation to the financial reporting process.

Most of these requirements apply only to listed companies, not to all PIEs. In addition, these requirements do not require public statements on the effectiveness of internal control to be made by directors.

2 What do auditors have to do in this area?

International and UK auditing standards require auditors to test the operating effectiveness of relevant internal controls over financial reporting (encompassing financial and associated IT controls) **if** the auditor intends to rely on them. In practice, this means that some audits include extensive, detailed testing of controls since that is an intrinsic part of the audit strategy. Typically, this might be the case in very large and sophisticated companies who process many millions of transactions and who are highly systems dependent. Other audits, however, can include little or no testing of controls; the auditor may have decided that audit evidence can be gained more effectively via another route, or that controls are unlikely to be reliable.

Auditors of companies applying the Code are also required to report to the audit committee (but not externally) their views about the effectiveness of the internal controls relevant to risks that may affect financial reporting, but the additional work effort needed to meet this requirement is often limited. Under the Listing Rules, premium listed companies must arrange for their auditors to review the directors' statement on their review of the effectiveness of the systems of risk management and internal control, although there is no clear definition of what such a 'review' should entail. In our experience, most auditors approach these responsibilities principally through taking account of work already performed over internal control as part of the underlying audit.

3 Why is the Government proposing a strengthened internal controls regime?

The Government describes in the Consultation that there have been well-publicised examples of company failures where weak internal controls and risk management have been key factors. The Government further explains that in some cases these companies had expanded too rapidly without integrating acquisitions into an effective internal controls framework, or had exposed themselves to the risk of fraud.

Both Sir John Kingman's review of the Financial Reporting Council and Sir Donald Brydon's review of the quality and effectiveness of audit proposed that serious consideration should be given to strengthening the company internal control regime in the UK. Both suggested the possibility of adopting a version of, or specific elements of, the US Sarbanes-Oxley regime.

The US Sarbanes-Oxley Act (US SOx) was implemented in 2002 to respond to financial scandals such as Enron and WorldCom. It led to the creation of a new regulator (the PCAOB) that is under the oversight of the SEC.

Amongst other things, the Act requires:

- In section 302 that the CEO and CFO certify in the annual report the completeness/accuracy of financial reporting, that an adequate internal control system has been maintained and that financial reports are not misleading or fraudulent; and
- In section 404 that the independent auditor assesses and opines on the effectiveness of internal controls over financial reporting (ICFR – financial controls and IT controls over financial systems).

In our experience, although the various regimes outlined in question 1 are well established, there's much variability in how they are applied and, in particular, the rigour with which companies approach the assessments required.

A strengthened UK internal controls regime could be an opportunity to 'level set' this variability in approach.

The proposal for a strengthened UK internal controls regime

4 What is being proposed by the Government?

The Government has proposed three potential options for a strengthened UK internal controls regime. The options are not intended to be mutually exclusive and could be combined in different ways in the final proposals. The Government highlights that initially, its preferred option is Option A, which we've set out below. We've also summarised the other options (Options B and C).

Option A. Require an explicit directors' statement (the directors' statement) about the effectiveness of the internal control and risk management systems.

This option is outlined in Table 2 on pages 48 and 49 of the Consultation:

- **Directors' responsibility statement** – Directors would 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 would need to:
  - Carry out an annual review of the effectiveness of the company's internal controls over financial reporting;
  - Explain in the Annual Report the outcome of that review, and make a formal statement as to whether they consider the systems to have operated effectively;
  - Disclose the benchmark system that has been used to make the assessment; and
  - Explain how they have assured themselves that it is appropriate to make the statement.

If deficiencies are identified, these would need to be disclosed, together with the remedial action and the timeframe.

- **Principles and guidance** – Directors would be guided by principles and guidance developed or endorsed by the regulator reflecting audit committee best practice.
- **External audit and assurance**
  - Decisions about whether the internal control effectiveness statement should be subject to external audit or assurance would be a matter for audit committees (and shareholders) to decide. Independent assurance would not be mandated in most situations.
  - Decisions would be based on judgements about the strength of companies' systems and controls and whether extra assurance would be proportionate. This would be covered explicitly as part of the proposed Audit and Assurance Policy.
  - Companies would be required to have their internal controls assured by an external auditor in limited circumstances (e.g. where there had been a serious control failure or where material control weaknesses had persisted over several years).
- **Enforcement**
  - The regulator would have powers to investigate the accuracy and completeness of the directors' internal control disclosures and, if necessary, order amendments or recommend an external audit of the internal controls.
  - There would be powers to sanction directors where they have failed to establish and maintain an adequate internal control structure and procedures for financial reporting.
- **Scope** – The requirements would be set out in legislation and phased in over a period of time. They would apply initially to premium listed companies (with possible temporary exemptions for newly listed companies where gross revenues remain below a specified threshold) and extended to other PIEs after two years.

Option B. Require auditors to report more about their views on the effectiveness of companies' internal control systems

Under this option, the auditors wouldn't actually do any 'new' work, but they would be required to say more in their annual report about the work they have undertaken to understand the company's internal controls system (i.e. the financial and IT controls) and how that has influenced their audit approach. This would not be a formal conclusion by the auditor on the effectiveness of internal controls.

Option C. Require auditors to express a formal opinion on the directors' assessment of the effectiveness of the internal control systems

This option would require the auditor to undertake additional audit and assurance work in order to express a formal opinion on the directors' assessment. It could have similarities to section 404(b) of the US's Sarbanes-Oxley Act which requires the company's auditor to attest to and report on management's assessment of the internal control structure and procedures for financial reporting.

5 Would this regime require me to assess ALL internal controls, or just internal controls over financial reporting (ICFR)?

The Consultation considers whether the directors' statement should cover all aspects of the company's internal control and risk management procedures or be restricted to ICFR. The Government's preferred option – as outlined in question 4 above – suggests the directors would only be required to perform an annual review of the company's ICFR, not of all internal control.

In our experience, assessment of control effectiveness is usually easier for ICFR than for broader controls (and would lead to more consistency between companies), as controls over financial reporting are usually more precise and easier to define.

If an ICFR regime is introduced alongside the existing requirements under the UK Listing Rules and Code, we expect there would be a need for companies to 'bridge' their compliance with existing requirements with the work needed to implement the new regime. Further guidance from the new regulator might be useful in this area to allow companies to design a single approach to achieve compliance with the various regimes.

6 Who would this proposal apply to and when would it become a requirement?

The Government is proposing that the strengthened internal controls regime would initially be applied to all premium listed companies and, after two years, to all PIEs. Separately, the Consultation proposes that the definition of PIE should be extended to include certain large private companies, large AIM companies and potentially certain third sector organisations. We've published a separate set of FAQs on the extension of the PIE definition which you can find here. The Consultation also notes that there could be temporary exemptions for newly listed companies where gross revenues remain below a specified threshold.

For comparison, we've looked at the US SOx regime, which is applied to large accelerated filers (i.e. companies with a market cap over $700m), with exemptions for smaller companies, companies registered overseas, emerging growth companies and for a period following a business combination.

In the UK, we don't expect that a strengthened internal controls regime would begin to apply to premium listed companies until 2023 and possibly not until 2024. Before implementation there are a number of different legal and regulatory steps to be taken, including:

- Government assessing responses to the Consultation;
- Draft legislation being developed (if the regime is implemented through law – see question 7).
- Further consultation, likely by ARGA, on the details of the regime.

We'd also expect that there would be transition arrangements allowing time for companies to implement a new regime.

7 How would the new requirements be implemented? Will there be new statutory requirements?

The Consultation doesn't conclude finally on how any strengthened internal control regime would be implemented. The most likely options would be to introduce a new statutory requirement for in-scope companies to comply with the regime, or to introduce the regime through the Code; the initial preferred option set out in the Consultation would be to implement the regime via a new statutory requirement.

The Consultation acknowledges that implementation through the Code would be easier, and also that the regime would be easier to refine if this route were to be taken. However, the Code currently only applies to premium listed companies and so would not enable the broader coverage contemplated by the Government. In addition, the Code has no specific enforcement mechanism other than through the FCA's general application of the Listing Rules and so arguably would not achieve the shift in accountability that appears to be desired.

Whichever route is chosen, the Consultation also suggests that the regime might be more, or less prescriptive. At one end of the spectrum, companies could be required to use a specified internal control standard (or one of a range of standards or control frameworks approved by the regulator – we assume that the COSO[1] framework would be included as this is the framework commonly used in the US). A more flexible approach would be to set a broad framework of principles for companies to follow, leaving much more discretion for companies to design their own approach.

In our experience, current practice for complying with the internal control requirements of the Code is varied, ranging from highly rigorous and documented to relatively informal. We believe that some degree of prescription would be desirable in order to achieve a greater level of consistency in the UK market.

[1] 'Committee of Sponsoring Organisations of the Treadway Commission'

8 How is this proposal different to what is done today in the UK?

There is still much uncertainty about what a strengthened UK internal control regime would actually entail. However, there are already some key differences between these proposals and the current UK frameworks, including:

Scope of application

As explained in question 1, many of the existing UK requirements on internal control apply only to premium listed companies. In these proposals, the Government proposes that a strengthened internal control regime would eventually apply to all PIEs. This is already a broader group than listed companies as it also includes unlisted banks and insurers. Furthermore, the Government is proposing to expand the definition of a PIE to include up to 2000 large private companies (even if owned by an overseas parent) and a number of large AIM listed companies.

Directors' statement

The proposal would require directors to make an explicit public statement on the effectiveness of internal control. Although some would feel that such a statement is implied by a number of today's UK regimes, there is certainly no explicit requirement for a statement to be made. It could be that this new requirement drives a change in approach from some companies.

Form and structure

Although it's unclear exactly how prescriptive the new regime would be, the proposals already suggest more structure than currently exists. For instance, directors would have to describe the benchmark system used in their assessment, disclose any deficiencies identified and the remedial action being taken.

Regulator enforcement powers

Other Government proposals to strengthen the enforcement powers of the regulator would enable the regulator to sanction directors where they have failed to maintain an adequate internal control structure for financial reporting and, presumably, if those directors had made a false or misleading statement under the new internal control regime. Although not explicitly mentioned in the Consultation, it seems feasible that there could also be a regulatory investigation into the directors' statement following company failure.

Assurance

As we explain in question 4, directors could be required to explicitly disclose their decision on whether to commission additional independent assurance over their statement on internal controls as part of the Audit and Assurance Policy (or under Option C their statement would be subject to an assurance opinion by the auditors).

9 How much work would I need to do to ensure that the directors of my company can make this statement?

There's still a lot of detail to be established in terms of what would actually be required under any strengthened UK internal control regime and as a consequence, it's impossible to estimate the additional work effort required by UK companies required to comply. As we explain in question 14, the Government has made a relatively modest estimate of the incremental cost that they expect companies to incur. Design criteria which could be important drivers of work effort include:

- Whether the assessment of control needs to take account of both design effectiveness and operating effectiveness. Design effectiveness assessment often includes walkthrough to establish the parameters of a process and judgement on the appropriateness of design, whilst operating effectiveness assessment usually includes detailed testing to confirm that controls were actually performed and operated as expected. We would expect both of these areas to be included in an overall assessment of controls.
- If the directors' statement needs to be 'auditable' (even if no independent assurance is actually commissioned), this could drive the need for documentation of the evidence and approach used to justify the directors' statement.
- Guidance on the required materiality and precision to which directors should work in making their assessment, including the level at which disclosures of deficiencies need to be made.

10 Who would make the statement on the effectiveness of internal control?

In the Government's preferred implementation approach, it's proposed that the directors collectively would make the statement of the effectiveness of internal control. However, elsewhere in the Consultation, the Government acknowledges that views are mixed on whether it would be more appropriate for the CEO and CFO to take responsibility for the statement (this is the approach under the US SOx regime). A collective board statement is more consistent with the UK concept of the unitary board, although this principle is already challenged by, for example, the introduction of the Senior Managers and Certification Regime (SM&CR) by the financial services regulators.

Practical considerations for a strengthened internal controls regime

11 What framework would companies use to support their assessment? Are there different options?

The Consultation explains that the Board would need to decide on, and disclose, the benchmark system used to make their assessment of internal control effectiveness. This suggests that there could be multiple frameworks used for this purpose. Two potential frameworks are referenced in the Consultation:

- The COSO[2] framework – This is a well-known framework setting out an approach to establishing governance processes and controls. It is commonly used by (although not mandated for) companies complying with the US SOx requirements.
- The Financial Position and Prospects (FPP) approach prescribed by the UK Listing Rules. Following the Brydon Review, the Audit Committee Chairs' Independent Forum (ACCIF) drafted a set of principles that could be used to support the directors' statement. These principles used the FPP approach as a basis.

Neither of these frameworks specify **how** to assess and test the effectiveness of controls. This means that further detail would most likely be required on how directors are expected to approach their evaluation of the controls in place.

12 Would the directors' statement be externally assured? If so, who by? What standard would be used?

As we explain in question 4, in the Government's preferred implementation option, assurance over the directors' statement would not be mandated (except potentially in cases of serious failure). Instead, the Government suggests that the board would consider the degree of assurance needed to satisfy itself that the control regime is designed and operates effectively.

This consideration could take account of work performed by internal auditors. Alternatively, or in addition, work could be commissioned from the external auditor, or another external assurance provider. This work could examine all, or specific aspects, of internal controls. Some boards may feel more comfortable making their own statement if there is some independent assurance that validates their conclusions.

The Government also suggests that as part of the proposed Audit and Assurance Policy, the directors would be required to explicitly state whether independent assurance has been commissioned over internal control effectiveness. We believe this could indicate that although the Government has stopped short of mandating independent assurance, there is an expectation that boards would consider the need for it carefully.

Even if the directors' statement is not to be audited or assured, we think it is important that the supporting work is performed to an 'auditable' standard. This would drive quality and consistency in performance and, in the event that directors are challenged on the basis for their statement, provide an evidence base for the directors' conclusions. Based on our experience of US SOx, where assurance on the directors' attestation is mandated in most cases, the directors' statement and the related assurance meaningfully contribute to the reliability of financial statements.

[2] COSO framework

13 If there is more than one PIE in a group, would this be a requirement for all PIEs?

As noted in question 6 above, the Government is proposing that the strengthened UK regime should eventually be a requirement for all PIEs. This could mean that where there are multiple PIEs in a group, different sets of directors could have to make different statements (supported by separate exercises) on the effectiveness of internal control. The Consultation isn't clear on whether a single 'group-wide' approach would be acceptable.

Our suggestion for a proportionate approach would be that the UK parent leads in making the statement on internal control effectiveness throughout the entire group, and that directors of other PIEs in the group should be able to cross-reference to that statement, without undertaking their own exercise.

14 This sounds like it could be quite a costly process. What is it going to cost and is it worth it?

In order for any ICFR regime to be rigorous and implemented consistently, it is inevitable that there will be cost and resource demands. Our view is that a careful impact analysis needs to show that the benefits of a new regime clearly outweigh the inevitable incremental cost that many companies could experience.

In the Impact Assessment that accompanies the Consultation, the Government has assessed the transitional costs and ongoing annual compliance costs associated with a directors' statement on ICFR (assuming that no independent assurance is commissioned). They estimate that the transition costs of implementing a regime (incurred over years 1-4) would be approximately £330k per entity, and that annual compliance cost thereafter would be £60k per entity. A recent study of annual compliance costs under US SOx[3] estimates that costs per company ranged from $0.8m to $1.7m.

This could indicate that the Government's aspiration is to create a regime that is less onerous and prescriptive than US SOx. However, we believe the Government's cost estimates could be understated. Further, the Government's Impact Assessment does not quantify the benefits of introducing a new regime. We'd also suggest that there needs to be consideration of the absolute availability of appropriately qualified professionals to implement such a regime if the ambition is to extend to all PIEs with a short transition period.

15 What if I am already compliant with another SOx regime, would this be an additional requirement?

There is no specific mention in the Consultation of equivalence between a strengthened UK regime and the US SOx regime. However, in the Impact Assessment, companies that already comply with the US SOx regime are excluded from the number of companies expected to be impacted by the strengthened UK regime. This could suggest that the Government considers that compliance with the US SOx regime would also meet the requirements of a UK regime. There is no indication of whether other SOX-style regimes (such as those in Japan, South Africa or India) would be considered equivalent.

Some companies have suggested that it would be helpful to have a specific exemption from the regime if an equivalent overseas regime has already been implemented.

[3] https://www.protiviti.com/sites/default/files/2020-sox-survey-protiviti.pdf

2021-05-14_RITM5326680