Implementing quality controls over financial reporting enhances trust in business and improves financial reporting. The UK already has requirements in this area but there is widespread agreement that they are not sufficient.

There is a vast amount of research and evidence from the United States demonstrating that the US Sarbanes-Oxley Act (SOX) has strengthened the capital markets and reliability of financial reporting there, and also that assurance over management’s assessments of the internal control environment within listed companies has benefits for investors and for the company itself.

In his Review of the Quality and Effectiveness of Audit, Sir Donald Brydon acknowledged that the effectiveness of internal controls is fundamental to the reliability of a company’s financial (and potentially other) reporting. Sir Donald recommended that a CEO/CFO attestation should be introduced supported by principles developed by the Audit Committee Chairs’ Independent Forum (ACCIF) and endorsed by the new financial reporting regulator.

KPMG hosted a roundtable discussion with investors, analysts and policy experts to discuss these topics in November 2020. At this roundtable, the discussion centred on five key questions:

1. What are the existing requirements in the UK?
2. What changes to the UK requirements is Sir Donald recommending?
3. What requirements exist elsewhere?
4. What can be learned from the US experience of implementing SOX?
5. What would strengthen the UK internal controls framework from an investor’s perspective?
What are the existing requirements in the UK?

The current requirements in the UK derive from the 1992 Cadbury Report, which predates the Sarbanes-Oxley Act (SOX) by over a decade. It set out that boards of directors should report on the effectiveness of a company’s system of internal controls (including, by definition, internal financial controls).

Since then, UK Corporate Governance guidelines have evolved significantly. The latest UK Corporate Governance Code, published in July 2018, covers all controls over financial, operational and compliance areas rather than being specifically focused on controls over financial reporting.

As of today, the board has the following responsibilities regarding internal controls.

— **Ongoing monitoring**: The board specifies requirements, scope and frequency for reporting and assurance. Management reports to the board on risk management and effectiveness of controls and the board forms its own evidence-based view on the effectiveness of internal controls.

— **Annual review of effectiveness**: The board considers all significant aspects of risk management and internal control for the year under review and up to the date of approval of the Annual Report. As part of this, the Board should obtain sound, appropriately documented evidence.

— **Reporting**: The board summarises the process applied in reviewing the effectiveness of the system of risk management and internal controls and explains what actions are being taken to remedy any significant failings or weaknesses.

What happens in practice?

There is no explicit requirement to disclose the failings and weaknesses found in the annual report and accounts, although some will argue it is hard to explain remedial actions without stating the weakness. That said, currently in the UK, reporting control failings and weaknesses is rare and generally reserved for issues already in the public domain. This could be due to a lack of a robust definition on what a ‘significant failing or weakness’ is and potentially the lack of independent assurance requirements to hold the Board to account, like in the US.
In his report, Sir Donald Brydon recommended that the Government give serious consideration to mandating a UK Internal Controls Statement. This would consist of:

- an attestation by the CEO and CFO to the Board that an evaluation of the effectiveness of the company’s internal controls over financial reporting has been completed; and
- their opinion on whether these controls were effective in the period under evaluation; and
- A report from the Board to shareholders that it has received such an attestation from the CEO and CFO.

Sir Donald proposes that:

- the guidelines for making the CEO/CFO attestation be developed by the Audit Committee Chairs’ Independent Forum (ACCIF); and
- final endorsement of these principles be made by the Audit, Reporting and Governance Authority (ARGA) – the intended successor organisation to the Financial Reporting Council (FRC).

He further proposes that if there is a failure of relevant controls within 12 months either side of the attestation, then future statements would be subject to mandatory audit for three years following the failure. This audit requirement would remain for as long as failures or weaknesses persist.

Shareholders in the company would be permitted to request more assurance where they consider it warranted as part of their approval of the three-year rolling Audit and Assurance policy at the annual general meeting (another of Sir Donald’s recommendations).

---

1. A summary of recommendations made by Sir Donald Brydon are explained in this article by KPMG’s Audit Committee Institute (ACI) at https://home.kpmg/content/dam/kpmg/uk/pdf/2020/01/brydon-assess-assure-and-inform-aci.pdf

2. The ACI held a conversation with ACCIF on their proposal. A summary of the discussion is available at https://assets.kpmg/content/dam/kpmg/uk/pdf/2020/19/a-conversation-with-the-accif-about-internal-controls.pdf
What requirements exist elsewhere?

The United States – home to the world’s largest equity capital markets – implemented similar requirements over 15 years ago in Section 404 of the Sarbanes-Oxley Act. Here, we took a closer look at the requirements for US listed companies, as well as other globally recognised requirements of those in Japan and Spain.

**United States:** Each company subject to SOX requirements issues an internal control report containing management’s assertions about the effectiveness of its internal controls over financial reporting. This requirement falls under part (a) of Section 404 of the Sarbanes Oxley Act.

For larger companies, part (b) of Section 404 also requires the company’s independent auditor to attest to the effectiveness of the company’s internal controls over financial reporting in accordance with standards set by the PCAOB – the US audit regulator.

**Japan:** Listed companies in Japan are required to produce ‘internal control reports’ along with their annual financial statements to demonstrate the soundness of their financial practices. A company representative is required to evaluate the effectiveness of the internal controls and submit a written statement attesting to the accuracy of the financial statements. Both the financial statements and the internal control report have to be audited by the external auditor.

**Spain:** Public companies in Spain are required to describe in their Annual Corporate Governance Report the mechanisms that comprise the risk control and management systems in relation to the company’s internal controls over financial reporting (ICFR). If the ICFR information supplied to the market has been reviewed by the external auditor, then the corresponding report should be attached. If this is not the case, then the report should explain why.

---

### SOX filer requirements

<table>
<thead>
<tr>
<th>Filer status</th>
<th>Management assessment of internal controls – SOX 404(a)</th>
<th>External auditor attestation – SOX 404(b)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Large accelerated filers</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Market cap: $700 million or more(i)</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Accelerated filers</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Market cap: $75 million or more but less than $700 million</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Non-accelerated filers (including ‘smaller reporting companies’ and public debt filers)</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Market cap: less than $75 million</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Emerging growth companies</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Period up to 5 years from initial public offering (IPO) or until reaching $1 billion in annual revenue</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Year of IPO</td>
<td>✗</td>
<td>✗</td>
</tr>
</tbody>
</table>

(i) Unless registrant is eligible to be treated as a ‘smaller reporting company’ under SEC Release No. 34-88365
Comparing SOX to the existing and proposed UK frameworks

<table>
<thead>
<tr>
<th>Filer status</th>
<th>US Sarbanes-Oxley Act</th>
<th>Existing UK framework</th>
<th>Proposed additions to the UK framework</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Who</strong></td>
<td>CEO/CFO evaluate</td>
<td>Board reviews the</td>
<td>CEO/CFO would evaluate</td>
</tr>
<tr>
<td></td>
<td>effectiveness of…</td>
<td>effectiveness of…</td>
<td>effectiveness of…</td>
</tr>
<tr>
<td><strong>Scope</strong></td>
<td>… internal controls</td>
<td>… all internal</td>
<td>…all internal controls, with</td>
</tr>
<tr>
<td></td>
<td>over financial</td>
<td>controls.</td>
<td>additional requirements for ICOFR (but more narrowly defined than for SOX reporting).</td>
</tr>
<tr>
<td></td>
<td>reporting (ICOFR)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Framework</strong></td>
<td>The internal control</td>
<td>There are implicit</td>
<td>The question remains open as to whether guidance for CEOs/CFOs should be developed (potentially drawing on recognised internal control frameworks).</td>
</tr>
<tr>
<td></td>
<td>framework used to</td>
<td>requirements indicating</td>
<td></td>
</tr>
<tr>
<td></td>
<td>conduct the evaluation</td>
<td>that an internal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>is explicitly</td>
<td>controls framework</td>
<td></td>
</tr>
<tr>
<td></td>
<td>identified.</td>
<td>should be used to</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>conduct the review</td>
<td></td>
</tr>
<tr>
<td><strong>Statement on</strong></td>
<td>An explicit statement is</td>
<td>Statement that the</td>
<td>The CEO/CFO would attest to the board that ICOFR provide a reasonable basis for making proper judgements as to the financial position.</td>
</tr>
<tr>
<td>effectiveness</td>
<td>issued outlining whether</td>
<td>the board has reviewed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>the ICOFRs are</td>
<td>the effectiveness of controls is issued, but no explicit statement required as to whether or not they are effective.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>effective.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Statement on</strong></td>
<td>Any material weaknesses in the ICOFR identified by management are disclosed.</td>
<td>Any actions that have been or are being taken to remedy any significant failings or weaknesses are disclosed.</td>
<td>Any identified material weaknesses / failures in ICOFR would be disclosed, along with the remedial action that has been taken.</td>
</tr>
<tr>
<td>weaknesses / failures</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Audit</strong></td>
<td>The external auditor</td>
<td>External auditor</td>
<td>Under the Brydon recommendation, auditor attestation would be triggered by control failures and/or Audit Committee policy. Shareholders would approve the audit and assurance policy.</td>
</tr>
<tr>
<td>requirements</td>
<td>attests to the</td>
<td>attestation is not</td>
<td></td>
</tr>
<tr>
<td></td>
<td>effectiveness of the</td>
<td>required. Internal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ICOFR in accordance</td>
<td>audit is the primary</td>
<td></td>
</tr>
<tr>
<td></td>
<td>with PCAOB standards.</td>
<td>source of assurance.</td>
<td></td>
</tr>
</tbody>
</table>

(i) “The board should define the review processes … such that it will obtain sound, appropriately documented, evidence to support its statement in the Annual Report.”

(ii) However, many companies are explicitly reporting on the effectiveness of their risk management and internal control systems.
What can be learned from the US experience of implementing SOX?

There is a considerable amount of research and evidence from the US demonstrating that SOX provisions have strengthened the capital markets and reliability of financial reporting. There is also evidence to suggest that external auditor attestation over management’s assessment of the internal control environment has benefits for the investors and for the company itself.

The key benefits that have been identified are:

- an improvement in the quality of financial reporting and internal controls;
- a chance to highlight problems early; and
- an early warning for fraud.

These benefits are echoed in a 2017 Centre for Audit Quality survey. 79% of CFOs who took part felt that the overall quality of information in audited financial statements had improved since the enactment of SOX and 85% believed the external audit of their company’s ICFR has helped their company. Overall 80% agreed that the benefits of SOX outweigh or is equivalent to the expense.

A reissuance restatement is required when a company identifies a material error in already issued financial statements which can therefore no longer be relied upon and need to be reissued.

The number of restatements reported by US public companies has steadily decreased since the introduction of SOX. It reached its lowest level in 2019 having decreased by over 90% in the last 15 years.
External auditor attestation on the effectiveness of an issuer’s internal control over financial reporting is required for larger US companies.

A steady decrease in adverse attestation was noted in the years following SOX implementation. As organisations become more familiar with the framework, it typically results in more effective processes.

Conversely, the trend observed for first-year auditor attestations shows much higher levels of negative attestations. As a company grows, it will trigger the requirement for an auditor attestation as opposed to a management-only assessment. When a company undergoes an external audit for the first time, there tends to be much higher deficiency rates.

In most years, between 10 and 20 percent of companies filing their first auditor attestation disclosed an adverse opinion on their internal controls over financial reporting.

**Overcoming implementation challenges**

In our experience, companies implementing SOX 404 for the first time grapple with issues such as fragmented IT architecture, lack of automated controls, the need to develop second line and testing capabilities and, crucially, cultural change.

It is not uncommon for companies to take up to four years of investment to get to a position where there are no material weaknesses or significant deficiencies reported. First-time adopters of a COSO-style framework would need to take steps to build out the basic foundations of their internal control systems. We have observed that implementation is typically easier for larger companies with more sophisticated IT systems that manage financial reporting and controls; smaller companies often face greater challenges obtaining and standardising their data and systems. That said, it typically takes between 12 and 36 months even for a large company to design, test and embed an automated control environment for SOX.
Investor viewpoint: What would strengthen the UK internal controls framework?

Investors at the roundtable discussion strongly supported a version of SOX being adopted in the UK. We discussed the following five key areas:

- scope of ICOFR;
- assurance expectations;
- applicability;
- reporting requirements; and
- impact of implementation.

Scope of ICOFR: Under ACCIF’s proposals published in their August 2020 position paper, the CEO and CFO would attest to the board on the establishment of procedures and controls over financial position (including primary statements) – this would not include notes to the accounts, or going concern, forecasting or budgeting. However, roundtable participants agreed with KPMG’s opinion that a wider scope of ICOFR is needed for the existing proposals.

They considered a scope focusing on the primary financial statements only to be too narrow, potentially raising questions over cost vs benefit if the scope is left unchanged. Areas such as segment disclosures, going concern, and disclosures of key judgments and estimates that support investment decisions would be missed.

They considered the US model, which covers all aspects of controls over financial reporting to be appropriate.

There was much interest in non-financial controls over areas such as alternative profit measures and non-financial key performance indicators, which investors and analysts use frequently.

Participants expressed frustration on the many inconsistencies between the front and back halves of the annual report. They see the proposals outlining a more robust control environment as an opportunity to address the inconsistency and believe that widening the scope of ICOFR to cover this aspect of reporting is essential.

Assurance expectations: ACCIF proposes that the audit committee decides whether the attestation would be subject to further assurance – this would not be mandatory.

Roundtable attendees believed internal assurance is needed in the first instance. They consider external assurance to be helpful, noting that ‘what gets measured gets done’. Some said that not having external assurance would be ‘a mistake’. One noted that benefit of assurance should far outweigh the cost, which for most companies would be insignificant.

Applicability: Participants expected that only companies above a certain size threshold would need to adopt any new requirement, indicating that they favour proportionality.

Requirements for a CEO/CFO attestation for all Premium listed UK companies was considered sensible given existing requirements. Participants noted that a model similar to that in the US, under which external attestation is triggered based on market cap, would be sensible.

Reporting requirements: Participants held strong views on their dislike of bland, boilerplate reporting both from companies and auditors. They felt it essential that the reporting be clear and meaningful to ensure the cost of undertaking it worthwhile.

They were especially concerned that if the scope of ICOFR was narrowly drawn as proposed then reporting could become yet another ‘box-ticking exercise’ in increasingly voluminous annual reports. They suggested that the binary nature of reporting in the US does not provide the narrative detail investors want.

**Impact of implementation:** Attendees were interested to know where companies might go to get help with implementation. They understand that the initial adoption period might require external resources while internal resources are being trained and/or recruited. Some expressed a preference for internal resources to be trained and upskilled as opposed to outsourced. Others expressed concern that the audit and accounting firms might provide this support.

Some noted that the choice of firm to help with support and implementation could in turn impact the firms available to compete for a future audit tender.

Participants favoured a phased approach to ease transition.

**Next steps**
At the time of writing, our understanding is that the FRC will review ACCIF’s proposals, given that the FRC (or ARGA) will be in charge of its implementation. The Department for Business, Energy and Industrial Strategy (BEIS) is expected to release its consultation on audit reform soon – this will be an opportunity for investors and other stakeholders to voice their views on the proposed move to a new UK financial controls framework.

We strongly encourage all stakeholders to respond to the consultation to ensure their voices are heard as regulatory and legislative changes take shape.
About KPMG Investor Insights

Our roundtable discussion on the effectiveness of UK internal controls was held on 4 November 2020. It is one of a series of investor outreach events where we discuss and share perspectives on how corporate reporting, auditing and assurance, and stewardship can evolve to meet investors’ needs today and in the future. To find out more, visit our web page or follow KPMG Investor Insights on LinkedIn. If you would like to discuss any of the areas in more detail on a one-to-one basis, contact us at investorinsights@kpmg.co.uk.