Deloitte.

Considerations for internal audit in light of UK SOX

February 2021

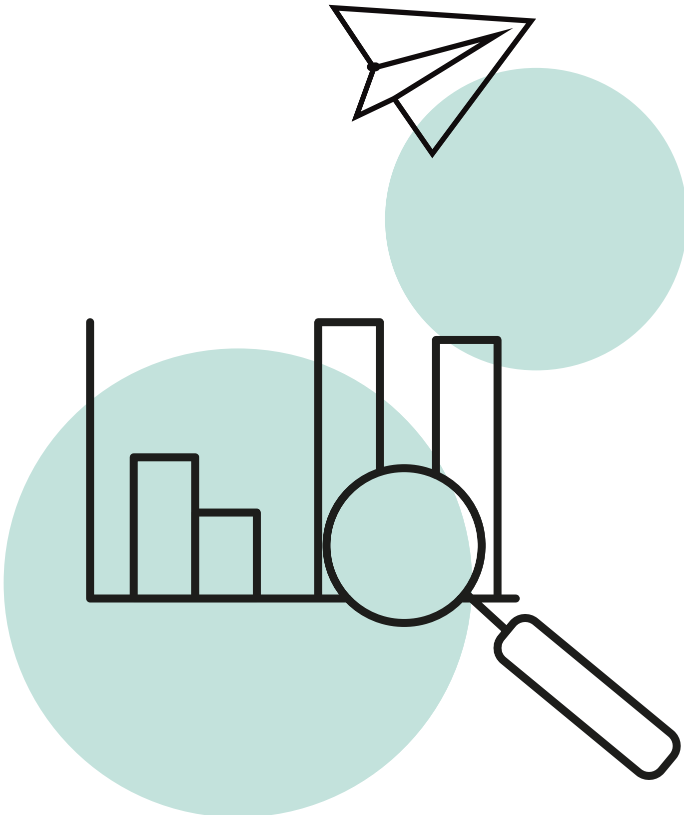
Introduction

In their reviews of financial reporting and the effectiveness and quality of audit reform, both Sir John Kingman and Sir Donald Brydon called for better internal controls over financial reporting. These recommendations reflect a wider, global sentiment from society that stronger internal control environments are needed to prevent material fraud and unexpected company failures.

Ask yourself the following questions to help you explore what the implementation of UK SOX means for your organisation:

- Do I have a good understanding of the UK Corporate Governance Code's requirements with regard to financial reporting?
- Do we fully comply with the UK Corporate Governance Code's requirements with regard to financial reporting?
- Do I think that the UK Corporate Governance Code is an effective framework to prevent financial reporting errors?

In short, the most common answer to each of these questions is no. As the UK continues on the journey of reforming corporate governance, companies and auditors are facing even tougher new obligations that will re-shape the approach to financial controls.



1. A reminder of current UK requirements

In principle, current UK requirements are already consistent with the Sarbanes-Oxley regime in the USA. The Companies Act requires the maintenance of adequate accounting records and the UK Corporate Governance Code states: "The board should monitor the company's risk management and internal control and, at least annually, carry out a review of their effectiveness, and report on that review in the annual report". However, there is currently no implementation guidance or perceived regulatory discipline; consequently, only notional compliance is being achieved by many UK corporates.

Kingman's recommendation:

The Department of Business, Energy, & Industrial Strategy (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.

Brydon's recommendations:

The CEO and CFO provide an annual attestation to the board of directors as to the effectiveness of the company's internal controls over financial reporting. This attestation should be guided by new principles on internal controls reporting developed by the Audit Committee Chairs Independent Forum and endorsed by the Audit, Reporting and GovernancE Authority (ARGA).

Companies are required to disclose when any material failure of their internal controls has taken place. A disclosed failure would lead to the CEO/CFO attestation being subject to audit for the following three reporting years.

2. What happens next?

A white paper from BEIS is due in early 2021 on the recommendations from these reviews.

In a recent interview Sir Jon Thompson, Chief Executive of the Financial Reporting Council, confirmed his expectation that a form of UK SOX will be introduced in 2023/24, that ministers are very engaged in the topic, and that in due course the scope of compliance will extend to large privates. He commented that companies can be superb, particularly at the top end, but more broadly performance across areas such as risk, governance and internal control, is mixed. Asked what UK corporates should be doing now, his response was clear:

01

Map out what the internal controls are

02

Identify those that are relevant to Internal Control over Financial Reporting (ICFR)

03

Get assurance they are working. Thompson went on to comment that internal audit should provide assurance over the activities of the second line.

3. The role of internal audit

As the prospect of UK SOX grows ever more certain, it is important that internal audit is proactive and prepared. In late 2019, Sir John Kingman suggested that given most corporates, (beyond the c. 50 corporates that already comply with US SOX) achieve only notional compliance with existing UK requirements and that change is coming, now is a good time for internal audit functions to undertake both an ICFR gap analysis and readiness assessment.

Internal auditors may find the below four step process a useful framework against which to conduct such gap analysis. These steps are implicit in current UK Corporate Governance requirements, although few apply them in practice, and are likely to be the foundation of any new regulatory framework with regard to ICFR.

How to conduct a gap analysis

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 • Identify outsource providers / third parties critical to in scope processes • 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

Other considerations

In addition to a gap analysis, internal audit should recommend that management scale the likely compliance task by completing the following preliminary steps:

01

Complete a financial risk assessment, to show the breadth of areas likely to be in-scope

02

Agree the in-scope IT systems. Failure to identify in-scope systems early enough is one of the top causes of non-compliance with US SOX as it leaves insufficient time to assess essential IT controls

03

Pick an area, perhaps purchase to pay, and undertake a pilot to understand what good looks like and the likely resource requirements for a full scope ICFR compliance project.

Whilst internal audit will be a key stakeholder for UK SOX and rich source of information and insight, we believe internal audit should not be tasked with implementation but should instead assist organisations with readiness for UK SOX by helping to bring challenge and drive accountability.

The time for change is now

In preparation for the potential implementation of UK SOX, many businesses today believe to be somewhat ready, but with significant improvement required to achieve full compliance. As any organisation who has transitioned into being subject to the regulation will know, SOX compliance represents a huge change in a business's approach to internal controls over financial reporting, with significantly more effort required to demonstrate reasonable assurance can be obtained over their adequacy and operating effectiveness.

While the timeframe for rolling out an equivalent piece of regulation in the UK market is still uncertain, this impact is going to be a lasting one. It is vital that organisations are ready to consider their controls, so not to be adversely impacted in the future and be required to plug any gaps with improvised solutions, to the detriment of the whole control environment.

The time for action is now.

Contacts

If you wish to discuss any of the topics covered in this publication and their implications for your business in further detail, please do not hesitate to get in touch with the team.

Peter Astley
Global Internal Audit Lead Partner
pastley@deloitte.co.uk
+44 20 7303 5264

Karl Williams
UK Internal Audit Lead Director
kdwilliams@deloitte.co.uk
+44 20 7007 6645

Deloitte.

Designed by CoRe Creative Services. RITM0642757