KPMG

UK SOx - FAQs

A summary of Q&A from the latest webinar

November 2021

Since the release of the Government's whitepaper on 'Restoring trust in audit and corporate governance', we've been looking at what this could mean for you, your controls and your company.

Our latest webinar, 'UK SOx: What does it mean for me, my controls and my company? Part 2' looked at what we've seen in the market so far, what 'good' looks like when it comes to a UK SOx programme, and its impact on the organisation overall.

This document summarises the questions you asked on the webinar, together with our responses.

We hope this document will help you with your thinking and planning for the changes ahead.

01 My company is headquartered abroad but has a subsidiary in the UK. How different do we expect the UK Government proposals to be from existing requirements in other countries?

We don't know the specifics of the UK legislation yet, but the current recommendations would allow the widely-followed COSO 13 guidelines to be used as a framework. However, there may be local considerations such as lower levels of materiality or specific scoping and disclosure requirements that would be unique to the UK.

Compliance with the requirements of COSO 13 will stand you in good stead but, once published, the detail of the UK legislation will have to be analysed in order to determine any gaps between your current environment and the UK legislative requirements.

02 Is there an expectation of a secondary consultation?

The current expectation is that the government will provide an update on the consultation by **December 2021** or soon thereafter. There is general support in the market for a potential further consultation on internal controls to confirm the specifics of how such a regime maybe implemented. However, there has been no official comment on this from government.

03 How can stronger internal controls prevent companies from failing?

Strong internal financial controls alone will not guarantee business success.

However, strong controls that are deliberately mapped to a careful consideration of financial statement reporting risk will certainly reduce the likelihood of reporting error, fraud and the restatement of accounts. We can see the evidence of this in the US, where restatements have fallen since the introduction of US SOx in 2003.

04 How closely aligned to US SOx is the UK legislation expected to be? Would it be beneficial to focus on corporate culture rather than SOx requirements?

It's not clear how the UK approach will compare to the US. However, there has been much commentary in the press and from key stakeholders about learning from the US experience and avoiding any of the pitfalls seen there - both in terms of the cost of implementation and the value that controls can bring.

It's our belief that, if implemented well, a SOx controls framework can help companies improve controls culture, drive standardisation and automation, and ultimately realise cost savings too. To achieve this, companies must adopt the right mindset and be strategic and thoughtful in their implementation approach

05 Are there UK software companies developing SOx IT programs to use?

There are many software companies who provide cloud-based technology to manage internal risk and controls, including to store control libraries and perform self-assessments. Many of these vendors are well-established and have mature products already used for other regulations and industry standards. In addition, software providers are working on new solutions and services as market requirements evolve.

KPMG would be happy to carry out an assessment of the viable options for your specific needs if required.

06 Where does internal audit fit into UK SOx? How does internal audit get involved or get the ball rolling?

We see internal audit as having a critical role in the framework. Ultimately, and under the Government's preferred option, in instances where the Audit Committee doesn't seek an external audit opinion, internal audit could well be the third line testing capability over the design and efficacy of key internal financial controls.

In the absence of an external audit opinion on internal financial controls however, internal audit will need to take extra care that it isn't involved in the remediation / design of new controls for fear of subsequently 'marking its own homework'. Such work should instead be a matter for the business (first or second line).

07 How do we ensure we are proportionate in our implementation? There is a risk that some companies may not understand proportionality and end up with a significant implementation cost.

Investing time in scoping and risk assessment upfront will enable you to identify your key financial reporting controls across each part of your business at both an entity and financial process level. Understanding this will allow you to determine where to focus your time and effort, and ultimately help you avoid the costly mistakes we saw through the original US SOx implementations of the past.

We have an in-house scoping tool which can help you automate your entity and process level scoping based on both quantitative and qualitative risk factors.

08 SOx was effectively a "big bang". Should we learn that lesson and promote a phased approach even for larger companies?

Our view is that a phased approach can result in controls being more widely adopted, and minimise disruption to the business. That said, it can take more time, with success dependent on starting the journey early.

Nevertheless, a phased approach allows for no-regret actions to be taken early, before the detail of the legislation is clear, whilst providing regular checkpoints to adapt the direction of the programme once the requirements are more certain. Overall, we believe the benefits of a phased approach are clear.

08 How does UK SOx apply to privately owned businesses?

In its White Paper, the Government proposes to extend the UK's PIE definition to include large companies within certain limits regardless of whether they are publicly listed.

This would mean that certain large private companies would be included within the definition of a PIE.

The Government believes that the size of a company is a significant factor in determining whether it is a public interest entity. Larger companies tend to have a higher number of employees, creditors and investors, with greater social and economic impacts should they fail. The continued success of large companies, whatever their legal status, also has a sizeable impact on the economy at large as well as on its employees, suppliers, customers, and others.

10 Who has been leading the Internal Controls improvement programmes that you have been supporting? e.g., Head of Internal Audit vs Group Financial Controller?

The majority of the programmes we are supporting on are being led not by internal audit but by the Group Financial Controller, CFO or Head of Financial Controls. This ensures independence – because internal audit is generally expected to provide assurance and so must be at a remove from the actual implementation.

In instances where internal audit does take the lead, organisations ensure that assurance is then provided independently by either a third party or dedicated assurance function.

11 What are some of the 'no regret actions' organisations can take now?

We view "no regret" actions as key outcomes which can be delivered before the detail of the legislation is known. These build the foundation of your control environment.

Key no-regret actions might include:

- A scoping exercise to determine a risk-based prioritisation of your finance processes and systems
- Developing a phased roadmap for the implementation of controls, and securing a mandate from your audit committee to deliver against it
- Documenting the control framework
- Designing the foundations of your BAU operating model, including roles, responsibilities, and estimated capacity requirements across teams
- Assessing the controls culture in the business, and creating a plan for upskilling and training sessions if required
- Assessing your technology needs for BAU

12 How important is automation in improving your control environment for SOx?

Using UK SOx implementation as catalyst to enable automation of processes and controls is one potentially significant benefit beyond pure regulatory compliance. Having a highly manual control environment increases the control risk and pushes up cost. Getting the right balance of manual and automated controls improves the control environment by enabling real time reporting, reducing key person dependencies, and bringing down the cost of control operation and testing.

13 It may be early, but are we seeing any Internal Audit functions working on and potentially launching the Audit & Assurance Policy now or for 2021 reporting?

There have been a few early adopters who have already published their audit and assurance policy publicly (3i Group Plc, Severstal etc). In addition, we are helping a number of our clients not only with documentation of the audit and assurance policy but with strategic transformation of their Internal Audit functions to help them get ready for upcoming and future corporate governance reforms.

14 For those organisations that do have a RACM in place and have identified a plethora of key controls, what factors should be considered when kicking off a testing plan?

We would recommend mapping your controls to your top risks in the business to prioritise for testing. In an ideal scenario these risks would be aligned with the external auditor's view.

15 Do internal audit need to be the ones doing the controls testing?

This depends on the approach your company is taking to attestation. Some clients view self-certification as sufficient evidence for the attestation process, in which case the first line can attest to the efficacy of the controls. Companies who prefer a more independent view of control effectiveness rely on internal audit for testing, or even consider outsourcing testing to a third party.

16 Segregation of Duties (SoD) is a key control, yet we rarely hear of a significant deficiency in this area. Does that mean the current environment is robust in regard to SoD, or are other controls mitigating the risk?

This is quite a complex question with multiple factors to consider. Typically, we see SoD issues contributing to a significant deficiency or material weakness, rather than being a sole cause. For example:

1. In aggregation with other access issues including privileged/ critical access, access review, provisioning, and configuration.
2. Where a key process is undermined such as in respect to payments, journals, or IT change management.

Access / SoD controls are usually preferable as proactive compared to detective, review type controls. In a SOx assessment, we would expect external audit to identify any deficiency relating to SoD unless a mitigating control is contained in management's control framework.

17 To what extent as external auditors do you engage on discussing key controls with audited entities as a starting point?

The current proposals are for the new requirements to be phased in. Premium listed entities are likely to be in the first wave of companies subject to compliance, followed by Public Interest Entities (PIEs) in a later phase.

In its White Paper, the Government proposes to extend the UK's PIE definition to include large companies within certain limits regardless of whether they are publicly listed. The current proposals are for the PIE definition to be expanded to either:

- **Option 1:** companies with more than 2,000 employees, or a turnover of more then £200 million and a balance sheet of more than £2 billion
- **Option 2:** companies with over 500 employees, and a turnover of more than £500 million

The Government believes that the size of a company is a significant factor in determining whether it is a public interest entity. Larger companies tend to have a higher number of employees, creditors and investors, with greater social and economic impacts should they fail. The continued success of large companies, whatever their legal status, also has a sizeable impact on the economy at large as well as on its employees, suppliers, customers, and others.

For more insights on UK SOx, visit our insights page

kpmg.com/uk

Designed by CREATE | CRT137924A