UK SOx (internal controls)

Corporate Governance Reform FAQ

April 2021

The Government's proposed corporate governance reforms, including stringent new internal controls requirements, raise many questions that business leaders need clarity on.

What do the internal controls requirements mean in terms of individual director responsibility? What are the likely timescales, and what actions should businesses be taking now? What does the experience of companies complying with US SOx teach us? And many more.

In this document, we have collated the range of questions that we received in our Corporate Governance Reform webinar held in March 2021, together with our responses.

We hope this document will help you with your thinking and planning about the changes needed.

Question 01 When do you expect the new requirements to come into force?

The White Paper does not include any timeframes for when future requirements would come into force. From our US experience, companies typically have two full reporting years before they are required to be SOx compliant. So, if UK legislation is finalised in 2022, it would not be unreasonable to assume a 2024 year-end start for premium listed entities.

The Government's preferred option is for the new requirements to apply to UK Public Interest Entity (PIEs) two years later.

Question 02 Does the White Paper specify which controls will be covered by the directors' attestation? For example, is it limited to internal controls over financial reporting?

The White Paper consults on three options for the areas covered by the Directors' Attestation:

- All aspects of the company's internal control and risk management procedures; or
- Limited to the internal control structure and procedures for financial reporting (similar to US SOx); or
- Limited to a subset of the internal control structure and procedures for financial reporting, focusing the auditors' work only on priority areas of particular interest to investors (similar to a SOC1).

The Government's preferred approach is option 2.

Question 03 Does the White Paper set out the consequences for directors?

The White Paper explicitly links the attestation Directors will need to make to Audit, Reporting and Governance Authority (ARGA) enhanced oversight regime over Directors. It focuses on whether the attestation is misleading and flows through to potential civil penalties (e.g. clawback / malus provisions) and the ability for the regulator to pursue an investigation and enforcement measures.

Question 04 Will we need to implement a controls framework over ESG, fraud, payment practices and other disclosures, and how can we do this in the absence of a defined standard?

There are a number of disclosures in the Annual Report and Accounts which go beyond areas covered by the statutory audit, including those over sustainability and corporate governance. The White Paper introduces the requirement for a publicly available Audit and Assurance Policy which will set out how the Directors get comfort over all disclosures in their AR&A, above and beyond the statutory audit, and where this assurance will come from over a three year period.

This Policy will also need to describe tendering arrangements for external audit and the role and scope of the internal audit function.

Question 05 What action would you recommend we take now, ahead of the legislation being enacted, and how can we avoid potential costly re-work once the specific requirements are known?

The White Paper sets out the Government's preferred option which really feels like a "minimum" position that companies will need to achieve. The challenges really come around the scope of controls and the framework you use. Our view is that it would be sensible to assume that:

— Management will need to give some form of external statement annually about the strength of internal controls over financial reporting.

— While there may or may not be a requirement for auditor review and / or opinion in relation to that statement, you would be wise to work on the basis that your controls and documentation to support those controls should be of an 'auditable standard'.

— Whilst you may be able to select the framework you use, given that COSO 13 is widely recognised as being a strong benchmark with lots of support materials already in place, this is likely to be the default option for many.

— If you're not already US SOx compliant there will likely be some work that you need to do to support making an external statement .

— Even if you are US SOx compliant, your larger non-listed entities that may currently be scoped out (perhaps due to materiality) could well come into scope under any new PIE definition.

There are a number of "no regrets" actions we believe you can take now:

— These changes will require a cultural shift, supported by effective messaging and tone from the top. Clear roles and responsibilities, scorecards, accountabilities and training will be key.
Where to start: Educate your Board on what this will mean for them - this will likely be well understood by the CFO and perhaps others but the impact of these proposed changes extends well beyond the Finance function.

— Be very clear as to the benefits you expect to drive. Our experience from other countries including the US is that those who see this as an opportunity to transform (and not simply as a compliance exercise) are the most successful.
Where to start: Set out a clear benefits case and use this to help your organisation understand 'why' they need to change and not simply 'what' they need to change.

— Take a look at any ongoing transformation programmes that you have running now. Are you addressing internal controls requirements already? If not, you should be - as retro-fitting these later will cost you up to three times more.
Where to start: Review your ongoing programmes. Do you have an internal controls workstream? Have you got internal controls SMEs embedded in the team? Review the approach and resourcing to ensure you address internal controls now.

— Get your risks right.
Where to start: Agree your principal risks in line with your future strategy and business model, starting with the key risks with a financial statement impact. If you don't know where your principal risks are, you will end up with the wrong control environment.

— Invest in the 1st Line of Defence.
Where to start: Establish your control owners and process owners now. These are people who understand the end to end finance processes, risks, associated controls and the supporting technology and tools. They need to operate a "show me don't tell me" mindset to start embedding good governance over your controls early on. Culture and good governance together are what will stop controls from failing.

— Define your key risk indicators.
Where to start: Can you confidently list your top 10 financial & IT controls? Do you know which processes present the highest risk and, therefore, need the most attention? Define your key risk indicators upfront with a balance between lagging and forward-looking indicators. This will help prioritise your efforts so that you are focused on what matters most.

— Standardise & Automate.
Where to start: There are easy wins to standardise processes, controls and leverage technology to drive resilience and efficiency. You can drive down the cost of controls if you really maximise the power of your systems. Our KPMG Powered solution defines leading practice for you and is a great starting point!

Do I need to retrofit controls into an ongoing Finance Transformation?

Question 06

Yes, we think there is enough detail in the White Paper to make it worth considering now which controls you will be expected to rely on, and whether they are designed and have been implemented effectively. Our experience shows that pausing a transformation to take account of this now is less costly than revisiting it at a later stage.

What impact do you expect the proposed changes to have on the external audit approach?

Question 07

Auditors in the UK currently adopt a controls approach in their audits in certain circumstances (for example, when testing balances subject to fraud risk or when testing areas of significant risk). The International Standards on Auditing guidelines on how to test those controls are similar in nature to Public Company Accounting Oversight Board (PCAOB) guidelines on how to test controls, and there has been increased convergence in recent years. We do not expect the basic common standards on how an auditor should test controls to change. It is possible that ARGA may expect auditors to undertake more controls testing as a result of the outcome of the consultation and we would expect the Financial Reporting Council (FRC) (or ARGA) to provide guidance at a later stage in respect of any associated auditing requirements.

Question 08

How do you expect the internal controls requirements to apply to US-listed companies which are already US SOx compliant?

If a company is premium listed, or meets the revised definition of a UK PIE, then we expect the new requirements set out in the White Paper to apply even if they are dual-listed. Based on the Government's preferred options for strengthening assurance over internal controls, however, we do not expect dual-listed companies which are already US SOx compliant to have additional work to complete, other than in making specific statements in the AR&A (likely as a "unitary Board").

Other aspects of the White Paper will likely be new to US SOx compliant companies and will therefore require action. These include the new Resilience Statement, Audit and Assurance Policy, and enhanced disclosure requirements.

Question 09

What changes to the definition of a UK Public Interest Entity (PIE) are outlined in the White Paper?

What requirements do you expect to apply to UK Public Interest Entities?

The Government plans to broaden the definition of a UK PIE to include any "large companies" (including private companies or those with a parent entity listed on a foreign exchange) if they meet certain size criteria. The two options for large company thresholds set out in the White Paper are:

— companies with either more than 2,000 employees or a turnover of more than £200 million and a balance sheet of more than £2 billion

— large companies with both 500+ employees and a turnover of more than £500 million.

In addition, the White Paper is consulting on whether Alternative Investment Market (AIM) listed companies with a market capitalisation over EUR200m should be brought into the definition of a UK PIE.

Question 10

We often hear of the issues associated with US SOx, such as an overload of controls and fostering a tick box culture. How can we avoid similar experiences with the UK Internal Controls Framework?

Avoiding tick box compliance will require at least two elements:

— Embedding the right culture, starting with tone at the top and reinforced with training. This will mean controls operators and owners understanding why they are performing controls, and the full requirements of their roles. This can be a challenge where staffing levels are not sufficient for individuals to take on these additional responsibilities and maintain adequate segregation of duties.

— Optimising control design to get the balance right between manual and automated control. This includes using "band aids" to patch over remediations with more manual controls. The best control environments won't have people operating controls they don't understand.

Question 11

How do you perform an impact assessment effectively at this stage (in terms of budget / people / audit fees / system costs)?

The White Paper does not include any timeframes for when future requirements would come into force. From our US experience, companies typically have two full reporting years before they are required to be SOx compliant. So, if UK legislation is finalised in 2022, it would not be unreasonable to assume a 2024 year-end start for premium listed entities.

The Government's preferred option is for the new requirements to apply to UK PIEs two years later.

Question 12

Can KPMG undertake a review of my company and assess how much work we have to do?

Yes, KPMG can undertake comprehensive health checks to help businesses understand their current position and identify gaps to the required future state. Please get in touch with us to discuss.

Question 13

What do the annual control testing cycles look like for US SOx? Is there time to remediate identified deficiencies during the year?

Design testing is usually performed by evaluating for a sample of one, whether a control is appropriately designed to address the risk.

Testing of operating effectiveness assesses the actual performance of the control throughout the year through sample testing to determine whether the control is operating as designed.

Any controls that fail either design or effectiveness testing would go through a remediation process. Once a control is remediated, it would go through another round of design and effectiveness testing.

Plan well. Seek to conclude on the testing of design and remediation as early as possible and ideally before the start of the financial year to give yourself enough time to remediate any test of effectiveness failures during the financial year.

Question 14

Has KPMG seen effective use of Robotic Process Automation (RPA) to perform control testing? We hear a lot about this but we have never seen any practical applications.

There has been an evolution of automation over the past 10/15 years, starting with data analytics which is now widely used in internal and external audit. There has been a substantial increase in the use of RPA in the more mature environment in the US, with over 50 clients using RPA for configurable controls, IT general controls and even process mining over standardised controls such as journals or POs. There are pockets of this in the UK which we expect to grow rapidly over the next 12-24 months as clients take advantage of the opportunity.

Question 15

Can our external auditor provide support with the implementation and testing of an internal controls framework?

External auditors are prohibited from providing support on implementations. Auditor independence rules will apply as is currently the case.

We would expect management to set up a dedicated SOx team, responsible for the execution of testing. These teams may be in-house, outsourced or a combination of the two.

Question 16

Do you expect to see the EU or other countries introduce similar requirements in the coming years?

Following the introduction of the US Sarbanes-Oxley Act in 2002, several other countries have introduced versions of SOx (eg Japan). There is currently no indication of an EU equivalent.

Question 17

In my experience, one of the main problems with controls is that people do not understand what makes a good control. Does the White Paper include any guidance on what is (and is not) a good control?

The White Paper does not cover this. Understanding what "good" looks like requires a number of lenses. The first is an end to end view and a consideration of the balance of controls between automated and manual and between detective and automated. Second is the precision of the control and how well designed it is in addressing the risk it was intended to cover. Third, each control needs to be well documented (i.e. if it isn't possible to easily describe the control operating, it is not a good control).

Question 18

Do you think we will end up with Dodd Frank type arrangements with the Securities and Exchange Commission (SEC) whistle-blowing fund coming to the UK under ARGA?

There are many aspects of the SEC's oversight regime which are not currently part of UK arrangements. The extent to which ARGA will mirror the SEC in its enforcement model is currently unclear. Clarity over this has not yet been given by Government. There are clearly a number of options available and we will update this FAQ as this develops.

Question 19

Under US SOx, where does responsibility for controls effectiveness testing typically sit within the Three Lines of Defence model?

Typically, in the first line of defence. In some companies, testing teams will sit in the second line. In both cases the role of the third line of defence (Internal Audit) is distinct.

Question 20

Does the White Paper provide any guidance on evaluating the severity of control deficiencies - material weakness vs. significant deficiency vs. deficiency?

No, the White Paper does not provide any information in this area.

Question 21

Are you able to share a link to a recording of the webinar?

Yes, a recording of the Webinar is available at the following link: https://m.marketing.kpmg.uk/webApp/sox-on-demand-webinar

Question 22

Without change in mindset, these reforms are not likely to prevent business collapses.

What will make the difference?

We agree!

For us the key thing is the cultural shift and tone from the top. Your Board needs to be behind this from the get-go, setting a clear agenda around it that flows down through the organisation. It's vital to articulate the benefits from all perspectives – for the company as a whole, for individual functions, and for individual directors/managers. It's also really important that individuals understand why good internal controls actually matter and not just the mechanics of implementing and running them. This is cultural change - it's not easy but it needs to be invested in if you are to make a genuine difference.

If you have any queries or would like to discuss further, please don't hesitate to contact us:

Richard Andrews
Partner
KPMG in the UK
E: richard.andrews@kpmg.co.uk

Nehal Jilka
Partner
KPMG in the UK
E: nehal.jilka@kpmg.co.uk

Craig Wright
Partner
KPMG in the UK
E: craig.wright@kpmg.co.uk

Rachel Woods
Director
KPMG in the UK
E: rachel.woods@kpmg.co.uk

Sarah Ward
Director
KPMG in the UK
E: sarah.ward@kpmg.co.uk

CREATE. | CRT133666G | April 2021