Take control

The right technology can be key to supporting the management of internal controls.

MARC JACKSON
PRACTICE DIRECTOR – INTEGRATED RISK MANAGEMENT,
TURNKEY CONSULTING

Key messages

- Despite the paring down of the 'UK SOX' element of the new corporate governance reforms announced in May 2022, organisations should not be deterred from controls transformation projects which deliver long-term value to the business, regardless of legislation.
- Implementing a controls transformation programme can be outsourced but, even without considering costs, by embedding an understanding of controls and the need for them within the organisational culture, an internal approach has much to recommend it.
- Technology has a key role to play in the management of internal controls.

In May 2022, the much-anticipated recommendations aimed at restoring trust in audit and corporate governance in the wake of several high-profile financial scandals were announced.

Based on a March 2021 white paper published by **BEIS,** and an industry consulting period, these had been dubbed 'UK **SOX**' due to the likelihood of UK directors being made personally liable for internal controls over financial reporting, as has been the case in the US since the introduction of the Sarbanes-Oxley Act in 2002. However, this element of the proposals has been dropped.

While this may be a relief to some organisations, for those that have prepared diligently in advance – as recommended by several players – some frustration would be understandable.

But the reforms will still introduce more scrutiny of UK businesses around financial reporting and corporate governance, as well as the effectiveness and resilience of audit firms. And the principles of understanding the risks faced by the organisation, applying effective controls and ensuring complete transparency are unchanged. Investing time, budget and resource early on should be regarded as good business practice, rather than having to undertake 'compliance for compliance's sake'.

Preparing thoroughly is also in line with the increasing lack of public and media tolerance for anything fraudulent or dishonest. Transparency is key; UK SOX principles, regardless of whether they are law, help to ensure that organisations do not stand out for the wrong reasons.

The current state of play

Some elements of the original proposals were retained; the operational separation of the audit and consulting practices at large audit firms will still be required to avoid any potential conflict of interest, while most or all of the group audits at UK-incorporated FTSE 350 companies will need to be performed via managed shared audits between 'challenger firms' and the 'Big Four' to help break up the latter's market dominance. Non-financial performance targets such as **ESG** will be audited along with financial ones, and the **FRC** will be replaced by **ARGA**, a new audit regulator with more powers

> **The design of the new controls framework should be tested internally before external auditors review it, and all controls and changes to them need to be well-documented.**

to influence and enforce change and impose fines where required.

But various parts have been scaled back, such as what constitutes a **PIE**; rather than sweeping 4,000 more private companies into the tighter regulatory system, the expanded definition reduces this figure to a rather underwhelming 600.

However, it is the significant watering down of UK SOX – the big-ticket item – that has caused the greatest disappointment among professional bodies and individuals within the industry.

It was intended to drive a change in attitude and approach to internal controls over financial reporting, as well as introducing an additional layer of rigour and establishing the risk and controls culture required to take UK companies to the next level of corporate governance. But with too few mandatory measures regarding formal internal control frameworks, directors' statements and the attestations needed to evidence everything, compliance cannot be regarded as compulsory.

Although 'UK SOX' is probably no longer an accurate reflection of the UK's audit and corporate governance reforms status, the term itself serves a purpose because it is well understood.

And despite the dilution of the reforms, the essence of what they are trying to achieve is certainly aligned with the founding principles of Sarbanes-Oxley; only time will tell whether the measures are strong enough to enforce changes in behaviour.

In the immediate term, the changes make robust internal controls essential. These ensure the integrity of information provided to stakeholders, so will also help to improve the much-needed dialogue between the board and investors to create that transparency for which everyone is pushing.

What should organisations do now?

When the term UK SOX first cropped up, some organisations took the opportunity to prioritise their controls transformation projects. These initiatives should not now be regarded as regret work – rather these organisations have taken a good-practice approach; strengthening internal controls regardless of the legislation is going to deliver long-term value. Internal controls offer extensive benefits in that they:

- help to safeguard an organisation
- minimise the risks to achieving business objectives
- protect assets
- ensure the accuracy of financial and non-financial records
- promote operational efficiency
- encourage adherence to policies, rules, regulations and laws.

Lessons from the US

UK companies can also learn from 20 years of Sarbanes-Oxley in the US, which was implemented following the demise of several public companies due to corporate crime. When it was first introduced, the tendency was for over-correction and a total focus on achieving compliance, rather than looking at the underlying principles of risk and controls, and what was right for the business in question. The result was a vast number of controls – the majority of which were potentially unnecessary – that all had to be tested and evaluated on a regular basis; a labour-intensive activity that was hugely time-consuming.

The bonus of today's UK landscape is that organisations can apply the principles of a US SOX style regime, but in a much more pragmatic and flexible way, one that is not over-controlled, that has a risk-based approach and in which controls are aligned to business objectives and associated risks.

Within that, guidance on implementing a controls programme can be taken from seasoned US SOX professionals. Recommendations include using a tried and tested internal controls framework and considering a flowchart, rather than narrative, to identify controls already in place. The design of the new controls framework should be tested internally before external auditors review it, and all controls and changes to them need to be well-documented. US SOX experts also advise that it's important to value the knowledge inside the organisation as it may be more efficient to lean on this, rather than rely on external consultants. Finally, technology is key and, although automation and continuous controls monitoring requires significant upfront investment, it pays dividends in the long run.

Outsource or handle internally?

One approach to a controls transformation programme is to outsource the whole process to an external provider. Costs aside, while this looks like a safe and straightforward route to compliance, it overlooks the benefits of using or developing internal experts. An internal approach reduces expense – but this is only one of the advantages. Engaging the organisation's own teams in the transformation process helps to embed it in the culture, meaning there is a better understanding of the controls and why they are needed, ultimately making it more likely they will be followed. It also offers the opportunity to upskill employees and ensure knowledge stays within the organisation. In addition, it helps every department to operate more efficiently because they have the best understanding of their function or business unit, their business processes and their risks; ultimately, their controls will be the ones that are best suited for their purpose.

However, practical considerations may make a fully internal approach unsuitable for some enterprises or mean that some external input is required. An internal approach increases the workload of employees that are already busy with day-to-day activities; the business needs to consider that some people will need to be dedicated to the transformation process for a period of time and work out how this will be handled.

Quality assurance is another potential flag, as the internal approach comes without the 'safety net' of external subject matter experts confirming that the programme delivers what is required. However, the counter argument is that internal involvement delivers more reassurance because there will be greater visibility of how compliance has been achieved. It is also worth noting that compliance is ultimately the responsibility of the business.

The internal route to compliance

Assuming most of the transformation process is handled by internal teams, the following checklist can guide most organisations towards effective compliance and more efficient business operations.

- Third-party help during the planning phase will ensure everything is covered and that the focus adheres to internal controls over financial reporting to meet UK SOX requirements.
- Internal auditors will be able to assist with scoping out the programme; their expertise will ensure only relevant areas of the business are included in the process, thereby preventing time, money and resources being used unnecessarily.
- High-risk processes take priority. As the foundational layer of the internal control environment, IT General Controls (ITCGs) will be a core area of focus. Order-to-cash is another priority given the financial remit of the proposals.
- The relevant internal stakeholders need to be engaged and on-board with the process; ideally this means someone from each business unit.
- Using a recognised internal controls framework is usually a better option than creating one from scratch which can be a daunting task.
- Not everything needs to be new and there will be activities already being performed that can be retained. Although some controls will need to be retired, some may only need fine-tuning, while others will be fit for purpose as they are.

The role of technology

A more regulated environment will require many new processes to be implemented; as noted from US experience, a technology-enabled internal controls management solution is essential for achieving compliance.

Technology increases overall efficiency, ensuring people's time is spent adding value, rather than undertaking repetitive tasks that can be automated. It uses workflows to provide people with the information they require at the time it needs to be actioned. And an automated, technology-based solution reduces risk by managing controls effectively, removing duplication and lessening the chance of human error; accuracy is increased and a full audit trail is created for each internal control department.

More extensive solutions support each line of defence in the three-lines model, a widely adopted framework for the management of risk and internal controls. The three-lines model outlines the organisational structures and processes required for a combined assurance model between the business and compliance teams – collectively known as 'management' – as well as internal audit. It requires collaboration to operate successfully, so the solution needs to be fully integrated across the three lines to avoid silos and to enable data to flow seamlessly between them all, as well as allowing the right level of information to be surfaced to the governing bodies sitting across the top.

Such technologies support management within the first two lines by allowing risks to be assessed and managed accordingly. Where controls need to be applied, technology enables them to be documented, evaluated, monitored and – where operating effectiveness issues have been identified – remediated and ultimately signed off by management. This supports the full life cycle of controls management up to the most stringent of regulatory requirements. In addition, audit management features allow internal audit teams to plan, prepare and deliver more effective and efficient internal auditing procedures, while retaining integration with supporting information and the status of live risks and controls where required.

Change control management is another benefit of automation technology in the new compliance-driven environment; it provides the organisation with a snapshot of its controls landscape at any given time and verifies that these tools are working correctly on a continual basis. This is a critical element in reducing risk and meeting governance challenges.

Ultimately, a robust, technology-led controls programme can reduce the cost of compliance. The current driver may be UK SOX, but implementing it now paves the way for a strong, future-proofed controls environment as both the risk management and legislative environments continue to evolve. That said, it's important to avoid an over-focus on the technical element; the key is to determine how the proposed tools support the business processes and ensure a strategic balance.

A catalyst for change

There is no denying that the pared down proposals for UK SOX are less than many had expected and some had hoped for. However, they do call for a more stringent way to handle risk and, in doing so, have the potential to act as a catalyst for real change that ultimately makes the UK a safer place to do business.