Is it time for SOX 2.0?

With some clever thinking you can take your control environment into the future

26 November 2024

It’s over 20 years since the Sarbanes Oxley Act came in and over ten years since the COSO introduced their COSO13 principles which underpin many SOX programmes. Since then, the pace of change across the financial services industry has been vast, with huge advances in technology and the backdrop of an ever-evolving regulatory landscape. And yet, despite significant investments, SOX controls haven’t kept apace.

The scope and nature of controls and testing tends not to have changed much, the inter-operability with other regulatory frameworks is limited and the level of automation is - at best - minimal. In contrast many internal audit functions, and indeed external audit techniques, have innovated through technology and are both more efficient and risk focused. So, is the time right for “SOX2.0”, and what would it look like?

As the saying goes; “there is no time like the present”. Many banks have now dealt with Significant Deficiencies and established a more stable and mature control environment which could act as a secure platform from which to drive real controls transformation.

Board focus on controls is not just about financial reporting anymore, the scope has been widened through issues with compliance with laws and regulations, UK corporate governance reform, PRA regulatory reporting themes and sustainability assurance. Coupled with regulators increasingly expecting 1st line testing. Ideally this leads to a more holistic and integrated approach to assurance across the three lines of defence.

A future-proofed control environment needs to leverage the technologies of today and be agile enough to adapt to the technological advances of tomorrow.

Across the market many organisations are embarking on large-scale GL / ERP modernisation programmes backed by large investments in data. Likewise, GenAI opens opportunities to automate more broadly, in areas that have been historically manual such as maintaining accounting policies or approving new products.

Significant spend programmes in technology present opportunities to redesign controls from the ground up, better leveraging automation and data analytics as well as investing in control infrastructure to enable real time insights across the piece.

There has been a focus in reducing reliance on detective controls and moving focus upstream to take more preventative measures, which are heavily automated. Leveraging advances in data and technology over recent years can help you to really shift the dial in this space.

- Implementing data analytics layers upstream can act as a control point to identify anomalous data and potential issues before they propagate downstream enabling earlier identification and reducing reliance on downstream controls.
- Controls should be considered by design when embarking on an ERP implementation or uplift programme, rather than an afterthought leveraging built-in system features (e.g. user access controls) where possible.
- AI and Machine Learning offer powerful tools for real-time controls testing, enabling organizations to continuously monitor and assess the effectiveness of their internal controls. E.g. automated exception detection and alerting, predictive analytics and risk forecasting, dynamic control adjustment and optimization.

Move away from controls for controls sake, and towards a truly risk based approach which allows for agility as risks change and materialise over time. Leaders in this space are seeking to embed an automated scoping process, developing automated risk scoring models and control mapping which automatically maps identified risks to controls based on pre-defined criteria and control libraries, before applying dynamic scoping and prioritization which automatically adjusts the scope of controls based on real-time risk assessments and changes in their business environment.

Additionally, Key Control Indicators (KCIs) and Trigger-Based Testing (TBT) are two complementary approaches that can significantly improve the effectiveness of internal controls. Establish KCIs to measure the effectiveness of key controls to provide early warning signals of potential control weaknesses. Embed TBT using data analytics to identify high-risk transactions that are more likely to be associated with control weaknesses. When used together, KCIs and TBT can provide a powerful framework for improving the effectiveness of internal controls. KCIs help identify the most important controls to monitor, while TBT helps focus testing efforts on the areas where they are most likely to find issues.

Above all, your approach should be enterprise wide, considering other programmes, initiatives, and frameworks in place across the business. Consider; integrated assurance in the 1st Line of Defence, how your enterprise risk management framework can be uplifted to recognise interoperability, and increased scope as well as ensuring controls are key in all transformations (particularly when designing data and/or technology solutions).

With some careful thinking, leveraging recent advances in enabling technologies and considering requirements across multiple regulators and environments you can reduce costs in your SOX programmes and future proof your controls environment.