Building a robust and resilient controls framework

By Bavan Nathan

Risk control test events can be costly and time intensive.

In fact, at a recent client conference we investigated the cost of these events and found the average cost was £2,000. That was only the direct cost, however. It didn't include hidden costs, such as management review or remediation.

Almost a third of those that responded said they undertook over 500 control test events a year. At an average cost of £2,000, that's a cost of £1 million. That considered, some organisations are spending in excess of £15 million on direct costs alone.

It's easy to assume that, given the costs involved, the control framework has a defined and valuable purpose.

Yet 81% of the companies that we surveyed stated that their SOX or Internal Controls (IC) strategy was in place in order to maximise external audit (EA). Two-thirds (69%) of the companies surveyed also said that their SOX/IC scopes were identical to the EA scopes.

This begs the question: What is the purpose of control framework? Is it for external audit? Or is it to manage the business effectively and optimise risk taking, as well as increase value?

The need for streamlined processes

We are increasingly being asked to help respond to these cost and purpose challenges. Over the last two to three years, discussions about control frameworks and of building a robust system of controls have increased substantially.

These discussions tend to revolve around three topics: simplifying and reducing costs; standardisation, streamlining and simplification across the business; and avoiding significant control failures or surprises in financial reporting.

There are other triggers though, such as the implementation of a new enterprise resource planning (ERP) system or significant business change.

There are some common issues that come up repeatedly when testing the robustness of an internal controls model.

Several of those pertain to ownership and accountability.

Internal control - who owns it and whose responsibility it is - remains unclear. In many cases, there is no clear ownership of the end-to-end control process.

Often, governance and accountability models have not kept pace with changes in the wider business. Risk controls have not been updated to reflect changes in the business. As a result, control activities do not always fully address the actual business risk.

In some cases, the testing methodology is not effective in identifying major control gaps, such as fraud. The testing of controls is fragmented, with minimal learning from period to period and little development of better practices.

This is exacerbated by a poor understanding of the SOX methodology and requirements. SOX controls are not being updated and maintained and the methodology is not documented. This is a source of the hidden costs we have talked about, which arise from not performing controls in the right way or for the right purposes.

Finally, companies aren't making full use of data and technology. In our survey, only 18% of respondents said they worked within a substantially automated

environment.

Discovering solutions

There are plenty of solutions to be had to these challenges, but there is not a one size fits all approach. The framework must be a tailored solution, one that suits an organisation's needs, culture, ways of working, and strategy.

There are several questions to be answered on the journey to building an effective framework.

For instance, who sets the standards? Does everyone in the organisation understand why those controls are being implemented, and what their purpose is? It's essential that the overall tone is set from the top.

The same is true for the design. It must be absolutely clear who holds the design authority, and that no changes, additions or deletions are made without the involvement of the design lead.

Who operates the controls? Does it fall under the finance function, for instance? The entire organisation must be clear about who operates and owns the process. There is no one answer, and each organisation must find its own approach.

Who determines how controls are monitored, tested and reported, and who owns this function? There needs to be end-to-end visibility and assurance that the risks are being managed to the appropriate standards.

What tools are you going to use? It's cheap and easy to build a framework, but it must be a user-friendly tool that can facilitate the efficient, accurate and reliable capture and reporting of risk and control information.

Cultural transformation

There is one final, but critical, component. There must be a clear shift in organisational mindset. The framework will fall at the first hurdle if there is no buy-in from the business.

The easiest way to achieve this is to involve the business early on, talking to the business functions about what they do and incorporating this into the framework.

A transformation of the controls framework needs a proper change transformation programme. It's not a part-time job and it needs resources, although it is likely to be a one-off cost, albeit an important one.

Any change needs to hinge on business strategy, and the control framework needs to articulate how it adds value back to the strategy by demonstrating tangible results such as cost savings.

There are plenty of benefits to building a robust and resilient controls framework.

The board and the audit committee gain transparency over the operating effectiveness of controls across the business. A strong framework also reduces costs and creates best practice that can be shared across different regions or business units.

A baseline set of controls allow a platform for future improvement, for example process alignment and system improvements. It will improve the understanding of controls across the organisation and will support policies and procedures at group level.

An effective framework allows the business to be managed more effectively and to optimise its risk taking. Ultimately, this minimises "surprises" or instances where control has failed. And those can cause irreparable damage.

kpmg.com/socialmedia