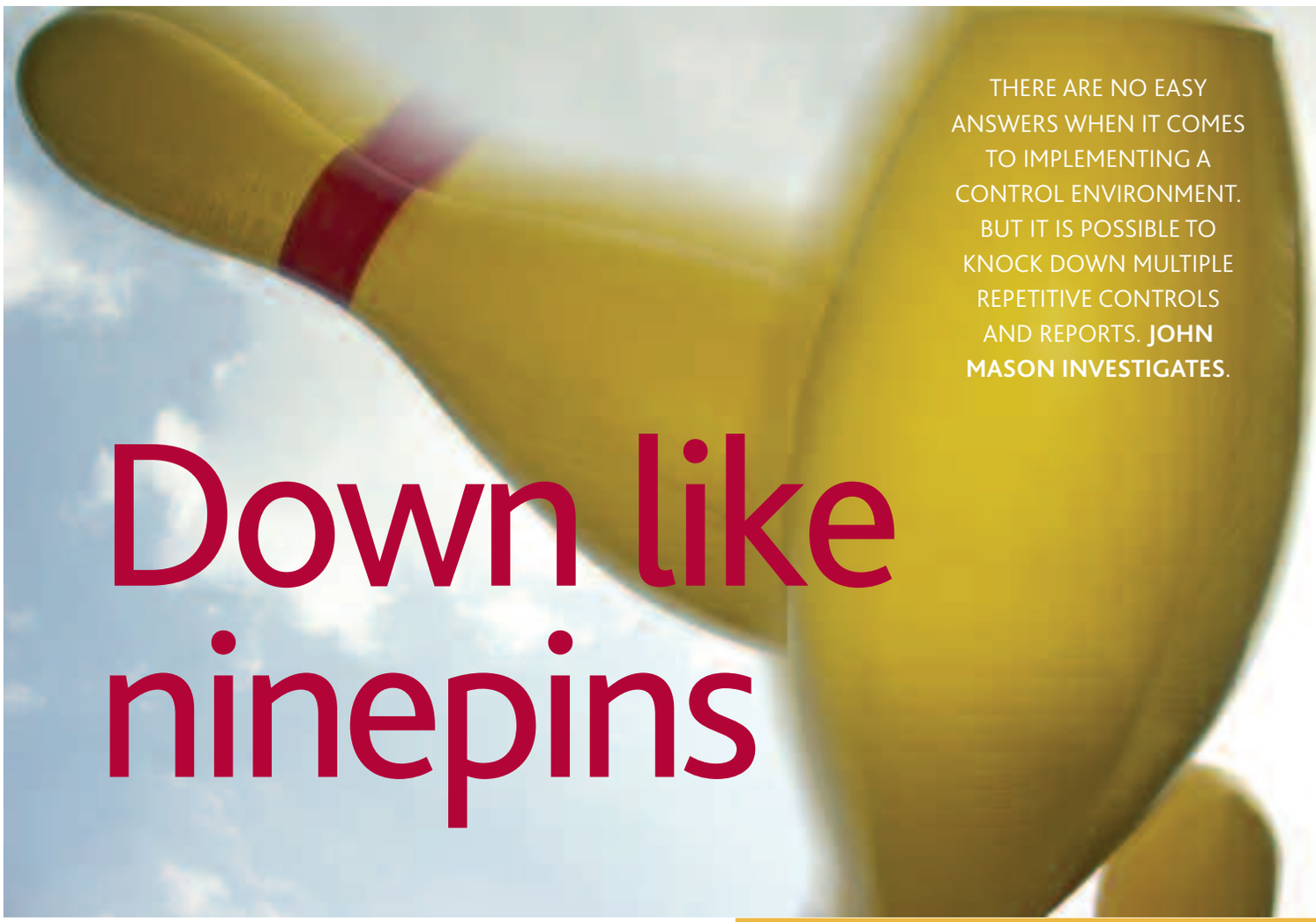

THERE ARE NO EASY ANSWERS WHEN IT COMES TO IMPLEMENTING A CONTROL ENVIRONMENT. BUT IT IS POSSIBLE TO KNOCK DOWN MULTIPLE REPETITIVE CONTROLS AND REPORTS. **JOHN MASON INVESTIGATES**.

Down like ninepins

As we have seen in recent years, some of the largest and most powerful companies in the world have suffered disastrous consequences through lack of internal control and rigour. Those companies have, in most cases, paid the price but they have also left a legacy of a costly burden of controls that remains and that is inflicted on organisations today.

Financial services compliance cost is astonishing. It is unlikely that an average bank will spend less than $50m on compliance in the next year. It is a matter of public record that some of the larger players have invested over $100m on Sarbanes-Oxley Act (SOX) s404 alone in 2004. At a recent compliance event, a Chief Information Officer (CIO) from one of the largest global banks admitted that no IT project would be completed in its North American division in 2005 unless it was SOX specific. If you start to add the costs of other regulatory initiatives – such as changes resulting from Basel II, The Directive on Markets in Financial Instruments (MiFiD) and the Prudential Source book and other governance activities – the numbers add up to billions.

So if you went to the average person in the street and said; "By the way did you know that your bank is spending millions of pounds to be in compliance," would they be taken aback? Actually apart from the magnitude they would probably not be surprised. However, if you asked the question another way: "Did you know that your bank is spending millions of pounds getting its business under control?", well the reaction would probably be to withdraw their cash and stuff it under their mattress.

Executive summary

- There is no difference between control and compliance as long as the processes controlled are compliant.
- Although there is no easing of the control burden, corporates can adopt a more sustainable and proactive approach to controls.
- Fundamental key controls are common across different regulatory environments and with planning it is possible to embed controls and processes within the organisation and eliminate duplication.
- Organisations should see regulatory issues as a business issue rather than silo projects.

SILO PROJECTS Fundamentally there is no difference between control and compliance as long as the processes that are controlled are compliant. The Turnbull Guidelines refers to "embedding of controls" within the business as part of the usual processes, yet banks have rushed to set up separate silo projects to meet the time demands of regulations without addressing the underlying process deficiencies. This becomes more acute if you examine how the larger banks have made their money and where their new margin improvements are coming from. The 'bulge bracket' banks have grown primarily through acquisition, which means more systems,

more processes and different practices all leading to an ever increasing control nightmare. The alternative growth strategy has been to take on teams doing increasingly complicated transactions – for example in credit derivatives – where the back office systems cannot cope with a straight-through process and there is growing piles of unmatched trade confirmations.

ADOPTING A PROACTIVE APPROACH TO CONTROL

The role of control within an organisation is therefore nothing new but increasingly companies are realising that a more proactive and sustainable approach to control is required. Many of the faults with the existing approach have materialised over time as new and more frequent regulatory demands have been placed upon organisations. The typical approach has been for companies to address regulatory requirements as multiple projects rather than as an embedded part of the normal business process. This is at its most obvious in large international banks where it is quite common to see a Head of Risk, a Head of the Basel II programme, a Head of Sarbanes-Oxley and so on. This approach can actually lead to increased risk of non-compliance due to the integrity issues created by multiple sources of the same control information. Increasingly however, more and more of the businesses are beginning to realise that most of the fundamental key controls are actually common across the regulatory requirements and with some initial forethought and planning the overall number of controls and associated reports can be reduced.

This approach has a fundamental impact on the control environment. The first major benefit is felt by the business line where the demands for answering the same questions but from different inquisitors are reduced. The other major beneficiaries are the likes of finance, internal audit, compliance, product control and operations. By basing the regulatory responses upon a single set of controls, the worry of controlling multiple control environments disappears.

Once a common set of corporate controls has been defined as a hub, it allows the business to define any business or country-specific controls into outlining spokes i.e. the corporate controls are held in a central library which offers various subscribing departments the ability to define subsets of these controls. This too has a fundamental impact on the company as now it allows the business line to adopt best practice management controls that actually help drive the quality and service of the business offering. Suddenly controls are no longer seen as the burden or overhead that they are regarded as today, but they are seen as being able to add genuine value to the organisation.

Control can become much more pro-active. Day-to-day and even intra-day tasks can be attested to, and if certain tasks are missed or undertaken with issues, those issues can be addressed in a much more timely fashion. By mapping controls embedded into the business line to specific regulations, managers can actively monitor compliance but from a business as usual perspective. Take nostro reconciliations as an example. There will be a number of daily controls around this process, such as

- Were the external files received on time?
- Have all the items been matched and all breaks identified?
- Have all breaks been distributed to the relevant parties for resolution?
- Have the breaks been aged and any previous breaks been followed up?

REPLICATED CONTROLS These controls are replicated for each nostro account and many banks will have hundreds of these. These controls, apart from being good business practice, are also relevant to the regulations, for example the Financial Services Authority (FSA) client money regulations require that client money is segregated correctly. Additionally, it will be a key SOX control. If the controls are not performed then it is likely that regulations have been breached.

This enables the central control teams to spend time stipulating policy and standards rather than chasing around ensuring divisional heads have completed questionnaires. The business heads too are happy as they no longer feel that they are answering questions from which they derive no benefit but have a more granular and specific set of controls from which they can control their area of interest.

Perhaps though, the major benefit that is derived from driving a business as usual approach is that a control culture is created within the organisation from the bottom up. Each individual within the organisation becomes aware of their responsibilities and accountabilities, ensuring there is a drive to accuracy and rigour throughout. This can often be regarded as a Big Brother approach to monitoring how staff are performing against their designated roles and tasks and therefore must be implemented with sensitivity to ensure all staff buy into the concept.

Once a company recognises that greater benefits can be achieved than just satisfying their regulatory obligations by providing a more proactive and sustainable control environment, they can look to implement such a culture and controls within their organisation. Management must move away from addressing regulatory requirements as projects and more as a business issue that is here for the long term and must be solved that way. In short, management must begin to concentrate on controlling the ball, not just the score.

John Mason, Head of Sales, Business Control Solutions.
john.mason@bcsplc.com
www.bcsplc.com

Sets of control standard

There are industry accepted sets of control standards which many organisations are looking to leverage. Control standards that companies are looking to adopt include COSO and COBIT.

The US-based Committee of Sponsoring Organisations of the Treadway Commission (COSO) was founded in 1985 to sponsor the National Commission on Fraudulent Financial Reporting. It is now a voluntary private sector organisation focussed on improving the quality of financial reporting through business ethics, effective internal controls and corporate governance. COSO now provides two control frameworks, one for larger enterprises and one geared towards smaller companies. Both have been accepted as internal control standards satisfying both the Sarbanes-Oxley Act (SOX) and also the US Public Company Accounting Oversight Board Standard 2.

Control Objectives for Information and related Technology (COBIT) issued by the US-based IT Governance Institute sets out technology related best practices. The idea is for organisations to instil a culture of control throughout their processes.

This aspect of control within the IT infrastructure of a business is often overlooked by organisations but is as vital as those controls that are implemented in the business lines themselves.

COSO and COBIT and others can offer companies an approach to a sustainable control environment based on best management practice which can not only provide the assurances that senior management are looking for to satisfy the ongoing regulatory demands of the present and the future but will enhance the business in general.