

SOX: MORE RED TAPE OR THE ULTIMATE BLACK MARK?

In the wake of corporate scandals, the US Government introduced even more strict financial reporting requirements – SOX. John Hookham (below) looks at the implications for UK finance and IT departments.



In the summer of 2001, Enron's share price plummeted to 20 cents as investors lost all confidence in the company and its management. Mistrust of the auditors would come later – a massive financial scandal was unfolding and it would not be the last to shake the foundations of Wall Street.

Based on market capitalisation, the US is the world's largest stock market, accounting for over 50% of global worth – and so desperate measures were needed to re-instil investor confidence. In July 2002, the US Government passed the Public Company Accounting Reform and Investor Protection Act, sponsored by US Senator Paul Sarbanes and US Representative Michael Oxley. This is the Sarbanes-Oxley Act, often referred to as SOX.

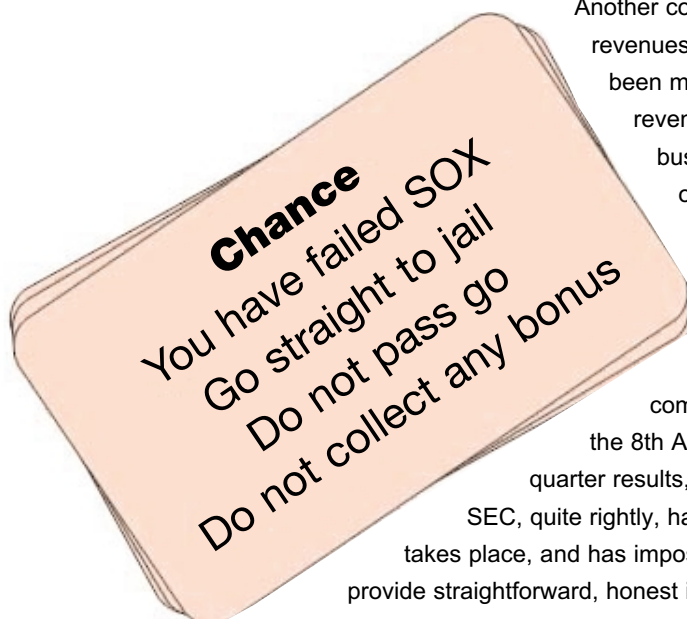
Initially seen as applying only to US companies, SOX is now becoming more important not only for UK companies listed on the US Stock Exchanges (who have to comply), but also as a general measure of corporate governance. After all, Europe is not free from financial scandals, as witnessed by the collapse of Parmalat in Italy.

National government legislation requires that public companies – ie, companies in which the public can buy shares – put into place controls and reporting procedures that will ensure their financial statements and reports are accurate. In the past, investors have relied on the companies being self-regulating and on the Securities and Exchange Commission (SEC) to vet and monitor company financial reports such as the 10-K and the 10-Q. These are the US formal annual and quarterly reports respectively, that need to be produced on a timely basis and comply with the Securities Exchange Act of 1934. Both of these reports are formally audited and signed off by an external accredited accounting firm.

Over recent years, many companies – as many as one in five according to the US General Accounting Office – have needed to re-state or re-issue their financial reports. For example, it is claimed that the management of Enron were responsible for hiding losses within part-owned subsidiaries so that profit figures became distorted.

Another common reason for re-stating financial reports is revenues being overstated, which implies the company has been more successful than it actually was. Overstatement of revenues has been particular prevalent in the software business where a company's share (or stock) price is often closely linked to revenue growth. A failure to 'meet revenue expectations' not just with annual results but even quarterly results, could easily wipe 30% off a company's share price in one day.

So in the past, it was fairly common for some companies to sign contracts on the 31st March! (actually the 8th April) and for the revenue to still make it into the first-quarter results, as the date on the contract was 31st March. The SEC, quite rightly, has ensured that this type of sharp practice no longer takes place, and has imposed ever more stringent rules to make companies provide straightforward, honest information for investors.



But as the scandals at Enron and WorldCom have shown, other measures were also needed. The Security Exchange Act of 1934 established rules for accounting standards and the reporting of company results. The aim was to provide investors – ie, people who are outside the company – with accurate information by concentrating on the content of these external reports.

The focus of SOX is not on external reporting, even though this is where the results and effects will ultimately appear, but on companies' internal processes. These business control procedures must be documented and certified to show that they are in place. The processes also need to be monitored to show that they continue to work effectively. Finally, the SOX report needs to be signed off by the company's executives and its external auditors.

For all its physical weight and length, like many legal tomes, the document produced by the SEC does not lay out in detail exactly what internal procedures and processes need to be followed. It is left up to individual companies to implement the necessary controls to ensure SOX compliance. But in essence, the controls need to ensure that records are kept which accurately reflect details of the acquisition and disposal of assets. These controls must also help the detection of any unauthorised or fraudulent activities and ensure that all accounting transactions comply with the General Accepted Accounting Principles (GAAP).

Not just finance

At first, SOX was seen by most companies as an issue for the finance director and the audit firm, but over time its impact has widened to affect other areas of the business and especially the IT department. This is entirely logical as in all modern businesses IT is the backbone that supports the company, and covers the supply chain and operations, as well as finance.

Studies have shown that large corporations tend to have a mix of IT systems. For example, a single corporation could be running ERP systems from SAP and Oracle at large sites, with Geac, Baan and Epicor at smaller sites. Finance systems will also vary, from those supplied as part of an ERP system to disparate non-integrated or standalone systems, again from a range of different suppliers.

Ensuring SOX compliance in this type of mixed environment can place a massive burden on the IT department. However, most ERP systems have integration tools and in-built rules to verify data integrity; and for very complex environments, there are a number of specialist middleware tools and systems available to help simplify the task.

At the heart of SOX is the demand for accurate financial reporting, which can only be achieved if the underlying data is itself correct. The other key requirement for SOX compliance is that the company's internal processes can be monitored and the base data can be checked and verified.

Clearly the best way to accomplish this is by controlling user access to financial data and using a detailed audit trail to record all transactions and any changes. Both these aspects are generally covered extremely well by all the ERP and finance system suppliers – from enterprise suppliers such as SAP, through mid-range companies like Lawson and IFS, to the smaller niche players such as QAD and Epicor. While the data remains inside the ERP and associated finance systems, SOX compliance should be relatively straightforward to implement and prove.

Spreadsheet problems?

It has been argued that IT systems, and in particular ERP systems, have helped companies generate efficiencies and drive out costs from the business. However in many cases the base data is being extracted from the ERP systems and put into spreadsheets to be manipulated, corrected and given a reality check, before being re-keyed back into the corporate ERP system. This in itself is seen as no bad thing – otherwise so many companies would not operate in this way.

But when questioned as part of a recent survey, more than half of the companies admitted to using spreadsheets as an integral part of their financial reporting procedures. For example, in the past, one UK subsidiary of a US corporation gathered data for its financial reports almost entirely from multiple spreadsheets. On a monthly basis the standard

corporate spreadsheet was emailed to each of the managers who were in charge of the company's 50-plus UK areas. Each manager would input the various sales figures and other operational data into the spreadsheet and when they were happy with it, they would email it back to the central office. When all the spreadsheets had been returned, the finance director would run a consolidation process that aggregated the results from the regions to produce a single summary spreadsheet, which was used to update the corporate ERP system.

Apart from the potential for mistakes in the consolidation process, errors could easily be introduced at the regional level. Fortunately, the UK-based managers and finance director were honest and diligent – but the opportunity for misreporting or fraud is self-evident. The honesty and diligence of individuals is not the problem: the issue is that reporting systems and processes such as in the example above do not comply with the SOX requirements at a number of different levels.

Firstly, financial data can be 'adjusted' by the individual managers without an audit trail and without the appropriate reports being produced. Secondly, at the regional level, there is no way of ensuring or even checking that the correct internal process has been followed. Thirdly, the rules built into spreadsheets (both the regional sheets and the summary) can be changed quite easily, data might be missing, last month's figures may be entered by accident, etc.

So the use of spreadsheets can present a fundamental problem when companies need to show SOX compliance. It will be a brave CFO who signs off on the integrity of the finance figures and the business processes behind them when much of the source data is manipulated or gathered from manual inputs to spreadsheets.

There are no quick and easy fixes to gain SOX compliance, yet much of what is required is already contained in existing ERP systems. However in some cases either the ERP software has been badly implemented or users have simply not been properly trained – or the IT department believes the individual users are using the ERP software in a prescribed way only to find that when the users are questioned in detail, an entirely different picture emerges.

This is often the case when the ERP system has been in place for a number of years, people have changed jobs and there has been a shortfall in the transfer of knowledge as to how the software operates and the functions that are available. In many cases, 'workarounds' using spreadsheets or separate standalone PC packages have been put in place. Consequently, most companies will need to review and document how their business is actually run, not just how they think it is run, to ensure SOX compliance.

Consequences of non-compliance

Whether SOX is viewed as yet more red tape or as a necessary protection for investors, there are serious consequences for non-compliance. SOX is subject to strict liability: put simply, this is the legal term where if an offence is committed, you are guilty. Even if the non-compliance was a mistake and there was no intent, you are still guilty and face a fine of \$1 million and up to 10 years in prison. In the worst-case scenario, where intent is proved, then the company official is looking at 20 years inside and a fine of \$5 million.

No wonder companies are investing significant cash and resources in SOX compliance – individual responsibility and accountability is a great motivator.

● *John Hookham is a director of management consulting and marketing services company Adrelia Ltd. Tel: + 44 (0)20 7286 7073 Email: john.hookham@adrelia.com.*

● *If you would like more information about this article or any of the products or companies mentioned in the article, please contact us at info@evaluationcentre.com.*