Act of punishment

Many non-US companies are seeking to sidestep the Sarbanes-Oxley Act rather than risk the threat of non-compliance.

Of all the compliance legislation being enacted around the world, the US Sarbanes-Oxley Act is the one that is causing most consternation, if only because of the powerful – and personal – penalty that people may pay if they fail to comply: prison.

For those companies that fall under the auspices of the act – companies listed on a US stock exchange – the 'to-do' list is long and far-reaching and will embrace every unit in every corner of the globe in which they operate. According to analyst estimates, about 1,000 non-US based companies are affected, some of which are now considering de-listing in the US in order to avoid Sarbanes-Oxley.

The first swathe of companies to be affected by the Act are those with a market value of greater than $75 million and a financial year that ended before 15 November 2004. They now have until 29 January 2005 to file Sarbanes-Oxley financial statements. Companies with later year-ends have 75 days after their year-end to submit their financial statements, while those with smaller market capitalisations have until 15 July.

The penalties for failure to comply include personal fines for board members of up to $5 million and jail terms of up to 20 years.

Even with the serious penalties that non-compliance may bring, many companies are still not sure if they will be able to hit the deadlines. "It's likely to be a sprint to the finish," says Donald Nicolaisen, the chief accountant for the US Securities Exchange Commission (SEC). Indeed, a survey by accounting firm PricewaterhouseCoopers (PwC) of 700 companies revealed that only one-fifth were on schedule.

"Companies have identified many more deficiencies than they originally anticipated and they've found some real control gaps," says PwC chairman and senior partner Dennis Nally.

In some cases, the most cost-effective solution – particularly for non-US companies with listings on US stock markets – will be to de-list. Travel web portal Lastminute.com has already de-listed and UK entertainment company Rank Group announced in December that it was considering a similar move.

In Germany, half a dozen top companies with US listings intend to withdraw rather than spend the time and money necessary to comply with the Act.

IT implications

One of the most onerous aspects of Sarbanes-Oxley is the associated IT cost. While most parts of the Act have nothing to do with IT, there are some sections that require major modifications to IT systems.

In addition to requiring CEOs and chief financial officers (CFOs) to personally certify the accuracy of their financial reporting, Sarbanes-Oxley also demands that CEOs, CFOs and outside auditors attest to the effectiveness of internal controls for financial reporting. They also have to report significant changes in their financial conditions "on a rapid and current basis".

Depending on how strictly these rules are interpreted, CEOs, CFOs and, by extension, CIOs might have to produce real-time reports on the

performance and use of the entire IT infrastructure for the relevant financial period.

"You do have to be very granular," says Philip Yarnall, head of compliance consulting at PinkRoccade. "The practical elements of compliance with Sarbanes-Oxley come down to people signing off on elements of the business. Do you know the impact of IT and IT risk on the business unit? Do you know if a particular communications link goes down how high an impact that can have on the business? A single cable might be a single point of failure."

Monitoring and mapping

To minimise the business risks, Yarnall advocates a combination of systems monitoring and dependency mapping by the IT department. The purpose of the dependency mapping is to help the IT department understand what to monitor. This should fall within an overall control framework designed to show an auditor that the IT department has systems under control.

Yarnall suggests that COBIT (Control Objectives for Information and Related Technology), a framework developed by the IT Governance Institute (ITGI) and based on a mixture of international standards documents, makes an ideal starting point. "Auditors have been using COBIT for many years. There are 17 areas of COBIT that relate directly to Sarbanes-Oxley," he says. Demonstrating compliance with COBIT ought to convince the auditor that the IT department has Sarbanes-Oxley compliance under control.

Yarnall's advocacy of COBIT is supported by the SEC's own rulings. It has published advice to clarify the intent of Sarbanes-Oxley, including rulings that limit the requirement for internal controls to financial reporting systems only.

It has also ruled that controls must follow a recognised framework. COBIT and ISO 17799, the international standard for information security management systems, are two such frameworks, although the SEC favours the US Commission of Sponsoring Organizations (COSO) set by the National Commission on Fraudulent Financial Reporting, since that encompasses other systems, as well as IT.

COBIT is an attempt in part to interpret COSO from an IT perspective, so many companies are using it as a guide for their IT Sarbanes-Oxley efforts.

Back to front

Given that financial reporting systems are the main focus of Sarbanes-Oxley, a cost-focused and practical approach to examining areas of Sarbanes-Oxley liability is to work from the final financial report backwards, to see which systems and processes affect it, says Peter Fawcett, director of Atos Consulting and the company's Sarbanes-Oxley expert.

"We tend to start with the balance sheet and profit and loss and work backwards through the various processes that feed into the balance sheet. Then we work backwards into applications that support the processes. Then we look at the infrastructure that supports the applications: anything that could a mis-statement on the balance sheet, be it a spreadsheet, an Internet process, or an Access database somewhere in the end-user system. It's not just the accounting systems," says Fawcett.

While many software vendors are now pitching their products – however, tenuously – as Sarbanes-Oxley 'solutions', Fawcett advocates looking at all of these systems purely in terms of this process. "If it turns out to be a storage problem or an email problem that can lead to a mis-statement of accounts, then those point solutions come in. It is premature to say, if I've got

Five key steps to compliance

Definition

An audit needs to be performed to determine where changes should be made for compliance with Sarbanes-Oxley. The focus should be on business applications, processes and procedures that directly and indirectly have an impact on financial reporting systems. CIOs should expect to participate extensively in this process, usually as a member of the compliance committee.

Assess

After the audit, the organisation will be able to determine its position relevant to Sarbanes-Oxley requirements. This 'gap analysis' should lead to a requirements document to identify those areas that need to be strengthened in order to ensure compliance. Financial reporting systems and business performance management systems are the typical project areas that will need some level of upgrade.

Implement

After determining the extent and level of internal controls required for compliance, initiatives must be drafted and implemented to upgrade systems and processes that are not in compliance with the law.

Measure, monitor, record

Once the desired state of compliance is implemented, all processes need to be regularly assessed for their quality and compliance with Sarbanes-Oxley.

Report/communicate

After the final audit has been signed off, it is time to communicate the status to appropriate management.

Source: NetSec

IN BRIEF: THE SARBANES-OXLEY ACT

Section 302

- The company directors have personally reviewed the report; the report does not contain any materially untrue statements or material omission to be considered misleading in any way; and that financial statements and related information must fairly represent the financial condition and results of the company in all material respects;
- The signing officers are responsible for internal controls and have evaluated these controls within the previous 90 days and have reported on their findings;
- A list of all deficiencies in the internal controls, as well as information on any fraud involving management or other employees who have a significant role in the company's internal controls; and any significant changes to internal controls or related factors that could have a negative impact on the internal controls.

Section 404

- Companies must publish information in their annual reports concerning the scope and adequacy of their internal control structure and procedures for financial reporting; this statement must also assess the effectiveness of internal controls and procedures;
- The auditor must, in the same report, confirm and report on the effectiveness of the internal control structure and procedures for financial reporting.

Section 409

- Companies must report significant changes in their financial conditions "on a rapid and current basis".

Section 802

- Public companies and their public accounting firms are required to retain records, including electronic records that impact the company's assets or performance. This can include email, instant messages, and spreadsheets that are used to analyse financial results.
- Penalties will include fines and/or imprisonment of up to 20 years for altering, destroying, mutilating, concealing, falsifying records, documents or tangible objects with the intent to obstruct, impede or influence a legal investigation. There are also penalties of fines and/or imprisonment of up to five years for any accountant who knowingly violates the requirements of maintenance of all audit or review papers.

a write-once, read-many storage system, I'm going to be okay."

So while instant message archiving and monitoring, email archiving, records management systems and other applications and systems might seem necessary at first, it is only if the systems they interact with could affect the financial reporting system or the balance sheet that they need to be fully controlled.

While some sections of Sarbanes-Oxley do impose penalties on companies that destroy records relating to problems with their balance sheets, these penalties only apply if the records were destroyed maliciously and deliberately. Companies with a blanket policy of deleting all emails after six months, for instance, would not be found liable under Sarbanes-Oxley unless it could be shown the company policy was motivated by a desire to destroy incriminating evidence. And although there is a provision stating that companies must reveal flaws in their internal processes, there is no penalty for actually having these flaws, other than public disclosure.

Nevertheless, working back through all the processes to uncover these flaws entails much work. But ITGI says that when the checking has been done, many will have little work to do afterwards: "Virtually all public companies have some semblance of IT control. They may be informal and lacking in documentation, but IT controls generally exist in areas such as security and availability. Many companies will be able to tailor existing IT control processes to comply with Sarbanes-Oxley. Frequently, it is the consistency and quality of control documentation and evidential matter that is lacking, but the general process is often in place, only requiring some modification."

The implication is that only companies whose IT systems are generally out of control should worry about the cost of compliance. "Sarbanes-Oxley is just a headline for many organisations, but not more than that," says Nigel Williams, vice president of software operations in Europe for EMC. Indeed, he adds, complying with Sarbanes-Oxley is likely to benefit many companies as a result of the savings they can make from stronger IT management.

Ultimately, compliance is about making sure the company's auditor feels that the CEO, CFO and CIO understand their company and their systems well enough that they can be sure that everything in their financial statements is true. Depending on the auditor and the existing state of the IT systems, that could take considerable investment – or very little. M

Article by Rob Buckley **edit@infoconomy.com**