

# Sarbanes-Oxley Act

## Basel II vs. Sarbanes-Oxley: which wins?

*Tim Leech* compares the corporate governance provisions of the Basel II bank accord and the US Sarbanes-Oxley Act and applies seven tests of effectiveness

**T**he new Basel capital accord on bank safety - Basel II - is a clear winner in the corporate governance cup stakes over the flawed US Sarbanes-Oxley regime, which is particularly defective in the area of control effectiveness reporting.

My view is based on comparing the forms of these two entrants for the corporate governance stakes, the one sired by banking supervisors seeking a stable global banking system and the other by the US Congress in response to the series of colossal corporate governance failures exemplified by the Enron scandal and similar disasters.

Basel II clears all but one of seven major hurdles, ranging from the role of directors to incentives to comply, where Sarbanes-Oxley stumbles from a lack of clarity. Only on timelines does Sarbanes-Oxley have the advantage. Sarbanes is already law, whereas Basel II's timetable remains under threat.

In 1998 the Basel Committee on Banking Supervision, the body of senior banking supervisors from the leading economies that in effect regulates international banking, put forward a framework to help banks and their supervisors strengthen internal control procedures. Deficiencies in internal controls were seen as a source of major problems and significant losses for banks globally.

The core elements of the 1998 framework are contained in the new Accord, the Basel II upgrade of international capital rules for bank safety that the Basel Committee wants to bring into effect for the world's major banks by the beginning of 2007. Basel II has a three-pillar regulatory structure of capital charges against credit, market and operational risk, supervisory review of bank risk management policies and greater information disclosure requirements.

The US Congress passed the Sarbanes-Oxley Act, which sets some of the stiffest corporate governance rules in the world, in July last year with the aim of protecting investors by improving the accuracy and reliability of corporate disclosures. Responsibility for implementing the act is assigned to the Securities Exchange Commission (SEC), the US investment markets regulator, and the new Public Company Accounting Oversight Board (PCAOB) that's charged with policing the accounting industry.

Both the Basel reforms and Sarbanes-Oxley are intended to prevent major corporate control failures. Basel focuses on ensuring the overall safety and soundness of banks. SOX focuses on restoring investor confidence in the integrity and fairness of financial disclosures to regulators and current and prospective investors.

Although both governance reform regimes are focused on achieving similar outcomes, the route chosen to accomplish the task varies widely. What are the similarities and differences? Which approach is most likely to achieve the stated aims? We compare the two regimes in seven areas: the role of the Board of Directors; the regulator's role; the role of management; internal and external audit; reporting requirements; incentives to comply and timeliness of solution.

### **Board of Directors**

The 1998 Basel internal control framework says directors should have responsibility for approving and periodically reviewing the overall business strategies and significant policies of the bank; understanding the major risks run by the bank; setting acceptable levels for these risks and ensuring that senior management takes the steps necessary to identify, measure, monitor and control the risks, approving organisational structure; and ensuring that senior management is monitoring the effectiveness of the internal control systems.

The message that regulators should carefully examine and score the oversight diligence of the board is repeated in numerous places in the draft Basel accord documentation.

Sarbanes-Oxley is largely silent on what is expected from the board of directors and audit committee, other than stating the audit committee should comprise independent directors who should review information they are provided with including whistle-blower reports. Although the 1987 Treadway Commission on fraudulent financial reporting in the US, and numerous other studies around the world since then, have all commented on the key role that should be played by boards and audit committees, Sarbanes did little to specify expectations in this area.

**My pick: the Basel reforms**

### **The Regulator**

The Basel reforms lay out a fairly detailed set of expectations that bank regulators will use to assess whether an organisation has met risk control requirements. The emphasis is on proving that an effective overall system exists to identify, measure, monitor and mitigate risks. The criteria are clearly described and linked to well-accepted and current best practices.

By contrast, Sarbanes only lays out fairly specific recommendations in some areas, such as whistle blowing, independence of directors and fraud involving accounting personnel. But on the central requirement of reporting on the effectiveness of control systems, it encourages companies to use the 1992 Committee of Sponsoring Organizations ("COSO") control criteria as reporting criteria. This now dated and somewhat obsolete control framework was never intended as a scoring grid for pass/fail analysis and is not well suited to objectively grade the quality of a company's external disclosure system.

Although COSO 1992 represented a milestone when it was released, in 1992, many major advances have been made in the area of risk and control management since that time. A new "ERM" (Enterprise Risk Management) version of COSO will be finalised in February, but it also, at least in exposure draft form, provides only limited help when attempting a pass/fail examination.

The SEC will find it very difficult to confirm or refute representations from chief executive officers and chief financial officers that a company has an effective control system in accordance with either the 1992 or the new COSO framework - despite investors paying billions of dollars for the information!

**My pick: the Basel reforms.**

### **Management**

The Basel reforms, crystallised in the operational risk provisions of Basel II,

focus on the elements of an effective risk management system and the role senior management must play to create and sustain it. Specific qualitative and quantitative requirements are described depending on the risk management qualification sought, namely the basic indicator approach, the standardised approach or advanced measurement approaches (AMA). Under AMA, the most sophisticated of the options, a bank will have to show that its op risk measurement system is closely integrated into the day-to-day risk management processes of the bank. Its output must be an integral part of the process of monitoring and controlling the bank's operational risk profile.

Sarbanes-Oxley by contrast focuses on forcing CEOs and CFOs to state that they have an "effective" system of control to ensure reliable financial disclosures. The representations must be made against the old 1992 COSO framework or, presumably, against the new 2003 COSO ERM framework. CEOs and CFOs will have to decide if they have passed or failed using vague and loosely defined criteria. The notion of reporting on the degree of conformity with control criteria selected is not an option.

**My pick: the Basel reforms**

### **Internal and External Audit**

Under Basel II the internal and/or external auditors must regularly review the op risk management processes and measurement systems. The review must include both business units and the op risk management function.

The new regime is expected to play a lead role helping to create and sustain a bank's op risk management system. To qualify for AMA, the validation of the op risk management system by external auditors and/or supervisory authorities is required to verify that internal validation processes are satisfactory and make sure that data flows and processes associated with the risk measurement system are transparent

and accessible. In particular, auditors and supervisors must have easy access to the system's specifications and parameters.

Again Sarbanes-Oxley is largely silent on the issue. It's not clear whether the PCAOB will accept the premise advanced by many companies that, when an effective and independent internal audit exists, external audit should focus on evaluating and reporting on the reliability of the system that produces the control effectiveness representations. The big four audit firms have lobbied hard for the right to evaluate independently and test all the processes that produce the external disclosures. The audit fees for examining all the systems that support external disclosures, versus examining the quality of the system that produced the CEO/CFO representation, will be much higher.

**My choice: again, the Basel II reforms.**

### **Reporting Requirements**

Under Basel II banks can select the level of risk management sophistication they wish to qualify for, unless regulators force them to qualify for AMA status. They will then have to make the appropriate filings with the regulators in the jurisdictions they operate in. Sarbanes-Oxley requires quarterly pass/fail reports on control effectiveness from CEOs and CFOs in SEC filings. Annual external audit opinions on those control effectiveness representations using the COSO control criteria will be required starting in 2004. Companies do not have to positively report on compliance with the other sections of Sarbanes-Oxley. Reporting requirements are defined in the Act, in SEC final rules, and soon, by the PCAOB.

**My pick: the Basel II reforms**

### **Incentives to Comply**

Basel II allows banks that can prove they have effective and sophisticated risk management systems to reduce their level of protective buffer capital, freeing up potentially hundreds of millions of dollars

for investment in profitable activities. The reforms also suggest that once a bank convinces regulators it has an effective and disciplined approach to enterprise risk management, it should attract less regulatory oversight.

Sarbanes-Oxley has created a range of incentives for companies to comply. These include personal fines and jail sentences for senior executives, denial of an opinion on control effectiveness representations by external auditors, obtaining restitution from offending organisations for victims, and additional ammunition to de-list offending public companies.

But there are no positive benefits under Sarbanes-Oxley for public companies to distinguish themselves by having particularly good risk and control governance systems.

**My choice: the Basel II reforms**

### **Timeliness of Solution**

Basel II has been under construction since the 1998. Implementation dates continue to be delayed and affected by political lobbying around the world by a range of groups with vested interests in delaying or altering the proposed reforms.

Sarbanes-Oxley was developed and passed into law in a political frenzy in a matter of months, supported by both Democrats and Republicans alike. Large portions of the legislation became effective immediately. In spite of its failings in some areas, it has had an immediate and profound positive impact on the behaviour of companies, their officers, their boards, their auditors, their lawyers, investment advisors and others in a very short space of time.

**My pick: on this it's Sarbanes-Oxley**

### **The winner is...Basel II**

There's still time to rectify the failings of Sarbanes-Oxley by moving to a regime that informs investors of the degree to which a public company manifests an "ideal" risk and control system to support reliable external disclosures. The Malcolm Baldrige quality assessment system in the U.S. developed to improve the competitiveness of U.S. companies provides all the basic structure components necessary to implement such a system. The new 2003 COSO ERM framework provides the core raw material to build appropriate and specific evaluation criteria using modern and well-accepted principles of good governance that are highly compatible with the core components of Basel II.

The implementers of Sarbanes-Oxley can learn from the careful and practical thought contained in Basel II. The Basel supervisors should learn from Sarbanes-Oxley and recognise solutions are needed now, not sometime in the distant future.

*Tim Leech is Managing Director and CEO of CARD®decisions Inc, an Ontario, Canada-based risk and assurance management software and consulting firm. Email: [Tim.Leech@carddecisions.com](mailto:Tim.Leech@carddecisions.com)*

*Additional articles and a White Paper on the deficiencies in the current Sarbanes-Oxley rules and interpretations can be downloaded from the Industry Info section of [www.carddecisions.com](http://www.carddecisions.com)*