*Feature Article:*

Corporate Accountability

# A Sarbanes-Oxley Primer

## What is it? Why it's here to stay? How do we make sense out of it?

*By Bill Smiley and Wes Helms*

### Introduction

There are many new business regulations coming down the pipe that information systems folks will need to get a quick handle on. New regulations such as Sarbanes-Oxley (SOX) and Bill C-198 have left information management professionals trying to understand exactly how these regulations will affect them. Let's look at the new compliance landscape to answer these questions.

### SOX and Bill 198: Where did they come from?

The failure of major US Savings and Loans establishments a decade ago, and the recent corporate malfeasance of Enron, Tyco and WorldCom devastated shareholder worth and overall confidence in the markets. This resulted in the U.S. Federal Government appointing a commission headed by Sen. Paul Sarbanes (MD) and Rep. Michael Oxley (OH), which concluded that these catastrophic business failures represented the epitome of poor corporate governance and greed. Their commission drafted legislation to hold corporate officers responsible for the financial health of their companies, and the resulting Sarbanes-Oxley Act (SOX) became law on July 30, 2002.

SOX mandates that CEO's and CFO's of companies listed on US stock exchanges must "certify" and sign off on interim and annual statements as well as their corporate governance framework. If the CEO's cannot comply by the stipulated date(s), the penalties can be swift and severe: the company's stock could be de-listed, heavy fines imposed, and top executives could be prosecuted. Good governance is no longer a "best practice": now it's the law. SOX's influence extends to subsidiaries of American companies operating outside the US (e.g. GE Canada) and foreign companies whose stock trades in the US (e.g. most of Canada's big banks). Bill C-198 is Canada's SOX equivalent. Any company complying with SOX will likely also comply with C-198.

### Involvement by Information Systems

Systems professionals will play a major role in achieving corporate compliance. IS will need to ensure that automated transaction processes, documentation, and records are authentic and not open to corruption or fraud. To help IS develop accountable information systems for this new compliance landscape we will lay out 5 principles to guide you through this project.

### Principle 1: A Corporation-wide Collaborative Approach

The internal champions for this compliance initiative will be CEO's and CFO's. It's their signatures that go on all documents forwarded to the regulators attesting to the fact that all the company's financial controls meet required guidelines.

The Compliance Teams that analyze the company's processes must operate cross departmentally. Getting all the financial processes documented quickly and accurately is a major undertaking, especially if there isn't enough slack in the organization to allow for enough qualified staff to execute the project. Most companies second key staff from their operating areas (content experts), augment their ranks with audit professionals from major accounting and audit firms, and contract a skilled Project Manager (process expert). Collectively, they form teams that conduct the actual process reviews.

### Principle 2: Avoiding Conflicts of Interest

It is vital to avoid conflicts of interests when assembling your team. In a large organization, such conflicts can cause corporate governance to fall flat on its face. Let's clarify this:

***U.S. President George W. Bush with Congressman Michael Oxley (R-Ohio) and Senator Paul Sarbanes (D-Maryland)***

#### *The Role of the Internal Audit Department*

Internal Auditors *cannot* participate in the review of existing processes because they will ultimately audit the team's findings; adjudicating their own work would be a conflict of interest. The team will review the internal processes and sub-processes, rate their applicable controls, and highlight areas requiring change in order to achieve compliance. The Internal Auditor cannot begin until the teams confirm that all the controls have been documented and comply with the guidelines. ▶

### *The Role of the External Auditor*

SOX and C-198 have the big audit houses very nervous, and rightly so. They will serve two roles in your compliance process: auditing your financial statements and (potentially) attesting to your governance framework. Obviously, they will require assurances to avoid liability, and will be unwilling to participate until you have confirmed that your part is completed and they can have full autonomy over the project.

However, your auditors will probably have a greater understanding of the compliance process, deadlines, and requirements than anyone in your organization, so it's in your best interest to incorporate their expertise into your thought management.

They will be mindful of the potential for conflict of interest issues (and will certainly be guarded in what they say and recommend) but it is essential to ask them to sit in on your board reviews, and participate in planning efforts. Be diligent and document all correspondence between the companies.

## Principle 3: Process Identification and Control Repository

Let's consider what the process of becoming compliant is all about. It's easy to understand that any process that deals directly or indirectly with the financial integrity of the company should be evaluated. Consider the idea of a process chain: each link of the chain represents the controls that secure the transaction. For example, one control when applying for a bank loan would be the applicant's sufficient unencumbered collateral to secure the loan. Another control might be a rule that says "no collateral, no loan."

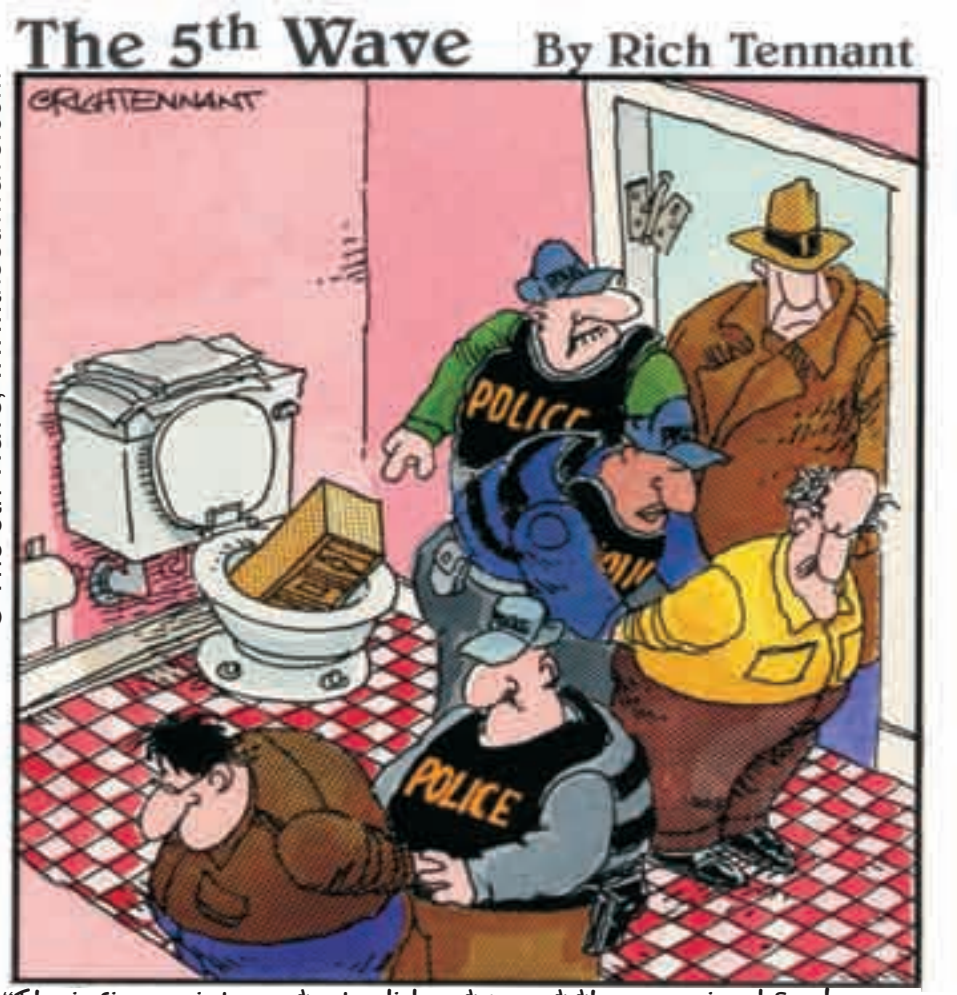
But what if there is collateral and the control can't detect or determine if it's unencumbered, or sufficient? And what if the loan is approved but the collateral is never assigned to the loan? You see the point; there have to be dozens of controls, dependant on each other.

Each control – dozens, hundreds or thousands – must be rated. A typical rating hierarchy might be:

- Unreliable – Undocumented, or simply doesn't work, either consistently or occasionally.
- Informal – The control exists but likely isn't documented or well understood.
- Standardized – The control meets standards and is adequately documented.
- Monitored – The control is standardized, documented and will flag activities outside certain boundaries and issue warnings without proceeding.
- Optimized – the control will automatically take the necessary corrective action to events that fall outside its threshold.

### *The Data Repository*

This is the other area for IS involvement. The Data Repository stores every attribute about every process, sub-process, and control that the team reviews. There are numerous repositories on the market that are suitable for analyzing and warehousing the data collected during the compliance project (almost every big audit firm has one), but be careful when defining what you want it to do. Every shred of information gleaned by the compliance team will end up here. This is also the place the Internal and External Auditors will visit as they conduct their reviews. IS will be mandated to keep the Repository's code current and secure its contents through suitable access controls, backups, off-site data storage, etc.






"Their financial controls did not meet the required Sarbanes-Oxley guidelines. We broke through the door just as their IT guys were trying to flush this harddrive down the toilet."

### *Negotiating with Outsourcers*

If you outsource any of your financial processes, their controls can become a major concern. For example; if you outsource your payroll, which controls do you keep and which do you vest to your outsourcer? Can you adequately rate the controls you've retained? Can your outsourcer attest that the controls you have empowered it to conduct will satisfy the new requirements? It's easy to achieve your own compliance dates, but it might be considerably harder to get your outsourcer to do the same. Consider and plan this area carefully.

### Principle 4: Document and Records Management

Even with our controls identified, rated, and placed in a repository, we are still generating countless reports, relying upon control documentation, and searching for multiple files across our companies. SOX Section 302 mandates that real time disclosure on changes to the firm's financial condition be made on a "rapid and current basis." Therefore, we will have to immediately access the unstructured data, reports and contracts that explain why our numbers appear the way they do beyond the usual financial statements.

The biggest challenge with unstructured content is that it is often disorganized and inaccessible. Information Systems Professionals must begin to organize this content at the organizational level by developing an *enterprise content management* and *records management* strategy. Companies should strive for faster access to information to meet reporting requirements, which can involve developing sophisticated internal file naming conventions, a record indexing model, or investing in an Enterprise Content Management solution. Many companies are deploying content management applications which provide auditors access to cross departmental control documentation from their desktops.

## The 10 Deadly Sins of 'Sarbox"

* In a Sarbanes-Oxley world, beware of these errors in financial record keeping:

1. Records-management policy isn't linked to regulatory requirements.
2. Retention schedule is no longer reflective of the law departments.
3. Formal policies are nonexistent or inconsistent across departments.
4. Records management covers paper records only.
5. No one is responsible for administering the program.
6. Retention periods aren't integrated with document management to purge documents.
7. Employees are unaware of policy.
8. There are no tools to authorize deleting documents.
9. There's no audit process to track what's happened.
10. There's no indexing, so it's impossible to retrieve documents when required.

## Principle 5: Testing and Training

Now that the compliance process is understood, it will be important to develop a testing and training methodology for the compliance team to follow. Every documented control, in every department, will need to be tested (the alternative is catastrophic – imagine the reporting impact on a financial statement if one field is not linking to the database).

When your new compliance systems are implemented and tested, training will be vital to ensuring end-user adoption. This opportunity provides an excellent opportunity to train not only on the applicable technology (software management tools, governance methods), but on the company's new governance processes.

## Conclusion: Y2K Déjà-Vu?

In the late 1990's as Y2K approached, analysts and coders who knew the old languages and legacy applications charged unbelievable rates and companies scrambled for their share of the available skills. The inevitable changes required for SOX and C-198 are similar, but with a twist.

Now that the laws of supply and demand are kicking in, Internal Auditors and CA's will become increasingly scarce. Companies will vie for professionals with these skills to get the work done before the compliance deadlines, and at the moment there aren't enough contract skills to meet the needs. The banks understood this very well when they positioned themselves to lead the pack; now they are contracting these skills in huge numbers. Smaller companies who haven't grasped this same fact will be in a precarious place if they cannot meet the regulatory deadlines.

### *The Timing*

The most important aspect of SOX with respect to financial statements is what is referred to as Section 404 and it deals with what we've been talking about: Management's willingness to attest to the completeness and accuracy of internal controls. Compliance with Section 404 of the Act is currently being re-negotiated (for Bill C-198, the date remains March 31st, 2004).

### *The Goal*

The goal, then, must be that for compliance at the conclusion of the project, the company documents and assesses the effectiveness of its internal controls consistent with SOX 404; which enables management to provide a clean assertion to its external auditors to obtain an unqualified Section 404 attestation.

### *The Benefits*

So, what are the benefits from this exercise, beyond legal compliance? Companies are learning that SOX and C-198 efforts will reveal errors, inconsistencies, and redundancies in their existing financial processes. A side benefit to the compliance project is that they will improve internal efficiencies relating to the processes and documentation at the same time.

Some companies have seen such significant benefits from their financial process reviews that they have initiated additional projects to look at their remaining processes with the same goal of reducing duplications and outdated operations. If sanctioned from the top down, the benefits appear to be well in excess of the cost of the project, and represent recurring savings. While initial costs and inconvenience may be frustrating, the benefits will likely outweigh the costs. TUG

## Useful Web Links

Bill C-198:
http://www.fasken.com/web/fmdwebsite.nsf/0/A69604E494A1AD7685256DDD0058D3E3/$File/BILL198.PDF?OpenElement

Sarbanes-Oxley Act:
http://news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf
http://www.sarbanes-oxley.com/

***Bill Smiley*** *is Managing Director of illumina Management Solutions. He can be reached at bill@illumina.ca.*
***Wesley Helms*** *is Director of Accountability Solutions with GSI International Consulting Group. He can be reached at whelms@gsigroup.com.*