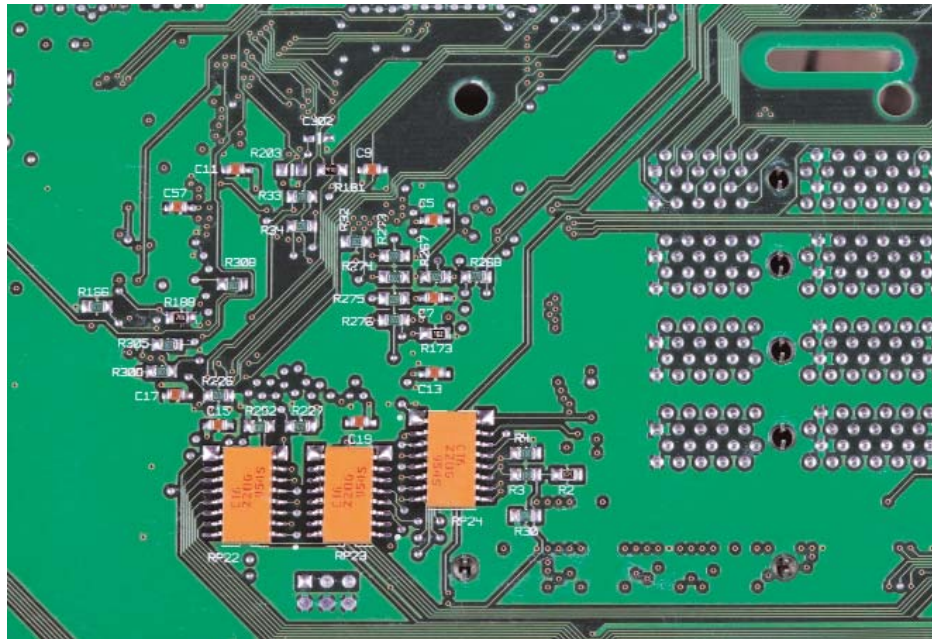


# Financial Services Firms

## Take the Sarbanes-Oxley Test



by Andrew Daly

In a world fraught with business risks, technology is often the Achilles heel of financial services organizations. Since Congress passed Sarbanes-Oxley (SOX) in 2002, the financial services industry has had much at stake. Information technology chiefs in financial services may long for the days when they were “merely” tasked with implementing a new infrastructure or migrating to a new operating system. Those jobs were the norm when it came to lost productivity or even temporary reputation damage.

Then came SOX, and IT risk hit a new threshold. Yet recent reports and discussion among IT thought leaders is encouraging. With an investment of

time and talent, it is possible to implement SOX in a way that is more efficient, less costly and yes—in compliance. In fact, now some are saying proper testing and quality assurance of the underlying IT could pay dividends beyond the compliance process.

### Tension and confusion on the road to compliance

Compliance with SOX, also known as the Public Company Accounting Reform and Investor Protection Act of 2002, has created hot tensions among financial services firms that have earned, and must sustain, public trust. While SOX is widely known as legislation aimed at improving corporate

## SOX compliance is a ball of confusion for accounting and IT departments, and it's going to get worse.

accounting and governance reporting standards, technology is playing a central role because software is the key to compliance. If there was any doubt, Congress dictated it:

*“The nature and characteristics of a company's use of information technology in its information system affect the company's internal control over financial reporting.”*

(Public Company Accounting Oversight Board Auditing Standard 2)

In other words, Congress insisted on a process (section 404) where all controls are reported after rigorous testing. Yet IT controls especially are gaining increased attention for the cost and hours dedicated to getting them right.

SOX compliance is a ball of confusion for accounting and IT departments, and it's going to get worse. Exposure has been found, and repairs are underway. This has created new Enterprise Resource Planning (ERP) financial modules for compliance and has also created openings for data architects.

Kevin Hudson, vice president of product development in IT for Kforce Professional Staffing said “IT auditors are in big demand” in an interview

with *TechTarget*, a Web resource for IT managers. Hudson believes more IT hiring is required to bring companies up to compliance. He also foresees increased hiring in IT security, as well as the rewriting of applications.

Because so much of SOX compliance depends on properly governed IT, CIOs—who must report to CFOs and CEOs—are on the hot seat. The SOX legislation is broad in its scope and threatening in its penalties. But it is vague in the guidance it provides on exactly how companies should comply. No wonder it's causing heartburn and nightmares for C-level executives all over the country. Some of those CIO nightmares are fueled by the requirement for tight internal controls over financial reporting in addition to disclosure and annual evaluation of the effectiveness of those controls.

### Best practices to mitigate your risk of non-compliance

When it comes to IT controls, there are proven steps financial services firms can take to mitigate the risk of non-compliance. In a recent report by the accounting and consulting firm of Deloitte Touche Tohmatsu, “Under Control,” Deloitte out-

lines a “Sustained Compliance Solution Framework.” Key areas of the Deloitte framework directly relate to IT controls:

- Effective and efficient processes for evaluating testing, remediating, monitoring, and reporting on controls.
- Integrated financial and internal control processes.
- Technology to enable compliance.
- Clearly articulated roles and responsibilities and assigned accountability.
- Education and training to reinforce the “control environment.”
- Adaptability and flexibility to respond to organizational and regulatory change.

The problem is that testing and quality assurance are all too often considered an operational function and are not given the strategic recognition they deserve. As part of any organization's risk management strategy and procedures, testing and quality assurance should be featured as a priority when, in fact, they are often only paid lip service.

IT testing is becoming a highly sophisticated process with accepted best practices that are certified by such organizations as ISO 9001. Testing experts start by identifying the business

### Include Testing and Quality Assurance During Six Key Steps of Technology Implementation

Testing and quality assurance are key to ensuring that damage limitation is as ironclad as possible in any technology implementation. If, as recommended, testing and quality assurance are involved from the outset, the standard steps where testing and quality assurance come to the fore are:

1. Idea: Is the idea viable and commercially sound?
2. Requirements definition: Are the requirements unambiguous and complete?
3. Specification and design: Will the design fulfill the requirements?
4. Development: Has the right outsourced system been built and has it been built correctly?
5. Implementation: Does the outsourced system/process match what was intended at the start of the implementation stage?
6. Value realization: Are the benefits measured the same as what was expected?

processes that are at the greatest risk of failure and those that present a high risk to the business if they did fail. With this information, the business can decide on the optimum quality and testing assurance strategy given the budget, time available, and quality objectives. Risk-based testing and quality assurance mean resources are focused purely on mitigating risk, which saves time and headaches in the long run.

This is exactly the case with IT's role in SOX compliance. As Ed Jones, managing director and CIO Americas at Deutsche Bank, told *Financial Services Technology* magazine, "IT can play a significant role in supporting the firm's compliance with new regulatory requirements. IT can develop solutions that minimize the bank's risk exposure. The solutions must be scalable, global, and robust; capable of looking at our position cross-business; and also adaptable to an ever changing regulatory environment."

Technology failures from testing inadequacies have been par-

ticularly prevalent in financial institutions' outsourcing arrangements. Sensing this, federal regulators expect the institutions to conduct due diligence on their technology service providers. To achieve verification and validation, it is essential to improve management of people and processes coupled with clarity and visibility of communications and information.

Outsourcing increases the challenges and the risks. While there are fewer people to manage, they are outside of the organization's direct control. Mature and robust processes, communications, and information flows are essential to ensure that the outsourcer delivers what is promised and to ensure SOX compliance.

#### Deadlines squeeze IT departments

Another reason why testing and quality assurance can often take a back seat in technology projects is that suppliers and internal IT departments are often under pressure to meet deadlines, fall within budget, and meet strin-

gent service provider guidelines. The pressure to push systems out on time can mean testing is compressed into a reduced time period. Often external systems integration suppliers are paid bonuses on meeting deadlines. These characteristics increase risk.

Since the success of any major technology implementation is dependent on testing and quality assurance procedures, testing deserves a place at the top of financial services organizations' agendas. Testing failures can result in reputation damage, lost customers, organizational disruption—not to mention huge cost. As each company is urged to get its house in order before embarking on any major technology implementation, a focus on testing and quality assurance is essential to keep up with SOX.

#### Does SOX compliance add value?

For all of the energy they are exerting, financial services executives want to know if they can claim SOX is actually good management strategy. They are looking for indications that SOX compliance can both decrease risk and add value. And lately those indications are emerging.

A report last year from a meeting on SOX by PriceWaterhouseCoopers Banking & Capital Markets industry specialists noted: *We have observed a move towards automating previously manual controls as a way of gaining efficiencies and improving risk management. In addition, some companies are more effectively employing benchmarking or base lining strategies. As companies continue to refine their testing approaches and timing, testing*

*information technology controls earlier in the year and leveraging the results of that testing can lead to significant efficiencies.*

Echoing this theme *BusinessWeek* proclaimed in its January 29, 2007, issue that “Not Everyone Hates SarBox” explaining that with SOX in place, “executives appear to have a firmer grasp of costs when they talk about operating margins.”

While SOX is still one of the most feared acronyms in the financial services industry (some even call it unconstitutional), executives are learning to live by it. Financial services companies, which touch and impact billions of people worldwide, know that IT is at the core of compliance

### Best practices to mitigate your risk of non-compliance

Deloitte Touche Tohmatsu, an accounting and consulting firm, recommends a sustained compliance solution framework. Key areas of that framework directly relate to IT controls and include:

- Effective and efficient processes for evaluating testing, remediating, monitoring, and reporting on controls.
- Integrated financial and internal control processes.
- Technology to enable compliance.
- Clearly articulated roles and responsibilities and assigned accountability.
- Education and training to reinforce the “control environment.”
- Adaptability and flexibility to respond to organizational and regulatory change.

and that proper testing of IT systems is critical to avoiding fines, shareholder revolt, and permanent reputation damage.

Gaining control of IT controls is easier said than done, but those who have made progress are reaping rewards in management confi-

dence. Plus, there’s now evidence of cost efficiencies that will pay off for firms even after the Sarbanes-Oxley Act of 2002 is just an entry in history books. □

*The author invites readers to visit [www.applabs.com](http://www.applabs.com).*