

How Sarbanes-Oxley Affects Your Disaster Recovery Planning



By [Leo Wrobel](#)

Date: Dec 29, 2006

[Return to the article](#)

Unless you're trying to land your CEO in jail, your disaster recovery plan had better be good. Leo Wrobel explains how the passage of the Sarbanes-Oxley Act of 2002 ultimately means that you really need a plan that protects your data.

Every so often it becomes necessary to write an article a little off the beaten path to describe what people should or shouldn't be doing in areas somewhat tangential to disaster recovery planning. One example is the legal and regulatory reasons for planning; for example, the Sarbanes-Oxley Act of 2002, otherwise known as SOX 2002.

Many people use SOX 2002 as justification for why they need a recovery plan. Indeed anything that could land you CEO in jail deserves more than a cursory look. But does SOX 2002 actually *mandate* having a recovery plan? The answer might surprise you. In order to understand the issues completely, however, you need at least a rudimentary idea of why the law was passed in the first place. So let's start the

NOTE

Portions of this article were adapted from Leo Wrobel's new book *Business Resumption Planning, Second Edition* (2007, Taylor Publishing). Leo Wrobel especially thanks his longtime friend [David "Dave" P. Mowery](#), CPA, for his insightful contributions to this article

SOX 2002 Basics

By now, you've probably heard the story of Enron. A whistleblower at Enron called the U.S. Securities and Exchange Commission (SEC) to report questionable accounting practices at Enron. She was first brought before an attorney to tell her story, and nothing happened for a year. After that time, she called back to see if they were going to investigate her complaint, but this time asked the question, "Don't you have any CPAs there I can talk to?" This time, in response, she was referred to an accountant instead of an attorney. The accountant not only understood the issues but also was amazed by her report, and launched an investigation. The rest, as they say, is history.

Enron was not the only one, by any stretch of the imagination:

- WorldCom wove a sordid tale of excessive loans to corporate officers to buy lavish homes and golf courses. Millions of dollars in expenses were hidden through capitalization and write-offs over a period of seven years.
- Dollar General's CFO failed to post an accrual of several million dollars in freight costs from overseas. He later convinced the auditors that, rather than restate 1999 figures, they should just write off the expenses over the next twelve months. For his actions, the CFO finally agreed to pay a fine of more than \$1.2 million.
- Ben & Jerry's CFO was sent to the slammer for 27 months for embezzling nearly \$30,000 from his employer.

The list grows daily. It would probably take a two-day seminar just to cover the companies that have been caught in the United States, and Europe is not exempt to the same things happen there.

Something had to be done.

Congress complained to the SEC about lack of oversight. The SEC had left oversight to the American Institute of Certified Public Accountants (AICPA) and the [Institute of Management Accountants](#) (IMA). These accounting associations in turn failed the American public. (In fairness to them, however, these organizations were never intended as de facto oversight bodies to take the place of federal regulators.)

The SEC was ordered to take charge and prepare a fix for this problem or an office would be founded that could

and would fix the problem. (This is somewhat of an oversimplification of what happened, of course, but you get the idea.) At this point, the SEC began work on its investigation and draft of a new law. This new law would tell management, internal auditors, and external auditors what they *must* do.

To ensure compliance, stiff penalties (both real and personal) were added. Penalties included jail time and personal fines. This is where SOX 2002 hit the corporate radar, and when it probably fell on your plate as an item related to disaster recovery. Indeed, if the boss were sent to jail, that *would* qualify as a disaster. But does the law mandate a plan? Read on.

The draft of the new law included the formation of a new board, the Public Company Accounting Oversight Board (PCAOB). The Sarbanes-Oxley Act, which is the core of the PCAOB's charter, was enacted in July of 2002. It begins with the following words

To protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities law.

The PCAOB (sometimes referred to as the *peek-a-boo*) reports directly to the SEC, which in turn enforces the decisions of the PCAOB and levies the fines. The PCAOB regulates audits and ethical standards of publicly traded companies. The organization is charged with promulgating auditing and ethics standards for such companies.

To audit a public company, any CPA firm must register with the PCAOB; the firm is so subject to audit and inspection by the PCAOB. If the CPA firm audits 100 or more publicly traded companies, it must be audited every year; if the firm audits less than 100 companies, the audits are every three years. Unsatisfactory audit results may be reported on the PCAOB web site.

With the advent of SOX, management's responsibility is reinforced for internal control, operations, and financial statements. A new emphasis is placed on organizational responsibilities and corporate governance. Management must now provide *personal assurance* with regard to internal control issues. It's no longer acceptable to dismiss operations with the phrase "to the best of my knowledge." CEOs and CFOs must now assert that their organization's operations and internal control are tight enough that they are *personally* sure that fraud, whether in misappropriation and misrepresentation is prevented. Management is also required to report all areas of weakness to the auditors through the audit committee.

Unlike in the past, the auditors cannot assist in the development or documentation of these procedures. After review, auditors also are not permitted to make recommendations to management on how to make improve these procedures. Management must respond to an auditor's negative comments on internal control procedures. Management's assurance is mandated to be submitted with the annual audit SEC filing as well as all quarterly filings to the SEC. All failures of internal control must be reported with all filings.

To ensure compliance with these guidelines, SOX 2002 established significant penalties in section 1350, "Failure of corporate officers to certify financial reports." Whoever does not comply with the certification of financial reports as outlined in paragraphs a and b of this section "shall be fined not more than \$1,000,000.00, or imprisoned not more than 10 years, or both." Furthermore, whoever willfully certifies the correctness of the internal control and certifies that the reports present fairly the financial condition and the results of operation (while knowing that they do not comply with all the requirements) "shall be fined not more than \$5,000,000.00, or imprisoned not more than 20 years, or both." The law further requires that each audit contain an "internal control report" that does the following:

- States the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting
- Contains an assessment, as of the end of the company's fiscal year, of the effectiveness of the internal control structure and procedures of the company for financial reporting

There are two key elements in reporting

- The company must assess and report on the company's internal control over financial reporting. This report cannot contain the former "get out of responsibility phrase" that included the word "to the best of my knowledge." The statement must not only assess and report its internal control, but must be positive. If you find something wrong or inadequate, you must fix it before issuing the report.
- Outside auditors must now audit and report as to the accuracy of management's report. The two audits of financial statement presentation and internal control must be done at the same time and as part of the same audit, because they are so closely related.

Furthermore, publicly traded companies must have an audit committee on the board of directors. Section 301 of SOX establishes general standards of this committee

[The audit committee] shall be directly responsible for the appointment, compensation, and oversight of the work of any registered public accounting firm employed by that issuer (including resolution of disagreements between management and the auditor regarding financial reporting) for the purpose of preparing or issuing an audit report or related, and each such registered public accounting firm shall report directly to the audit committee

In addition, internal auditors no longer report to management but to the audit committee. They may perform audits and assist management in compliance with sections 302 and 404 of the SOX Act to the extent that these activities do not interfere with the requirement of the standards for the internal auditor's independence and objectivity. Management, however, has the ultimate responsibility to ensure that proper internal control procedures and philosophy are in place to assure the CEO and CFO that the financial statements are presented in accordance with generally accepted accounting principles, and that the statements are free of any material misstatements, omissions, or misrepresentations. Management is further required to communicate to the audit committee and to the auditor all significant deficiencies and material weaknesses it discovers

How SOX Affects Your Disaster Recovery Plan

If you're looking for a sentence in SOX 2002 that mandates a disaster recovery plan, you won't find it. As far as I am aware, the Sarbanes-Oxley Act of 2002 does not mandate that a company have such a plan. Yes, you read that correctly. Then why, you might ask, are the terms *Sarbanes-Oxley* and *disaster recovery plan* used almost in the same sentence in many organizations? To answer this question, consider all the new exposures that management faces these days with the advent of the new law, including potential jail time. Now ask yourself how you would feel if you had to provide such reporting only to be told by technical staff the equivalent of, "My dog ate the data."

If you ever want to contemplate a career-ending move, try telling your boss that the data he or she needs to meet these stringent new requirements is gone due to some disaster. That's why disaster recovery planning is so closely entwined with SOX 2002.

Ultimately, your boss (or your boss's boss) is personally responsible if something goes wrong that prevents compliance with the new law. That's why recovery planning has taken on such new urgency. And, in case you hadn't noticed, these things roll downhill. That's why this issue is probably on your desk at this moment. You have the job of covering your boss's posterior, and a workable disaster recovery plan is part of that responsibility.

Summary

The Sarbanes-Oxley Act of 2002 has brought to light areas of concern regarding internal control and the impact of a potential disaster on those new requirements for many companies. Internal control has always been an area of great concern and potential loss for any recovery plan. The fact that a CEO can now be held personally and criminally responsible only makes it more of an issue of concern.

This all may look like something that's beyond your control. You can't control the ethics or behavior of your employer. But there are concrete steps you can take today to protect the internal processes and controls for your company that are supported by the information systems you provide.

I hope that this article has answered a few of your questions about SOX 2002 and that it's such a big deal. In the process, you should have gained some ammunition to foster more effective communication with management and maybe even additional justification for getting your planning effort funded. Thank for this opportunity to write for you again, and good luck in your pursuits.
