

Thinking Outside the SOX

A review of the BCP Implications of the Sarbanes-Oxley Act

The Sarbanes-Oxley Act (SOX) of 2002 was passed in the wake of numerous, high-profile corporate accounting scandals. Its intention is to protect investors by improving the accuracy and reliability of corporate disclosures. The majority of the act discusses how publicly held companies must ensure accurate reporting to stockholders.

The main thrust of the act was to establish the, "... Public Company Accounting Oversight Board, to oversee the audit of public companies that are subject to the securities laws, and related matters, in order to protect the interests of investors and further the public interest in the preparation of informative, accurate, and independent audit reports for companies the securities of which are sold to, and held by and for, public investors."

In general, the Board's purpose is to register public accounting firms that prepare audits, and establish standards for auditing firms in addition to conducting investigations of alleged improprieties.

According to Section 103 of the act, auditing firms must "describe in each audit report the scope of the auditor's testing of the internal control structure and procedures of the (company)..."

In addition, auditors must present the findings of its test and provide an evaluation of the company's internal controls including any "material weaknesses in such internal controls, and of any material noncompliance found on the basis of such testing."

Additionally, Section 404, titled *Management Assessment of Internal Controls*, discusses procedures that must be in place to help ensure accurate reporting. While the section does not specifically mention business continuity planning (BCP), it states that management will be held responsible for ensuring adequate internal controls are in place. The internal control report, which must be included with all annual reports, should "contain an assessment, as of the end of the most recent fiscal year of the (company), of the effectiveness of the internal control structure and procedures of the (company) for financial reporting." Auditors are required to "attest to, and report on, the assessment made by the management of the (company)," with regards to internal controls.

While the act does not specifically mandate that companies have a business continuity planning program, it definitely has implications on continuity planning. In fact, auditors, wary of receiving any more bad publicity, have already begun to ask that companies show they have a continuity plan in order to be compliant with sections 103 and 404.

Below is a brief discussion on who, what, when, and why of compliance with Sarbanes-Oxley as it relates to BCP.

Who

The Sarbanes-Oxley Act pertains to all publicly held companies in the United States. In addition, non-US companies who are listed in the US must also comply. More specifically, it has direct implications for CEOs, CFOs, and auditors.

Senior executives at publicly held companies must take all reasonable measures to ensure that their financial data is available in a timely man-

Internal Controls

The Securities and Exchange Commission (SEC) has released a preliminary definition of "internal controls." The definition states, in part, that internal controls are a process controlled by the CEO and CFO designed to provide reasonable assurance regarding the reliability of financial reporting. The definition further states that a company's policies and procedures should, "Provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the registrant's assets that could have a material effect on the financial statements."

The protection of assets clause is what concerns business continuity planners the most. Under that clause, internal controls could cover the following:

- **Risk Assessment/Impact Analysis** – A corporation will first need to understand the risks they face and the potential financial impacts to the business before devising strategies to protect the assets.
- **Incident Response** – In order to mitigate damage from a disaster or business disruption, a company should have a proper incident response program in place. It should include an emergency response organizational structure, teams, and tasks to be completed.
- **Business Continuity Planning** – A comprehensive business continuity plan ensures investors that the management team has made an effort to protect the company's assets in the event of a disaster or business disruption.
- **Plan Testing** – A business continuity plan cannot be considered viable unless it is tested. In addition, testing allows company's to adjust recovery strategies and recovery time objectives to real-world situations.
- **Data Back Up and Recovery** – In order to ensure timely delivery of accurate financial information, a company must have a reliable data backup and recovery system in place.



Thinking Outside the SOX

A review of the BCP Implications of the Sarbanes-Oxley Act

(continued)

ner. This can be interpreted to mean that they must have a business continuity plan in place should a disaster occur.

The act stipulates that auditors “who willfully violated, or willfully aided and abetted the violation of, any provision of the securities laws...” may be barred from practice and face monetary penalties up to \$15 million. Auditors at large accounting firms, not wanting to besmirch their reputation will be scrutinizing corporate records more thoroughly. The act also places many other restrictions on services which accounting firms can offer to their auditing clients.

What

Sarbanes-Oxley makes companies responsible for understanding and mitigating foreseeable risks involved in the financial reporting process. Among the many risks involved in the financial reporting process are operational risks and IT-related risks. For example, if a building were destroyed in a fire, the company would need to have a back-up plan to recover all of the financial data that may have been lost.

Since BCP covers operational risk and IT-related risks, it is reasonable to assume that auditors will scrutinize a company’s continuity planning effort. A business continuity plan is a collection of procedures and information that is developed, compiled, and maintained in readiness for use to help an organization respond, recover, and resume in the event of a disaster. Aside from being a prudent business process, BCP should now be considered a required function at companies covered by Sarbanes-Oxley.

Additionally, the Sarbanes-Oxley Act also requires auditors to keep all documents regarding clients for at least seven years. Ensuring continuity for the systems and processes, which account for these communications between auditors and clients, becomes paramount for accounting firms and must be taken into account in their business continuity plan as well.

When

US companies with a market capitalization of \$75 million or more must be compliant with Sarbanes-Oxley on or after June 15, 2004. Non-US companies and smaller businesses must be compliant by April 15, 2005.

Why

By now, most companies should be aware of the reasons to have a comprehensive, well-tested business continuity plan. Sarbanes-Oxley compliance only serves to strengthen the need.

In an informal interview, an auditor with a large accounting firm has confirmed that they are now reviewing corporate continuity plans as a direct result of Section 404 of the Sarbanes-Oxley Act. The auditor said that if the company does not have a BCP,

has an inadequate BCP, or an untested plan, the auditors are asking that the CEO and CFO sign a statement acknowledging that they are accepting the risk.

What would happen to the CEO and CFO who signs off on that risk and then faces a disaster – even something as small as a software error in their accounting system? What would happen to the auditor who overlooked a company’s inadequate BCP?

Certainly, fully meeting the compliance requirements of Sarbanes-Oxley means having a lot more than a business continuity plan. Companies need to rethink how they report and record financial data, but can not overlook the importance of having a well-tested, comprehensive business continuity plan. Auditors are already reviewing continuity plans in accord with the act and companies who want to pass those audits need to start thinking outside the “SOX.”

How Strohl Systems Helps

Strohl’s **LDRPS**® enables organizations of all sizes to build comprehensive business continuity plans that will meet or exceed auditor expectations. Aside from the regulatory reasons, LDRPS helps companies build plans that can help recover in the event of a disaster. In addition, using LDRPS enables corporations to catalog their critical financial reporting systems, making it easier to start the Sarbanes-Oxley compliance effort.

Strohl’s **BIA Professional**® provides the foundation of a sound BCP by highlighting organizational vulnerabilities and costs associated with potential disasters. Companies that conduct a business impact analysis with BIA Professional can be sure of uncovering risks associated with the financial reporting process and can use LDRPS to mitigate or respond to those risks as needed.

Incident Manager® enables organizations to test and adjust continuity plans and manage incidents. It also enables organizations to track incidents for insurance and auditing purposes, showing a commitment to risk management and business continuity planning.

NōtiFind®, Strohl’s emergency notification system, provides the communication tool necessary to inform or mobilize employees, vendors, and customers to help minimize losses in the event of a disaster.

Finally, **Strohl Consulting Services** consists of handpicked, certified senior consultants who work directly with customers to discover weaknesses and provide guidance through the entire planning process.

