DISASTER RECOVERY JOURNAL

The Journal Dedicated to Business Continuity

Spring 2004 • Volume 17, Number 2
$4.00

www.drj.com

Business Continuity in a Sarbanes-Oxley World

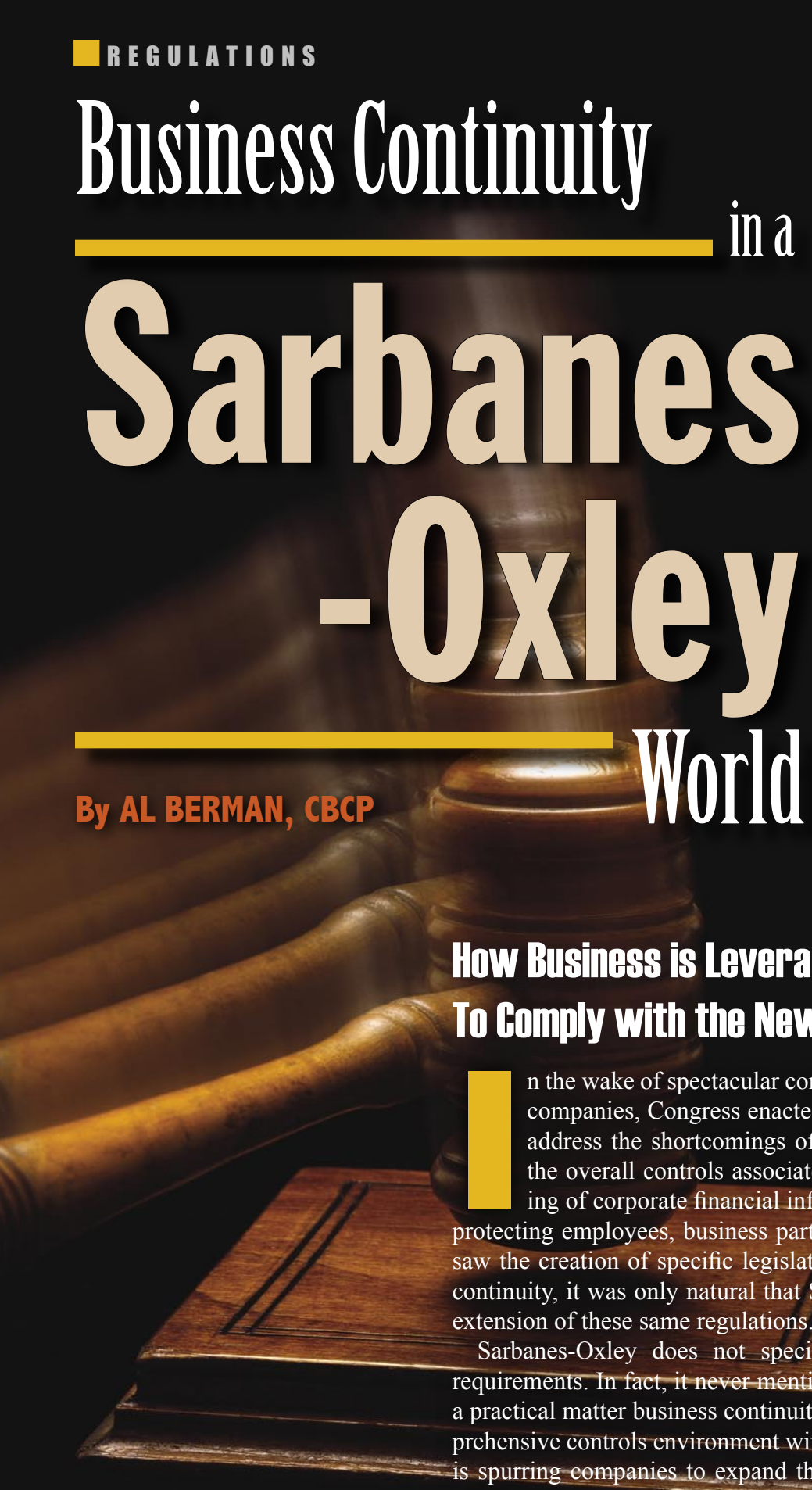
ALSO . . .

- 20 Rules for Effective Communication in a Crisis
- Systems Continuity on a Shoestring
- Never a Good Time to be Without E-mail
- 2004 Other Services Survey

Photo by Williams James Warren/CORBIS

Business Continuity in a Sarbanes-Oxley World

By AL BERMAN, CBCP



How Business is Leveraging Business Continuity To Comply with the New Regulation

In the wake of spectacular corporate governance failures at several companies, Congress enacted the Sarbanes-Oxley Act of 2002 to address the shortcomings of corporate governance and improve the overall controls associated with the management and reporting of corporate financial information. The legislation is aimed at protecting employees, business partners, and corporate. In a period that saw the creation of specific legislation and regulations around business continuity, it was only natural that Sarbanes-Oxley would be seen as an extension of these same regulations.

Sarbanes-Oxley does not specifically address business continuity requirements. In fact, it never mentions business continuity at all. But as a practical matter business continuity is seen as a means to create a comprehensive controls environment within an organization. Sarbanes-Oxley is spurring companies to expand the scope of their business continuity initiatives to be more comprehensive in nature, even to the point of a company looking outside its own organization to suppliers and vendors.

Genesis of the Sarbanes-Oxley Act

Corporate governance has moved on and off organizations' radar screens since it first emerged as an issue in the late 1960s. That was a time when huge conglomerates – holding companies with unrelated assets – were being criticized for failing to run their corporations efficiently.

In the 1980s, when the savings & loan crisis and third-world debt sparked concerns over markets and credit risk, corporate governance took a back seat. In the mid-1990s, operational risk issues and the subsequent trend toward corporate "re-engineering" were all the rage. In the late 1990s and 2000, concerns centered on new economy demands: new technologies, becoming a "dot-com," and hiring the most tech-savvy employees.

In mid-2002, legislation addressing corporate governance reform languished in Congress. Arthur Andersen's June 15 obstruction of justice conviction seemed to mollify public outrage over a series of corporate governance debacles. However, later that month accounting irregularities were uncovered at other larger companies. Overnight, Congress was inundated with demands for tough new anti-fraud legislation aimed directly at corporate malfeasance.

The result was Sarbanes-Oxley, signed into law on July 30, 2002. Sarbanes-Oxley is one of the most comprehensive corporate anti-crime laws in American history, addressing a broad range of wrongdoing, from altering financial statements to misleading auditors, to intimidating whistle-blowers. The passage of Sarbanes-Oxley marked a watershed event in the evolution of corporate governance. But more importantly, it placed the responsibility for creating a set of comprehensive controls squarely on the shoulders of the CEO.

Corporate governance, through the prism of Sarbanes-Oxley, is today not only a C-suite issue, but perhaps *the* primary corporate board level issue. Managers and board members now see governance risk everywhere: rogue offices and officers, out-of-control corporate entrepreneurs, intentionally misstated financial statements, and conflicts among different businesses.

Using Business Continuity to Comply with Sarbanes-Oxley

Why has legislation that does not even mention business continuity become a primary driver for the business community's increased interest in and application of business continuity management processes to their overall management of risk? Section 404 of Sarbanes-Oxley mandates that organizations must understand the risks that may impact their financial reporting processes and requires them to put in place the proper controls to deter financial misconduct. This is how business continuity became an inherent part of compliance. Without an understanding of the risks and their consequential impacts it would be difficult to understand the nature and extent of maintaining an adequate internal controls structure.

Section 404 of Sarbanes-Oxley requires companies that file an annual report to include an internal control report that states the responsibility of management for establishing and maintaining an adequate internal controls structure and procedures for financial reporting. It also requires an annual assessment of the effectiveness of the internal control structure and procedures of the issuer for financial reporting. Section 404 also requires the company's auditor to attest to, and report on, management's assessment of the effectiveness of the company's internal controls and procedures for financial reporting in accordance with standards established by the Public Company Accounting Oversight Board.

Compliance with Section 404 becomes effective on June 15, 2004, for all SEC reporting companies with a market capitalization in excess of $75 million. For all other companies that file periodic reports with the SEC, the compliance deadline is April 15, 2005. Failure to comply with Sarbanes-Oxley exposes senior management to possible prison time (up to 20 years), significant penalties (as much as $5 million), or both. Failure to comply could also expose companies to other losses, for example, reputation, public trust, and company value, all of which can impact an organization's financial health.

Compliance with Section 404 requires companies to establish an infrastructure designed to protect and preserve records and data from destruction, loss, unauthorized alteration, or other misuse. This infrastructure is designed to ensure there is no room for unauthorized alteration of records vital to maintaining the integrity of the business processes.

This involves establishing the necessary controls, engaging in risk assessment,

> **On July 30, 2002, President Bush signed into law the Sarbanes-Oxley Act of 2002, which he characterized as "the most far reaching reforms of American business practices since the time of Franklin Delano Roosevelt." The Act, named after authors Sen. Paul Sarbanes (D-Md.) and Rep. Paul Oxley (R-Ohio), was a quick response to recent corporate accounting scandals. The Act mandated a number of reforms to enhance corporate responsibility, enhance financial disclosures and combat corporate and accounting fraud, and created the "Public Company Accounting Oversight Board," also known as the PCAOB, to oversee the activities of the auditing profession.**

Sen. Paul Sarbanes (D-Md.)

Rep. Paul Oxley (R-Ohio)

implementing control activities, creating effective communication and information flows, and monitoring, all of which are key elements of any business continuity program. When developing this infrastructure the organization must follow a structured internal control framework, such as the Internal Controls – Integrated Framework of the Committee of Sponsoring Organizations (COSO) of the Treadway Commission. The COSO framework applies to operations, finance, and compliance in the following five areas:

1. **Control Environment:** This sets the tone of the organization in order to influence the control consciousness of its people by providing the necessary discipline and structure.
2. **Risk Assessment:** This is the identification and analysis of internal and external risk, which is used to determine how risk should be managed within the organization.
3. **Control Activities:** These include policies and procedures that help to ensure that management directives are carried out throughout an organization.
4. **Information and Communication:** Relevant information must be identified, captured, and communicated in a form and time frame that supports all other control components.
5. **Monitoring:** This refers to the processes that, over time, assess the quality of an organization's internal control performance.

As part of its Sarbanes-Oxley compliance effort, organizations need to identify and document all electronic and manual financial reporting processes. Business continuity continues to evolve beyond the IT arena into the entirety of an organization's business operations. At the foundation of any business continuity program is the assessment of risks and their associated effects upon business operations. This is derived through two fundamental analyses: a risk assessment that identifies and evaluates those causes that could lead to a business interruption and a business impact analysis (BIA), which evaluates and quantifies the impacts of a risk. The understanding of these risks and their resulting impacts is fundamental to creating the controls environment necessary in the creation of an infrastructure.

Once a BIA is created an analysis is done to understand the resource requirements necessary to meet an organization's recovery time objectives (RTOs), recovery points objectives (RPOs), and recovery resources (technical, operational, and administrative resources). These resource requirements articulate what is needed in order to provide a cost-effective means of minimizing the impact of a business interruption.

These resource requirements are then compared against current capabilities in order to identify the recovery gaps between what is required and what currently exists. The gaps fall into three categories:

1. **Data:** This refers to the data that is lost between the time of an organization's last backup and the business interruption event.
2. **Time:** The difference between an organization's recovery time objective and the actual time it will take the organization to reestablish business and/or technology operations to a pre-established recovery level.
3. **Resources:** The difference between the recovery resource requirements and the current recovery or continuity resources available.

Any of these three types of recovery gaps could create an obstacle to maintaining a controls environment. For example, assume that an organization's data is backed up and safely stored off-site every night by midnight. A major system interruption (ranging from a fire to a virus) at noon results in the loss of all data on the system that had been entered since the previous evening's backup. Provided the data can be restored at all, it will reflect only the information contained in the last backup. This means that all data entered, processed, received, or sent between midnight and noon is no longer reflected within the records of the company. This will certainly create inaccuracies. A solid controls environment would be able to identify these gaps and provide remediation to restore the data to its proper state. Similar processes must be in place to deal with recovery times and resources.

Looking Up and Down the Supply Chain

It is also important to understand that controls must cover the processes that extend beyond an organization's four walls. By identifying external dependencies the organization will begin to create a holistic controls environment. Therefore, consideration of an organization's use of external parties – such as vendors, suppliers, outsourcing parties, for example – is critical. When outsourced processes have a direct impact on financial statements, the SEC reporting organization will be required to assess the effectiveness of its vendors' internal control structure pertinent to their contractual agreements in order to provide sufficient documentation and sign-off for Section 404. An end-to-end view of its supply chains has companies requiring their suppliers/vendors to provide written documentation of their state of readiness and their ability to recover from disruption. This new emphasis, together with Section 404, has helped to elevate business continuity into a critical business issue. As an example, recently a global wireless and broadband communications manufacturer started requiring all its suppliers to provide evidence of their business continuity plans to prove their state of readiness.

Sarbanes-Oxley Impact on Business Continuity

As a result of Sarbanes-Oxley, business continuity has attracted renewed attention from C-suite executives, who are viewing it as an effective means of ensuring compliance. At the same time, Sarbanes–Oxley is altering how companies implement their business continuity programs. These changes include:

Annual Assessment of Business Continuity Plans

Historically, senior management has taken a rather perfunctory attitude towards their company's business continuity plans, assuming there even were business continuity plans. The plans were often very narrowly focused – typically on IT functions – were the responsibility of middle management, and tended to be updated on an "as-needed" basis. There was very little executive oversight and accountability. The exception to this are those banks covered under the Federal Financial Institution Examination Council (FFIEC) guidelines that mandated senior management review of plan development and signoff on testing results. This execu-

tive lack of interest is changing, driven not only by regulations but also by sound business practices. Companies are now mandating, at a minimum, annual testing of its business continuity plans, which are now more comprehensive in nature, exercised, and updated regularly.

Involvement of Senior Management

As a result of Sarbanes-Oxley, senior executives are required to be directly involved with internal management processes. One result is that companies are forming senior management steering committees to oversee the overall planning process, including all business continuity-related initiatives. In fact, some organizations are adding a chief continuity officer to its leadership team.

Planning Beyond the Four Walls of the Organization

Senior executives are looking beyond their own organizations to assess and address outside risks, such as supply chain vulnerability. Historically, management had been almost solely concerned with the risks associated with their internal operations and have not even identified external risks, much less taken steps to address and mitigate them.

Requiring Business Continuity Plans as Part of Service Level Agreements

As the overall awareness level of risk increases, those companies that engage in risk management best practices are more inclined to conduct business with like-minded organizations. As a result, companies are requiring their business partners to include business continuity programs in their service level agreements.

Expanding Business Continuity Budgets

Budgets for business continuity efforts, and not just for IT disaster recovery, continue to be expanded as senior management's understanding of the criticality of business continuity within their enterprise-wide risk mitigation increases.

Conclusion

With the deadline for compliance with Sarbanes-Oxley fast approaching, all public companies, regardless of their industry, need to ensure that evaluations of their internal control structure and procedures for financial reporting are completed. Companies are finding that the process is taking longer than expected – certainly more than the minimal hours estimated by the SEC.

However, taking a business continuity approach at an early stage can provide companies with the means to report to the SEC accurately and on time. This approach also provides valuable information for updating and/or establishing company-wide business continuity plans.

Therefore, the value of business continuity and Sarbanes-Oxley compliance should not be underestimated by C-suite executives. Not only will it help them comply with the letter of the law, it will generate invaluable information that can be leveraged to create new control structures that will improve corporate governance and, by extension, the overall operations of the organization.

❖

Al Berman, senior vice president, is the national business continuity planning practice leader at Marsh Inc. He has been providing business continuity planning solutions for more than 15 years and is a Certified Business Continuity Professional.

■ To comment on this article, go to 1702-01 at www.drj.com/feedback.