12-2007

Disaster Recovery Planning: What Section 404 Audits Reveal

Dana R. Hermanson
Kennesaw State University, dhermans@kennesaw.edu

Daniel M. Ivancevich
University of North Carolina - Wilmington

Susan H. Ivancevich
University of North Carolina - Wilmington

Recommended Citation
Hermanson, Dana R., Daniel M. Ivancevich, and Susan H. Ivancevich. "Disaster Recovery Planning: What Section 404 Audits Reveal." CPA Journal 77.12 (2007): 60-62.

The CPA Journal

Print

Disaster Recovery Planning: What Section 404 Audits Reveal

By Dana R. Hermanson, Daniel M. Ivancevich, and Susan H. Ivancevich

DECEMBER 2007 - While many articles have been written on what companies should do to implement effective disaster recovery plans (DRP), much less attention has been given to how well public companies are doing with their disaster recovery planning efforts. This article summarizes recent Sarbanes-Oxley Act (SOX) section 404 internal control reports that reveal material weaknesses due to inadequate disaster recovery planning. Section 404 currently applies to public companies with over $75 million in public float. Auditors evaluating internal control over financial reporting must consider key IT-related risks and controls that affect financial reporting, including issues related to disaster recovery planning. By profiling DRP-related material weaknesses, the authors hope to offer insights to those who are struggling to achieve DRP effectiveness, including the smaller public companies that will soon face section 404 audits.

Magnitude of the Problem

Using the Audit Analytics database (www.auditanalytics.com), the authors searched for reported material weaknesses in internal control from November 2004 (the effective date of section 404) through August 29, 2006, to identify which ones specifically related to DRP. (See Dana R. Hermanson, Daniel M. Ivancevich, and Susan H. Ivancevich, "IT-Related Material Weaknesses in Internal Control: Initial Evidence from SOX Section 404 Reports," *Review of Business Information Systems*, First Quarter 2007, for a broader analysis of IT-related material weaknesses.) This search revealed 16 public companies with material weaknesses in internal control over financial reporting that were DRP-related. From Audit Analytics, the authors also gathered financial and other data on these companies.

These 16 companies represent a small fraction of the companies that have undergone SOX section 404 audits to date. One can conclude that the vast majority of public companies examined have effective DRPs. It is important to note, however, that section 404 deals only with internal control over financial reporting—it does not encompass all of a company's internal controls and systems. As a result, it is possible that other public companies have DRP-related weaknesses unrelated to their financial reporting systems (e.g., product development system, customer relationship management system, or human resources system). In addition, smaller public companies are not yet subject to section 404 audits, and the DRP weakness rate may be higher in that segment.

Company Profile

The median company in the sample had annual revenues of $27 million, a market capitalization of $180 million, and a net loss of $3 million. Most of

the companies trade on AMEX or Nasdaq, and half had a non-national CPA firm as their auditor. It is clear that companies with DRP-related material weaknesses fall within the smaller end of the market now subject to SOX section 404. With respect to industry, there are three companies in Standard Industrial Classification (SIC) 48XX (Communications) and four companies in SIC 73XX (Business Services). The sample companies have a number of material internal control weaknesses in addition to their DRP-related problems. The average number of total material weaknesses ranged from 1 to 10, with an average per company of 4.9.

Specific DRP Weaknesses

The Exhibit presents information on the 16 companies with DRP-related material weaknesses. The specificity of material weakness disclosures varies widely across companies. Among the 16 companies, there are 10 cases in which the deficiency appears to involve a general failure to implement a DRP or backup and recovery plan (six companies mention "backup and recovery" or "backup," and four companies mention "DRP" or "disaster"). In the event of a disaster, such companies would risk catastrophic damage, including the inability to file financial reports.

In five companies the primary issue appears to involve improper handling or storage of backups, especially in keeping backups on-site rather than off-site, or in failing to back up to removable media. In these cases, it seems that some effort was made to create backups, but the backups were not handled in a way that provided much protection to the company. While these companies might fare well in a simple computer system failure, enabling them to use their on-site backups, they would be at risk of great damage if a disaster destroyed their local computer system and backups.

Finally, one company's disclosure related to the documentation of the backup and recovery controls. Disaster recovery plans can be very complex and detailed. The risk of inadequate documentation is that the backup plan may not be followed properly after a change in personnel. Such an event could be costly to a company.

What Should CPAs Do?

Based on the patterns described above, the authors believe that CPAs should emphasize "DRP 101" with all kinds of businesses (see Joel Jacobs and Stanley Weiner, "The CPA's Role in Disaster Recovery Planning," *The CPA Journal*, November 1997). DRPs are like insurance: They may not seem important until they are needed.

The first step is to actually have a backup and disaster recovery plan. Moving companies toward effective DRPs requires management to have the right mindset. Management should ask itself: "If this office and everything in it were destroyed tonight, would it be possible to do business tomorrow, or at least next week?" If the answer is no, then the company should develop or modify its disaster recovery procedures. (Companies that outsource IT functions should be aware that DRPs may fall outside of the controls covered by an SAS 70 report on the service organization.)

The second step is to carefully consider how backups are handled and stored. Although on-site storage is easy, it will not provide protection from a major disaster that destroys an entire office. With today's ability to easily transmit data to remote locations, businesses should strongly consider off-site storage strategies. It is a good idea to store backups in a different geographic location because a natural disaster, such as a hurricane, can

devastate an entire region.

Finally, in the case of a disaster, affected businesses will need a different location to commence IT operations. As part of the DRP, an alternate processing site must be arranged. Whether this site is a "hot site" (complete and ready to go with all the necessary processing equipment), a "cold site" (a location that can be equipped with the necessary processing equipment), or a contract with a service provider that will provide processing services if a disaster occurs, arrangements must be made in advance so that operations can be resumed as quickly as possible in the event of a disaster.

Looking Ahead

SOX section 404 audits reveal some public companies with significant DRP-related weaknesses, and several indicated that remedial efforts were underway. The authors believe that many more private and small public companies are facing such challenges as well. Creating an effective DRP is a significant undertaking for management, and CPAs can provide important leadership in this area.

***Dana R. Hermanson, PhD**, is the Dinos Eminent Scholar Chair of Private Enterprise and a professor in the department of accounting at Kennesaw State University, Kennsesaw, Ga.*
***Daniel M. Ivancevich, PhD**, is a professor and **Susan H. Ivancevich, PhD**, is an associate professor, both in the Cameron School of Business at the University of North Carolina Wilmington, Wilmington, N.C.*

Close