

CPA Audits Now Focusing on IT!

© 2008 by Nick B. Nicholaou, all rights reserved

President, Ministry Business Services, Inc.

Reprinted from *NACBA Ledger*

Church and ministry computer systems and networks have grown in response to perceived needs over the years, and most have grown with very little intentionality or strategy. The results are often higher than necessary complexity, cost, and risk. CPAs are now being required to look at IT during audits for fiscal years ending 12/15/2007 and later. Are you ready?

Why Does Your CPA Care About IT?

Computers definitely help our team members to be more effective in their ministry, including helping leadership get a grip on trends earlier in the game than they could have twenty years ago. If it's all about productivity, why does your CPA care?

It's Really About Risk Management

The Auditing Standards Board recently issued eight Statements on Auditing Standards that are effective for audits of fiscal years ending 12/15/2007 and later. They are SASs 104 through 108, and it appears the goal is to change the focus of the audit somewhat from financial statement balances to an assessment of risk in key business processes and the environment in which we operate. That includes IT since we've become heavily dependent on our computer systems.

Imagine, for instance, the cost to your ministry if your systems are unavailable for more than a week. This happened recently to a large church who came to us afterwards... I imagine the outage cost the church tens of thousands to pay their staff to do—effectively—very little during that time. Another church came to us after being unable to access their database for nearly three months!

In light of those that were put out of business because they lost their systems on 9/11 or during Katrina, this is an important issue.

Isolated Incidents?

We're a community that believes Jesus' words in Luke 21 when he was asked about the end times. Verses 10-11 and 25-26 say, "Nation will rise against nation, and kingdom against kingdom. There will be great earthquakes, famines and pestilences in various places, and fearful events and great signs from heaven.... There will be signs in the sun, moon and stars. On the earth, nations will be in anguish and perplexity at the roaring and tossing of the sea. Men will faint from terror, apprehensive of what is

coming on the world, for the heavenly bodies will be shaken." (NIV)

So we should anticipate that the frequency of these incidents will continue to increase as we get closer to the end of time. And if we want to be used by The Master during those times, making reasonably certain our systems are going to be up is important.

SAS 105 & 109

These two SASs seem to impact IT the most. They will require more involvement by your IT staff—whether in-house or outsourced—and the more that can be prepared in advance, the better. They require your auditor to gain an understanding of your risks and evaluate your internal controls—including those in IT. More than that, they require evaluating the effectiveness of your internal controls and ensuring that practice matches policy.

COSO Internal Control Framework

COSO is the Committee of Sponsoring Organizations (and you thought IT had weird acronyms!), and is comprised of

- American Accounting Association
- American Institute of CPAs
- Financial Executives International
- Institute of Management Consultants, and
- The Institute of Internal Auditors.

They have published a set of standards auditors are to rely on when assessing IT. Their standards are divided between "less complex" and "more complex" operations. Surprisingly, you are "more complex" if you:

- Have custom developed software,
- Have packaged software that's been modified or supplemented,
- Rely on the internet to transmit transactional data (more than just email and browsing), and/or
- Heavily rely on spreadsheets with complex calculations and macros.

Most in Ministry Will Need to Improve Their IT Approach

COSO will have the auditor asking:

- *Are there controls over system design and implementation?* The focus will be on the role senior management plays in the process of setting and approving of IT strategies and changes.
- *Are updates tested before installed?* Not many churches and ministries have the ability to test updates before they're applied, so this may best be outsourced. For example, our firm tests Microsoft and other changes for our clients.
- *Is system security adequate?*
 - COSO wants minimum 8-digit alphanumeric passwords that are un-guessable. However, they don't understand our computing environment. It's been our observation that most users will put passwords that difficult on notes stuck to their monitor or under their keyboard, which defeats their effectiveness! Instead we recommend passwords at least four digits long that are acronyms of praise or worship songs or verses. They're easier to remember and still hard to guess.
 - Multiple failed login attempts should automatically lock a user's account for a period of time. This blocks programs and others from trying to guess a password.
 - Anti-malware should be in place and current.
 - Servers and wiring closets should be locked with a limited number of keys.
 - Data is backed up, regularly stored off-site, and regularly tested.
 - Firewalls should be in place and current. Our favorites are Barracuda's SPAM Firewall for email, and SonicWALL's Pro series for all other firewall security.
 - Vulnerability assessments are regularly performed.
- *Are operational errors identified and corrected in a timely manner?* This refers to user help desk activity.
- *Do applications ensure complete transactions?* Are spreadsheet formulas tested and proven error free? This also includes folder and file naming

conventions to ensure that only the latest files are being used.

Additional IT Risk Management Steps

- *Identify / inventory your hardware.*
This list should include your IT infrastructure (switches, routers, WiFi router security settings, internet connection providers and IP addresses—and what they're connected to), servers, desktop computers, notebook computers, and printers. Record manufacturer names and model numbers along with any warranties or service contracts.
- *Identify / inventory your software.*
Document what software you use and what computer(s) it's installed on. In addition, gather all your licenses in one location. This will help you make certain you have enough (be sure to buy them from an organization offering charitable licensing discounted pricing, like Consistent Computer Bargains, 800/342-4222).
- *Test your vulnerabilities.* Document your disaster recovery plan and make certain it includes business continuity. Make certain you have a solid backup strategy and that it is regularly tested. And, test your firewalls.

If you're like most churches and ministries, you're probably thinking this will take more time to accomplish than you have. If that's the case, then outsource it. But getting this done now will mean that you'll be able to present the documentation on all of these issues to your auditor. If your audit fees are based on the auditor's time spent performing the audit, this may keep your audit fees from going up! Oh yeah... it'll also increase the likelihood you'll survive a disaster and be there to meet the needs of those around you.

Nick Nicholaou is president of MBS, a consulting firm specializing in ministry computer networks, operational policies, and CPA services. You can reach Nick via email (nick@mbsinc.com) and may want to check out his firm's website (www.mbsinc.com) and his blog at <http://ministry-it.blogspot.com>.