

CLIENT CONNECTION



General Conference Auditing Service, 12901 Old Columbia Pike, Silver Spring, MD 20904
telephone: 301-680-5040; fax: 301-680-5054

Mission Statement

The mission of the Seventh-day Adventist Church is to proclaim to all peoples the everlasting gospel in the context of the three angels' messages of Revelation 14:6-12, leading them to accept Jesus as personal Saviour and to unite with His church, and nurturing them in preparation for His soon return.

All employees of denominational entities play an integral part in fulfilling this mission. Whether employees are teachers, maintenance workers or pastors, they each contribute to the fulfillment of the mission.

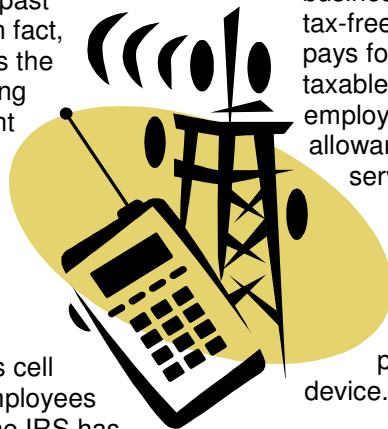
The General Conference Auditing Service has created a mission statement that describes our commitment to supporting our denominational clients. We share our mission statement with you:

We serve God by delivering excellent audit services to the Seventh-day Adventist Church!

Taxation of Cell Phones

The use of cellular telephones over the past few years has increased dramatically. In fact, you probably know which company uses the "can you hear me now" phrase. According to Infoplease.com, cell phone users went from 340,213 in 1985 to 233,000,000 in 2006. Employers provide their employees with mobile devices that include voice, data, internet and other services in the performance of their employee duties.

The Internal Revenue Service considers cell phones to be "listed property." Since employees can use cell phones for personal use, the IRS has developed substantiation requirements to identify the business and personal use of the phones. The IRS has identified the personal use of employer provided cell phones as a significant area of untaxed "income" to the employee and under reporting of payroll taxes by the employer.



INSIDE THIS ISSUE

Mission Statement	1
Taxation of Cell Phone Reimbursement	1
Sarbanes-Oxley Act for Nonprofit Organizations	2
Payment Card Industry Data for Security Standards	3
Preparing for an Audit	3
New Auditing Standards Related to Risk Assessment	3

The cost of cell phone service provided by the employer is fully taxable under a "nonaccountable" plan. If the employee is not required to substantiate the business usage of the cell phone (i.e. providing the employer with documentation of total usage and identifying work calls and the business purpose of the calls) than this practice is considered "nonaccountable." If employees are required to substantiate the business use of the cell phone, then the total cost of the service should be allocated between business and personal use and the business portion of the cell phone expense is considered tax-free to the employee. However, when the employer pays for any personal portion of the cost, this represents taxable income to the employee. This is true whether the employer provides the employee with a cell phone allowance or whether the employer pays the cell phone service provider directly.

The cost of the cell phone device (whether provided directly by the employer or purchased with an employer provided allowance) should also be allocated between business and personal, based on the subsequent use of the device.

Many employers find that it is not cost effective to allocate the cost based on the usage, so they have elected to treat the total cost of cell phones and the related service as taxable to the employees. This is acceptable to the IRS.

As common with all tax issues, please consult with your legal counsel to make sure your organization complies with the applicable tax laws regarding cell phones.

For more information, please refer to the following websites:

IRS -
<http://www.irs.gov/govt/fslg/article/0,,id=167154,00.html>

Thompson -
<http://www.thompson.com/public/headlines.jsp?id=39>

Sarbanes-Oxley Act for Nonprofit Organizations

The Sarbanes-Oxley Act (officially known as The American Competitiveness and Corporate Accountability Act) was signed into law on July 30, 2002. This was the result of corporate and accounting scandals from such corporations as Enron, Tyco, WorldCom and others. The purpose of the law was to rebuild the public's trust in corporate America.

The majority of the Act applies to publicly traded corporations. However, nonprofit organizations (including Seventh-day Adventist organizations) need to be aware of the Act because there is a trend by state legislatures to adopt laws similar to provisions of this Act to be applied to nonprofit organizations. You may want to check your state laws to determine if they are similar to any provisions of the Act.

There are two provisions of the Act which apply to all entities, including nonprofit organizations. Those two provisions deal with document retention and retaliation against whistle blowers.

Document Retention

The destruction of documentation is prohibited by Section 802 of the Sarbanes-Oxley Act. The Act describes illegal actions such as knowingly altering, destroying, concealing or falsifying any record or document with the intent to impede, obstruct, or influence shall be punishable by fines or imprisonment up to 20 years. Section 802 is not limited to companies that report under the Securities and Exchange Act of 1934, therefore it is generally understood that this applies to nonprofit organizations.

Denominational entities would be best served by developing and implementing a record retention/destruction policy. This policy will identify the timelines for maintaining various categories of documents (financial, payroll, fundraising, personnel, contracts, leases, etc.). The policy needs to address the ever increasing role of electronic documentation (e-mails, paperless data, voice mails, etc.). The timelines need to address the point at which specific documentation (tangible and electronic items) can be destroyed. To safeguard the retention/destruction policy practices, organizations need to provide adequate back-up procedures, archiving procedures and tests of the system's reliability. Remember, an ounce of prevention is better than a pound of cure!

There may also be legal requirements for record retention by various state or province, and federal regulatory agencies. Because of this, an entity's legal counsel should always be involved in the preparation of and any changes to its record retention/destruction schedule.

The General Conference Archives department has a retention schedule which can be obtained from the following web site:
http://ast.gc.adventist.org/records_center.asp

Whistle Blower Provision

The Act provides protection for corporate whistle blowers. Section 1107 of the Act is not limited to publicly-traded companies. That section states, "Whoever knowingly, with the intent to retaliate, takes any action harmful to any person, including interference with the lawful employment or livelihood of any person, for providing to a law enforcement officer any truthful information relating to the commission or possible commission of any Federal offense, shall be fined under this title or imprisoned not more than 10 years, or both."



The Act does not require that nonprofits create a written whistle blower policy. However, each organization should develop procedures for dealing with employee and volunteer complaints. Such procedures may include creating a confidential and anonymous method for employees and volunteers to report inappropriate matters. Leaders of the organization need to ensure that all complaints are taken seriously and investigated accordingly. The leaders should document their actions by identifying any problems that were fixed or justifying why action was not needed.

For more information on how the Act applies to nonprofit organizations, please refer to the following web links:

“The Sarbanes-Oxley Act and Implications for Nonprofit Organizations” –
<http://www.boardsource.org/clientfiles/sarbanes-oxley.pdf>

The actual bill passed by Congress:
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_bills&docid=f:h3763enr.txt.pdf

Payment Card Industry Data Security Standard (PCI DSS)

The theft of electronic data continues to be a significant issue that affects all businesses. As our society becomes more comfortable with using electronic payment options, nonprofit organizations are increasing their efforts to tap into this money source in receiving donations or receiving payment for services. Without the proper safeguards in place, nonprofit organizations are vulnerable to data theft.

Nonprofit organizations that use the internet to solicit and receive donations via credit and debit cards have the responsibility to ensure that the personal data received will be adequately safeguarded. Failure to do so will erode donor confidence in the organization which may lead to fewer donations.

Several of the large credit card companies realized the importance of safeguarding personal data and the need to develop common industry security requirements. As a result, the Payment Card Industry Data Security Standard (PCI DSS) was created by collaboration between MasterCard and Visa. The PCI DSS consists of twelve basic requirements:

1. Install and maintain a firewall configuration to protect cardholder data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.
3. Protect stored cardholder data.
4. Encrypt transmission of cardholder data across open, public networks.
5. Use and regularly update anti-virus software.
6. Develop and maintain secure systems and applications.

7. Restrict access to cardholder data by business need-to-know.
8. Assign a unique ID to each person with computer access.
9. Restrict physical access to cardholder data.
10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.
12. Maintain a policy that addresses information security.

PCI compliance is not a legal regulation, rather it is a contractual obligation with the credit card companies. If your organization accepts credit or debit cards from American Express, Discover, MasterCard and/or Visa, then compliance with PCI standards is necessary.

A best practice to ensure compliance with PCI standards is to use a transaction processing vendor that complies with PCI standards. Thus, nonprofit leaders need to verify that their third-party vendors (such as their website host, database and credit and debit card processing agents) are PCI compliant. It is also important to review the organization's capture and storage of personal data to make sure that donor information is safeguarded.

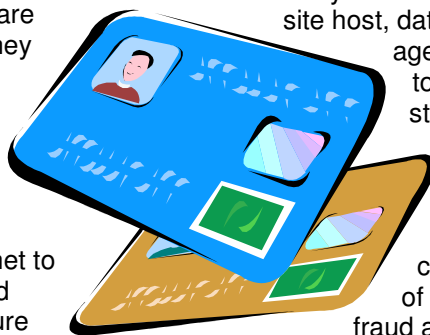
Steve Klein, VP of Business Development for Kintera in San Diego, wrote that “PCI compliance can afford nonprofits the peace of mind of shielding contributors from identity fraud and theft, maintain a positive reputation surrounding the safeguard of sensitive information, minimize risk, and contribute to increased consumer confidence in donating online.”

For additional information, please visit the PCI Security Standards Council website at:
<https://www.pcisecuritystandards.org/index.htm>

Preparing for an Audit

Have you ever wondered what you could do to please the auditors (or if it is even possible)?

A lot of hard work goes into being an accountant or treasurer. The art of accounting is often an underappreciated function. At year-end, there are numerous administrative chores, endless committees, and the arduous task of closing the books.



The treasury staff is often overworked and overstressed by the time the auditors arrive with their questions and requests.

This article includes suggestions that will help you to have an easier audit. Auditors are not that hard to please.

As you close your ledgers, you already analyze each line item of your financial statements to be satisfied there are no mistakes. Making copies of these analyses for the auditors is a sure fire way to shorten their stay.

Each item on your statement of financial position should be proven before the books are closed for the year.

If you have had an unusual accounting problem during the year, please inform the auditors. They might be able to provide you with some suggestions on how to deal with the problem.

To assist you in preparing for your audit, the auditors will provide you with an audit preparation binder. The following items are generally utilized with the audit preparation binder:

1. **Cash** – copies of bank reconciliations and year-end bank statements for each account.
2. **Investments** – copies of year-end financial institution statements and a schedule of the yearly investment activity.
3. **Notes Receivable** – copies of new notes, amortization schedules, activity schedules and a reconciliation of interest income accounts.
4. **Inventories** – copies of the inventory count sheets (or for large inventories the total sheets).
5. **Prepaid Expense** – copy of the prepaid expense schedule with supporting contracts and/or insurance policies.
6. **Plant Assets** – a schedule showing beginning fixed asset cost, additions, deletions and ending plant assets cost; copies of invoices or contracts on major additions; supporting documentation on disposals.
7. **Accounts Payable** – detail listing of accounts payable.
8. **Notes Payable** – copies of new notes signed during the year with amortization schedules; copies of notes paid off during the year; and a reconciliation of the interest expense account.
9. **Restricted Income** – schedule showing the beginning restricted net assets, restricted income received during the year, releases of restrictions during the year, and the ending balance; provide supporting documentation for large restricted donations.

Utilizing the audit preparation binder while you perform your closing procedures will result in a more efficient and fun audit. Now you know how to make your auditors happy!

New Auditing Standards Related to Risk Assessment

In March 2006, the Auditing Standard Board issued eight Statements on Auditing Standards (SASs) relating to the assessment of risk in an audit of financial statements. The SASs are effective for audits of financial statements for periods beginning on or after December 15, 2006. In other words, denominational entities with years ending December 31, 2007 and later will have audits performed in accordance with these SASs.

The arrival of these SASs represent a significant change in the audit process. The auditor now must place greater emphasis on assessing risks for each organization. This will result in more questions from the auditors and the obtaining of additional documents and records. It boils down to the need for the auditor to develop a greater understanding of your organization, its mission, its activities and how you address organizational risks.

According to the AICPA, the primary objective of the SASs is to enhance the application of the audit risk model in practice by requiring, among other things:

- A more in-depth understanding of the entities environment, including its internal control. This knowledge will be used to identify the risk of material misstatement in the financial statements (whether caused by error or fraud) and what the organization is doing to mitigate them.
- A more rigorous assessment of the risk of material misstatement of the financial statements based on that understanding.
- Improved linkage between the assessed risks and the nature, timing, and extent of audit procedures performed in response to those risks.

You may be wondering how these SASs will impact your preparation for your upcoming audit. The best preparation by management is to understand and document your internal control structure. This understanding should include organizational controls as well as transaction level controls, including information systems and major processes.

New audit standards generally involve a learning curve for the auditors to appropriately incorporate these procedures into their audits. This also means that

entities being audited should expect to field additional questions from their auditors. Furthermore, there may be new audit procedures which the auditors will incorporate to comply with the new SASs. The ultimate goal of these new SASs is for your auditor to create an audit that is tailor-made for your organization.

The North American Division Accounting Manual provides information on internal controls in chapter four. Reviewing this chapter and applying this information to your organization will help you to develop a greater understanding of your internal control structure.

A copy of the NAD Accounting Manual can be downloaded at the NAD website by clicking the following link: <http://www.nadadventist.org/article.php?id=98>

Abandoned Property Might Belong to State

Under the heading, *I didn't know that*, exists a law in almost every state which requires businesses to remit abandoned property to the state. You may be asking, what is abandoned property? It includes – credit balances, deposits, uncashed checks, unused gift certificates, and other items.



The law varies from state to state but in general, property is considered to be abandoned if it remains unclaimed on your books from one to five years.

In most cases annual returns are required to identify abandoned property. State laws provide interest and penalties and even criminal charges for failure to comply with the law. A review of your state laws should be made to insure compliance with any reporting requirements.

After researching your state law and consulting with legal counsel (always a good practice), you should create procedures so that uncashed checks and other unsettled claims are investigated and resolved in a timely manner. The longer these items remain on your accounting records, the harder it is for your accounting staff to determine the reasons why these items are unresolved.

If your state has an abandoned property law, it is important that your organization complies with the law to avoid unnecessary liability for noncompliance.

This newsletter is published quarterly by the General Conference Auditing Service. It is sent without cost to administrators of SDA organizations within the North American Division of the Seventh-day Adventists.

If someone in your organization should be receiving it, but is not, please e-mail this information to Linda Fredlund: clientconnection@gc.adventist.org

Please send us your comments, questions, suggestions, or contributions (of articles, not money) to:

Jeremy Smith, Editor
General Conference Auditing Service
PO Box 5005
Westlake Village, CA 91359
Smithje@gc.adventist.org
(805) 413-7138

This newsletter is intended to provide general information about a variety of topics of interest to Administrators of Seventh-day Adventist organizations. If you read an article of interest to you, we suggest that you study further or seek counsel to clarify your understanding of the subject, before taking action. This is a complicated world - be careful.

Not on our mailing list and would like to receive a copy of *Client Connection*?
Send your e-mail address to Linda Fredlund,
clientconnection@gc.adventist.org



GENERAL CONFERENCE
AUDITING SERVICE

An audit service of the Seventh-day Adventist Church