A BIMONTHLY PUBLICATION DEDICATED TO PROVIDING IDEAS AND EDUCATION TO TAX-EXEMPT ORGANIZATIONS

MUSE

Ideas and education for tax-exempt organizations on everything from vital tax and accounting issues to tips on improving operations.

In this issue:

Getting ready: Revenue recognition and not-for-profit entities

Form 990-N, 10 years later

Cybersecurity for nonprofits: Understanding threats and weaknesses

2017 annual nonprofit accounting update webcast

Getting ready: Revenue recognition and not-for-profit entities

It is not too early to begin anticipating and mapping out the impact on your organization of FASB Accounting Standards Update (ASU) 2014-09, *Revenue from Contracts with Customers (Topic 606)*. The first step is determining when it will be effective for your organization; that will impact your timeline of activities. For information about the effective dates of the new guidance, refer to our article, *Are you sure you know when the revenue guidance in ASC 606 is effective*?

The next implementation step is to determine which revenue streams will be impacted by Topic 606. As a reminder, contributions are not considered contracts with customers and therefore would not fall under Topic 606. Topic 606 requires expanded disclosures related to revenue recognition; modeling disclosures under the new standard should be a key activity in your Topic 606 adoption timeline. Often the time it takes to create clear, effective and complete disclosures is underestimated.

A great place to begin getting an understanding of the key concepts underlying Topic 606 is to listen to RSM's recorded webcast, *Revenue recognition under ASC 606*. It includes technical content and multiple examples that illustrate key concepts in an understandable format. The March *Journal of Accountancy* article, *Get revenue recognition right at not-for-profits*, includes not-for-profit (NFP) industry-specific ideas and concepts. Other RSM resources include:

ATCHLEY & ASSOCIATES LLP
CERTIFIED PUBLIC ACCOUNTANTS & BUSINESS ADVISORS

RSM US Alliance | RSM

- *Revenue recognition: A whole new world*
- Update on revenue recognition: Health care
- *Changes coming for health care revenue recognition*

In addition to changes for revenue recognition, NFP entities also have to anticipate the impact of the financial reporting project (FRP). For more information on ASU 2016-14, *Not-for-Profit Entities (Topic 958): Presentation of Financial Statements for Not-for-Profit Entities*, see our article, *Not-for-profits: Important changes ahead*.

You also may be wondering how the FRP will impact your reporting to the IRS. The American Institute of Certified Public Accountants (AICPA), through an ASU 2016-14 Tax Working Group that is collaborating with the AICPA NFP Expert Panel, is developing a communication to the IRS recommending changes to the 2018 Form 990, Schedule D and related instructions. Absent changes to the actual forms, the letter could recommend changes to the instructions to facilitate reporting on existing forms. Suggestions also may include a recommendation for a general "clean-up" of the forms and instructions to remove outdated SFAS 116/117 and FIN 48 terminology and replace it with current FASB ASC 958 language.

Form 990-N, 10 years later

By: Bill Turco, Senior Director

Prior to the passage of the Pension Protection Act of 2006, small exempt organizations, other than black lung benefit trusts (Form 990-BL) or private foundations (Form 990-PF) that did not meet the $25,000 gross receipts test of the Form 990-EZ, were excused from filing with the Internal Revenue Service (IRS). As a result of the lack of any filing requirement, these nonreporting entities would remain on the IRS books as tax-exempt organizations in perpetuity. There was no way for the IRS to tell if these organizations operated below the filing threshold, operated above the filing threshold but neglected to file, or were no longer operating or even in existence.

The Pension Protection Act of 2006 brought into force a new set of filing requirements for most small exempt organizations. Beginning in 2008, almost all organizations that were previously exempt from filing as a result of the organization's gross revenue amount were required to file annually with the IRS. The IRS developed a Form 990-N to be used by applicable organizations to meet the filing requirements. Further, as a result of the change in the law, the IRS is now required to revoke an organization's exemption if it has not filed an exempt organization information return in one of the last three years. Per a 2014 Government Accountability Office (GAO) report on tax-exempt organizations, initially more than 570,000 organizations have had their exemptions revoked as part of the automatic revocation process.

For the years 2008 and 2009, the maximum average gross revenue permitted for the filing of the Form 990-N was $25,000. For years ending or after Dec. 31, 2010, small organizations that normally have annual gross receipts of $50,000 or less are permitted to file a Form 990-N. Where the Form 990-EZ has both a gross receipt (less than $200,000) and a total asset test (less than $500,000) that must be passed to file the EZ, the Form 990-N has only a gross receipts test. To determine the ability to use the Form 990-N, an applicable organization is only required to consider its gross receipts as defined in the appendix instructions to the Form 990.

While most organizations that are required to file from the Form 990 series may file a Form 990-N if the organization meets the gross receipts test, supporting organizations as described in section 509(a)(3), and political organizations as described in section 527, are not permitted to file a Form 990-N and must file either a Form 990-EZ or Form 990. Other organizations that are not permitted to submit a Form 990-N to satisfy their filing requirements include sections 501(c)(1) U.S. government instrumentalities, (c)(20) group legal services plans, (c)(23) pre-1880 armed forces organizations, (c)(24) ERISA section 4049 trusts, 501(d) religious and apostolic organizations, 529 qualified tuition programs, 4947(a)(2) split-interest trusts, 4947(a)(1) charitable trusts treated as private foundations, all other private foundations and black lung benefit trusts.

For most organizations, having zero gross receipts will not present any issues regarding the organization's status as an exempt entity. For publicly supported charities described in sections 509(a)(1) and (a)(2), a revenue-based test must be met in order to remain a publicly supported charity. For the first five years (60 months) of its existence, a publicly supported charity is presumed to meet its public support test. At the end of the first five years, an organization that wishes to remain a publicly supported organization, and not be treated as a private foundation, will need to pass one of the public support tests as described in sections 509(a)(1) or (a)(2).

The public support test for organizations filing a Form 990 or Form 990-EZ is calculated in Schedule A. The section 509(a)(1) test requires that an organization receives at least one-third of its support from contributions from the general public, or meets a 10 percent facts and circumstances test. The section 509(a)(2) test requires that the organization receive more than one-third of its support from contributions from the general public and/or from gross receipts from activities related to its tax-exempt purpose. Under section 509(a)(2), the organization cannot receive more than one-third of its support from gross investment income and unrelated business taxable income. These tests are measured over a five-year period beginning at the end of the organization's first 60 months of existence. A new organization filing a Form 990 or Form 990-EZ is not required to show its public support percentage, but is required to show all items that make up the calculation of the percentage in Parts II or III of Schedule A. A publicly supported organization that fails to meet its public support test for two consecutive years is considered to be a private foundation. As a private foundation, the organization would then be required to file a Form 990-PF.

To read the complete article, go to: http://rsmus.com/our-insights/newsletters/muse/form-990-n-10-years-later.html

Cybersecurity for nonprofits: Understanding threats and weaknesses

By: Jay Schulman, Principal

Many nonprofit organizations do not consider themselves as potential targets for a cyberattack because they think they do not possess information hackers want. However, the NetDiligence 2016 Cyber Claims Study ranked nonprofit organizations as a top-five affected industry. With these threats in mind, many nonprofits must evaluate their security posture to avoid data and system loss, business interruption and reputational harm.

While many think that credit card information is the most stolen, the NetDiligence® study found that the majority of information that is stolen is personally identifiable information (PII). PII includes names, addresses, email addresses, social security numbers and banking information. Most nonprofits possess a wide range of valuable PII from employees, donors and other types of constituents.

In RSM's recent 2017 cybersecurity outlook and key considerations for nonprofits webcast, it was discussed how nonprofit organizations can better evaluate their cybersecurity posture.

The challenge to securing an organization is that data can reside in many places, and is difficult to manage and trace. Today's nonprofit organizations are highly dependent on technology, with a network including applications, databases, remote users, service providers and mobile devices typically storing and sharing vast amounts of private data. In addition, nonprofits are increasingly outsourcing several key functions, transitioning data to third parties or cloud vendors. Even though the data is stored elsewhere, the responsibility for that information stays with the organization.

Cybersecurity threats can come from many places, both online and offline. The causes of breaches are typically thought of as malicious, but they can also be unintentional. Common cyberthreats that can face nonprofit organizations include:

- **Inside attackers:** Malicious and disgruntled employees can change, delete or destroy data, damage systems, and steal or sell sensitive information.
- **Outside attackers:** Attackers don't necessarily target a specific organization. They can hack into systems, launch denial-of-service attacks, develop social engineering attacks and perform email hacking or even extortion.
- **Viruses and malware:** An organization can become infected or infiltrated by a host of viruses or malware that can originate with a phishing email or infected file. These can give an intruder access to a network to control or steal sensitive data.
- **Employee accident:** Employees can cause a breach through innocent errors, such as losing a laptop, or sending an email with a file or clicking on a link that installs malicious software.
- **Non-malicious system or coding errors:** Information technology (IT) personnel can inadvertently create vulnerabilities in software or applications, especially when implementing new systems.
- **Trusted third-party vulnerabilities:** Vendors such as cloud providers that control an organization's data or systems can suffer a breach or mishap that exposes critical information. Again, outsourcing those systems or data does not absolve the organization of the responsibility for protecting that information.

Unfortunately, many nonprofit organizations are unaware of the technical weak spots that could directly lead to a breach. For example, many attacks can go completely undetected. In addition, organizations often do not have an effective strategy for encryption or patch management that helps to keep hackers out of the system. Vendor mismanagement is another concern, with third parties lacking thorough oversight and due diligence practices.

Just a single breach can significantly damage an organization's finances and reputation. NetDiligence's survey found that the average breach costs $665,000 in covered costs. This is considerable since the majority of respondents were small organizations. For example, a small health care organization with $50 million in revenue lost 10,000 records in a breach. The organization suffered a $256,000 loss after providing notice to victims and paying legal and forensics costs. Breaches can lead to regulatory fines that can make financial losses climb quickly.

To begin to implement an effective cybersecurity strategy, organizations must first assess their readiness. Employees must understand applicable regulations such as state privacy regulations, payment card industry (PCI) and Health Insurance Portability and Accountability Act (HIPAA) guidelines.

To read the complete article, go to: http://rsmus.com/our-insights/newsletters/muse/cybersecurity-for-nonprofits-understanding-threats-and-weaknesses.html

2017 annual nonprofit accounting update webcast

LIVE WEBCAST | April 25, 2017

By: Ian Benjamin, Partner

Join us on Tuesday, April 25 as Ian Benjamin, partner and leader of the nonprofit practice in RSM's New York office, will lead an informational session to discuss the latest accounting updates and issues that could affect nonprofit organizations.

Register

During this webcast, we will present:

- New financial statement presentation standards
- The latest on leases
- Information about revenue recognition
- Highlights of other recent Accounting Standards Updates

ATCHLEY & ASSOCIATES LLP
CERTIFIED PUBLIC ACCOUNTANTS & BUSINESS ADVISORS

6850 Austin Center Blvd., Suite 180
Austin, TX 78731

Phone: (512) 346-2086
Toll Free: (877) 977-6850
Fax: (512) 338-9883
Website: www.atchleycpas.com

Like us on Follow us on Find us on

Address Service Requested

For additional information or change of address, contact Atchley & Associates, LLP at (512) 346-2086.

MUSE

March/April 2017

Printed in the U.S.A.

NL-NT-ALL-NFP-0516