Williams Overman Pierce, LLP
Certified Public Accountants and Consultants

Summer 2018

An Introduction to Robotic Process Automation for Nonprofits

By Joe Sremack, CFE

Robotic process automation is helping both for-profit and nonprofit organizations do more with less. Robotic Process Automation (RPA) is transforming the way organizations across different industries do business. It allows organizations to automate certain types of work processes to reduce the time spent on costly manual tasks and increase efforts to deliver mission-critical work. RPA is helping organizations do more with less, helping them automatically process and store data without having to perform manual data entry, generate financial status reports without spending considerable amounts of time in Excel, and execute outreach campaigns without spending hours in a customer relationship manager (CRM) program. These types of optimizations have been made a reality through RPA, with organizations just beginning to scratch the surface of the possibilities.

RPA Defined

RPA is the use of software that automates manual tasks. It eliminates the need for employees to perform repetitive tasks by integrating software that performs the same set of steps the employee does. The software is designed to perform routine tasks across multiple applications and systems within an existing workflow. It performs specific tasks to automate the transfer, editing, reporting and/or saving of data.

At least some portion of white collar employees' time is spent on repetitive computer tasks. That includes the CEO's time–about 25 percent of the CEO's tasks could be automated and RPA can help achieve this. Repetitive work typically involves the collection of data from one or more sources, performing a data manipulation—such as applying data formulas in Excel—and then exporting or saving the information to a readily available location. These are just some of the kinds of work that RPA automates.

One of the main differentiators of RPA from other solutions is that it performs tasks that do not require deep cognitive capabilities. RPA is the automation of a process, but the software is not improved or changed based on the inputs or its results. This is different from machine learning or artificial intelligence (AI) software, which can learn and improve based on the continuous evaluation of its inputs and results. Instead, RPA software simply repetitively performs the same task(s) based on business requirements.

RPA provides several major benefits. The most immediate impact from RPA is that routine tasks are performed in an error-free, consistent manner. RPA also provides an audit trail of work performed, which can be valuable in regulated industries or when the output of a process produces an unexpected result. In addition, RPA solutions can be configured to identify anomalies or red flags that may not be identifiable to an employee.

The long-term benefits are also valuable. Perhaps the most important benefit is increased job satisfaction. When employees are asked which parts of their jobs they dislike the most, the tasks they list usually involve a type of manual work that is a good candidate for an RPA solution.[1] This increased job satisfaction results in a better work environment and more productive employees. Moreover, the results of the formerly manual processes become better and the cost savings can be recognized.

[1] *Gartner Research, "Role of Machine Learning in Accelerating Automation," 2016.*

Applications of RPA

The list of potential uses for RPA is robust. Most manual computer-based tasks performed by employees can be automated with RPA. RPA is often used for back office functions but can extend to customer relationship management, data analysis, and other key areas that involve manual work.

The best way to understand RPA is to learn about the kinds of problems RPA can solve. For example, an RPA program–called a "bot"–can be used to manage customer email inquiries. The bot monitors a sales inquiry email account and automatically imports the information into the CRM, sends alerts to the sales team, sends an automated message to the customer, and imports the information into other systems that are used to track employee availability and sales campaign successes. This works well when timely responses to customers are required.

An example of a nonprofit-specific use of an RPA solution is the management of fundraising campaigns. In many organizations, this process involves pulling past donor information, generating marketing materials, contacting past and new donors, collecting donor payment information, and entering it into an accounting software, updating financial information, and updating a donor database. Most of these steps are performed manually, slowing down the process and introducing the risk of error. With an RPA solution, most of this process can be automated, allowing the organization to spend more time interfacing with donors and working on other mission-critical tasks.

The following is a chart that lists several types of tasks that can be automated by department in most organizations:

HR	New employee forms	Employee termination documentation	Employee benefits
Finance / Accounting	AR/AP tracking	Financial reporting	Vendor management
IT	New user setup	Employee termination	Inventory tracking
Sales / Marketing	Email sales campaign management	Outreach campaigns	CRM automation
Others	Executive analysis reports	Regulatory compliance documentation	Inventory management

While the list above appears to be limited to single-department tasks, many of these are cross-department tasks in nature. Consider a process where the finance department needs to work with IT and sales to request multiple data sets, get input, and share the results. Rather than emailing those departments to pull the same data set every quarter to develop an Excel-based report, an RPA solution automatically performs the data pull and generates the entire Excel report. This not only saves time and effort across the various departments, it also enables the finance team to spend more time doing meaningful analysis of the reports and develop projections and deeper insights.

RPA and Nonprofits

RPA is well-suited for solving problems encountered by nonprofits since they face many of the same challenges associated with reducing the time employees spend on manual tasks as for-profit organizations. Whether the work involves manually entering accounts receivable and accounts payable data in accounting software, generating compliance reports, or performing outreach campaigns, time is being spent by employees on less valuable work. Employees would agree that they would rather work on mission-specific tasks rather than repetitive tasks.[2]

- Several examples of the types of nonprofit processes an RPA solution works well with are:
- Pledge campaigns.
- Recurring donation management.
- Digital and print marketing campaigns.
- Outreach campaigns.
- Government and regulatory issue tracking.
- Volunteer management.

Service providers and software developers have begun offering solutions geared toward nonprofits. Several major RPA software developers have recently launched commercial software solutions specifically designed for nonprofits, and service providers who understand the nonprofit sector are able to implement tailored RPA solutions.

Implementing RPA

RPA solutions can be implemented in several ways. The most common method for organizations is to implement individual bots. These are single programs that perform tasks automatically. The bot can be accessed through a desktop or web-based application. The second method is to implement a server that controls a set of bots within a department or across the organization. The server-based approach is a more robust system that is typically employed when there are a larger number of bots utilized throughout an organization that need to be managed centrally, whereas the individual bot method is appropriate when only several bots are used.

The cost of an RPA solution, a common concern for any organization, depends on these factors:

- Complexity.
- Number of bots.
- Time to develop and implement.
- Level of customization.

An enterprise-wide RPA solution of hundreds of bots can be expensive. A smaller implementation with only ten 10 bots or less, however, can be implemented relatively inexpensively and within a short period of time. Companies who sell RPA solutions often have a suite of pre-built bots that can be quickly customized and implemented without requiring a new bot to be developed. As the RPA market matures, the cost will continue to decline.

The key steps for determining whether an RPA solution is appropriate are to:

- Identify where most time and effort is being expended on manual tasks.
- Identify bottlenecks of key processes—specifically identifying manual tasks.
- Implement a pilot program to tackle a high-value discrete task that can have immediate value.

RPA is an exciting new way for organizations to improve their operations while also improving employee job satisfaction. RPA solutions have become a widely adopted strategy for enhancing various parts of organizations' operations by allowing employees to focus their time and efforts on more high-value and meaningful work. It has helped organizations do significantly more with less while reducing errors, increasing workforce job satisfaction, and better ensuring that deadlines are met. These benefits have been possible with relatively small capital investments and IT resources. While RPA is not applicable to all types of work, it is a good option for reducing hours spent on routine, manual tasks.

Benefits of RPA

- Error-free, consistent results
- Employees can be utilized for higher value work
- Increased job satisfaction (not spending time doing repetitive, low value work)
- Faster, more predictable delivery timing
- Documented trail of work performed
- Identify anomalies or other red flags

[2] *L. Willocks and M. Lacity, Service Automation: Robots and the Future of Work 2016, 2016.*

Pay Data for 'Similarly Qualified Persons in Comparable Positions at Similarly Situated Organizations' – *We've got that…don't we?*

By Michael Conover

Valid information on competitive pay levels and practices for "…similarly qualified persons in comparable positions at similarly situated organizations" has long been the basis for responsible management, and Internal Revenue Service (IRS) enforcement, of appropriate pay practices among all tax-exempt organizations.

When the IRS Intermediate Sanctions (Internal Revenue Code 4958) were enacted, the importance of good comparative data was underscored by its inclusion as one of the three elements of the protection offered in the Rebuttable Presumption of Reasonableness. The data provides a critical context for determining how much and how to pay a nonprofit's executives.

Regardless of its importance, however, many organizations fail to devote the attention to this important element of their compensation program that it deserves. We regularly work with organizations that have difficulty describing or producing the data used as the basis for executive pay decisions. References are made to "a report done a while ago," "a survey we had," or "some Form 990s from organizations like us." Examining the Form 990s and Schedule Js of these same organizations, we find they have checked all the appropriate boxes related to these data sources and yet there is little or nothing to be found.

Another group of organizations we find has a different competitive data issue. They have competitive data to offer as the basis of compensation decisions, but there are serious issues about the quality and comparability of the data being used. The data may be drawn from organizations that are not at all comparable, positions that are marginally similar or based on such a small sample that the data's validity is very questionable. In these situations, this poor data may be as bad, or possibly worse, than having no data at all because it may lead to problematic pay decisions.

Obtaining and properly using good data for compensation purposes requires some thoughtful examination of your organization, its positions, and the requirements for individuals holding those positions. Only after accurately understanding your own circumstances can a search

begin for the sources of valid data needed. Areas that need to be explored include:

- **Details of your organization:** This information includes the type of service(s) your organization performs as well as the broad organizational metrics that reflect its size and scope (e.g., revenue, operating budget, total assets, number of employees, etc.). These are usually among the factors most readily used for identifying similar organizations.
- **Primary role(s) of your position(s):** Competitive data sources (surveys, Form 990s, etc.) usually offer only brief descriptions of positions and generic titles for job-matching purposes so the focus here is on the central focus and impact of your position in terms of overall impact on the organization. The chief/principal executive officer and chief/principal financial officer positions tend to be very similar from one organization to another and are Disqualified Individuals from an Intermediate Sanctions perspective. Therefore, they are routinely included in competitive data needs. Ensure you note any significant difference in the role played by your position vs. the typical benchmark. The presence of an additional role not associated with the typical benchmark for the position (or the absence of some portion of the role commonly associated with it must be taken into account to ensure appropriate comparisons will be made.
- **Position requirements:** The emphasis on position ***requirements*** is intentional. The purpose is to focus on the essential education, expertise, and experience required to perform the role, not what the current

incumbent happens to have or acquired in the role. For example, the fact that the current receptionist has five years of experience at the front desk does not mean that five years is a requirement for a qualified incumbent. On the other hand, your position may require a type of professional certification, education, or experience that is unique and essential for successfully performing the role. For example, an individual holding the position of executive director in an association of athletic coaches and involved with external organizations regulating the conduct of the sport must have credible experience in the sport.

Armed with an accurate understanding of your own organization and the positions that will be examined in the competitive compensation assessment, attention now is focused on the identification of the data that will be sought for use in the analysis. The process follows the same criteria referenced above in the descriptors of your organization and positions, as follows:

- **Organizations selected for inclusion in the analysis:** Typically, these are organizations offering the same types of services that your organization provides. In some instances, there are other types of organizations, perhaps even for-profit ones that employ and compete for executive resources that are very similar to your specific organization. These can also be included in the search for competitive data. Compensation surveys are conducted among many different types of nonprofit organizations (e.g., higher education, social service organizations, professional/trade organizations, philanthropic foundations, etc.). In addition, Form 990 filings from other organizations like yours are also a source of competitive data. If necessary, a custom survey and/or consultant may be required to obtain data for specialized/hard-to-find sources of data.

The size and scope of organizations included in the analysis must be comparable to your organization. Revenue and budget levels for a group of organizations ranging from 50 percent to 200 percent of your size are typically viewed as reasonable for inclusion. Of course, care must be taken to avoid "skewing" the data in the direction of organizations much larger than your own.

I often explain the objective for identification of comparable organizations as comparing "apples to apples" but doesn't necessarily need to be as specific as comparing McIntosh to Fuji.

- **Selection of benchmark positions:** Positions selected for comparisons should closely resemble the role described in your organization. Titles alone may not fully describe a position's role or they may be misleading. A controller may be the chief/principal financial officer or a subordinate, depending on the data source in question. In those cases where a significant difference has been identified between your position and the external benchmark, it may be advisable to make adjustments (upward or downward) to competitive data to appropriately compare them.
- **Special position requirements:** Bona fide ***requirements*** for your organization's position that are not typically associated with the benchmark position may also require an adjustment to competitive data in order to produce an appropriate comparison.

Collecting this information about your organization and the external benchmarks planned for use prior to an analysis of competitive compensation is not the end of this process. Two critical steps remain. First, it is important to engage the organization's governing body (e.g., board, compensation committee) and involve them in a review of this information and affirmation/modification of it for use in the analysis. Involving the independent members of the organization in the process performs a very helpful educational role about compensation and the importance of good competitive data. It also enlists individuals with a critical oversight role in the governance of pay in an independent validation of the plan to secure the data before it is collected. A sound rationale has been prepared and ratified for the analysis of competitive data which board and management should view as valid for this purpose.

Second, this description of your organization and positions, as well as the external benchmark criteria or the comparative framework, should be documented. It will become part of the other important documents maintained to support the compensation program (e.g., board minutes, compensation strategy/guiding principles, etc.). The framework should be reviewed periodically and updated as needed to ensure its continued relevance to your organization as well as the external marketplace(s) in which you compete for executive resources.

Privacy Is a Must-Have These Days – Guide to Implementing a Holistic Privacy Program

By Karen Schuler, CFE, IGP, IGP and Taryn Crane, PMP

Notwithstanding the EU General Data Protection Regulation (GDPR)—the most sweeping change to data privacy in 20-plus years, with extraterritorial scope that went into effect on May 25, 2018—there are numerous privacy laws that are often overlooked.

Earlier this year companies like Facebook have come under fire for privacy violations while Congress is looking for ways to protect the privacy of American citizens. These movements are just the beginning of widespread change that we expect for privacy laws over the next several years.

As discussed in the Spring 2018 issue of the *Nonprofit Standard* in an article entitled "The Integration of Data Privacy into a Data Governance Program," nonprofits can't afford to ignore regulations like GDPR as many organizations are impacted due to their global reach. But now that May 25, 2018 has passed and GDPR officially went into effect, it's time to think about your holistic privacy program—or implementing a Privacy Operational Life Cycle that helps your organization keep employees apprised of new privacy requirements, embraces recordkeeping and sound data protection practices while offering enhanced data privacy for your donors, employees, and constituents.

Think about these areas to develop a sound Privacy Operational Life Cycle:

- Develop an organizational privacy vision and mission, and document the program's objectives.
- Identify legal and regulatory compliance challenges that are relevant to your organization.
- Locate and document where personal information resides throughout your organization or across third parties (e.g., hosting vendors, outsourced applications).
- Develop a privacy strategy that identifies stakeholders, leverages key functions throughout the organization, creates a process for interfacing within the organization, and outlines a data governance strategy.
- Conduct a privacy awareness workshop to highlight to the entire organization the goals of the program.

- And, finally, develop a structure for your privacy team with a governance model that is clear and consistent for the size of your organization.

The above-mentioned items are a starting point, but there is more to do after you develop your initial structure and communicate the purpose of the program. Below is a guide to developing the Privacy Operational Life Cycle.

Develop and Implement a Framework

The framework should provide you with an implementation road map that outlines your privacy procedures and processes. Developing a framework helps you identify high risk areas, reduce data loss, and provide a measurement against compliance to laws, regulations, and standards. Frameworks that provide initial guidance include the AICPA and CICA Privacy Framework, ISO 17779/BD7799, or OECD Privacy Guidelines.

Develop Privacy Policies

Once you have selected an overall framework to govern your privacy program, look at your existing policies, procedures, and guidelines. During this phase you should evaluate the goals of the privacy program and determine what business initiatives are the baseline of the privacy program. Just remember, as you look to update policies, procedures and guidelines for the organization, ensure that there is a mechanism to enforce these policies. And

don't forget to review the current website privacy notice. This has become a critical target of privacy watchdogs to ensure that you can fulfill the commitment of the statements in that notice.

Develop Mechanisms to Measure Performance

Within your privacy life cycle, it will be important to develop the ability to measure performance of the program. To implement metrics, consider your audience—will it be the board, external parties, regulatory agencies, or the staff? Determine how you will report on these metrics that you have identified. Decide what measurements you are interested in sharing with your audience and how this could impact funding positively or negatively. Next, determine how you will measure progress toward the organization's business goals and objectives. Do your best to limit improper metrics that do not support the organization's mission. And finally, determine the best methods to collect the data you need. Your goal is to demonstrate compliance while establishing the privacy program's return on investment (ROI).

Develop the Privacy Operational Life Cycle

The Privacy Operational Life Cycle should consider measurement, improvements, and the ability to sustain and support the program. To effectively do this, develop an operational life cycle that considers the assessment, protection, governance, and response phases. Some tips to consider for each aspect of the life cycle:

- **Assess –** embed Privacy by Design (PbD) into the design of technology, business practices, and physical design of new programs. In addition to PbD, regularly evaluate third-party compliance, as well as internal program compliance.
- **Protect –** ensure that information life cycle management (ILM) is built into your data protection strategy. While it is important to ensure that your data protection strategies mitigate the risk of a data breach, you need to consider sound ILM practices to promote the organization's data protection strategies. Remember, the less you have, the less you have to protect.
- **Govern –** while it's important to be able to evaluate and protect information, you also need to monitor, audit, and communicate the privacy framework. Develop a strategy and operational procedures that allow your organization to maintain a transparent and visibly sound program. And don't forget to monitor regulatory changes that impact your organization. Develop ongoing processes that allow you to measure the privacy program's effectiveness.
- **Respond –** traditionally privacy and security teams viewed their ability to respond as responding to a security event. Today that has changed – it's much broader and requires the ability to respond to complaints, requests for information, corrections of inaccurate data, clarifications of privacy matters and access requests. When developing your response capabilities, take into consideration these items in addition to your ability to respond to a security event.

Holistic privacy program development is the wave of the future, especially in a competitive world where data is at the core of every business or organization. Establish a program that fits your organization to ensure that you remain ahead of the curve and out of the sight of regulators.

Transportation Fringe Benefits Are Now UBI – Effective Jan. 1, 2018

By Laura Kalick, JD, LLM in Taxation

Does your tax-exempt organization provide transportation and parking benefits to employees? If so, you may have another commuter headache: a new tax. Under the Tax Cut and Jobs Act of 2017 (the Act), a provision was added to the Internal Revenue Code that is likely to require many tax-exempt organizations to pay unrelated business income tax (UBIT). Certain costs of qualified transportation, including transit passes, qualified parking and more, will now be taxed as unrelated business income at 21 percent.

The Act added the following provision to the Internal Revenue Code: **Internal Revenue Code (IRC) Section 512(a)(7): Increase in unrelated business taxable income by disallowed fringe.**

This provision was an attempt to put exempt organizations on the same footing as taxable organizations that will no longer be able to deduct these costs. The provision is effective for amounts paid or incurred after Dec. 31, 2017.

Under this provision, **certain qualified transportation fringe benefits, including those relating to parking garages, must be reported as unrelated business income (UBI).** All tax-exempt organizations (and a college or university owned and operated by a state or other governmental unit) will have to include as unrelated business taxable income any amounts paid or incurred for any qualified transportation fringe benefit, including the following:

- A ride in a commuter highway vehicle between the employee's home and workplace.
- A transit pass.
- Qualified parking.

Qualified parking is parking you provide to your employees on or near your business premises. It includes parking on or near the location from which your employees commute to work using mass transit, commuter highway vehicles, or carpools. If an organization has its own garage that is used for parking that is already reported as UBI (e.g., parking for the general public), then the percentage of those costs attributable to the amount already included in its UBI does not have to be included in the amount treated as UBI under the new provision.

The UBIT on these employer costs is 21 percent at the federal level and state taxes may apply as well. Organizations should consider making estimated tax payments on these taxes.

These employee fringe benefits are still excluded from an employee's income. Employers can generally exclude the value of transportation benefits provided to an employee during 2018 from the employee's wages up to the following limits:

- $260 per month for combined commuter highway vehicle transportation and transit passes.
- $260 per month for qualified parking.

See IRS Publication 15-b for more information.

Even if the benefit is provided under a compensation reduction agreement, the payment will still result in UBIT for the organization. The only way the organization can avoid counting these benefits as UBI is to have the employee pay for the benefits with after-tax dollars.

Compensation Reduction Agreement Example:

For 2018, the monthly limit on the amount that may be excluded from an employee's income for qualified parking benefits is $260. Commuter employees can receive both the transit and parking benefits up to $520 per month tax-free.

On a per employee basis, **for commuter and transit passes only,** $260 monthly is $3,120 annually, and the UBI tax on this amount at 21 percent is $655 plus state

taxes, if applicable. With 100 employees, the federal tax alone would be $655 per employee and approximately $65,500 in total. To the extent your organization provides a commuter benefit of up to $520 per month, the UBI tax can be much more.

Next Steps:

- Organizations should determine whether they provide these transportation and parking benefits, and if so, to how many employees, what kind and how much?
- Calculate the estimated tax payments for Federal UBI and the state, if applicable.
- If your organization has not filed Form 990-T in the past, enroll the organization in the Electronic Federal Tax Payment System in order to remit the taxes.

5 Suggestions to Perfect Your Audit Committee Charter

By Lewis Sharpstone, CPA

The quality and completeness of the audit committee charters that I have seen typically range from very good to great. This is why there is no mention in this article, other than here, of core audit committee responsibilities such as auditor appointment, audit review, monitoring of whistleblowing incidents, or conflicts of interest reporting. However, here are my top five suggestions that should be considered for strengthening even a great audit committee charter.

1. Incorporate All Your State Audit Committee Requirements Into the Charter

For example, under California law there are stated guidelines as to who can and cannot serve on the audit committee. The most well-known California rule is that no more than 50 percent of the audit committee can comprise finance committee members. Most California audit committee charters I see cover this rule. But many California audit committee charters I see don't include the lesser known but equally important rules. For example, in California the chair of the audit committee is also prohibited from serving on the finance committee. Make sure you know your state audit committee requirements, if any, and ensure that they are embedded into your charter.

2. Minutes of Meetings

Part VI, Section A, question 8 of IRS Form 990 reminds us that as a best practice, organizations should memorialize all board meetings with documented minutes. This also applies to all meetings of subcommittees of the board. The audit committee is a subcommittee of the board, so documented minutes should be produced for each meeting. Accordingly, this should be stated in the charter.

3. Executive Sessions

Most audit committees build into their charter the notion that they can hold executive sessions with specific parties. In almost all cases it is either written or implied that executive session means organization staff members are excused from the meeting and the audit committee meets alone with the external auditors or other parties. However, executive sessions can be much broader than this and should probably be defined as such. For example, since the responsibility of audit committees includes a broad understanding of risk, and since a significant risk facing any organization today is cybersecurity, it is probably appropriate for the audit committee to want to meet in executive session with the chief information officer.

4. The Authority to Independently Consult With and Retain Outside Legal Counsel

The audit committee should be collaborative most of the time but function objectively all the time. The authority of the audit committee to retain outside legal counsel, if needed, is recommended to be included in the charter. If the need arises, having this documented within the charter will be important to the audit committee in exercising its responsibilities. Conversely, it might prove almost impossible in certain circumstances for the audit committee to exercise its duties without this authority.

5. Self-Review

Self-review is a powerful and useful process if performed correctly and periodically. It provides an appropriate time and forum for members of a committee to voice suggestions to improve the effectiveness of the committee on which they serve. Certainly, the absence of an appropriate time and forum to voice these suggestions for improvement can lead to problems down the road. This is why embedding a periodic audit committee effectiveness self-review requirement and process into the charter is highly recommended. The audit committee charter should also be self-reviewed periodically.

---

10 Things Keeping Internal Audit Up at Night

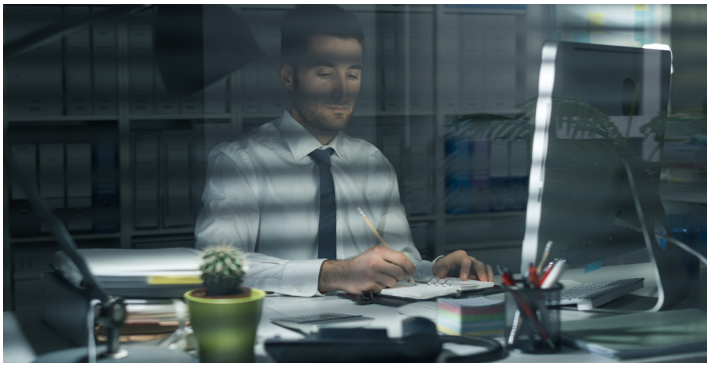
By Ken Eye and Andrea Wilson

The internal audit (IA) function is vital to the health of any nonprofit, regardless of mission or scope. The audit committee and its individual members are crucial partners in safeguarding the integrity, purpose and, ultimately, the success of organizations.

But, they often face challenges navigating a strained regulatory environment, all while trying to do more with less. Adjusting to these new realities means that proper management is more important than ever. This article outlines the top 10 challenges keeping internal auditors up at night, and providing remedies to help them continue their critical work.

1. Changes to Operations or Strategy

For most nonprofit organizations, change is inevitable. As the needs of communities, internal dynamics, priorities and leadership transform, nonprofits adjust their mission and strategies. While this dynamism is essential for organizations to further their work, change can create strain for internal auditors. Whether its expanding operations to a new location, working with new donors or rolling out a new organizational structure, internal auditors are often left scrambling to ensure compliance.



The Remedy: Change is unavoidable, but compliance headaches don't have to be. Nonprofits should be proactive about integrating internal audit into large scale organizational changes. This means allocating IA resources to evaluate emerging compliance and legal requirements, incorporating IA into the strategic decision-making process at the outset, revising policies and procedures with the new compliance environment, and developing succession plans to facilitate smooth personnel changes. And, IA should not just be involved in the change process—organizations should allow internal auditors to conduct post-implementation assessments to ensure ongoing compliance.

2. Organizational Culture

The organizational culture of nonprofit organizations usually centers on a mission that employees are passionate about. This passion attracts staff personally motivated to help the overall organization succeed, but can come at the cost of internal controls. For nonprofits, "the cause" can often be promoted at any cost. Mid-level management professionals can be highly skilled in technical areas, but may lack knowledge in compliance, financial accountability and oversight. A lack of interactive communication between key administrative and program units within the organization can result in insufficient internal controls.

The Remedy: To balance maintaining organizational culture with proper operational management, communication is essential. Nonprofits should develop a sound communication strategy that brings the internal audit and compliance functions in regular contact with the rest of the staff. During these interactions, IA professionals should be sure to communicate how risk management practices align with overall organizational strategy and mission objectives. Bringing people together in this way helps make IA an integral part of an organization, rather than an afterthought.

Even when strong communications are in place, breakdowns are sometimes inevitable. Organizations should conduct regular assessments of business processes to determine where breakdowns in communication between business units occur. These assessments should help identify gaps that could pose significant risks to the organization.

Based on the results of these assessments, organizations should design and implement remediation plans, including scheduling necessary trainings for all employees and rolling out new process flows and accountability points to close any gaps.

3. New Technology

Technological advances help organizations store and share data, but new technology is often implemented without the knowledge or involvement of the internal audit function, to potentially disastrous and costly results. Ideally, internal auditors should assess new technology well before it's utilized to review issues like control over sensitive data, continuity of the technologies between offices, and adherence to compliance and regulatory requirements. Without this review, nonprofits leave themselves open to a number of risky consequences, as well as operational inefficiencies.

The Remedy: Technology can be a huge boon to nonprofit organizations, but only when it's used wisely. IA should work with nonprofit leaders to first assess technology currently being used organization-wide, and then identify what the organization still needs to address. Internal auditors can assist with researching and proposing approved technologies for organization-wide usage, to facilitate cohesion and compliance and to help management improve system efficiencies.

Organizations also need to implement proper internal controls to ensure they're mitigating technology risk as much as possible. IA can conduct a risk assessment of each technology used and implement policies to restrict or prevent the use of high-risk programs or devices. Organizations should also require similar checks and risk assessments for all new technology prior to usage.

4. Cybersecurity

With new technologies exploding in popularity, cybersecurity risks abound. Nonprofit organizations often mistakenly believe they aren't of interest to cyber criminals, but the amount of personal data they store from donors and employees, and the tendency to underinvest in cybersecurity measures, make them an ideal target. It can be difficult for nonprofits to maintain up-to-date technology and hardware, keep pace with technological changes and navigate the shifting regulatory landscape with their limited funding. Nonprofits also frequently partner with technology suppliers and other contractors that leave them open to third-party cyber risks.

The Remedy: The first step to mitigating cyber risk is to conduct an organization-wide cybersecurity risk assessment that includes partner, contractor and technology supplier cybersecurity as part of the due diligence process. This assessment should shed light on where internal and external gaps exist. Following the assessment, organizations should implement

additional controls by updating policies, procedures and internal controls to address identified gaps.

A startling number of cyber incidents arise from employees unknowingly exposing the organization to bad actors. Training staff to recognize these exposures is fundamental to their prevention. Nonprofits need to regularly communicate risks to employees and vendors to ensure everyone is adhering to established policies.

Monitoring cyber risk needs to be an ongoing effort. Nonprofits should develop a risk assessment schedule to examine internal partner, contractor and technology supplier cybersecurity on a quarterly or annual basis. Internal audit can assist with implementing these assessments.

5. Compliance With Funder Requirements

Nonprofit organizations often have the unique challenge of negotiating compliance requirements across multiple funding sources including government entities, individuals, private foundations or other organizations. This challenge is only growing as budget cuts force organizations to focus on diversifying revenue streams and expanding donor pools, and with a recent increase in donor audits of specific grant activity at the materiality level. Further complicating the matter is a growing emphasis on international accounting standards (as opposed to relying on U.S. generally accepted accounting principles).

The Remedy: To clarify exactly what funding requirements an organization faces, it should conduct a compliance assessment, comparing requirements across all donor agreements to determine areas of overlap and areas of discontinuity. These agreements should then be compared against written policies and current practices to identify gaps.

Remediation plans can amend policies and procedures, and staff trainings should be conducted to ensure all levels and functions understand their role in maintaining compliance with funding requirements.

Staying current is critical. Nonprofits should develop a compliance assessment schedule, and IA and compliance departments need to stay on top of new funding streams and emerging trends so they can pivot when necessary.

6. Financial Controls

Even though nonprofits are motivated by making an impact rather than money, organizations still face a host of hurdles when it comes to financial management. Many international nonprofits operate in countries with cash-based economies, making it tough to maintain adequate control of funds and sufficient supporting documentation. And new payment technologies, while enabling new and widespread operational tools, are often accompanied by verification and other control challenges. Nonprofits also face resource constraints and may have a limited number of finance staff to oversee financial management processes, which can be manual and prone to human error. For organizations with several offices, branches often operate with little to no centralized oversight over their accounting and cash management procedures.

The Remedy: Nonprofits should review cash management procedures and evaluate typical expenditure cycles to identify potential risk areas across the entirety of an organization. Internal audit is central in assisting management in testing cash management controls.

- Organizations can then implement additional controls in keeping with best practices, like limiting cash handling or volume of cash transactions where possible. Nonprofit managers should consider investing in technologies and resources that limit high risk processes.

Standardizing procedures will help cut down on variance of practices between offices. All branches should centralize accounting and reporting procedures. At a minimum, each location should maintain copies of supporting documentation of all expenditures and financial reporting and should regularly review them with staff.

7. Reliance On Third Parties

Vendor actions can create extremely adverse consequences for nonprofit organizations. Concerns range from reputation damage to the vendor's illegal acts being attributed to the nonprofit organization. This risk applies to all types of organizational relationships with vendors and nonprofits, especially those administering federal grant programs given increased subrecipient monitoring and due diligence requirements.

Despite the risks, most nonprofits rely on partners or contractors for critical program functions. This makes it difficult to conduct due diligence reviews and monitoring activities, particularly when the partners/contractors are numerous, geographically dispersed or operating overseas. Partners are normally tasked with self-reporting, meaning frauds like ghost employee payments are easily hidden. Contractors also usually have access to organizational networks and information, creating an additional layer of risk.

The Remedy: Organizations should review current policies and procedures to ensure robust due diligence and monitoring processes are in place for all third-party relationships. This should include an assessment of partner/contractor access to project data, systems and networks, and the limitation of access where possible.

Nonprofits need to implement additional monitoring and verification processes, including:

- Conducting regular spot reviews or investigations of reported data
- Requiring partners and contractors to certify financial and programmatic assertions
- Verifying number of partner/contractor staff and salary payment amounts
- Conducting unannounced site visits
- Considering third-party verification systems

These processes should be re-evaluated on a regular basis to ensure their effectiveness.

8. Procurement Procedures

Nonprofit organizations rely heavily on non-competitive procurement processes due to several reasons. Often, procurement procedures, selection criteria and selection decisions are inadequately documented, leaving organizations unable to show that there was no bias in the selection process. Preferred vendor lists are rarely updated, and control of vendor solicitation, selection and site visits is often left with just a few individuals.

The Remedy: IA should review current procurement procedures against industry standards and donor requirements. They should also be transparent about their procurement policies including:

- Publicly announcing tenders as much as possible
- Updating vendor lists through open competition as frequently as possible
- Verifying vendors and prices through in-person or third-party checks
- Comparing bids against market prices
- Documenting criteria and selection procedures to bid samples with procurement files
- Ensuring procurement/selection committees are rotated on a regular basis

9. Transportation and Distribution

For organizations that distribute goods, inventory management and oversight can prove to be major sources of stress for internal auditors. Often, nonprofits have difficulties verifying receipt of goods or services by their intended beneficiary, and confirming the goods provided are in the same quality and quantity as what was purchased. Diversion, theft and product substitution are especially difficult to identify. Despite resource and capacity issues, recent increased scrutiny of internal controls and supply chain management means that organizations need to address these issues sooner rather than later.

The Remedy: To help combat issues in the distribution chain, organizations need to shore up monitoring procedures by:

- Establishing monitoring teams for critical points along the supply chain
- Implementing two-step or three-step verification procedures at each critical stage
- Hiring a third party to conduct site visits and monitor transportation and distribution
- Using technology to assist in tracking and monitoring, including unique identifiers on products for inventory and tracking purposes and requiring distributors to take time-stamped photos/videos of deliveries
- Another effective risk mitigation strategy is to communicate directly with beneficiaries. Organizations can hold pre-distribution meetings with communities to review any past issues or concerns. Detailed packing lists and/or photographs of parcel contents should be inside packages. Nonprofits can include in the contract clauses with distributors to withhold payments

to distributors until delivery is confirmed. This further ensures the distributor is holding up its end of the agreement.

10. Fraud and Corruption

It's the job of the internal audit function to uncover fraud, waste and abuse in nonprofit organizations, but often they are set up for failure. Due to a lack of communication between functional and program units within organizations, increased used of third parties, outdated systems, increased regulations (and the list goes on…), the opportunity to exploit a nonprofit's controls is growing at a time when IA resources are shrinking and reputational risk for organizations is at an all-time high.

The Remedy: Preventing fraud starts within an organization itself. Stakeholders should evaluate current fraud prevention, detection and investigation measures against regulatory requirements and develop a plan to remediate any identified gaps. They should also be sure to provide accessible fraud reporting mechanisms for all employees, partners, grantees/beneficiaries and stakeholders.

- Despite resource constraints, organizations need to ensure IA has the appropriate level of resources to detect and investigate potential cases of fraud. Funds should also be set aside for visits to third parties and office locations and the establishment of a fraud hotline. Put a process in place to notify any impacted funders in a timely manner and in line with donor requirements to prevent exacerbating the impact when fraud does occur.

It's also key to establish a fraud prevention and detection assessment schedule so practices can stay up-to-date and make sure nothing falls through the cracks.

Internal auditors at nonprofits have a tough, but essential job that's key to keeping the organization focused on mission fulfillment. By assessing current practices, developing action plans and regularly monitoring activities, organizations can mitigate risk and serve their beneficiaries more effectively.

Article reprinted from the *BDO Nonprofit Standard* blog.

Podcast: 7 Steps to Revenue Recognition Readiness

By Lee Klumpp, CPA, CGMA and Carla DeMartini, CPA

The Financial Accounting Standards Board's (FASB) new revenue recognition standard (ASC 606) is a significant change that affects nonprofits of all types and sizes. While the deadline for public companies has already passed, many nonprofits and private companies have until Jan. 1, 2019 to implement the new standard. Meanwhile, entities with a June 30, 2018 year-end have until July 1, 2019.

What prompted the new guidelines, and how can nonprofits prepare? We had the opportunity to answer these questions in a recent *New York Nonprofit (NPN) Media* podcast with Aimee Simpierre.

Please see a summary of the podcast's top questions and answers below.

What prompted the FASB to issue the new revenue recognition standard?

There are two main reasons the FASB would issue an accounting standard update (ASU). The first is to address diversity in practice and standardize common

practices. Why, for example, would one nonprofit that was awarded a contract mark it as a contribution, while another in the same situation mark it as an exchange or reciprocal transaction? Through the ASU, the FASB addresses such differences. The second reason is to keep up with the times. For example, the FASB recently issued an ASU on cloud computing, which would have been an alien concept 30 years ago.

ASC 606 was born out of the FASB and the International Accounting Standards Board's (IASB) desire to converge multiple accounting standards. One of the biggest areas where the U.S. generally accepted accounting principles (U.S. GAAP) was different from those of other countries was revenue. In the U.S., revenue recognition principles varied widely by industry sector. The new standard is meant to help organizations around the world and across industries recognize revenue in the same way, barring a few exceptions.

How will organizations need to shift their accounting practices to accommodate the new standard?

The new standard prompted many organizations to switch from a risk and rewards-based model to a control-based model when it comes to dealing with contracts with a customer, or a relationship where there's a reciprocal transaction. Basically, organizations are recognizing revenue when they earn it, which is usually when they transfer control.

For example, let's say you went to Starbucks, and you ordered a cup of coffee. When will Starbucks recognize the revenue? When you get the cup of coffee, and they get $5—in other words, when both parties are satisfied and receive something of reciprocal value.

Many nonprofits have fee-for-service contracts, in which they're getting a fee from the government in return for the services performed. Under the new standard, they're going to have to look at each contract and fee, and determine whether each one is an exchange transaction, contribution or both. Nonprofits will need to use judgment in assessing all these different components. When they're coming up with the estimates, they will need documentation to support those estimates.

How can nonprofits prepare for revenue recognition?

Nonprofits should start early and be as proactive as possible so that there are no surprises when the ASC 606 deadline comes.

We recommend a seven-step model to readiness:

1. **Become familiar with the standard.** The 700-page standard may seem daunting, but reading the summary is a great starting point for nonprofit board members and management, in addition to working with an independent accountant.
2. **Take inventory of all your current revenue streams.** Nonprofits often have several different types of revenue streams, even within one organization. They should walk each stream through the five-step model in ASC 606.
3. **Identify any differences between your organization's current practices and the new standard for each contract.**
4. **Review how your revenue is currently being recorded**. Determine if it's going to be recorded over time or at a point in time.
5. **See if any additional resources are needed,** including personnel, systems and internal controls.
6. **Determine how your disclosure requirements may need to change.**
7. **Prepare mock-up financial statements.** These will help you assess the standard's impact.

Board members should also become familiar with the standard and management's plans to implement it. While some nonprofits may discover that their reporting still looks the same under the new standard, it's important they go through all the steps to ensure they are in compliance.

Listen to the original *NYN Media* podcast here.

For more information on nonprofit financial reporting, visit our resource center.

Article reprinted from the *BDO Nonprofit Standard* blog.