Nonprofit Observer

SPRING 2022

WW&D WHEELER WOLFENDEN DWARES

CERTIFIED PUBLIC ACCOUNTANTS

4550 New Linden Hill Road • Suite 201 • Wilmington, DE 19808 • (302) 254-8240
17577 Nassau Commons Blvd. • Suite 204 • Lewes, DE 19958 • (302) 360-2040

WEBSITE
www.wwd-cpa.com

4 tips for rebuilding your operating reserves

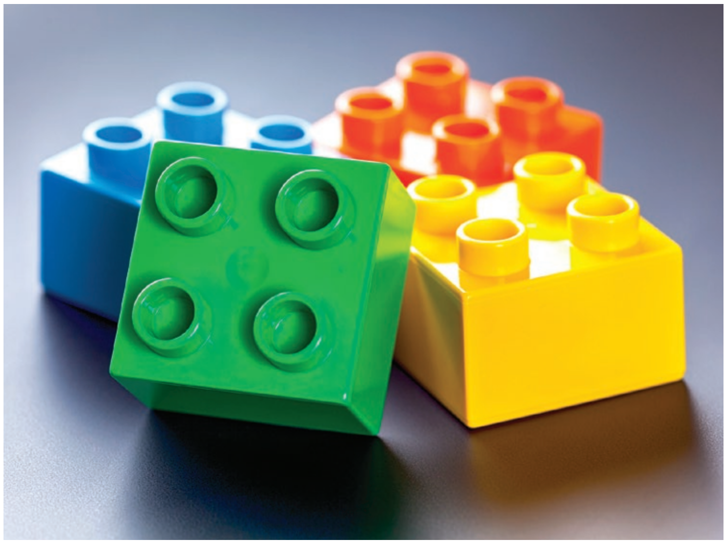
The COVID-19 pandemic has driven home many lessons for nonprofits, perhaps none so much as the importance of operating reserves. If your nonprofit is among those organizations with dramatically depleted — or nonexistent — reserves, here are some steps you can take to remedy the situation.

1. Achieve buy-in.

It sometimes can be difficult to win support from leadership for allocating funds to build reserves that could be used for programming, especially when the demand for services is high. You might need to communicate with your board and other stakeholders about why operating reserves are essential.

Perhaps they're already familiar with general arguments in favor of reserves. Strong reserves can empower an organization to take advantage of sudden opportunities or weather unexpected storms. If that's not enough to convince your audience, you may want to delve into the short- and long-term risks your organization faces.

For example, maybe your nonprofit is heavily reliant on a handful of funding sources that, if cut off or reduced, would jeopardize its future. On their own, individual risks may have a low probability, but, when aggregated, the wisdom of operating reserves should become more apparent.



2. Commit (or recommit) to a formal policy.

If your organization doesn't already have a formal written reserves policy, now is the time to develop one. And, if it does, review it to see how it holds up in light of two tumultuous and unpredictable years (with the possibility of more to come).

Among other things, your reserve policy should set the target amount to hold in a separate fund. Although no universal benchmark applies to every nonprofit, a common rule of thumb is to set aside six months of operating expenses. Your leadership's risk appetite and your current financial position may dictate a lower or higher target. Avoid setting the target too high, though. Stakeholders generally don't favor "stockpiling" of funds that could otherwise be used to pursue your mission.

The policy also should establish "triggers" for when your organization can dip into the fund. Note that triggers that made sense in earlier years may require adjustment at this point.

3. Develop a funding plan.

Assuming your current reserve level falls below the target, develop a plan for getting it back on track. Some organizations have reported increased donations over the past two years, which could allow them to fully fund their reserves with unrestricted net assets. Others use large bequests or unexpected windfalls.

NONPROFITS ARE GETTING THE MESSAGE

A recent survey from BDO, a tax, consulting and advisory firm, suggests that nonprofit organizations have begun to prioritize operating reserves more than they have in the past. The survey defined operating reserves as liquid, unrestricted net assets not needed for current operations.

"Nonprofit Standards: A Benchmarking Survey," conducted in June 2021, found that the number of nonprofits reporting at least four to six months of reserves ticked up, from 24% in 2020 to 28%. Organizations with more than 12 months of reserves jumped from 27% to 38%. Only 1% of nonprofits indicated they have no reserves.

Interestingly, those nonprofits with budgets under $25 million, so-called "mid-range organizations," seem to have better liquidity than their larger counterparts. For example, 33% have reserves equal to four to six months of expenses and 42% have them for more than 12 months of expenses. By contrast, only 27% of organizations with budgets greater than $75 million have reserves for at least four to six months of expenses and 26% of them have reserves for more than a year of expenses.

Most organizations, however, need to include a line item for contributions to the reserves in their budgets. This amount shouldn't hinder day-to-day operations, but it will help you begin to make real progress toward your reserves goal. It may be necessary to cut expenses, cancel projects or divest investments to free up funds. You might need to eliminate, or at least delay, projects that aren't helping your organization's mission or simply come with too high a price tag for now.

> *Strong reserves can empower an organization to take advantage of sudden opportunities or weather unexpected storms.*

Remember to leave illiquid fixed assets (buildings and equipment), endowments and temporarily restricted funds out of the equation. Similarly, budget surpluses aren't necessarily available to fund reserves, as they might include funds already earmarked for future expenses.

4. Be realistic.

Building or replenishing operating reserves takes time and your stakeholders must understand that it's an ongoing, long-term project. You're typically looking at a timeline of several years to build months of reserves, and that's if everything goes according to plan. Unfortunately, the pandemic has taught us that you may need to dip into the reserves with little warning, setting back your efforts.

That's one reason why it makes sense to set quarterly or even annual goals, rather than monthly. It gives you greater flexibility to adjust for changed circumstances, whether it's the traditional ebb and flow of donations over the year or crises like the pandemic. Quarterly or annual goals also reduce the risk of frustrations that can erode commitment.

Time to step up

As the economy moves into some type of new normal, guiding your organization's financial health will be crucial. If you have questions about how to build and replenish your nonprofit's reserves, give us a call. ●

Internet phishing schemes

How to protect your nonprofit from cyberattacks

The COVID-19 pandemic has resulted in numerous risks for nonprofit organizations. In addition to health-related risks and financial challenges, the pandemic has intensified the threat of cyberattacks. Hackers have grown more sophisticated in recent years. They often target nonprofits because charities hold confidential donor data but may fail to safeguard such data.

And the cost of a cyberattack can be steep. According to the IBM Security "2021 Cost of a Data Breach Report," breaches initiated through phishing schemes had an average total cost of more than $4.65 million per incident. You owe it to your stakeholders to stay current on hacking threats and do what's necessary to secure your systems.

What's phishing?

Most attacks are made via phishing schemes, where cybercriminals dupe victims into providing personal information (including login credentials). Phishing emails generally include links or attachments that, when clicked, infect computers with malware that enables fraudsters to unlock your systems.

For example, someone on your staff might receive an email with a link to a "spoof" (a fake site that looks like that of a reputable company) of a legitimate document-sharing site, such as Dropbox or Office 365. Once the criminals obtain that employee's login information, they'll have access to all of the information stored on the staffer's computer, as well as access to your nonprofit's network. This can include donor data, accounting records and HR information about employees.

Increasingly, cybercriminals are using phishing emails to perpetrate ransomware attacks. They gain control of an organization's network and data and lock legitimate users out. They then hold the data hostage until the victim organization pays a ransom. The criminals might leak some confidential information to the public or on the "dark web" to show they're serious and to encourage quick payment. Most ransomware perpetrators release the data after they receive a ransom — but not always.

What prevention training can be done?

Don't think that nonprofits are immune from cyberattacks, including ransomware demands. Criminals have hacked everything from government agencies to hospitals to large charities, so it's critical that you act defensively and provide training to *all* staffers. Training should cover various phishing schemes and include testing so employees can see how easy it is to fall prey to scams.

Red flags of phishing include messages with a sense of urgency, such as a subject line that says, "Are you available right now?" Or subject lines might include references to upcoming meeting agendas, job applications, payroll questions and password verifications. Still others may reference important messages from HR regarding vacation or COVID-19 policies.

In addition, phishing messages frequently are peppered with bad grammar and misspelled words. They may use numbers and special characters that look like letters to dodge anti-phishing software. And, of course, they usually include URLs that are close, but not identical, to the addresses of real company sites.

Are there other security steps?

To fend off cyberattacks, your organization should consider using password managers. A surprising number of employees still use easily hacked passwords such as 1234 and PASSWORD. Password managers generate much more complex passwords and store them for users. At the very least, require employees to come up with complex passwords and change them frequently.

Two-factor authentication — which requires users to log in normally *and* confirm their identity via text or phone — is also advisable. And be sure to implement hardware and software updates on a timely basis. Finally, stop using programs that are no longer supported by their makers.

Ask for help

Staying on top of your cybersecurity takes effort. We can help you take the next steps. ●

Changes are coming to your auditor's report

The American Institute of Certified Public Accountants (AICPA) Auditing Standards Board's latest standards are kicking in, and many nonprofits will notice resulting changes to the format and content of auditor reports on their organizations' financial statements. The updates are intended to make auditor reports more meaningful and transparent for the users of financial statements, including potential funding sources.

The new rules generally are effective for audits of financial statements covering periods ending on or after December 15, 2021. Here's what you need to know about some of the changes most likely to matter to nonprofits.

Your auditor's opinion

The Opinion section of an auditor's report states whether an organization's financial statements are reliable. It's generally regarded by users as the most critical component of the report.

In the past, the auditor's opinion didn't have a prominent position in the report. Now, it must be placed at the beginning of the report. Also, the opinion will now be immediately followed by the Basis for Opinion section. Previously, this section was included only in reports with modified opinions. Now it's required for all auditor reports.

Key audit matters

Perhaps one of the most significant changes to the report is the introduction of optional key audit matters (KAMs). KAMs are similar to the "critical audit matters" that auditors must include in their reports on audits of public companies. The AICPA standards define them as those matters that, in the auditor's professional judgment, were of most significance in the audit of the financial statements of the current period. They're selected from matters communicated with those charged with governance (typically, the board of directors or the audit committee).

KAMs generally require significant auditor attention. For example, they include:

- Areas with a higher assessed risk of material misstatement,
- Areas involving significant management judgment (for example, accounting estimates or the information included in disclosures), and
- Significant events or transactions during the period.

Note, though, that KAMs are addressed in the context of the audit of the financial statements as a whole and in forming the auditor's opinion about the reliability of the financial statements. The auditor won't provide a separate opinion on these matters.

KAM designations

As noted above, KAMs are optional. Your nonprofit's leadership and your auditor should discuss in advance whether to include KAMs in the auditor's report or if the auditor should simply provide a standard report.

The new standard addresses how the KAMs must be reported. Specifically, for each KAM, the auditor should describe the primary reason for the KAM designation, how the KAM was addressed in the audit, and the financial statement accounts or disclosures related to the KAM. This will produce a more customized report, which your users of financial statements may favor over the boilerplate reports they've often seen in the past.

At first glance, your organization might find it preferable to skip the KAMs, but you may want to opt in. Including them won't change the auditor's opinion, and it might even give you a competitive advantage when pursuing grants and other funding. In time, funders may come to expect KAMs in auditor reports. It might be a good idea to get ahead of the curve now.

Next steps

The new standards mean that you should expect revisions to your auditor's standard engagement letter. Among other things, this letter should expressly address whether the auditor's report includes KAMs. Contact us to learn if reporting KAMs in your next audit opinion is right for your organization. ●

News for Nonprofits

Support for female causes growing slowly

While women's and girls' organizations have seen some gains in recent years, a new report from the Lilly Family School of Philanthropy at Indiana University finds they still account for a small percentage of giving. According to "The Women & Girls Index: Measuring Giving to Women's And Girls' Causes," such organizations made up 3.5% of registered charitable organizations in 2018 (the latest year with available data) but received only 1.9% of giving.

Yet women's and girls' organizations matured more quickly than other organizations from 2014 to 2018 in terms of financial measures like revenue and expenses. They also saw strong growth (6% overall) in philanthropic support from 2017 to 2018, especially those organizations focused on the environment (37.1%) and civil rights and advocacy (32.3%). But their assets are growing at a slower rate, suggesting gaps in long-term financing.

Do your employees qualify for loan forgiveness?

The U.S. Department of Education (DOE) is revamping the Public Service Loan Forgiveness (PSLF) Program, which cancels loans after 10 years of public service by eligible borrowers. Among other things, the DOE is providing a temporary opportunity (through October 31, 2022) for borrowers to get credit for payments they've made that wouldn't otherwise count toward PSLF. Any prior payments made while working for a qualifying employer will count as a qualifying payment, regardless of loan type or repayment plan. The DOE says this change will be particularly important for borrowers through the Federal Family Education Loan Program, many of whom received inaccurate information from their servicers about PSLF. The waiver also includes borrowers with Direct Loans, those who have consolidated their loans into the Direct Loan Program and those with other types of federal student loans who apply to consolidate while the waiver is in effect.

Microsoft bolsters nonprofits' cyber defenses

Software giant Microsoft recently launched its Security Program for Nonprofits, a set of robust security offerings. Nonprofits are often perceived as vulnerable because they may not have adequate resources to safeguard the data they need to operate. Microsoft's "2021 Digital Defense Report" found that non-governmental organizations and think tanks were the second most targeted sector by cybercriminals (government was the most targeted).

Microsoft plans to support 10,000 organizations in the program's first year, with a three-year goal of providing these services to 50,000 organizations worldwide. The program includes free threat notification in certain circumstances. It also offers security assessments of existing endpoints, identity access, infrastructure, network and data. Microsoft plans to provide no-cost access to some of the top recommended training for both IT staff and end-users. Employees can learn, for example, the latest strategies to protect themselves from online scams and work from home more securely.

This publication is distributed with the understanding that the author, publisher and distributor are not rendering legal, accounting or other professional advice or opinions on specific facts or matters, and, accordingly, assume no liability whatsoever in connection with its use. ©2022

WW&D WHEELER WOLFENDEN DWARES

CERTIFIED PUBLIC ACCOUNTANTS

4550 New Linden Hill Road
Suite 201 • Linden Park
Wilmington, DE 19808

INSIDE PUBLIC ACCOUNTING BEST OF THE BEST FIRMS 2020

Helping you make a difference by going beyond the numbers

Your nonprofit organization faces the challenge of raising the funds you need to fulfill your mission, while navigating the often-complicated landscape of financial reporting and government regulations. You need a partner who will collaborate with your leaders to help you efficiently use your financial resources.

WW&D's accounting and auditing services go beyond the required financial audit, review or compilation to help you make better business decisions. As your advisor, we work with your team to leverage your financial information to increase efficiency and impact. We carefully review your data, make recommendations for improvements, and help you look ahead with projections and forecasts. In addition, there may be times when you need an independent professional to clarify an issue or confirm a process; our firm can help through an agreed-upon procedures engagement.

Our diverse nonprofit clients include independent schools, human service providers, churches, professional/trade associations and economic development organizations.

Please call us at (302) 254-8240 to discuss how we can serve you and your organization.

WW&D is an active member of
Delaware Alliance for Nonprofit Advancement
AICPA Government Audit Quality Center