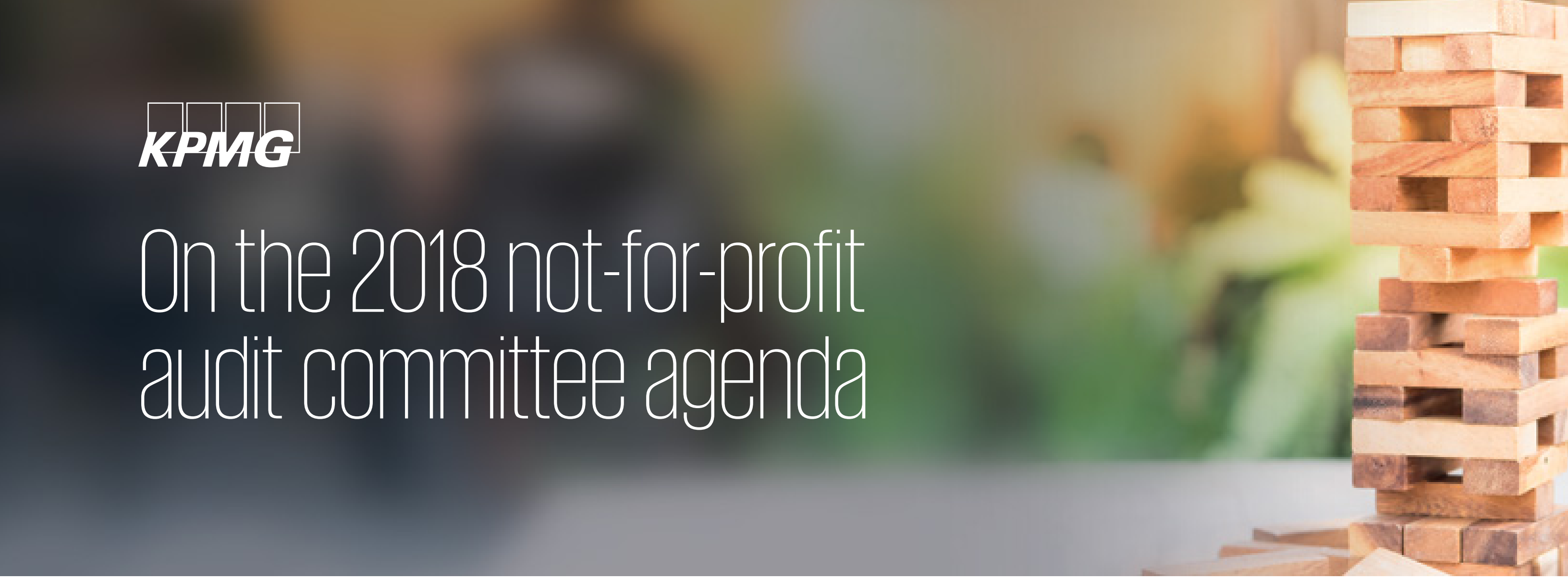

KPMG

On the 2018 not-for-profit audit committee agenda

Financial reporting, internal control, risk, and compliance oversight will continue to be put to the test in 2018. Focused, yet flexible agendas—exercising judgment about what does and does not belong on the committee's agenda and when to take deep dives—will be critical. Drawing on insights from our recent survey work as well as interactions over the last year with audit committees and senior management of not-for-profit organizations, we have highlighted several areas under two banners—core responsibilities and enterprise risk management—that audit committees should keep in mind as they consider and carry out their 2018 agendas.

Core responsibilities: Financial reporting, internal control, and external/internal auditors

Management is responsible for the preparation of the organization's financial statements and related disclosures, as well as maintaining effective internal controls. That said, the experience, skills, and leadership of board members can provide real value in terms of effective oversight.

With respect to its review of the annual audited financial statements, the audit committee should be satisfied that they are consistent with information known to committee members and convey well the organization's financial story. That story may be expanded upon in an annual report or MD&A, or conveyed in the Form 990 and within Web site content. Management should seek consistency in the messages across those venues. The financial reporting risk associated with those areas where management may need to make difficult judgments and estimates require a disciplined, robust, and unbiased process. The audit committee should understand management's framework and related controls and ask for the independent auditor's views.

There should also be robust discussion with respect to significant and unusual transactions as well as material related-party transactions. Tap the external auditor's industry-specific expertise as well as experience in dealing with different business transactions and arrangements to help put issues into context.

The audit committee's oversight over internal control, including fraud prevention and detection controls, relies upon management's representations and the auditors' recommendations. The committee should help ensure that management is setting the appropriate tone in communicating the importance of internal control. The committee should also consider the integrity, ethical values, and competence of employees, as well as the appropriateness of assigned levels of authorities and responsibilities. Changes to internal controls that may result from technology-driven or other business transformation activities should also be monitored.

Because external and internal auditors play a vital role in the financial reporting process, effective oversight of auditors is at the core of the audit committee's responsibilities. Audit committee effectiveness is enhanced when a good working relationship between the audit committee chair and the lead audit engagement partner is developed. From walking together through the agenda and pre-meeting materials to discussing important developments on a real-time basis, informal conversations represent time well spent.

For those organizations with an internal audit function, audit committees typically review the internal audit plan and results. Is the audit plan risk-based and flexible, and does it adjust to changing business and risk conditions? Is collaboration between the internal and external auditors maximized? Are advisory services, if any, provided by internal audit to other departments clearly distinguished from traditional audit responsibilities and are appropriate safeguards in place? Does internal audit have the skills, resources, and stature—and a direct line to the audit committee—to ensure that its voice is heard and valued? The challenge for the audit committee is to establish a relationship that helps the head of internal audit and internal audit staff operate effectively in their dual management/monitoring role.

In our annual audit committee agenda publications since 2014, we have discussed major financial reporting and accounting changes on the horizon. We have covered important aspects of FASB's Accounting Standards Update (ASU) 2016-14, *Presentation of Financial Statements of Not-for-Profit Entities;* ASU 2016-02, *Leases;* and ASU 2014-09, *Revenue From Contracts with Customers.*

Developments relative to these updates since the issuance of our 2017 paper include the early adoption of the *Presentation* standard (effective no later than for fiscal 2019) by a handful of NFPs in their most recently issued financial statements, with more early adopters expected for calendar 2017 and fiscal 2018 statements. As anticipated, the quantitative and qualitative disclosures with respect to liquidity and availability were among the most demanding aspects of implementation. Generally, early adopters found that implementation did not require accounting system or chart of account changes.

The adoption of the *Presentation* standard provides opportunity to consider other areas where financial statements and/or disclosures might be modified to better tell an organization's financial story. For example, the *Presentation* standard requires all NFPs to present expenses by functional category (which is currently the only required information for all except voluntary health and welfare organizations) and natural classification, typically in matrix format. This information may be presented either in the statements or as footnote disclosure. With respect to functional categories, GAAP requires information with respect to "major classes of program services and supporting activities." Is reporting by function limited to those programs that are significant to the organization? If too many programs are identified, important information may be obscured or readers may question whether "mission creep" has occurred. Organizations should consider whether certain separately reported programs are in fact part of the same major class. The matrix reporting of expenses by both function and nature in one location provides options to preparers when choosing how to report expenses in the statement of activities, e.g., by function or nature. Ultimately, the new matrix should be built for the long-haul: it should include components that are well-defined, including any necessary narrative disclosure, utilizing a consistent methodology that facilitates understanding by the board and management of activities and trends over time.

In response to questions with respect to revenue recognition of grants and contracts, in August 2017, FASB issued a proposed ASU, *Not-for-Profit Entities: Clarifying the Scope and the Accounting Guidance for Contributions Received and Contributions Made*. Per FASB, this proposed ASU would "provide a more robust framework to determine whether a transaction should be accounted for as a contribution or as an exchange transaction... whether a contribution is conditional or unconditional, and better distinguish a donor-imposed condition from a donor-imposed restriction." FASB intends to further deliberate and issue a final ASU in mid-2018 with the same effective dates as the *Revenue* standard, although a one year deferral will be extended to resource providers with respect to contributions made.

FASB's activity with respect to the *Leases* standard over the last year has been intended principally to ease implementation for financial statement preparers. That said, the move of most lessees' obligations from footnote disclosure onto balance sheets—grossing up assets and liabilities and making leases more prominent—will occur when the standard is effective for years beginning after December 15, 2019 for most NFPs.

For those NFPs with public debt, the effective dates of the *Revenue* and *Leases* standards are one year earlier than indicated above.

The results of a blind third-party survey of 150 companies for whom the *Leases* standard will be effective in 2019 were published in KPMG's *Reality Check* in February 2018. In the survey, KPMG found that only 15 percent of the respondents had completed their implementation work. In addition to assessing the impact well before the effective date, NFPs may view the adoption of the new lease standard as an opportunity to enhance processes to ensure all significant lease obligations are recognized and calculated properly, as well as to amend financial debt covenants that may be impacted.

Enterprise risk management (ERM)

One of the more recent published looks at the state of ERM among not-for-profit organizations is included in the 9th Edition of *The State of Risk Oversight: An Overview of Enterprise Risk Management Practices*, released in March 2018 by the AICPA and NC State's Enterprise

Risk Management Initiative. Noteworthy findings with respect to the more than 100 NFP respondents include (i) 67 percent reported having a complete or partial formal ERM process in place, with another 11 percent reporting plans to implement one; (ii) the audit committee continues to play a leading role, with 54 percent of respondents reporting that risk oversight responsibility is delegated there when the board formally assigns such responsibility; and (iii) 57 percent noted formally reporting top risk exposures to the board at least annually, with only 43 percent indicating that the board reviews and discusses those risks (by contrast, these percentages were 89 percent and 75 percent, respectively, for public companies).

Our own experience is that a large majority of organizations have assigned responsibility for oversight of risk management *processes* to the audit committee. Among the questions to be addressed in the oversight role are: How rigorous are management's processes to identify and assess risks, including emerging risks, to the organization? Who is involved and who is championing management's effort? How far down in the organization does it go? Is there a good understanding of the risks inherent in the organization's strategy and a process in place to monitor changes in the environment that might alter key assumptions? And, in organizations with the function, does internal audit provide added assurance regarding the adequacy of risk management systems? Oversight of individual risks is generally assigned to other board committees (for example, management of donor-related risks may be overseen by the Development or Fundraising Committee), although certain risks such as compliance with laws and regulations and cybersecurity are frequently deemed to be within the purview of the audit committee. When delegation of specific risks to committees occurs, the audit committee should address these additional questions: How effective are we and other committees in coordinating and communicating risk oversight activities? Does the full board understand the nature of committee-based oversight activities and the top risk areas?

It is the responsibility of management, with the oversight of the board, to ensure that the organization's operations are conducted in accordance with the provisions of laws and regulations. Noncompliance may result in fines, litigation, or other consequences that could have a material effect on the financial statements or damage the organization's brand. The sheer number and breadth of the legal and regulatory requirements confronting NFPs, including those pertaining to international activities, makes compliance a challenge for management and the board as well. Board members should seek to stay informed about the regulatory environment and changes thereto. Management (including general counsel, HR, and compliance officers) as well as outside counsel and independent auditors are often the principal providers of such education. The new tax law is an example of regulatory action that has the potential to impact financial results, related policies and internal controls, and much more. While the final version of the tax law did not include several of the most alarming elements of the House proposal, there is much to be concerned about. NFPs are uncertain about the impact on contributions of both the near doubling of the standard deduction and the doubling of the exemption level (and ultimate repeal) of the estate tax. This uncertainty may challenge organizations' ability to project 2018 results. Other provisions, including those associated with unrelated business income, executive compensation, and advance refunding bonds, may also impact operations.

In last year's audit committee agenda paper, we devoted considerable attention to cybersecurity risk and continue to see organizations include this risk among their most significant because of the potential to disrupt operations, be financially painful, and threaten reputation. As of this writing, the National Council of Nonprofits' Web site includes discussion of cybersecurity in which it warns that for NFPs engaged in (i) processing donations or event registrations, (ii) storing and/or transfer of personally identifiable information, or (iii) collecting information on preferences and habits of donors or others, "it's time to get serious about taking steps to address cybersecurity risks."

In late 2017, Microsoft released *Nonprofit Guidelines for Cybersecurity and Privacy*, in which they state, "Nonprofits often lack the budget, staffing resources, or management time needed to implement cybersecurity and privacy protections effectively… even large nonprofits with dedicated IT staff have a significant amount of work to do to bring their cybersecurity and privacy practices up to date." This paper was informed in part by a survey of 50 nonprofit organizations (14 small, 6 medium-size, and 30 large) in which "62 percent of respondents reported they did not have, or were unaware of, policies that clearly identify personal data (whether of staff, beneficiaries, or donors) among the other data the nonprofit collects…74 percent reported that they did not use multifactor authentication to access agency e-mails and other business accounts…and 92 percent stated their staff could access organizational e-mails and files using their personal devices." Microsoft recommends that NFPs implement the following cybersecurity controls as soon as practicable: create backups of all data regularly, timely update software and hardware, implement multifactor authentication, use virtual private networks for remote access, allow mobile access only to specific applications on a network that employees need to do their jobs, and enable endpoint protection. With respect to privacy, Microsoft suggests a few basic steps including determining when and for what purposes personal data is collected and stored; identifying applicable data protection laws and assessing their requirements; and adopting appropriate policies, procedures, and organizational safeguards for data.

The National Association of Corporate Directors (NACD) *Director's Handbook on Cyber-Risk Oversight* notes that "directors don't need to be technologists or cyber experts to play an effective role in cyber-risk oversight…. Ask questions such as: What are our organization's most critical data assets? Where are they located? Who has access? How are they protected?"

We believe that not only is cyber risk not going away, it is growing more sophisticated and aggressive. Is the audit committee getting the information/reports it needs to oversee cybersecurity efforts? Is there a C-suite executive who can effectively communicate with the committee on cyber issues in a business context and language the committee understands? How is the organization keeping up with new regulatory changes and legal requirements? Does the organization have an incident readiness and response plan that has been reviewed and tested?

According to the aforementioned 9th Edition of *The State of Risk Oversight*, more than 20 percent of respondents reported not having a complete or partial ERM process in place nor plans to implement one. The ERM process and structure need not be cumbersome, nor is inordinate precision in risk measurement required. We have seen risk ranking handled effectively with an "A", "B" or "C" delineation under which the governing board or designated committee may receive regular updates with respect to the A-rated risks and, if any, less frequent reporting on management's activities relative to B- and C-rated risks. In addition to prioritizing risks, it is common for risks to be grouped within categories such as strategic, financial, operating, compliance, reputational, etc. This can be a useful framework unless it becomes a source of controversy. For example, debating whether reputation risk is its own category or is a "risk of risks", or whether a particular risk is compliance or financial may not be an effective use of valuable time.

Final thoughts

Effective handling of the audit committee's core responsibilities (financial reporting related risks) and other risk-driven agenda items requires efficiency. Committee meetings can be streamlined by insisting on quality pre-meeting materials, making use of consent agendas to address items that do not require discussion, and reaching a level of comfort with and confidence in management and auditors so that some aspects of financial reporting and internal control can be addressed more routinely but with appropriate attention. The audit committee chair's leadership is vital to the committee's effectiveness and efficiency, but spreading the workload among committee members can enhance overall committee performance.

Contact us

KPMG's Higher Education, Research & Other Not-for-Profits Audit Practice

David Gagnon
National Industry Leader
T: 617-988-1326
E: dgagnon@kpmg.com

Rosemary Meyer
Deputy National Industry Leader
T: 410-949-8425
E: rameyer@kpmg.com

Regional Leaders

Renee Bourget-Place
Northeast
T: 802-651-5634
E: rbourgetplace@kpmg.com

Rosemary Meyer
Mid-Atlantic
T: 410-949-8425
E: rameyer@kpmg.com

Kurt Gabouer
Midwest
T: 312-665-3308
E: kgabouer@kpmg.com

Mark Thomas
West
T: 949-885-5630
E: mtthomas@kpmg.com

Jamie Klein
Metro New York and New Jersey
T: 212-872-6708
E: jhklein@kpmg.com

Eileen McGinn
Southeast
T: 615-248-5619
E: emcginn@kpmg.com

Drew Corrigan
Pacific Northwest
T: 503-820-6629
E: dcorrigan@kpmg.com

Travis Hunter, Jr.
Southwest
T: 214-840-2117
E: thunterjr@kpmg.com

kpmg.com/socialmedia