On the 2025 not-for-profit audit committee agenda

January 2025

Audit committees can expect their organization's reporting, compliance, risk, and internal control environment to be put to the test in 2025. Heading into the new year, the U.S. not-for-profit (NFP) sector is contending with political polarization and heightened scrutiny of mission relevance and outcomes. Certain other pervasive ongoing challenges—from cybersecurity attacks and advances in artificial intelligence (AI), to growing regulatory burdens and geopolitical instability—will continue to warrant attention by most NFPs and could impact strategies. In addition, federal policy shifts from the new administration and Congress could impact the operating and risk environment that such organizations must navigate. Once again, NFP boards and audit committees will need to refine and diligently monitor their risk-driven agendas.

Drawing on insights from our interactions with NFP audit committees and senior administrators, we've highlighted six objectives to consider as audit committees consider and carry out their 2025 agendas:

Help ensure the organization's enterprise risk management (ERM) program is keeping pace with the rapidly changing environment.

Clarify the audit committee's oversight of generative AI (GenAI), cybersecurity, and data governance.

Monitor recent revisions to federal grant regulations.

Stay focused on leadership and talent in finance and other functions.

Help internal audit stay attentive to the organization's key risks and be a valuable resource for the audit committee.

Take a fresh look at the audit committee's agenda, workload, and capabilities.

Help ensure the organization's enterprise risk management (ERM) program is keeping pace with the rapidly changing environment.

In 2025, the magnitude, complexity, and velocity of many organizational risks—and their interconnectedness—will require more proactive and holistic risk management, as well as effective oversight by the audit committee. In addition to ongoing risks, several executive and legislative priorities of the new administration and Congress have the potential to create new risks or amplify existing ones in the organization's ERM profile. Among those potential issues the sector is watching (and that are developing quickly) are:

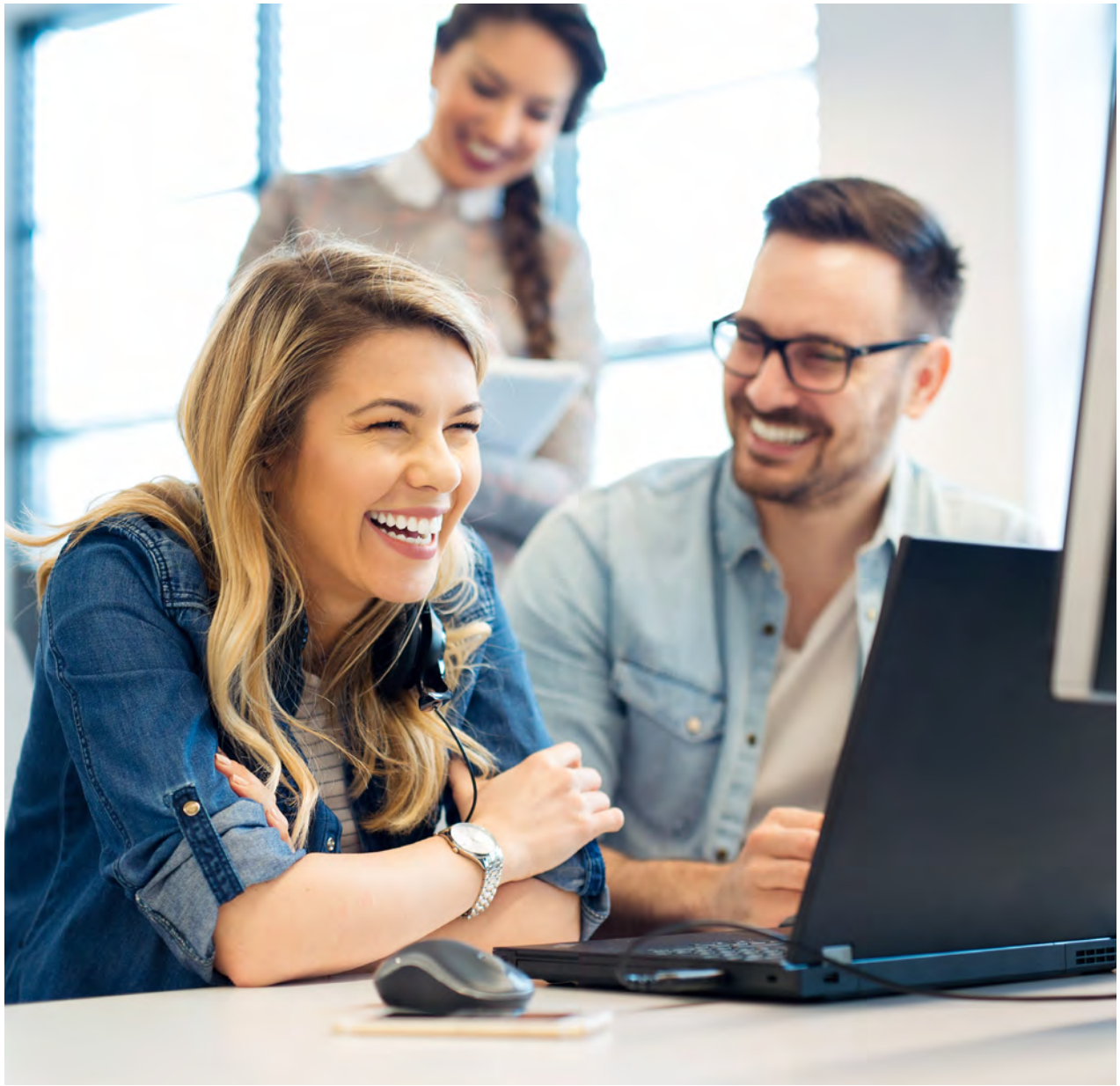
- Pauses on federal grants and loans and stop-work orders, as well as a redirection or reduction of research and other federal program priorities
- A pivot away from clean energy and climate change initiatives and regulations
- An increase in targeted investigations under the False Claims Act
- Changes to immigration and international travel policies that could significantly impact colleges and universities, hospitals, non-governmental organizations (NGOs), and other NFPs
- Changes to federal tax policy affecting donors and exempt organizations
- Gridlock affecting the federal debt ceiling and budget, as well as legislation
- Evolving regulations around the control and use of AI
- For NFPs with health-related missions and employee health plans, changes to Medicare, Medicaid, and the Affordable Care Act
- Further geopolitical developments amid the post-election landscape.

The degree to which some of these risks or other initiatives could materialize in the year ahead—and how they might affect NFPs—is uncertain. It is clear, however, that a robust ERM program can facilitate an organization's ability to monitor and assess these and other fast-changing risks and opportunities based on their likelihood over time. Recognize also that low-probability, high-impact events could quickly materialize (as several have in recent years), and their interaction with other risks could magnify impacts. While building and maintaining such a program can be difficult, the goal should be to transform ERM from a transactional risk register to a high-maturity program, allowing the organization to go beyond operational resilience to using risk to create opportunity and competitive advantage.

A successful ERM program starts with fundamentals. Outside the NFP sector, sometimes the full board has primary responsibility for ERM, with the audit committee overseeing risks within its scope and other committees having responsibilities tied to their scope. In our experience, a leading practice in the NFP industry is to assign responsibility for oversight of the risk management process to the audit committee and oversight of risk areas to appropriate board committees (including the audit committee for risks within its scope). Also fundamental to an ERM program are mechanisms to ensure that risk information is reaching the full board. The board should receive regular reports on risk, especially "mission-critical risks": in hindsight, organizational crises and failures are often traced to inadequate board oversight of such risks. In what is expected to be a very active year ahead in terms of risk identification and mitigation, the audit committee can help the organization advance ERM effectiveness by asking:

- How rigorous are management's processes to identify and assess risks, including emerging risks? Who is involved, and who is championing management's efforts? How far down in the organization does it go? For example, does the organization have a chief risk or compliance officer? In the absence of such a role, does the responsible official have capacity and authority to move the ERM program forward?

- Do we have a complete understanding of the risks in our organization's strategy and our risk profile, as well as how the profile is changing? Are there emerging risks that are not being addressed? Scenario planning, tabletop exercises, and updating crisis response plans may be critical.
- If a risk event were to occur, how quickly would it adversely affect operations? Is a process in place to monitor changes in the environment that might alter key assumptions?
- How do individual risks aggregate and interrelate to determine the top risks that require senior management's focus and merit presentation to the board?
- Are our resources being applied as efficiently and effectively as possible to achieve a risk outcome commensurate with our risk appetite?
- Are our risk, compliance, and internal audit functions aligned with respect to risk identification and mitigation throughout the organization?
- 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?



Clarify the audit committee's oversight of GenAI, cybersecurity, and data governance.

Data Security ranked near the top of United Educators' December 2024 Top Risks Survey of colleges and universities, while respondents identified AI as both an emerging risk and opportunity.[1] These results align with increasingly disruptive cyberattacks throughout the NFP sector, where sensitive donor, patient, and research data can make valuable targets and resource constraints frequently limit cyber defenses. They also appear to reflect a deepening recognition among NFPs that GenAI has the potential to modernize administrative processes and amplify impact, but also to enable cyber criminals to launch more sophisticated attacks—using GenAI's ability to write code and mimic voices in verification techniques. Indeed, many larger NFPs such as hospitals and educational institutions have already integrated AI to improve patient care, learning, and operational efficiency, and some are adopting AI-driven threat detection systems and zero trust strategies to bolster their cybersecurity. Still, most NFPs are just beginning to recognize the importance of having policies in place to guide the ethical and responsible use of GenAI. [2]

The growth in the use of GenAI across potentially multiple platforms necessitates a focus on data quality, having a responsible use AI policy, complying with evolving privacy, intellectual property, and AI laws and regulations, and rigorously assessing data governance practices or, in some cases, developing data governance practices. As a result, audit committees at NFPs should be probing whether the organization's data governance framework and interrelated AI, GenAI, and cybersecurity governance frameworks are keeping pace. In addition, a key question for boards is how to structure oversight of these areas at the full board and committee levels, including the audit committee. In assessing the audit committee's oversight responsibilities in these areas, we recommend the following areas of focus:

Assessing audit committee oversight responsibilities for GenAI. As they seek to understand GenAI's potential impact on strategy and the operating model, many boards are still considering how best to oversee AI and GenAI, including the appropriate roles of the full board and standing committees.

As we discuss in On the 2025 board agenda, oversight in many companies is often at the full board level—where major strategic and transformational business issues are typically addressed. In the NFP sector, the full board should be discussing issues such as GenAI's impact on the organization's strategy and operating model. However, some audit committees, including at NFPs, may already be involved in overseeing specific GenAI issues, and it is important to clarify the scope of the audit committee's responsibilities. GenAI-related issues for which audit committees may have oversight responsibilities include:

- Oversight of compliance with evolving AI, privacy, and intellectual property laws and regulations.
- Use of GenAI in the preparation and audit of financial statements, as well as in other regulatory filings.
- Use of GenAI in donor management, finance, internal audit (as applicable), research, and other administrative functions, and whether personnel involved have the necessary talent and skillsets.
- Development and maintenance of internal controls and procedures related to AI and GenAI, as well as controls around data, including the potential for inadvertent biases in algorithms (e.g., research data sets, diagnostic tools for patient care, etc.).
- Consistent with cybersecurity awareness and training for employees and volunteers, deployment of comprehensive AI training programs focused on ethical use, practical applications, and security.

[1] Source: United Educators, *Top Risks Report: Insights for Higher Education*, December 2024.

[2] Source: NTEN, *Generative AI and the Social Sector, Policy Narrative*, 2024.

Some audit committees may have broader oversight responsibilities for GenAI, including overseeing various aspects of the NFP's governance structure for the development and use of the technology. How and when is a generative AI system or model—including a third-party model—developed and deployed, and who makes that decision? What GenAI risk management framework is used? Given how fluid the situation is and the audit committee's bandwidth and skillsets—and with GenAI gaining rapid momentum—the allocation of oversight responsibilities to the audit committee may need to be revisited.

Assessing audit committee oversight responsibilities for cybersecurity and data governance. At most NFPs, the board's oversight responsibility for cybersecurity and data governance largely resides with the audit committee. Nevertheless, given the explosive growth in GenAI and significant risks posed by the technology, boards should rigorously re-assess their data governance and cybersecurity frameworks and processes. Given the audit committee's heavy agenda, should a subcommittee be established to focus on and assist in the oversight of data governance and perhaps cybersecurity?

Monitor recent revisions to federal grant regulations.

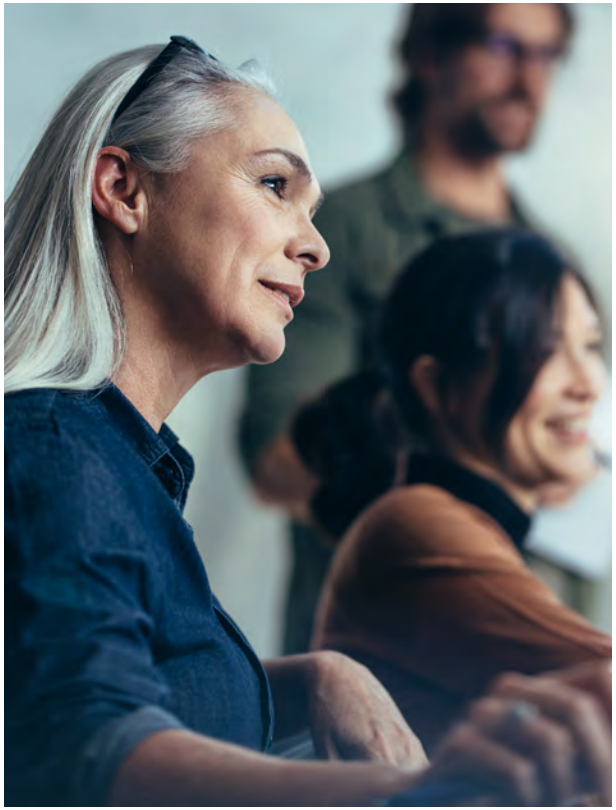
Audit committees at NFPs that receive federal funding should be aware that in April 2024, a Federal Register was updated to revise portions of the Uniform Guidance (UG). The UG applies to recipients of federal awards, as well as to auditors performing Single Audits. The revisions were generally effective October 1, 2024.

The revisions clarify existing regulations, are intended to reduce agency and recipient burden, and impact both auditees and auditors. Among the key revisions are:

- An increase in the Single Audit threshold from $750,000 to $1,000,000 (effective for fiscal periods ending on or after September 30, 2025)
- Changes to certain areas of cost principles, including clarification of pension costs
- Removal of written approval for certain cost items
- An increase in the threshold for items defined as capital expenditures (e.g., equipment) from $5,000 to $10,000
- An amendment of the definition of "modified total direct costs" to exclude subaward costs above $50,000 (up from the current level of $25,000) in the application of indirect cost recoveries
- An increase in the de minimis indirect cost rate from 10% to 15%
- Clarification that recipient and subrecipient entities must establish, document, and maintain effective internal controls.

Organizations should note that federal agencies were granted flexibility in adopting revisions relative to existing awards as described in M-24-11 that was issued by the Office of Management and Budget (OMB) on April 4, 2024. Attention should be paid to agency requirements in amendments and new awards, as well as related impacts to any subawards. Moreover, revisions generally took effect on October 1, 2024, i.e., during many NFPs' fiscal 2025, and certain revisions (e.g., changes in the capital expenditure threshold) may require resubmission of indirect cost rate proposals to adopt, which could take time. Accordingly, differences in the timing and application of certain revisions may result in different policies, compliance requirements, and controls within the same fiscal year, which could make compliance and auditing more challenging.

As it is possible that the new administration's plans could affect these and other regulations, NFPs subject to the UG should closely monitor executive orders and announcements by federal agencies. In addition, the 2025 Compliance Supplement, which applies to Single Audits for fiscal years beginning after June 30, 2024, identifies compliance requirements subject to audit but is not expected to be issued by OMB until the second quarter of 2025. Accordingly, NFPs subject to the Single Audit should discuss any compliance and audit implications with their auditors as the year progresses.



Stay focused on leadership and talent in finance and other functions.

During the COVID crisis, the workloads of senior executives at many NFPs increased significantly due to disruptions in fundraising and mission-based activities. Other industry pressures since then have only intensified and perhaps added to the strain, with many NFPs citing burnout as an emergent risk. While remote and hybrid work modes have become common for some organizations—providing flexibility and easing the burden—administrative roles in the sector generally have become more demanding.

Recruitment of top talent in finance and other administrative functions remains a risk at many NFPs, especially those with limited resources, and an aging demographic in senior roles continues to contribute to this risk. While hiring pressures have abated over the last few years, filling certain finance, IT, risk, compliance, and internal audit roles continues to be challenging for some organizations. As chief business officers seek to transform the organization's business processes with more robust technologies, including GenAI, audit committees can help ensure that the talent and technical acumen needed to support operations, risk management, and new strategies—as well as appropriate succession planning—are in place. The audit committee should consider the following questions to help monitor and guide the organization's progress:

- While bolstering recruitment, retention, and wellness programs may result in higher costs—which could add financial strain to the organization—employee workloads and morale, as well as internal controls, could be adversely impacted if the organization is unable to attract and keep the appropriate talent. Does the audit committee understand how the organization is addressing risks in these programs and how it is managing any staffing issues, particularly as to specialized roles in IT, compliance, and other areas?
- Do we have the appropriate infrastructure to monitor and manage the tax, compliance, culture, and cybersecurity ramifications of remote work arrangements?
- Are our finance and internal audit functions attracting, developing, and retaining the talent and skills needed to match their increasingly sophisticated digitization and other transformational strategies?

- Do our chief business officer, chief compliance officer, chief audit executive, and chief information security officer have the sufficient organizational authority and stature, organizational structure, bench strength, and succession planning to be effective moving forward?

Help internal audit stay attentive to the organization's key risks and be a valuable resource for the audit committee.

As we have observed, at a time when audit committees are wrestling with weighty agendas and putting risk management at the forefront, internal audit should be a valuable resource and a crucial voice on risk and control matters. This means focusing not only on reporting and compliance risks, but also on critical operational and technology risks and related controls, as well as sustainability and reputational risks.

Is internal audit's annual plan risk-based and flexible, and does it adapt to changing operational and risk conditions? Internal audit must be able to effectively pivot to address unanticipated issues and risks, as well as ongoing organizational risks highlighted in the audit plan. The audit committee should work with the chief audit executive and chief risk officer to help identify areas in which significant risks to the organization's reputation, strategy, and operations exist or could arise, such as tone at the top and culture; emerging applications for GenAI; supply chain management; research compliance and conflicts; workforce and wellness programs; international activities; third-party vendors; and the quality and integrity of data in reports available to the public and regulatory bodies. Financial and nonfinancial data can vary by type of NFP but may include, for example, data included in indirect cost proposals, creditor requests, the IRS Form 990, and reports on mission impacts. Whether or not the NFP has an internal audit function, audit committees should understand the controls that management has in place to verify the scope, accuracy, and consistency of such data.

Expect the internal audit plan to address these emerging issues, reconcile to the organization's business processes and risks, and incorporate a multi-year perspective on focus areas—how does the current plan compare to last year's and what has changed or could change in the year ahead?

Set clear expectations and ask whether internal audit has what it needs to succeed. In terms of ERM, clarify internal audit's role—which is not to manage risk, but to help guide its audit priorities and provide an important sanity check on the adequacy of management's risk identification and mitigation processes. Does internal audit have the skills and resources needed to handle the fast-evolving IT and GenAI issues affecting the organization? Internal audit is not immune to talent pressures. Help the chief audit executive think through the impacts of advanced technologies on internal audit's workload and effectiveness—using tools such as dashboards to enhance risk assessment and routines for real-time auditing. What is internal audit doing to be a valued business advisor to other departments?

Take a fresh look at the audit committee's agenda, workload, and capabilities.

Keeping the audit committee's agenda focused on its core responsibilities—oversight of financial reporting and compliance, internal controls, and internal and external auditors—is essential to the committee's effectiveness. Beyond these duties, audit committees at NFPs oversee a growing list of other risks, compounding the workload challenge and making efficiency paramount. As the role and responsibilities of the committee continue to evolve, the committee should periodically assess its composition, skillsets, independence, and leadership to ensure they are keeping pace and to mitigate "agenda overload." The committee—with input from management and auditors, as appropriate—should also conduct self-evaluations annually.

In our interactions with NFPs across the country, we've observed that evaluating the audit committee's effectiveness in the context of each organization's unique mission and operating environment can be difficult. Compared to audit committees at public companies—which are regulated and for which industry benchmarking on board activities and executive education opportunities are more common—NFP audit committees have a different focus and scope (e.g., NFP accounting, research compliance, etc.) and are less regulated and more insular, complicating determination of optimal practices. External and internal auditors and industry organizations such as the Association of International Certified Professional Accountants (AICPA) may offer relevant and objective guidance. Moreover, there may be opportunities to learn from and collaborate with audit committees at similar NFPs.

We recommend the following questions to consider (including as part of the committee's annual self-evaluation):

- Does the committee's charter align with and reflect the actual goals and work of the committee?
- How many members have direct experience with financial reporting, compliance, and internal controls? Is the committee relying too heavily on one member to do the "heavy lifting" in overseeing these areas?
- Does the committee include members with experience necessary to oversee emerging areas of risk that the audit committee has been assigned—such as GenAI and data security? Is there a need for a fresh set of eyes or deeper (or different) skill sets? The committee may also need to periodically engage outside specialists to navigate certain areas (e.g., forensic audits).
- Does the committee spread the workload by allocating oversight duties to each audit committee member, rather than relying on the committee chair to shoulder most of the work?
- Are committee meetings streamlined by insisting on quality premeeting materials (with attention paid to their volume and expectations they have been read), use of consent agendas, and reaching a level of comfort with management and auditors so that certain activities can become routinized (freeing up time for more substantive issues facing the organization)? A best practice is for the chair to summarize key focus areas for committee members when distributing meeting materials.
- Is the chair spending sufficient time outside the boardroom with management and auditors to plan for committee meetings, get a fuller picture of the issues, and enhance the productiveness of committee meeting time?
- Are separate executive (nonpublic) sessions with management, internal and external auditors, and members only at the beginning or end of meetings scheduled? Establishing a regular cadence of such meetings helps ensure that sensitive matters, if any, can be addressed without raising unnecessary flags and allows for more open sharing of ideas and perspectives.
- Do members have access to robust orientation and continuing education programs? Are they provided with relevant industry information sourced from outside the organization? Are mechanisms available to network with counterparts at similar organizations?

About the KPMG Board Leadership Center

The KPMG Board Leadership Center (BLC) champions outstanding corporate governance to drive long-term value and enhance stakeholder confidence. Through an array of insights, perspectives, and programs, the BLC promotes continuous education and improvement of public and private company governance. BLC engages with directors and business leaders on the critical issues driving board agendas—from strategy, risk, talent, and sustainability to data governance, artificial intelligence, audit quality, proxy trends, and more. Learn more at **kpmg.com/blc**.

About the KPMG Not-for-Profit practice

The KPMG Higher Education, Research & Other Not-for-Profits (HERON) practice is committed to helping colleges, universities, and a variety of other not-for-profits carry out their missions. Our experience serving private and public higher education institutions and other charitable organizations across the U.S. allows our professionals to provide deep insights on emerging issues and trends—from financial reporting, tax, compliance, and internal controls to leading strategic, operational, technology, risk management, and governance practices. Learn more at **institutes. https://kpmg.com/us/en/industries/government-public-sector/higher-education.html**

Contact us

The KPMG HERON Audit practice

David Gagnon
U.S. Sector Leader
E: dgagnon@kpmg.com

Rosemary Meyer
Deputy U.S. Sector Leader
E: rameyer@kpmg.com

Regional leaders

Renee Bourget-Place
Northeast
E: rbourgetplace@kpmg.com

Ed Lee
Metro NewYork and New Jersey
E: enlee@kpmg.com

Rosemary Meyer
Midatlantic
E: rameyer@kpmg.com

Jennifer Hall
Southeast
E: jchall@kpmg.com

Cathy Baumann
Midwest
E: cbaumann@kpmg.com

Drew Corrigan
Pacific Northwest
E: dcorrigan@kpmg.com

Christopher Ray
West
E: cray@kpmg.com

Byron Corwin
Southwest
E: bcorwin@kpmg.com

kpmg.com/us/blc
T: 808-808-5764
E: us-kpmgmktblc@kpmg.com

Learn about us: **kpmg.com**

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.