protiviti®
Risk & Business Consulting.
Internal Audit.

Volume 6, Issue 1

The Bulletin

Setting the 2016 Audit Committee Agenda

This issue of *The Bulletin* continues our practice of commenting on agenda items that may be relevant to audit committees of many organizations in the coming year. As in the past, our observations are based on our interactions with client audit committees, roundtables we have conducted, discussions with directors at conferences and other forums, and an annual survey.

The agenda items we discuss herein consist of five enterprise, process and technology risk issues and five financial reporting issues. Our focus is on significant issues that we believe warrant the attention of audit committees at most companies and organizations. We do not focus on audit committee best practices that are covered comprehensively in the public domain.

Enterprise, Process and Technology Issues

Ensure the risk profile reflects current business realities – Most organizations conduct some form of risk assessment in the form of risk maps, heat maps and risk rankings based on subjective assessments of such risk criteria as severity of impact of potential future events and their likelihood of occurrence. These assessments provide an overall picture of the enterprise's risks. The question is, however, does the risk profile adequately reflect current business realities?

This is an important question because many audit committees are responsible for making inquiries regarding the company's risk assessment process and risk management capabilities. Even audit committees that do not have this specific responsibility often desire, for a variety of reasons, to see a summary of the entity's top risks.

The business environment is constantly changing. Digital technologies, the forces of globalization, changing demographics and other megatrends are compressing the half-life of business models. Given these realities, the board of directors should take a look at the company's risk profile at least annually. This evaluation should be supported by an updated assessment by management. For the most significant risks, the audit committee (or another committee of the board, depending on how the board is organized for risk oversight) should determine whether appropriate action plans are in place to manage the critical enterprise risks.

The 2016 Mandate for Audit Committees

Enterprise, Process and Technology Risk Issues

1. **Ensure the risk profile reflects current business realities –** Does the organization's risk profile consider emerging risks or changes in existing risks as well as highlight the critical enterprise risks and adequacy of risk management capabilities?
2. **Understand the technology-related risks that present threats to the business model –** Are cybersecurity, privacy/identity management, information security/system protection issues, and potential disruption risks adequately addressed?
3. **Pay attention to risk culture and the tone of the organization –** Is the tone at the top and in the middle, and their respective impact on the control environment and the effectiveness of risk management capabilities, considered?
4. **Consider the need for expanded capabilities of the finance organization –** Are capabilities of finance aligned with company needs?
5. **Consider the need for expanded capabilities of the internal audit function –** Is internal audit delivering value and sufficiently resourced to deliver to expectations?

Financial Reporting Issues

6. **Make the necessary process adjustments to enable the new revenue recognition standard –** It's time to decide what's needed and implement it. Is the company ready?
7. **Review the PCAOB inspection report on the audit firm, and understand how it impacts the audit process –** Has the PCAOB raised concerns that are likely to impact the company's audit? If so, what is the impact?
8. **Consider the PCAOB Audit Committee Dialogue –** Do the PCAOB's issues warrant committee attention?
9. **Pay attention to developments on the lease accounting front –** A new accounting for leases standard is on the horizon. Is its impact on the company understood?
10. **Ascertain implications of the SEC's concept release on audit committee disclosure –** Would the SEC's proposal significantly alter proxy and other related disclosures?

To illustrate, we include the top 10 risks for 2016 at right.[1] This summary shows whether the risk is increasing (↑), decreasing (↓) or remains unchanged (↔) compared to the prior year's survey. The list illustrates several key risks with which audit committees should be concerned. Specifically, with respect to significant risks with financial reporting implications, the audit committee should understand those risks, how they are managed, their potential impact on the financial statements and how they are being considered by the external auditor during the audit process.

The audit committee also needs to know that emerging risks are being incorporated into the organization's risk assessment process in a timely manner. For example, management needs to focus on the implications of changes in the business environment on the critical assumptions underlying the organization's strategy and business plan, key risk indicators and trends that signal relevant early warning signs, and the analysis of interdependencies among risks to identify risk themes germane to the organization and its business model. In summary, the company's risk assessment process should consider changes in existing risks, the emergence of new risks, the adequacy of the organization's capabilities for managing risks, and the implications of the most critical risks to public disclosure requirements.

Understand the technology-related risks that present threats to the business model – Amid major technology transformation and change, danger lurks on multiple fronts. Advances in digital technologies – including intelligent devices and machines; virtual reality; mobile technologies; cloud computing; social business; and smart grids, factories and cities in an app-centric world – are driving disruptive change to established business models by improving customer experiences, engaging targeted communities, creating convenience and expanding markets. These advances are also adding increased security and privacy risks. Cyber predators are playing for keeps, threatening to penetrate organizational cybersecurity defenses. It all adds up to increasing demands on the chief information officer (CIO), chief information security officer (CISO), and lines of business in addressing this unrelenting pace of change – as well as on the board of directors itself because of the significance of the potential reputational consequences of a high-profile breach.

Outwitting the wolves at an organization's "cyber door" and managing transformational change in the enterprise with confidence requires the capability to deploy a vast array of information security approaches, processes, tools, skills and collaborations – all of which were highlighted in Protiviti's *2015 IT Priorities Survey*.[2]

2016 Top 10 Risks[1]

		Year-Over-Year Change
1.	Regulatory changes and heightened regulatory scrutiny may affect the manner in which our products or services will be produced or delivered.	↔
2.	Our organization may not be sufficiently prepared to manage cyberthreats that have the potential to significantly disrupt core operations and/or damage our brand.	↑
3.	Economic conditions in markets we currently serve may significantly restrict growth opportunities for our organization.	↓
4.	Our organization's succession challenges and ability to attract and retain top talent may limit our ability to achieve operational targets.	↔
5.	Ensuring privacy/identity management and information security/system protection may require significant resources for us.	↑
6.	Resistance to change may restrict our organization from making necessary adjustments to the business model and core operations.	↔
7.	Rapid speed of disruptive innovations and/or new technologies within the industry may outpace our organization's ability to compete and/or manage the risk appropriately, unless we make significant changes to our operating model.	↑
8.	Our organization's culture may not sufficiently encourage the timely identification and escalation of risk issues that have the potential to significantly affect our core operations and achievement of strategic objectives.	↓
9.	Anticipated volatility in global financial markets and currencies may create significantly challenging issues for our organization to address.	↑
10.	Sustaining customer loyalty and retention may be increasingly difficult due to evolving customer preferences and/or demographic shifts in our existing customer base.	↓

Note: The risk that the organization may not be sufficiently prepared to manage an unexpected crisis, which could significantly impact its reputation, was included in the 2015 top 10 list, but did not make the 2016 list.

[1] This list is based on the results of the annual survey conducted by North Carolina State University's ERM Initiative and Protiviti on the top risks identified by senior executives and directors, which will be available in early 2016 at www.protiviti.com.

[2] *Today's Enterprise – Cyberthreats Lurk Amid Major Transformation: Assessing the Results of Protiviti's 2015 IT Priorities Survey*, available at www.protiviti.com.

The top two findings in this year's survey include:

- **Security concerns are paramount –** No surprise here: Addressing and strengthening cybersecurity represent critical priorities among all survey respondents, CIOs and companies of all sizes.
- **Major IT changes and upgrades continue –** Well over half of all organizations are undergoing a major IT transformation that will last a year or longer, intensifying demands on IT departments to manage these changes successfully while addressing other critical business needs (e.g., cybersecurity).

IT executives and professionals have a vast number of pressing duties, with priorities increasing across the board in volume and significance. To address and manage these challenges successfully, they must develop and strengthen the expertise and business savvy necessary to strike the right balance between activities that enhance business value and those that protect organizational value. Boards of directors need to ensure that they and IT have the necessary resources to succeed. Because of the potential audit and disclosure implications, audit committees should have an interest in this conversation.

Pay attention to risk culture and the tone of the organization – Audit committees should watch for the signs of dysfunctional behavior from a risk management and internal control standpoint (e.g., failure to heed established risk limits, fear of repercussions from raising contrarian viewpoints, "shoot the messenger" environments, undue organizational complexity, lack of transparency as to the underlying economics of significant transactions, and potential conflicts of interest, among other signs of a weak risk culture).

A strong risk culture is important to directors because it is the keystone for balancing the inevitable tension between, on the one hand, creating enterprise value through executing the strategy and driving performance, and, on the other hand, protecting enterprise value through an appropriate risk appetite and managing risk. The audit committee should ensure that the organization has an effective risk culture in which the leaders responsible for the units and processes that create risks are accountable for managing the risks their units and processes create. A strong risk culture should establish the proper tone in the middle for managing these risks consistent with the tone at the top. Finally, it is vital that management sustain that culture because of its impact on the control environment over internal and external financial reporting. The audit committee should ensure that executive management acts on risk information on a timely basis when significant matters are escalated and that the board is likewise involved in a timely manner when necessary.

Consider the need for expanded capabilities of the finance organization – Finance functions drive much of the information falling within the audit committee's oversight. In the coming year, between maintaining margins, forecasting cash flow, complying with new regulations and combatting cyberthreats, finance functions will have much to monitor on their radar. The results of the *2016 Finance Priorities Survey* indicate that chief financial officers (CFOs) and finance professionals remain alert to intensifying volatility on the radar while continuing to address a large and growing set of priorities.[3] Among the top findings:

- **Margins matter most, not market share –** Finance functions are focused on preserving margins and sustaining a strong focus on working capital management and earnings performance.
- **Cybersecurity concerns permeate the finance function –** There is little doubt that IT security and privacy are far more than just IT issues today – together, they represent a strategic organizational risk and, not surprisingly, one that ranks near the very top of finance functions' priority lists, just as it does in our other studies. Effective cybersecurity requires strong board engagement, appropriate policies, and an understanding of the enterprise's most valuable and sensitive data.
- **Wanted: a single, real-time version of the truth –** To help strengthen overall business performance and strategic planning, and to drive value from financial data within the organization, finance functions desire better, more accurate and timely data collection, data analysis, reporting, budgeting and forecasting capabilities to enable profitability analyses tied to customers, products, operating units and geographies.

The finance function's specific priorities may vary according to the organization's industry, structure, culture, business performance issues, and internal and public reporting requirements. That said, audit committees should ensure that finance is appropriately resourced to deliver to the organization's specific expectations.

Consider the need for expanded capabilities of the internal audit function – Chief audit executives (CAEs) and their functions face increasingly demanding expectations, requiring that they be more anticipatory, change-oriented and highly adaptive. As with the CIO organization and finance function, internal auditors play a vital role in securing the organization by working closely with executive management and functional leaders to ensure that cybersecurity is adequately considered in the audit plan.

The findings of this year's *Internal Audit Capabilities and Needs Survey* show that cybersecurity is among several issues on internal audit's plate.[4] Among the findings:

- **Board engagement and the audit plan represent keys to effective cybersecurity –** Top-performing organizations have both high board engagement and defined cybersecurity measures in the annual audit plan.

---

[3] *Maintaining Margins While Staying Vigilant: Assessing the Results of the Financial Executives Research Foundation/Protiviti 2016 Finance Priorities Survey,* Financial Executives Research Foundation and Protiviti: www.protiviti.com.

[4] *From Cybersecurity to Collaboration: Assessing the Top Priorities for Internal Audit Functions, 2015 Internal Audit Capabilities and Needs Survey,* Protiviti: www.protiviti.com.

- **The list of internal audit priorities continues to grow** – In addition to cybersecurity issues, there are risks related to emerging technologies (e.g., social media, cloud computing and mobile applications), increasing regulatory compliance requirements, and new guidance and standards from The IIA, ISO and COSO. These and other priorities are requiring internal auditors to be nimble and adaptive in helping their organizations address rapidly evolving demands.
- **Technology-enabled auditing is on the rise** – Competing urgencies on a lengthy priorities list are driving more internal audit functions to increase their investment in, and use of, technology-enabled auditing approaches and tools.
- **Increased focus on marketing and collaboration** – CAEs are focused more than ever on conveying to the rest of the organization the function's mission, value and risk-related concerns. They also want to increase their collaboration as strategic partners with executive management, other functional leaders and the board to help the organization understand its risks and achieve its strategic objectives.

Audit committees need to ensure that internal audit receives the support it needs to succeed in executing its risk-based audit plans and in meeting expectations to keep pace with change.

Financial Reporting Issues

While financial reporting issues are not necessarily among most companies' top risks, they are nonetheless relevant to the audit committee's oversight responsibilities. Following are five such issues for the committee's consideration.

Make the necessary process adjustments to enable the new revenue recognition standard – Developed in collaboration with the International Accounting Standards Board (IASB), the new revenue recognition standard has been issued by the Financial Accounting Standards Board (FASB). Public companies must adopt the standard no later than annual reporting periods beginning after December 15, 2017, including interim reporting periods therein (e.g., a calendar-year reporting company must adopt in 2018). Private companies must adopt the new rules no later than annual reporting periods beginning after December 15, 2018, including interim reporting periods therein.

The standard introduces a single comprehensive, principles-based model that eliminates existing industry-specific guidance and expands revenue-related qualitative and quantitative disclosures. Companies must ascertain the extent of changes to the timing or amount of their revenue recognition and determine which transition method to use – either retrospective or prospective. As the effective date has been delayed from that which was required when the standard was initially released, the FASB and the IASB have allowed companies to comply using the original due date, resulting in yet another option for companies – to adopt early or to adopt just in time.

The standard's implementation could be a significant undertaking. Time is needed to fully assess its impact and implement the necessary changes across the company's processes, systems and controls, and possibly even to its current contractual relationships. Unfortunately, many executives and directors don't have an understanding of how the standard will impact their companies. A lot of work remains in terms of sizing that impact and determining the method (and, for those considering the allowed one-year earlier option, the timing) of adoption. The reality is that 2015 is almost over, so there isn't much time left.

Audit committees should ensure that management is taking the following steps to get on top of the transition process:

1. Educate executives and their teams with overall responsibility for the transition.
2. Assess the current revenue recognition policy against the standard, and identify expected changes.
3. Depending on the significance of accounting policy gaps, consider the need for involving others.
4. Perform a high-level analysis of any data gaps.
5. Develop a high-level approach to the transition method.
6. Identify and assess additional resource needs.
7. Inform the decision-makers.

The previous issue of *The Bulletin* discusses the above steps in greater detail, as well as several other important topics relating to the new standard, including the potential significant accounting and reporting changes, industry implications, and a transition road map.[5]

Review the PCAOB inspection report on the audit firm, and understand how it impacts the audit process – The Public Company Accounting Oversight Board (PCAOB or the Board) has released several reports that provide direction to public accounting firms in conducting their audits, and has also provided recommendations to audit committees in an effort to enhance audit quality. In addition, the Board issues reports on the results of its inspections of the audits of individual firms. These reports may have an impact on the demands and expectations that issuers receive from their external auditors and therefore warrant the audit committee's attention.

When the external auditor communicates the overall audit strategy – including the timing of the audit, significant risks identified by the auditor, significant changes to the planned strategy or identified risks, and other related matters – the audit committee should inquire whether PCAOB inspections of the firm and recent PCAOB guidance are having an impact on the audit approach in any significant way, and, if so, how and in which areas. If the PCAOB has included the company's particular audit in its scope, the committee should expect the auditor to outline any specific issues raised and the implications of the resolution of those issues.

[5] "Accounting for Revenue Recognition: A New Era," *The Bulletin*, Volume 5, Issue 12, 2015, Protiviti: www.protiviti.com.

In July 2015, the PCAOB issued for public comment 28 potential audit quality indicators (AQIs) as a set of measures around the professionals performing the audit, the audit process itself and audit results. The Board's objective is to provide new insights about how to evaluate the quality of the audit process. As envisioned by the PCAOB, AQIs may enhance ongoing discussions among audit committees, audit firms and others concerned with a company's financial reporting and the transparency of the external audit process. In presenting these AQIs, the Board continues to advance the theme that audit committees are in the best position to monitor and assess auditor performance as part of their overall oversight responsibilities. As the PCAOB evaluates the comments it has received, audit committees need to watch for further developments on this front.

Consider the PCAOB Audit Committee Dialogue – Earlier this year, the PCAOB also issued a communication to audit committees to provide insights from inspections of audit firms that can assist audit committees in their various oversight activities. The first of a series, the communication highlights key areas of recurring concern in PCAOB inspections of large audit firms, as well as certain emerging risks to the audit. In addition, the communication provides targeted questions that committee members may want to ask their auditors on each topic.[6]

Audit areas in which significant deficiencies have been found in recent years in PCAOB inspections include auditing internal control over financial reporting, assessing and responding to risks of material misstatement, auditing accounting estimates (including fair value measurements) and deficient "referred" work in cross-border audits in certain countries. The PCAOB's communication offers some indicators of potential emerging risks that the Board's inspection process will consider in the coming year, such as an increase in mergers and acquisitions, falling oil prices, undistributed foreign earnings, and maintaining audit quality as the audit firm grows other business lines (e.g., consulting services).

In addition, audit committees should pay attention to the impact of new PCAOB standards. For example, the Board's auditing standard on related party transactions, significant unusual transactions and financial dealings with executives is now in play.

Pay attention to developments on the lease accounting front – Another major accounting standard resulting from a joint effort by the FASB and the IASB is to be released no later than early 2016. It will bring leasing assets and liabilities onto lessee company balance sheets. This new lease accounting standard will – like its revenue accounting counterpart – require many lessee companies to implement new policies, processes, systems and internal controls. For lessor companies, the good news is that there will be less change.

For public companies, the new lease accounting rules will likely take effect in fiscal years beginning after December 15, 2018, including interim periods therein. As with the revenue recognition standard, the timetable for private companies is delayed another year. Early adoption will likely be permitted.

The new standard will introduce a right-of-use principle for lessees – providing that a lease conveys the right to control the use of an asset – creating an asset and a liability that must be reflected on the lessee's balance sheet. Accounting will differ for capital/finance leases and operating leases; however, both types of leases would result in lessees recognizing a right-of-use asset and a lease liability. The IASB's approach will be slightly different for lessees. With respect to lessor accounting, both U.S. generally accepted accounting principles (GAAP) and the International Financial Reporting Standards (IFRS) will be substantially consistent with the current accounting model.

Ascertain implications of the SEC's concept release on audit committee disclosure – In July 2015, the U.S. Securities and Exchange Commission (SEC) approved the issuance of a concept release exploring possible revisions to audit committee disclosures. Concept releases provide the SEC with an opportunity to "test the waters" before undertaking rulemaking. Therefore, it is an important step in the rulemaking process and one to which issuers (and their audit committees) should pay attention.

This particular concept release focuses on current audit committee disclosure requirements with an emphasis on the committee's oversight of independent auditors, including specific potential changes to committee disclosure requirements related to its oversight of the auditor, the process for appointing or retaining the auditor, and evaluation of the qualifications of the audit firm and engagement team.[7] While this concept release is far from the weight of a final rule, the audit committee should be familiar with its contents and evaluate whether the forthcoming proxy disclosures require enhancement.

Summary

Interesting challenges are in store for audit committees in the coming year. The items we have put forth in this issue of *The Bulletin* are significant matters warranting consideration by audit committees for inclusion on the 2016 agenda.

[6] Audit Committee Dialogue, PCAOB, May 2015: pcaobus.org/sites/digitalpublications/Pages/auditcommittees.aspx.

[7] *Protiviti SEC Flash Report: The U.S. Securities and Exchange Commission Issues Concept Release on Enhanced Audit Committee Disclosures*, August 27, 2015: www.protiviti.com.

protiviti®
Risk & Business Consulting.
Internal Audit.