IT and emerging technologies, systemic risk and disruption are top-of-mind for boards, audit committees

Dodd-Frank whistleblower rules, antibribery laws driving reassessment of compliance

Boards are learning to live with uncertainty. From the impact of cloud computing and emerging technologies to the ripple effect of supply chain disruptions and other systemic risks across a complex globalized economy, the speed and volatility of change is keeping risk oversight high on board agendas. At the same time, regulatory compliance remains front and center as governments and agencies continue to roll out regulatory reforms—including the SEC's Dodd-Frank whistleblower rules and the UK Bribery Act.

"Our board is now thinking in terms of constant change, if not major disruption," noted one of the directors attending KPMG's 27-city Spring Audit Committee Roundtable Series—*Changes and Challenges Driving the Audit Committee Agenda*. "We expect the unexpected."

Nearly 75 percent of 1,500-plus roundtable attendees said their board or audit committee has discussed the company's vulnerability to systemic risks—with "economic and financial risk," "cyber risk," and "supply chain risk" topping their list. And while most attendees said updates from the company's CIO over the past year have focused primarily on information security and to some extent risks posed by emerging technologies, 84 percent said the company's strategic planning process is either "not effective," or only "somewhat effective," in dealing with the pace of innovation and technology change.

As highlighted below, KPMG's national roundtable series explored a number of timely issues—and offered key takeaways—for boards, audit committees, and management to consider as they help their companies move forward in the months ahead.

Events in Japan and the Middle East bring the challenges of globalization and systemic risk—and the realities of a "new global disruptive economy"—into sharper focus, with lessons to be learned. With the recent devastation in Japan impacting global supply chains, and events in the Middle East threatening critical energy supplies, the risk of systemic disruption is becoming an "assumed operating reality."[1] Indeed, supply chain disruptions starkly illustrate the potential impact of systemic risk in an increasingly global economy, including:

- Vulnerability of just-in-time business models
- Risk of a systemwide shutdown caused by failure of a single—but critical—component
- Dependency on sole-source suppliers

Roundtable participants discussed a number of key lessons to consider, including:

- The need to think beyond the "predictable"—the most significant risks to the business may be outside the four walls of the company

- Focusing on the plausible, but unlikely, that has devastating impact
- Unrealistic expectations of the company's ability to avoid a crisis
- Ensuring robust scenario planning and crisis response
  - *"We've broadened our risk horizon, significantly."*
  - *"It's about learning to live with uncertainty—the need for flexibility, resilience, and agility…What's our Plan B, Plan C, Plan D…?"*
  - *"Crises literally can come out of nowhere—that's what we worry about."*

[1] *Supply Chain Risk Management*: What's working? What's not?, Corporate Compliance Insights, March 2011

Systemic risks posed by interconnected world

In your opinion, which systemic risks pose the greatest threats to your company? (Select three)

Economic and financial risk*

Cyber risk (assault on global IT infrastructure)

Supply chain risk

Geopolitical risk

Risk to critical infrastructure (electricity, gas, telecom, water, transportation)

Natural disaster

Environment/climate-change risk

Global pandemic risk (including bioterrorism)

Food security

*(*Listed by "most frequently selected")*

Systemic risk discussions

Has your board or audit committee discussed your company's vulnerability to systemic risks?

Yes
72%
No
28%

Pace of technology change

How effective is your company's strategic planning process in dealing with the pace of innovation and technology change on the business?

Very effective
10%
Somewhat effective
63%
Not effective
21%
Unsure
6%

– *"[Supply chain] choice and flexibility are key—and IT is starting to give companies brighter headlights and more visibility into problems their vendors and suppliers may be having."*

IT risk and governance continues to pose key oversight challenges, particularly given the pace of innovation and technology change. Is the company's IT governance model keeping pace? "It used to be clear which firms were technology businesses… but today, every business is a technology business."[2] That said, IT continues to be a major blind spot for many boards. As one roundtable participant said, "IT is a different language and it's constantly changing." Noted another: "We're a software development company and even *we* continue to be surprised at how fast IT is moving."

Three IT developments are having a profound impact on business: cloud computing, the "democratization of IT" (through mobile devices, cloud applications, virtualization, etc.), and social media. As highlighted during our roundtables, these developments pose a host of well-publicized "defensive" risks—e.g., data privacy and security, cyber security, and regulatory compliance.

At the same time, IT poses an underlying "offensive" or strategic risk, namely the failure to understand IT as a critical business driver and to leverage technology innovation as part of the company's strategy and business model. Nearly 85 percent of roundtable attendees said their company's strategic planning process was either "not effective" or only "somewhat effective" in dealing with the pace of innovation and technology change.

The impact of these major IT developments is causing directors to probe more deeply in several areas, including:

- Does the management team understand the capability of IT to change the business?
- Do we have the leadership to leverage new IT capabilities?
- How effective is our strategic planning process in dealing with the pace of innovation and technology change on the business?
- Do we understand the risks? Can we manage them?

Directors are also insisting on more robust and *regular* communication between the audit committee/board and the CIO—in plain-English and business context.

– *"Our IT discussion is not a technology discussion—it's a business discussion."*

– *"Board-level conversations about IT should be much more frequent to keep pace with technological change. Our IT discussions may be dramatically different six months from now."*

– *"Internal audit has a big role to play in getting better assurance around IT risk."*

– *"A third-party assessment of your IT risks can be a real eye-opener for everyone."*

– *"Data security threats are also internal, so we now take a hard-boiled egg approach…a hard shell on the outside, but tough security on the inside, too."*

[2] *Taming Information Technology Risk:* A New Framework for Boards of Directors, Oliver Wyman and NACD, 2011

Audit committees are devoting significant agenda time to legal/regulatory compliance risk, with the SEC's final whistleblower rules and the UK Bribery Act front and center. As detailed in our *Highlights from the 7th Annual Audit Committee Issues Conference* (www.auditcommitteeinstitute.com), audit committees are discussing with management the potential impact of the SEC's "whistleblower bounty" program on corporate compliance programs. And with final SEC whistleblower rules now in place, directors are sharpening their focus on the company's whistleblower hotline process:

- Are existing hotline systems operating effectively?
- Are policies and procedures, training, and communications related to the whistleblower/hotline program up to date?
- Is staffing of the company's whistleblower function adequate in the event of an increase in whistleblower reporting?
- Is management's process for addressing whistleblower complaints sensitive to the Dodd-Frank prohibitions against impeding employees from being whistleblowers and retaliation against an employee whistleblower?
- Does the board make use of all channels and sources available to evaluate tone at the top and culture (e.g., whistleblower hotline activity, customer complaints, input from auditors, employee surveys, social media, and site visits)?
  - *"This is about walking the talk—every day and at every level of the company."*
  - *"Be careful about overrelying on a single head of compliance—he or she may not be able to effectively manage all the various compliance issues. An 'aggregator' role may be effective—but be sure the role is clearly defined."*
  - *"Continually ask your internal and external auditors if they have any concerns or issues with how compliance is working."*

The UK Bribery Act—effective July 1, 2011—is a significant change to UK antibribery laws. In many ways more stringent than the US Foreign Corrupt Practices Act (FCPA), the UK Bribery Act makes companies doing business in the United Kingdom responsible for bribery committed on their behalf—e.g., by employees, agents, and subsidiaries. This new law, along with increased global enforcement activities generally, is causing boards to reassess corporate compliance programs to ensure that:

- Management understands the global risks the company faces with respect to bribery—particularly risks posed by agents and intermediaries
- The company has a strong compliance program tailored to the company's risk profile—including training for employees and others throughout the supply chain
  - *"The UK Bribery Act goes beyond FCPA—and all it takes is a UK presence for your company to be at risk."*
  - *"Focus on FCPA, but don't lose sight of compliance with local anticorruption laws."*
  - *"Expect to see a lot more FCPA tips being made to the SEC through the whistleblower bounty program."*

Updates from the CIO?

During the past year, on which of the following topics has your audit committee or board received updates from the company's CIO or equivalent? (Select all that apply)

Company's information security policy*

How the company is managing the risks posed by emerging technologies

Company's policies regarding use of social media

How the company plans to leverage emerging technologies

No updates on any of these topics

Company's plans to use cloud computing

*(*Listed by "most frequently selected")*

Compliance oversight

Does your company's chief compliance officer (or equivalent) provide reports to the board/audit committee at least annually on the status of the company's compliance program and advise promptly of matters involving potential criminal misconduct?

Yes
78%
No
15%
Unsure
7%

Prospects for 2011

What change do you expect in your company's profits in 2011 compared to 2010? Profits will:

Increase moderately
54%
Remain approximately the same
18%
Increase significantly
17%
Decrease
11%

Concerns about the economy

What is your biggest concern right now with regard to the economy?

Economic uncertainty
45%
Continued joblessness
27%
Dealing with regulatory changes
17%
Inflation
8%
New competition
3%

Spring 2011 Roundtable locations

Atlanta
Boston
Charlotte
Central North Carolina
Chicago
Cleveland
Dallas
Denver
North Florida (Tampa)
South Florida (Miami)
Houston
Kansas City
Los Angeles
Milwaukee
Minneapolis
New York
Orange County, CA
Philadelphia
Pittsburgh
Portland, OR
San Diego
San Francisco
Seattle
Short Hills, NJ
Silicon Valley
St. Louis
Washington, DC

Given these developments, it's not surprising that the vast majority of roundtable attendees said their company's chief compliance officer (or equivalent) provides reports to the board/audit committee at least annually on the status of the company's compliance programs and advises promptly of matters involving potential criminal misconduct (although 15 percent said this does not happen, and 7 percent were "unsure").

Two initiatives underway—the PCAOB's project on the "auditor's reporting model," and the European Commission (EC) green paper on "audit policy"—will be of interest to the director community. The PCAOB issued a Concept Release (June 21) on possible changes to the auditor's reporting model, including requiring:

- An "auditor discussion and analysis" (along with the auditor's report) that would include information on matters such as significant audit risks, audit responses to those risks, materiality, auditor independence, and views regarding certain aspects of the company's financial statements
- Use of an emphasis-of-matter paragraph in certain additional circumstances
- A paragraph in the auditor's report that explains the critical decisions made during the audit, with references to the footnotes in which such issues are discussed
- Further auditor association with, or assurance of, the MD&A (or a portion of it)
- Auditor association with an expanded audit committee report.

These potential changes reflect input to PCAOB staff from investors and others who support requiring auditors to provide more information about the audit, as well as the auditor's views on significant aspects of the financial statements. Preparers and audit committee members generally agreed only with the former. Audit committee members/directors can share their views on the Concept Release during the public comment period until September 30 (at pcaobus.org) or at a PCAOB roundtable slated for the fall of 2011.

The EC's green paper—*Audit Policy: Lessons from the Crisis*—poses a number of questions regarding the value of the audit, the independence of auditors, and concentration of the audit market, and proposes ideas to address these topics. A European Parliament report on the green paper is expected in mid-2011.

About KPMG's Audit Committee Roundtable Series

Launched in 1999, the Audit Committee Roundtable Series is hosted by the KPMG's Audit Committee Institute (ACI) in approximately 30 cities every spring (May/June) and fall (November/December). Highly interactive and panel-driven, the roundtable sessions bring together audit committee members, directors, senior executives, and leaders in governance to discuss challenges, emerging trends, and leading practices affecting the oversight of financial reporting and related risks. For more information about the Roundtable Series and resources and events offered by ACI, visit auditcommitteeinstitute.com, or contact ACI at 1-877-KPMG-ACI or auditcommittee@kpmg.com.