

Regulatory compliance

On February 3–4, 2011, members of the Audit Committee Leadership Network (ACLN) met in New York. In one session, members addressed the issue of regulatory compliance.¹ This document reflects a summary of the key points that members raised in the discussion, along with background information and perspectives that members shared before the meeting.² For this discussion, members did not address compliance issues related to the Foreign Corrupt Practices Act (FCPA), which will be discussed at the June summit with the members of the European Audit Committee Leadership Network. [For further information about the network, see “About this document,” on page 10. For a list of participants, see Appendix 1, on page 9.](#)

Executive summary

A number of major themes emerged as ACLN members engaged in a wide-ranging discussion of trends and strategies in the area of regulatory compliance:

- **Audit chairs see a challenging regulatory environment** (*Page 2*)

Regulatory compliance is becoming an ever more demanding challenge for companies as governmental regulation expands and enforcement becomes more rigorous. Even companies’ approaches to compliance itself are becoming subject to governmental directives. ACLN members said company management must engage with regulators to build trust and stronger relationships. Increasingly, even board directors may need to interact with regulators, a development already under way in some sectors, such as financial services.

- **Companies are strengthening their compliance functions** (*Page 4*)

Achieving compliance is a complex endeavor involving the legal function, internal audit, dedicated compliance staff, and ultimately the whole company. Members noted that companies are applying more resources to the task and that they are trying different organizational approaches, spurred partly by governmental directives such as the Federal Sentencing Guidelines. Although the government has pushed companies to have independent chief compliance officers (CCOs) who report to the CEO, most audit chairs believe that the best way to organize the compliance function depends on a company’s specific situation and that a compliance-oriented culture is as important as a specific structural solution. The costs and consequences of noncompliance are clear, but many audit chairs are wondering how to assess the effectiveness of their increased spending on compliance.

- **Audit committees are spending more time on compliance oversight** (*Page 7*)

¹ In another session, members discussed relations with the Public Company Accounting Oversight Board (PCAOB). See Audit Committee Leadership Network, [“Audit Committee Perspectives on the PCAOB,”](#) *ViewPoints*, March 4, 2011.

² *ViewPoints* reflects the network’s use of a modified version of the Chatham House Rule whereby names of members and guests and their company affiliations are a matter of public record, but comments made before and during meetings are not attributed to individuals or corporations. Member quotes appear in italics.

Compliance oversight is an increasing burden for boards. While some boards are creating separate compliance committees, most audit chairs reported that responsibility for compliance falls to the audit committee or a subcommittee of the audit committee. Audit committees hear frequently from the compliance officer, and they are interested in how they might engage more deeply on compliance issues. At the same time, they are worried that a mounting emphasis on compliance could distract the board from other important issues, such as company strategy.

For a list of discussion questions for audit committees, see Appendix 2, on page 10.

Audit chairs see a challenging regulatory environment

The various regulatory initiatives of the last two years are very much on the minds of ACLN members as they consider regulatory compliance. The Dodd-Frank Act and the healthcare reform legislation are two of the more prominent generators of new regulations. Each is highly complex and broad enough to affect companies in a variety of sectors beyond financial services and healthcare. ACLN members pointed to new initiatives coming from other federal agencies as well, such as the Food and Drug Administration (FDA) and the Environmental Protection Agency, as well as to regulations and legislation from state and foreign governments.

Regulators are also becoming tougher in their enforcement efforts, particularly in sectors such as financial services.³ Compliance experts note that regulators are asking for more information, and they want it delivered more quickly.⁴ One ACLN member noted that *“financial institutions must now also achieve the ‘spirit and intent’ of regulations, not just compliance with the rules. How do you know what that means?”* Members also commented on the general demeanor of regulators in interactions with regulated companies. One member said, *“The conversations used to be enlightened, but now they’re reactive – there’s no ability to have a reasonable dialogue.”*

Increasingly, the government is not content merely to establish regulations; it is making efforts to shape companies’ compliance organizations. For example, recent amendments to the Federal Sentencing Guidelines and agreements between regulators and pharmaceutical companies include provisions on how the compliance function and the board of directors should be organized to achieve better compliance.

For ACLN members, the whistleblower provisions in the Dodd-Frank Act are another worrisome aspect of the new regulatory environment. Under these provisions, whistleblowers could earn a bounty as great as 30% of any settlements over \$1 million resulting from allegations of securities law violations.⁵ Critics have pointed out the possibility of harmful unintended consequences, including damage to company compliance programs as employees are tempted to bypass them. An ACLN member remarked, *“It sets up an incredible misalignment of interests.”* Another member said, *“We haven’t yet figured out the best way to handle this.”* The Securities and Exchange Commission is debating the final rules, which, under Dodd-Frank, are due by April 21.⁶

³ Melissa Klein Aguilar, [“Keeping Compliance Effective in Difficult Times.”](#) *Compliance Week*, June 9, 2009.

⁴ Melissa Klein Aguilar, [“Shop Talk: Can IT Save Compliance at Financial Firms?”](#) *Compliance Week*, January 4, 2011.

⁵ Melissa Klein Aguilar, [“Unintended Consequences of the SEC Whistleblower Program.”](#) *Compliance Week*, December 13, 2010.

⁶ *Ibid.*

Responding to the concerns of businesses and others, President Obama recently acknowledged the burden of excessive regulations and issued an executive order calling for a government-wide review of current regulations and the regulatory system: “We’re looking at the system as a whole to make sure we avoid excessive, inconsistent and redundant regulation.”⁷

The cost of compliance – and of failure to comply

The costs of complying with regulations are high, and they were increasing even before the current wave of regulation. A recent study by the Small Business Administration found that the compliance cost of all US federal regulations in 2008 was 3% higher (in real terms) than in 2004. For US businesses, that burden was \$970 billion (in 2009 dollars).⁸ While the burden varies significantly from company to company, this cost works out to be just over \$8,000 per employee per year and can have a significant impact on US competitiveness.⁹

A member pointed out that it can be difficult to measure the total cost of compliance: *“The discrete costs of people with compliance in their title can be quantified. But then there are the structures and processes that are part of the business – they are hard to separate.”* Speaking of a company on whose board he formerly served, another member confirmed that costs have been increasing for some time: *“[Compliance] was the only area, since 2006, where expenses increased.”*

Whatever the costs of compliance may be, the costs of failing to comply are likely to be even higher. One company agreed in 2009 to pay \$2.3 billion in a healthcare fraud settlement with the Department of Justice.¹⁰ As an ACLN member noted in a pre-meeting conversation, fines can be steep: *“You can end up with billions of dollars of liability. For example, you could receive fines for HIPAA data that is [accidentally] released, even if there is no damage done – the fact that it happened is enough to trigger fines.”* In addition to fines and legal fees, noncompliance may also result in remediation measures such as product recalls that can significantly affect both revenues and the company’s reputation.

Engaging with regulators

Faced with burgeoning federal and state regulations and more rigorous enforcement, companies are reexamining their relationships with regulators. Members said it is important to establish good relationships before any problems are identified. As one member put it, *“In dealing with regulatory bodies, it pays to be overprepared and proactive. Get information in front of them; it can create good relations.”* Another member agreed: *“Engagement is key. Most of these folks have way too much on their desks. To the extent that we can facilitate [their work] and educate them, they appreciate it. We can help them look good and build trust.”* One member pointed to the importance of accommodating regulators’ needs in managing the relationship: *“As much as you might want*

⁷ Barack Obama, [“Toward a 21st-Century Regulatory System,”](#) *Wall Street Journal*, January 18, 2011.

⁸ Jaclyn Jaeger, [“Study: Cost of Compliance on the Rise,”](#) *Compliance Week*, December 7, 2010.

⁹ *Ibid.*, 2.

¹⁰ Department of Health and Human Services, [“Justice Department Announces Largest Health Care Fraud Settlement in Its History,”](#) news release, September 2, 2009.



to buck the system, it doesn't work. At [one agency], they wanted one person that they could go to – that was very critical for them.”

Most audit chairs do not participate in meetings with regulators themselves, as that is primarily a management responsibility, but board directors in the financial services sector are more likely to do so, and audit chairs thought this practice might spread to board directors in the healthcare sector.

Companies are strengthening their compliance functions

ACLN members noted that many of their companies are strengthening their compliance functions to meet the new challenges. One member said, *“Everybody has to think on their feet. We’re asking, ‘Do we have the right staff? The right structure? How are we driving [compliance] through the organization?’”* Another member said, *“At [my company], we’re adding people. It’s burdensome and expensive, but it’s a safe harbor. You’re protected from regulators and shareholder suits. We’re working with regulators to identify new requirements.”*



Components of the compliance process

Three basic components can be distilled from compliance experts' perspectives on the process:¹¹

- **Tracking and assessing regulations.** The company needs to understand what regulations are in force or emerging and how they apply to the company and its operations. ACLN members note that this can be very difficult, given the vast body of regulations: *“One big issue around the compliance function is getting our hands around all the regulations we are subject to – making sure we are not missing something.”* For companies operating in multiple jurisdictions, the challenges are even greater.
- **Developing and implementing policies.** The company needs to decide what specific measures are required for compliance and put them in place throughout the organization, using codes of conduct, new procedures and controls, and various forms of training and communication. As a compliance expert notes, new policies must be “considered in the context of existing procedures to avoid unnecessary layers” of requirements.¹²
- **Monitoring, auditing, and documenting.** The company needs to make sure that policies and procedures are being followed and that compliance efforts are being clearly documented. Disciplinary actions must be sufficient to send a clear message that failure to comply will not be tolerated. The goal is to ensure not only that compliance is actually occurring, but that the company can demonstrate that fact to regulators and others.

Reassessing the compliance function's place in the organization

Compliance professionals are currently debating how the compliance function should be organized to tackle its responsibilities successfully. A number of functions within an organization are directly involved in compliance activities, including legal, internal audit, finance, and the compliance function itself. How should their efforts be directed and coordinated? In a recent article, Ben Heineman, the former general counsel (GC) of General Electric, lays out three organizational approaches:¹³

- The chief compliance officer (CCO) is independent of the GC and chief financial officer (CFO) and reports directly to the CEO and board.
- The GC is also the CCO.
- The CCO reports to the GC and the CFO.

Mr. Heineman prefers the third approach because it supports a strong legal function and avoids organizational overlap and confusion, but recent governmental guidance points to different approaches:

¹¹ See, for example, Richard M. Steinberg, *The High Cost of Non-Compliance* (Waltham, MA: OpenPages, 2010), and Ben W. Heineman, Jr., [“Don't Divorce the GC and Compliance Officer.”](#) *Corporate Counsel*, January 2011.

¹² Richard M. Steinberg, *The High Cost of Non-Compliance*, 8.

¹³ Ben W. Heineman, Jr., [“Don't Divorce the GC and Compliance Officer.”](#)

- **Amendments to Chapter 8 of the Federal Sentencing Guidelines.** Chapter 8 of the Sentencing Guidelines outlines the features of an effective compliance program and serves as a benchmark for companies designing such programs. If a company's program is deemed effective, judges can reduce the fines imposed for violating the law. The recent revisions, which came into effect on November 1, 2010, state that a compliance program may be deemed effective even if high-level employees were involved in an offense, as long as certain conditions are met, one of which is that the head of compliance has "direct reporting obligations" to the governing authority, such as the audit committee of the board of directors.¹⁴
- **Corporate integrity agreements (CIAs) in the pharmaceutical sector.** A CIA between a pharmaceutical company and the Office of the Inspector General of the Department of Health and Human Services lays out compliance obligations for the company that have been agreed to as part of a settlement for wrongdoing. While most relevant in the pharmaceutical sector, CIAs are drawing broader attention for their governance provisions, such as their requirement that the compliance officer report to the CEO rather than the general counsel.¹⁵

At the meeting, ACLN members acknowledged the importance of organizational structure. Some members argued for an independent compliance officer along the lines specified in pharmaceutical CIAs: *"We have an independent CCO who reports to the CEO and works closely with internal audit. In a regulated industry, the role is an important function that has to have that level of seniority."* Another member commented, *"The CCO reports to the CEO at one of my companies. In less regulated industries, the compliance officer is with the general counsel."*

Nevertheless, the consensus was that the best structure for a given company depends on its particular circumstances, including but not limited to the level of regulation in its industry. One member explained, *"It's driven by what the company has been through. It can depend on the available talent. At one company, the legal chief reported to the compliance officer. Compliance was very important because of problems they had had."*

If the compliance function is organizationally distinct from the legal department and internal audit, it is critical that all the functions communicate and coordinate their efforts to avoid unnecessary overlap and confusion.¹⁶ Some companies have created compliance committees consisting of senior executives involved in compliance, a measure required in many CIAs.¹⁷

The compliance function should also have close working relationships with the business units, and it can benefit from having operational experience in its ranks. A member said, *"Compliance has to be built into the business processes ... The business units have to think for themselves about what they're doing."* Another member noted that depth of operational experience could be a reason for separating compliance from the legal department or at least ensuring that compliance was not exclusively the domain of lawyers: *"[Lawyers] haven't walked the factory floors, and they haven't worked up the chain."*

¹⁴ Jay G. Martin and Ryan D. McConnell, ["How Revised Sentencing Guidelines Impact CCOs,"](#) *Compliance Week*, May 4, 2010.

¹⁵ John Soriano, ["When the CCO Should Report to the General Counsel,"](#) *Compliance Week*, June 29, 2010.

¹⁶ Melissa Klein Aguilar, ["Tips for Structuring the Compliance Department,"](#) *Compliance Week*, June 8, 2010.

¹⁷ See, for example, ["Corporate Integrity Agreement Between the Office of the Inspector General of the Department of Health and Human Services and Pfizer,"](#) August 31, 2009.

One member remarked on the challenge posed by a dynamic regulatory environment: “One risk for a company that has been around for awhile and is good at compliance is, where do you put the responsibility for new regulations? A new regulation comes up, and companies don’t [necessarily] think through how to reorganize [the compliance function].”

The importance of a strong compliance culture

Some compliance experts argue that a company’s reporting structure is less important than trust and communication among senior executives involved in compliance.¹⁸ These experts also stress the importance of a company culture – nurtured by the CEO – that grants the compliance director adequate clout.¹⁹

Members discussed policies that support a strong compliance culture. One member said, “We have a zero-tolerance policy. We have 15–20 terminations every year. We put it out on the Internet – the incident and the result, but not the name of the person.” Another member noted, “When the company takes action, especially if someone is a ‘producer,’ it sends a strong signal because you’re applying the same standard to everyone.”

Maintaining a strong culture of compliance can be a challenge when integrating acquisitions, particularly acquisitions overseas. One member described the dilemma and his company’s response: “When you make an acquisition, the company doesn’t always have the same control structure. We send someone new into a key financial role to install the proper culture. With regard to control and compliance, it’s a matter of shifting your culture into the [acquired] organization.”

Measuring the effectiveness of the compliance function

Members brought up the importance – and the difficulty – of assessing the effectiveness of the compliance function. One member described the problem: “We introduced a very aggressive anticorruption program worldwide. The question is, how do you know if it’s effective? By the number of hotline calls? By how much corruption is found? We’ve been pushing the compliance officer on how to measure effectiveness. Should we spend less? Or should we spend more?”

Another member offered different criteria for assessing the compliance function: “My personal view is that if they are proactive about steps we can take to protect against certain risks, if they are constantly working to identify material risks, that’s a real plus. But it’s hard to point to results. It’s hard to know if it’s going well.”

Audit committees are spending more time on compliance oversight

The current debate on compliance encompasses not only management’s efforts in this area, but also the question of how the board should oversee their efforts.

Which board committee should oversee compliance?

For one member, the workload associated with overseeing compliance was heavy enough to require a distinct committee of the board: “Risk and compliance are so big in our industry. We have separate compliance committees, with separate leadership. It wouldn’t surprise me if the model spread.”

¹⁸ John Soriano, “[When the CCO Should Report to the General Counsel.](#)”

¹⁹ Ben W. Heineman, Jr., “[Don’t Divorce the GC and Compliance Officer.](#)”

One company's new board-level compliance committee (set up as part of its derivative lawsuit settlement for illegal marketing) will have \$51 million in independent funding for its first five years, with sole authority over how the money is used. It will have five members, three of whom must be independent directors and one of whom must also serve on the audit committee. The committee's oversight responsibility will extend across a number of compliance areas, including drug marketing, Medicare and Medicaid, FCPA, clinical studies and manufacturing quality control, and FDA drug safety reporting.²⁰

Most ACLN members, however, reported that their audit committees oversee compliance. In some cases, audit committees have established compliance subcommittees. A member with such an arrangement said, "Compliance needs time and attention, hence, it's separate. But it also needs integration, so it's a subcommittee. It added workload for the audit committee members, but they're specialists."

How does the board discuss compliance?

ACLN members said their audit committees address compliance frequently, receiving briefings from the head of compliance on a regular basis. As previously noted, the revised US Sentencing Guidelines stipulate that the establishment of "direct reporting obligations" to the "governing authority" for the head of compliance can reduce penalties in the event of violations,²¹ an incentive to deepen contact between the compliance function and the board.

One member noted, "At [one of my companies], we hear from compliance at every single meeting, and we may move in that direction [at my other company]." Some members focus in more depth on specific issues by parceling them out over multiple meetings. A member explained, "At each meeting, we have a compliance report, but at every other meeting, we have an in-depth report on one aspect. We can't cover everything at every meeting, but we do get through it on a rotating basis. The compliance officer is there so we can ask questions."

One member noted that their discussions of compliance are not limited to sessions focused specifically on compliance: "Compliance comes through in lots of areas – it's pervasive." Another member pointed out that employee whistleblower hotline issues also come to the audit committee: "I get emails, we also have a postbox, and we have a phone number. The letters are scanned in, and they tell us what they are working on."

Some compliance experts believe boards should do more in the area of compliance, delving more deeply into how the compliance function works and asking more challenging questions.²² Ernst & Young's toolkit for audit committee members recommends that the audit committee ask a variety of questions about compliance, many of which target the same criteria that management itself would use to gauge effectiveness.²³ For example, how has responsibility for compliance been assigned? Are effective training programs in place? Is there monitoring and auditing? Does the company respond appropriately to noncompliance?

ACLN members, by contrast, expressed concern that too much attention to compliance might adversely affect their ability to address other important issues: "One of my concerns is that we're spending less time at the board

²⁰ Melissa Klein Aguilar, "Pfizer Board Settles on Compliance Committee," *Compliance Week*, December 14, 2010.

²¹ Jay G. Martin and Ryan D. McConnell, "How Revised Sentencing Guidelines Impact CCOs."

²² Jaclyn Jaeger, "Audit Committee Checklist: Compliance Programs," *Compliance Week*, July 27, 2010.

²³ Ernst & Young, *Audit committee member toolkit* (Ernst & Young Global Limited, 2009).



talking about strategy.” Another member described how the audit committee lessens the burden for the full board: “Our audit committee meetings are two hours long, but we condense [the compliance issues] to 10 minutes for the board, so we can talk about strategy. We have an executive session to decide what the board really needs to focus on.”

Conclusion

In the face of increasing government regulation and stricter enforcement, audit chairs see the need for companies to build good relationships with regulators. Companies are enhancing their compliance functions by adding resources, trying out different organizational structures, and bolstering a culture of compliance. While companies and boards are struggling with how to measure the effectiveness of these efforts, they are well aware of the financial and reputational consequences of noncompliance. Boards are also testing different approaches to their oversight of compliance, though the audit committee tends to take the lead. Moving forward, boards will need to balance the increasing demands of compliance oversight with the continuing need for adequate attention to broader strategy issues.



Appendix 1: Participants

Audit Committee Leadership Network members participating in all or part of the session, who sit on the boards of over 30 large, mid-, and small-cap public companies between them, included:

- Denny Beresford, Kimberly-Clark
- Leslie Brun, Merck
- Dick Harrington, Aetna and Xerox
- Judy Richards Hope, General Mills and Union Pacific
- Labe Jackson, JPMorgan Chase
- Mike Losh, AON and TRW Automotive
- George Muñoz, Altria and Marriott International
- Oscar Munoz, United Continental Holdings
- Bill Osborn, Caterpillar
- Bernd Voss, ABB and Continental AG (European Audit Committee Leadership Network member)
- Steve West, Cisco Systems
- Chris Williams, Wal-Mart

Ernst & Young professionals participating in the meeting included:

- Tom Hough, Americas Vice Chair of Assurance Services
- Steve Howe, Americas Area Managing Partner

Appendix 2: Discussion questions for audit committees

- ? What are your biggest concerns about the current regulatory environment and how it might evolve?
- ? What are the costs of regulatory compliance for your company? Do you measure them? Are they increasing? What are the costs of noncompliance?
- ? What do you think will be the impact of the Dodd-Frank whistleblower provisions?
- ? How is your company engaging with regulators?
- ? What aspects of achieving compliance are most challenging?
- ? How has your company organized the compliance function? Is it a separate function, or is it part of another group? Has this arrangement been effective?
- ? Does the CCO (or head of compliance) focus exclusively on compliance, or is this job part of a broader role? To whom does the CCO report?
- ? How are compliance-related policies communicated and implemented across the company?
- ? How does your company assess the effectiveness of the compliance function?
- ? What board committees should oversee compliance? Should it be chiefly the audit committee, or should other committees or subcommittees play a role?
- ? What kind of reports does the committee overseeing compliance receive from compliance staff? What types of issues are addressed?
- ? What kinds of questions does the board ask about the compliance function?

About this document

The Audit Committee Leadership Network is a group of audit committee chairs drawn from leading North American companies committed to improving the performance of audit committees and enhancing trust in financial markets. The network is convened by Ernst & Young and orchestrated by Tapestry Networks to access emerging best practices and share insights into issues that dominate the new audit committee environment.

ViewPoints is produced by Tapestry Networks to stimulate timely, substantive board discussions about the choices confronting audit committee members, management, and their advisers as they endeavor to fulfill their respective responsibilities to the investing public. The ultimate value of *ViewPoints* lies in its power to help all constituencies develop their own informed points of view on these important issues. Anyone who receives *ViewPoints* may share it with those in their own network. The more board members, members of management, and advisers who become systematically engaged in this dialogue, the more value will be created for all.

The views expressed in this document represent those of the Audit Committee Leadership Network. They do not reflect the views nor constitute the advice of network members, their companies, any Ernst & Young member firm, or Tapestry Networks. Please consult your counselors for specific advice. Ernst & Young refers to the global organization of member firms of Ernst & Young Global Ltd., each of which is a separate legal entity. Ernst & Young LLP is a client-serving member firm in the U.S.

This material is copyrighted to Ernst & Young LLP and prepared by Tapestry Networks. It may be reproduced and redistributed, but only in its entirety, including all copyright and trademark legends.

© 2011 Ernst & Young LLP.
All Rights Reserved.
SCORE no. CJ0178