



CULTIVATING A HOLISTIC Compliance Culture

BY JOSEPH M. KELLY, SENIOR EDITOR

CREATING, CULTIVATING, AND SUSTAINING a culture in which compliance and risk management are everyone's responsibility is not a new concept, but it has emerged as a sound model for success. Because regulators have stressed that managing risk across the entire enterprise is the way to meet today's regulatory obligations, bank executives and boards of directors are taking a proactive approach to changing the compliance culture in their institutions. Adopting a bank-wide compliance approach can nevertheless be difficult and requires a mindset change.

Spreading compliance responsibility across the entire enterprise requires a serious commitment from the top of the corporate hierarchy, and employees at all levels must be held accountable for their compliance-related behaviors. Without that top-down buy-in, change is slow and rarely comprehensive. Making compliance a top priority in any bank is challenging, but there are ways to accomplish it.

This article draws on a host of sources—most notably presentations from the 2006 ABA Regulatory Compliance Conference in Orlando, Fla., and the 2006 ABA/ABA Money Laundering Enforcement Conference in Washington, D.C.—to provide a framework for a holistic compliance culture that permeates all aspects of a financial institution. Through this paradigm shift, compliance officers become coaches or mentors, educating and nudging the entire employee base. If bank executives aren't successful in changing the mindset of a bank's employees to focus on compliance, federal regulators are willing to help.



Fear of Reputational Damage

Sometimes it takes a jab from regulators before a bank implements an enterprise-wide approach to compliance. After the very public October 12, 2004 cease and desist order issued jointly by the Federal Reserve and the Financial Crimes Enforcement Network (FinCEN), Birmingham, Ala.-based AmSouth Bank had to make major upgrades to its Bank Secrecy Act (BSA)/anti-money laundering (AML) program. Deficiencies in that area sparked the federal order and seriously damaged the bank's reputation. Today, AmSouth has a fortified BSA/AML program that Cynthia M. Rogers, executive vice president and operations division head, considers among the best in the nation.

Speaking at the October 8-10, 2006, ABA/ABA Money Laundering Enforcement Conference in Washington, D.C., Rogers said, "We focused on cultural adaptation." The new AmSouth BSA/AML program shed its "silo mentality" and made compliance part of its overall culture. The bank reorganized risk management on an enterprise-wide

so to avoid taking a huge reputation hit from a page-one headline, bank leaders are learning from the mistakes of their peers and trying to change the culture in their banks. As Bank of America Senior Vice President and AML Strategy Executive John J. Byrne said during the ABA/ABA Money Laundering Enforcement Conference in October, to see the full power of reputational risk, simply look at the Riggs Bank example. He said Riggs Bank no longer exists because of reputational damage sustained after the May 14, 2004, Federal Reserve cease and desist order and coordinated enforcement actions by the OCC and FinCEN. Reputational damage, while not easy to quantify, can be the type of damage with the deepest impact. So where do bank executives begin when they realize the entire compliance culture at their banks must change?

Defining Compliance

Before you can implement an enterprise-wide compliance cultural change, you must first define compliance. In his June

Spreading compliance responsibility across the entire enterprise requires a serious commitment from the top of the corporate hierarchy, and employees at all levels must be held accountable for their compliance-related behaviors. Without that top-down buy-in, change is slow and rarely comprehensive. Making compliance a top priority in any bank is challenging, but there are ways to accomplish it.

basis under a chief risk officer. That cultural swing began with new policies and procedures. Specific lines of business are now held accountable for developing risk ratings. Extensive training and education throughout the bank is a critical element of the new program, as is monitoring.

Accountability, likewise, must be built into the new culture. "We built in both carrots and sticks," Rogers said, alluding to the rewards and consequences attached to the new compliance initiative. Because of hard work and a serious commitment from management to make compliance—specifically BSA/AML compliance—a priority, AmSouth quickly emerged from the cease and desist order, which was officially lifted April 20, 2006.

"There is life after enforcement action," said Daniel P. Stipano, deputy chief counsel at the Office of the Comptroller of the Currency (OCC), during his remarks on October 10 at the same conference session. He added that about 98 percent of the banks regulated by the OCC have compliant BSA/AML programs. That's a sign that things are getting better, but it doesn't cover the breadth of compliance-related issues. BSA/AML might grab the biggest page-one headlines since the 2001 passage of the USA PATRIOT Act, but it remains just one—albeit a very important—aspect of an overall risk-management program.

No bank wants to be the next example for the industry,

12 general-session presentation at the 2006 ABA Regulatory Compliance Conference, Bank of America's Global Compliance Executive Charles Bowman defined compliance as "the art of enabling businesses to operate legally and ethically in an increasingly complex regulatory environment." He emphasized the word "art." Bowman clarified his definition by saying compliance is many other things, including the following:

- keeping terrorists and money launderers from using your bank
- having accurate and readily reportable mortgage disclosure data
- preventing market timing by associates of mutual funds in your 401(k) plans
- avoiding predatory or unfair lending practices
- ensuring that you protect customer data
- making sure that your entire workforce is properly aware of and trained on your code of ethics, AML, information protection, and Regulation W
- managing regulatory exams effectively
- understanding your legal department's interpretation of new regulations
- working with audit partners to design a control that can be effective and properly validated
- surveilling the e-mail messages of your investment bankers to ensure they're not misusing information



SOURCE: BANK OF AMERICA

- understanding the interplay between the European directive on information protection and the business's demand to consolidate information in common data-bases
- making that crisp and convincing presentation to your finance department on why new monitoring technology you just installed takes 30 more headcount to deal with the output

Implementing a new compliance culture at Bank of America began when then Chief Risk Officer Bill Vandiver told Bowman in July 2001 that he wasn't happy about the bank's inability to develop a "consistent, systematic, enterprise-wide approach to how we talked about compliance." Bowman and his leadership team went into a room and no one left until they had rock-solid answers. One of those answers was a "house of compliance" known as "The Seven Elements of a Compliance Program." The first element, "commitment and accountability," forms the foundation for the remaining six pillars:

- policies and procedures
- controls and supervision
- regulatory oversight
- monitoring
- training and awareness
- reporting

Accountability with Sharp Teeth

As "keepers of the ethical culture of the company," Bank of America's compliance officers were charged with creating cultural change throughout the enterprise, which Bowman described as "the hardest change you'll ever make in any organization." Having management buy-in was a critical catalyst for that initiative. The bank's leadership backed the new compliance approach from the beginning, as evidenced by a memo issued by CEO Ken Lewis. The memo instituted a rating system that directly impacted compensation for the top 100 executives at the company. Each of those executives would be evaluated on his or her compliance-related behaviors and rated on an "exceeds, meets, does not meet" basis.

In the first round of evaluations, Bowman said, some executives didn't take the new compliance initiative seriously, falling into the "does not meet" grouping. Lewis opened eyes when he made it clear that he needed leaders at Bank of America who could meet the expectations of the compliance department. Word spread quickly that the new rating system had teeth and by hitting employees in the wallet, Lewis drove home the point that compliance is important to everyone who works for the bank.

Executives from the bank's main business lines now meet with Lewis annually to provide a snapshot of compliance in their particular business. In one instance, Bowman said, a

division didn't score well and the executive in charge of that division mandated that the code of ethics and compliance training must be completed on time without prompting from the compliance officer. Otherwise, he added, bonuses would be cut. The first offense would result in a 50 percent bonus reduction, while the second would erase the bonus altogether. The third offense would result in termination.

By reinforcing accountability for compliance, Bank of America has been able to implement an enterprise-wide culture that placed compliance at the top of everyone's agenda. "It works," Bowman said. "We haven't had any delinquencies in that group in a while."

Reserve examinations for compliance risk management are not designed to be 'gotcha' games in which examiners look for one-time breaches of specific regulations or laws. Rather, these examinations are designed to assess the adequacy of the structure and processes the institution uses for managing compliance risk. Examiners are expected to look for the bigger picture and to look at the effectiveness of the program (including policies and processes) for managing the organization's compliance risk. We want to understand whether you have the controls in place to manage the risk of your organization."

Later in his presentation, Governor Olson said the Fed-

The key, then, is to set up a strong compliance program that can persevere through negative publicity. How well a bank weathers those inevitable storms depends chiefly on how effectively bank leaders manage risk and cultivate a holistic culture of compliance in their institutions.

Understanding Compliance Expectations

And while accountability has to be part of the compliance culture, positive and negative consequences cannot work alone. There has to be a deeper understanding of why compliance is important. According to Bank of America's Deborah D. Davis, senior vice president and compliance risk executive for global consumer and small business banking, the "first cornerstone is to make sure associates understand why the culture in your organization values compliance. ... If they don't understand why, it won't resonate. You can't just focus on penalties and fines; it has got to be more than a punishment or deterrent." Davis said associates must understand that it's about protecting the brand and the reputation of the brand.

Other compliance professionals agree. During his June 13 ABA Regulatory Compliance Conference presentation, Michael D. Maher, CRCM, CRP, senior vice president for risk assessment at Wells Fargo Home Mortgage, said, "Too often incentives are tied only to an increase in profitability without balance to legal or reputational risk."

Risk management across the entire enterprise has been a common theme at compliance- and AML-related conferences because it's integral to compliance success. To effectively manage risk everyone must be involved. During his June 12 speech at the ABA Regulatory Compliance Conference, Federal Reserve Board Governor Mark W. Olson defined compliance risk as "the risk of legal or regulatory sanctions, financial loss, or damage to reputation and franchise value that may arise when an organization fails to comply with laws, regulations, or standards or codes of conduct of self-regulatory organizations applicable to the business activities and functions of the banking organization."

Governor Olson was specific about what examiners will be looking for when they show up at banks: "Federal

Reserve has "seen organizations silo critical compliance information rather than share it with all levels of the organization, which can handicap an organization's ability to identify systemic risks. As a result, examiners are interested in whether a compliance program is designed to monitor and report compliance concerns."

In essence, then, the trend is toward breaking down silos, improving communication, and managing risk across the whole bank. How do you accomplish that? The answers might lie in the layers of accountability built into a compliance structure.

Structure of a Compliance Culture

Primary compliance accountability lies within individual business lines, but there should be three lines of defense to effectively manage risk, according to Bank of America's Davis:

- First line of defense: lines of business
- Second line of defense: risk management
- Third line of defense: audit (internal and external)

Bank of America has also clearly defined criteria that measure compliance performance and engage executive management commitment and accountability through executive leader compliance ratings, annual compliance business reviews, and periodic executive compliance reports.

For example, Bank of America's annual compliance business reviews with the chief executive office include a standard meeting template and mitigation plan document. Meetings are aligned to line of business (LOB) executives, including major staff support groups and include attendance by the chief executive officer, LOB executive and business leaders, chief risk officer, global compliance executive, general counsel and LOB executives from compliance, risk and legal. The LOB executive is responsible for the presen-

tation and executing mitigation plans. The compliance department is responsible for coordinating meeting preparation, monitoring action plans, and follow-through by the lines of business.

The executive compliance reporting process facilitates an effective and consistent approach for managing compliance risk by:

- providing current quarter and historical trends of compliance program effectiveness
- translating LOB compliance risks into the top significant risks and level/direction of risk
- assessing the 12-month outlook for compliance risk in each LOB
- highlighting significant regulatory activity and accomplishments toward driving a culture of compliance

And while detailed rating systems from large banks demonstrate how a complex system can be set up to change the culture of compliance, smaller banks can still learn from the example. “While all banking organizations should have a program in place to effectively manage compliance risk, these programs can vary considerably depending on the size, complexity, and geographic reach of the banking organization and the inherent risks of its activities,” said Federal Reserve Governor Olson. “As with other types of risk, large multinational organizations will require more elaborate and formal compliance risk management systems to address their broader and typically more complex range of financial activities and to provide senior managers and directors with the information they need to monitor and direct activities.”

Wells Fargo Home Mortgage’s Maher said it is important to build a compliance program properly on the front end for the culture to take hold. For both large and small banks, a compliance program should be built right in the first place, built “fail-safe,” built to be easy to use and intuitive as possible for employees, and built with embedded, preventive controls.

Stuart J. Lehr, CRCM, then senior vice president for compliance risk at Wells Fargo Consumer Credit Group (now an executive at PayPal), said during that same presentation that enterprise risk management (ERM) “provides a way to get the 25,000-foot view of risks.” He said ERM doesn’t replace risk management practices of the business lines, but instead builds upon them. “It is very important to retain business line functions, as the staff in these functions understand the activities of the business and know where control breakdowns have occurred in the past.”

Maher agreed, saying, “ERM seeks to develop the big picture encompassing and having access to all business and support areas.” He said a bank “might be practicing good risk management on an exposure-by-exposure basis but not pay close enough attention to the aggregate exposure across the entire organization.”

Lehr said the structure of a compliance program must be “tailored to fit strategies and business activities” of each



organization. Each bank has to evaluate its businesses and its risks to determine “risk appetite.” That structure must then be shared across the entire enterprise with clear expectations to change the culture.

Training Challenges

Sharing that vision might be one of the most critical steps in changing the culture of a bank. “While the depth and breadth

of training that an employee receives depends on that employee’s role and responsibilities, examiners generally assess whether staff at all levels understand the organization’s compliance culture, general compliance-risk issues, and high-level compliance policies and procedures,” said the Federal Reserve’s Olson.

Unfortunately, training might be one of the most difficult elements to implement in efforts to change a bank’s culture of compliance. Bank of America’s Bowman said banks’ training and awareness efforts are still largely “ineffective because we are still in a ‘check the box’ mentality.” He said there’s still a lot of work to do in the training facet of cultivating a culture of compliance.

“Training and communications are key,” agreed Maher. “Teams need to know they’re accountable and have the training and resources they need to live up to that accountability.”

Conclusion

Said Bank of America’s Bowman, “We’re all going to be in the headlines—that’s a fact. The difference today for me is the level of confidence in the strong health of our institution. I know that people are intent on having a strong culture of compliance.”

The key, then, is to set up a strong compliance program that can persevere through negative publicity. How well a bank weathers those inevitable storms depends chiefly on how effectively bank leaders manage risk and cultivate a holistic culture of compliance in their institutions.

Wells Fargo’s Maher said that regulators expect “clarity of roles, responsibilities, and accountability.” His comments mirror those of the Federal Reserve’s Olson, who said, “As with the broader area of compliance risk management, examiners will look closely at how the compliance culture established at the top of the organization filters down into the everyday responsibilities of business-line managers and how those managers are held accountable for compliance.”

As Bank of America’s Bowman said at the conclusion of his presentation, “It’s all about culture.” BC

ABOUT THE AUTHOR

Joseph M. Kelly is senior editor in the periodicals group at the American Bankers Association. Reach him by telephone at (202) 663-5071 or via e-mail at jkelly@aba.com.