Deloitte.

When "should" becomes "shall"
Rethinking compliance management for banks

Deloitte Center for Regulatory Strategies

Contents

Introduction

In the world of banking supervision and regulation, there is a familiar, longstanding cadence to the issuance of new guidance: regulators issue new guidance; banks parse and interpret it, set a strategy for compliance, begin operationalizing it, and press forward with the knowledge that most new guidance is simply a set of expectations rather than hard-and-fast requirements. In today's environment, the assumption that guidance is just an expectation, not required, is no longer acceptable. A strategy for how a bank assesses its compliance with applicable guidance and then enhances its enterprise compliance management program is of the utmost importance.

Over the past few years, a new wrinkle has emerged, hinging on one small word: "should." Historically, regulatory guidance was delivered in the context of "should." As in, banks should do x, y, or z. Recent developments make it clear "should" is increasingly being interpreted as "shall," at least for larger organizations. New and existing regulatory bodies such as the Consumer Financial Protection Bureau (CFPB), Federal Deposit Insurance Corporation (FDIC), Board of Governors of the Federal Reserve (FRB), the Basel Committee on Banking Supervision, and Office of the Comptroller of the Currency (OCC) are leading the charge on this front, examining banks against compliance risk management guidance, and in some cases bringing enforcement actions for an underlying weakness if it rises to an unsafe or unsound condition or practice and/or a regulatory violation. And, as discussed further below, the OCC's recently proposed rulemaking titled "Heightened Expectations" provides a minimum baseline for effective compliance and risk management.

This environment is creating a new challenge for bank leaders and boards, which must come to terms with the new reality of compliance. Which "shoulds" are really sometimes "shalls?" What is the size and shape of the compliance infrastructure (e.g., people, process, and technology) they need to have in place to remain compliant – and avoid the major fines and reputational risks that come with enforcement? Is the entire organization on firm ground when it comes to compliance? These are the types of questions many banks have been wrestling with recently. As a result, the outlines of a new compliance framework have begun to emerge and take shape. In this paper, we will describe some of the many important tools and considerations being used by industry leaders as they respond to more stringent and forceful regulatory scrutiny.

What if we don't?

While an organization would be ill advised to overtly weigh the cost of noncompliance against the cost of compliance before investing in its compliance risk management program, here are some compelling considerations in today's environment:[1]

- The most severe actions are formal and public. They include written agreements, require prompt corrective action, and may involve consent or cease-and-desist orders. These may be entered into without the board's consent.
- The increased use of formal actions has translated into unprecedented monetary penalties and reputational impacts.
- Since 2009, public actions taken by the CFPB, FRB, and OCC against large banks with more than $25 billion in assets include a total of 64 formal actions in addition to numerous cease-and-desist orders, with 14 such orders being issued in 2013 alone.

[1] Details shown were compiled using enforcement action information published via the following regulatory agency websites: Office of the Comptroller of the Currency (http://www.occ.treas.gov/), Federal Deposit Insurance Cooperation http://www.fdic.gov/), Federal Reserve (http://www.federalreserve.gov/), and Consumer Financial Protection Bureau (http://www.consumerfinance.gov/).

Find your baseline: Strategic self-assessment

A starting point for a bank in determining its compliance with all laws, rules, regulations, and regulatory guidance is to perform a strategic self-assessment of the overall compliance risk management program in light of the new post Dodd-Frank Act regulatory environment. For many banking organizations this is a common technique used today; however, few have actually undertaken the effort required to proactively assess their level of compliance with regulatory guidance, largely because "knowing" hasn't been mission-critical. Today, what you don't know may hurt your organization, and many banks find themselves becoming reactively proactive.

An example of regulatory guidance that has historically been considered by many banks is the Federal Reserve's SR 08-8 guidance on compliance risk management.[2] Another is the proposed regulation involving the OCC's "Heightened Expectations" that codifies its "getting to strong" expectations for banks over $50B in assets, effectively evolving regulatory guidance into requirements.[3] Many banks understand the concepts of SR 08-8 and the OCC's "getting to strong" mantra and have implemented compliance risk management frameworks to address them. However, many banks' execution upon these frameworks is increasingly being viewed by the regulators as inadequate in meeting the arguably heightened regulatory expectations. The shortfalls often involve establishing true independence for compliance management and staff and decisions around the adequacy of the compliance budget, compensation for personnel, performance evaluations, compliance testing, training, policies, procedures, and effective escalation of compliance issues, and may impact the bank's ability to effectively aggregate, analyze, report, and holistically address compliance issues across the enterprise.

Strategic self-assessments can be important tools for the identifying and assessing of how compliance risks are being overseen at both the line-of-business and enterprise levels. In addition, they can be critical in helping organizations prepare for internal audit and regulatory examinations by assisting in proactively identifying issues and noncompliance and allowing for time to address such issues prior to examination start dates. When performing a self-assessment, it is prudent to anchor regulatory guidance to business/enterprise controls and processes, which helps to provide additional insight and transparency of where requirements are being met (or where they are lacking) within an organization.

The self-assessment may be used as a basis for analyzing certain aspects that are key components for a compliance program framework (see Exhibit 1). These key components include governance, risk assessment program and controls, policies and standards, compliance monitoring and testing, reporting and communication, compliance training, compliance technology, and regulatory interaction and coordination. With respect to these components, there appears to be emerging and common industry challenges towards designing and executing effective compliance programs. These challenges underscore the focus of SR 08-8 and include among others:

- A firm-wide approach to compliance risk management that generates meaningful compliance risk information and analysis capabilities, not just static reporting
- Formalized and systematic processes and clear responsibilities and accountabilities to support independent compliance oversight
- Comprehensive and risk-focused compliance monitoring and testing that evaluates control effectiveness as well as compliance with laws and regulations
- Analysis and reporting tools to facilitate effective board and senior management oversight

[2] Board of Governors of the Federal Reserve System. Supervisory Letter SR 08-8. 2008. Compliance Risk Management Programs and Oversight at Large Banking Organizations with Complex Compliance Profiles. http://www.federalreserve.gov/boarddocs/srletters/2008/SR0808.htm

[3] U.S. Department of the Treasury, Office of the Comptroller of the Currency, 2014. OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Bank, Insured Federal Savings Associations, and Insured Federal Branches; Integration of 12 CFP Parts 30 and 170.

Exhibit 1. Critical components of a robust regulatory-compliance risk-management program

Make the map: Strategic planning

Once an organization has determined its baseline and identified any compliance program gaps, the next step is to build a strategic plan. Banks have no shortage of strategic plans in place, but when it comes to compliance, there is often comparative radio silence. For many, that's largely due to the fact that the compliance function is viewed as less important than a growth-oriented, profit-driven line of business. To quote former Federal Reserve Board governor and subsequent outside director for a top-tier U.S. bank Susan Bies, "A culture of compliance should establish—from the top of the organization—the proper ethical tone that will govern the conduct of business. In many instances, senior management must move from thinking about compliance chiefly as a cost center to considering the benefits of compliance in protecting against legal and reputational risks that can have an impact on the bottom line."[4]

In reality, the cost-center view of compliance is quickly becoming outdated, as compliance becomes increasingly enmeshed with core business strategy. In this industry, it is difficult to imagine accomplishing any strategic goal without incorporating regulatory compliance. In fact, a strong compliance function can help an organization gain competitive advantage by mitigating legal and reputational risks and further unlocking value through efficient and effective risk management. So after taking the important step of self-assessment, there's another fundamental question to answer: "How do we take the assessment of our current state of compliance and leverage that information to build our future-state vision and goals?" Building an in-depth strategic plan is the next critical step.

The strategic plan for compliance is a formalized vision and strategy for the compliance function – one that answers familiar strategy-level questions such as:

- What does our compliance function seek to achieve?
- What is the mission and vision of compliance?
- How will compliance support core business goals?
- Is there an opportunity to drive further cost efficiency through the use of technology and tools?

What a strategic plan should look like

While there's no official view on what a strategic plan should look like, the contents listed below offer a good guide as to what key components should be considered. As you can see, the intent of the plan is to go well beyond a gap analysis. It should be a practical, strategic guide to compliance risk management.

- Executive summary
- Mission statement
- Vision statement
- Global regulatory environment
- Current-state observations
- Future-state vision

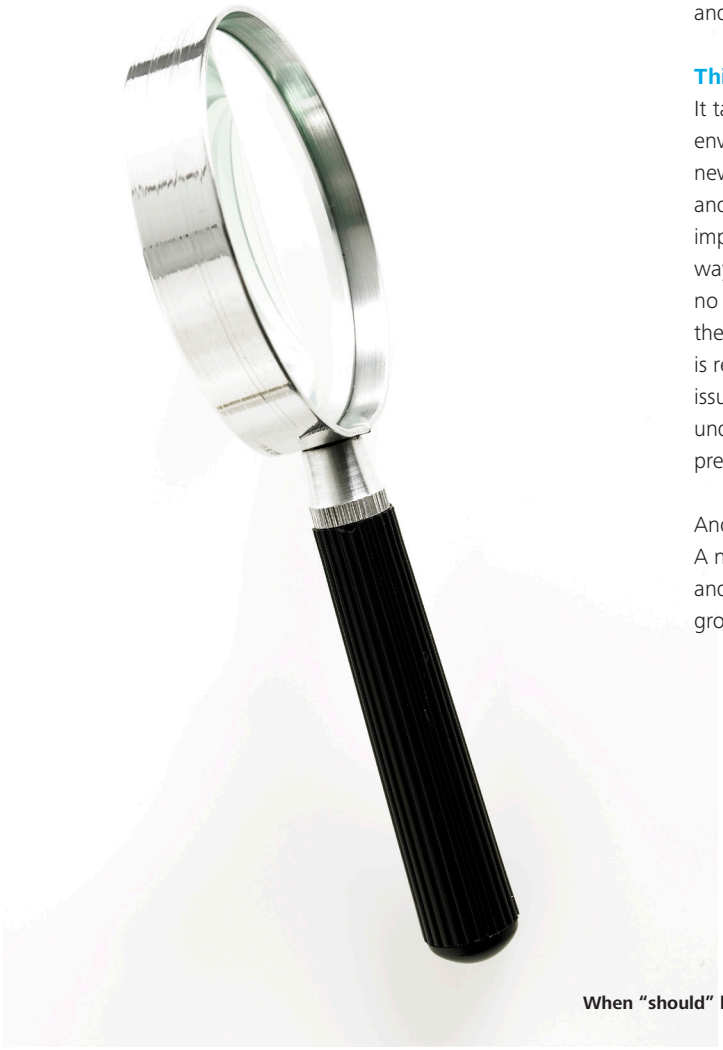
It is also important to remember that this is a strategic plan just for compliance risk, not risk management overall. An organization may already have a strategic vision for risk management. But compliance risk is too critical to be addressed merely as a subset of the overall risk management plan. A compliance-specific strategic plan should be developed to align with the overall vision of the organization while diving deeper to compliance-specific development needs.

In addition to providing the organization with significantly increased clarity on the desired role of the compliance function, such a plan can be a useful tool in communicating with regulators. Regulators recognize that to maintain or become compliant in a radically changed environment is a challenging proposition that won't happen overnight with the waving of the proverbial magic wand. Besides the fundamental core day-to-day compliance activities, regulators also want to know that an organization has a plan for getting there – along with the board and executive team. The strategic plan certainly may help.

[4] Bies, Susan Schmidt, "Enterprise-Wide Compliance Programs," Remarks at the Bond Market Association's Legal and Compliance Conference, New York, NY, February 4, 2004. http://www.federalreserve.gov/boarddocs/speeches/2004/20040204/default.htm

All about execution: The action plan

Once the strategic plan has been built, detailed actions and milestones for executing the plan should be defined and documented via an in-depth action plan. The action plan should address gaps identified during the self-assessment process, actions required for implementation of the strategic plan, and any open regulatory findings pertaining to the bank's management of compliance. Associated target completion dates for each action should be identified. These dates should be heavily considered and discussed prior to being documented as it is likely that the action plan will be shared with internal audit and the regulators and dates will be socialized, especially if there are any open regulatory findings related to any actions.



In addition to dates, accountable executives should be aligned to each action. Demonstration of executive accountability and tone at the top is key in satisfying regulatory expectations and, more importantly, in cases where an organizational transformation is taking place, the bank's associates. It is critical that associates experience the commitment to change at the top of the house as their willingness to play an integral part in the operationalization of the bank's strategic plan and target operating model is vital for the success of the future-state vision. Successful execution of the action plan will typically lead to the development of or revision to various elements of the enterprise compliance management program, including but not limited to the following: governance and critical compliance risk management committees, global compliance policy and procedures, risk assessment process, and a monitoring and testing methodology.

This doesn't happen overnight

It takes time to move the needle on compliance in a new environment like the one banks face today. There are new policies and procedures to be developed, socialized, and implemented with people, process, and technology impacts to address across the organization. But the only way to gain momentum is to begin making some moves, no matter how small. In this case, the place to start is with the self-assessment. Just remember that the assessment is really a commitment. It will uncover gaps and other issues that must be addressed. An organization shouldn't undertake the step of conducting an assessment unless it is prepared for the demands that follow.

And, many could say that this exercise is not just a nicety. A new approach to managing compliance risk is necessary and is now a more-important-than-ever component of a growth plan.

Contacts

J.H. Caldwell
Partner
Deloitte & Touche LLP
+ 1 704 227 1444
jacaldwell@deloitte.com

Susan Jackson Redman
Senior Manager
Deloitte & Touche LLP
+1 312 486 1879
sujackson@deloitte.com

John Graetz
Principal
Deloitte & Touche LLP
+ 1 415 783 4242
jgraetz@deloitte.com

Anna Blythe Papson
Manager
Deloitte & Touche LLP
+1 704 887 1870
apapson@deloitte.com

Thomas Nicolosi
Principal
Deloitte & Touche LLP
+1 215 405 5564
tnicolosi@deloitte.com

DCRS
Deloitte Center
for Regulatory Strategies

About the Deloitte Center for Regulatory Strategies
The Deloitte Center for Regulatory Strategies provides valuable insight to help organizations in the financial services, health care, life sciences, and energy industries keep abreast of emerging regulatory and compliance requirements, regulatory implementation leading practices, and other regulatory trends. Home to a team of experienced executives, former regulators, and Deloitte professionals with extensive experience solving complex regulatory issues, the Center exists to bring relevant information and specialized perspectives to our clients through a range of media including thought leadership, research, forums, webcasts, and events.

www.deloitte.com/us/centerregulatorystrategies