



© PM Images/Getty Images

R I S K

Compliance in 2016: More than just following rules

The traditional approach is losing effectiveness. Banks must turn the page and build a new model.

Piotr Kaminski and Kate Robu

The tougher compliance environment has not only multiplied the various regulations that financial institutions must follow but has also made it necessary for banks to think about compliance in an entirely different way. Those that throw out the old playbook and adapt to this new reality may enjoy a distinct competitive advantage.

Since 2009, regulatory costs have increased dramatically relative to banks' earnings and credit losses. More important, the scope of regulators' focus continues to expand, with new issues emerging and getting more attention. They include conduct risk, the quality of banks' corporate and risk culture, the next generation of anti-money-laundering measures, and third-party risk management. Banks, as they must, have continued to respond to these immediate pressures.

But the industry also needs to implement more structural changes in its compliance processes to make its risk and internal-control frameworks more effective and sustainable over time.

The traditional model for bank compliance was designed in a different era for a different purpose. An institution's compliance professionals would operate largely in an advisory capacity, having less to do with identifying and managing risks. Rather, they would lend their insight to higher-level executives, resulting in inconsistent influence on actual business practices.

Under this model, the compliance team has a limited understanding of business operations and underlying risk exposures. As a result, many banks still operating this way struggle with fundamental

control issues in the first line of defense, such as compliance literacy, accountability, performance incentives, and risk culture. Compliance activities tend to be isolated, lacking a clear link to the broader risk-management framework, governance, and processes. More often than not, the net result is a dramatic increase in compliance and control costs, with either limited or unproven impact on a bank's lingering risks.

To turn the page and enable a more sustainable compliance model, banks should consider these four principles.

Own the risk-control framework

In most cases, banks need to transform the role of the compliance department from serving in an advisory function to having direct influence on risk management and monitoring. In practice, that means becoming an active co-owner of risks and providing independent oversight of the control framework. Given this evolution, compliance specialists now must focus on these four responsibilities: having an independent and objective perspective on the quantum of residual compliance risk; translating laws, rules, and regulations into specific operational requirements; requesting and approving remediation activities; and shaping the bank's overall risk culture and literacy.

These expanded responsibilities require an unprecedented level of insight into business practices, necessitating new compliance practices such as incorporating process walk-throughs into risk assessments, monitoring significant operational changes, and developing residual-risk metrics and markers.

Integrating a common compliance vision into an institution's separate business units is also increasingly important. Institutions should stop thinking about different compliance risks as being embedded just within individual business

units. That silo model should shift to one where business-unit coverage is combined with horizontal expertise around key compliance areas.

Focus on what's getting through the cracks

A common compliance practice is to mandate business-led identification of high-risk processes, as well as all risks and all controls that pertain to them. But this approach falls short of achieving transparency into all material-risk exposures. It often becomes merely a mechanical exercise, resulting in lengthy, qualitative, and indiscriminate lists of risks and controls instead of identifying material-risk exposures and their root causes. Essentially, this model means a bank's understanding of the residual risks, which might be getting through the cracks, is insufficient.

The new compliance approach needs to focus instead on residual-risk exposures in order to ensure that no material risk is left unattended and then enable effective corresponding oversight and remediation. It should tie regulatory requirements directly to specific process break points by defining which risks apply to a given business process, identifying exactly where they could occur and why, and defining objective key risk indicators in the areas where a process creates material residual-risk exposure.

Tie compliance to operational-risk concerns

A modern compliance framework must be integrated with the bank's operational-risk view of the world.

Integrating the management of these risks offers tangible benefits. It ensures a comprehensive coverage of risks, lessens the burden on the business and the control functions, and facilitates a more efficient allocation of enterprise resources and management attention.

Banks can start this journey by developing an integrated inventory of operational and compliance risks; standardizing risk, process, product, and

control taxonomies; coordinating risk assessment, remediation, reporting methodologies, and calendars; and clarifying roles and responsibilities among control functions for each material-risk type to ensure there are no gaps or overlaps.

Some banks are also making changes in the organizational structure and placement of the compliance function. A few global banks have moved compliance under the supervision of the risk department, which reinforces the view of compliance as a control function rather than an advisory function and facilitates an integrated view across all risk types.

Monitor and measure progress from the top down

The three previous principles help in executing a multifaceted compliance transformation. But banks can maximize the impact of a new compliance approach by rigorously monitoring how progress is meeting desired outcomes. A clear tone from the top and active board oversight in measuring the success of a more structural compliance system are important. An institution should monitor progress

in raising the stature of compliance, creating an integrated view of all risks, achieving a strong risk culture, driving risk ownership, employing a risk-based program to assess compliance risks, using quantitative metrics and qualitative markers to measure compliance risk, and ensuring that the first line of defense is taking action and owning compliance and control issues. ■

[This article appeared in *American Banker* on January 27, 2016, and is reprinted here by permission.](#)

Piotr Kaminski is a senior partner in McKinsey's New York office, and **Kate Robu** is a partner in the Chicago office.

The authors wish to thank Andreas Kremer and Daniel Rona for their contributions to this article.

Copyright © 2016 SourceMedia. All rights reserved.