FEBRUARY 2017

RISK

Sustainable compliance: Seven steps toward effectiveness and efficiency

Banks do not control the demand for compliance, but they can optimize the effectiveness and efficiency of their response.

Piotr Kaminski, Daniel Mikkelsen, Thomas Poppensieker, and Kate Robu

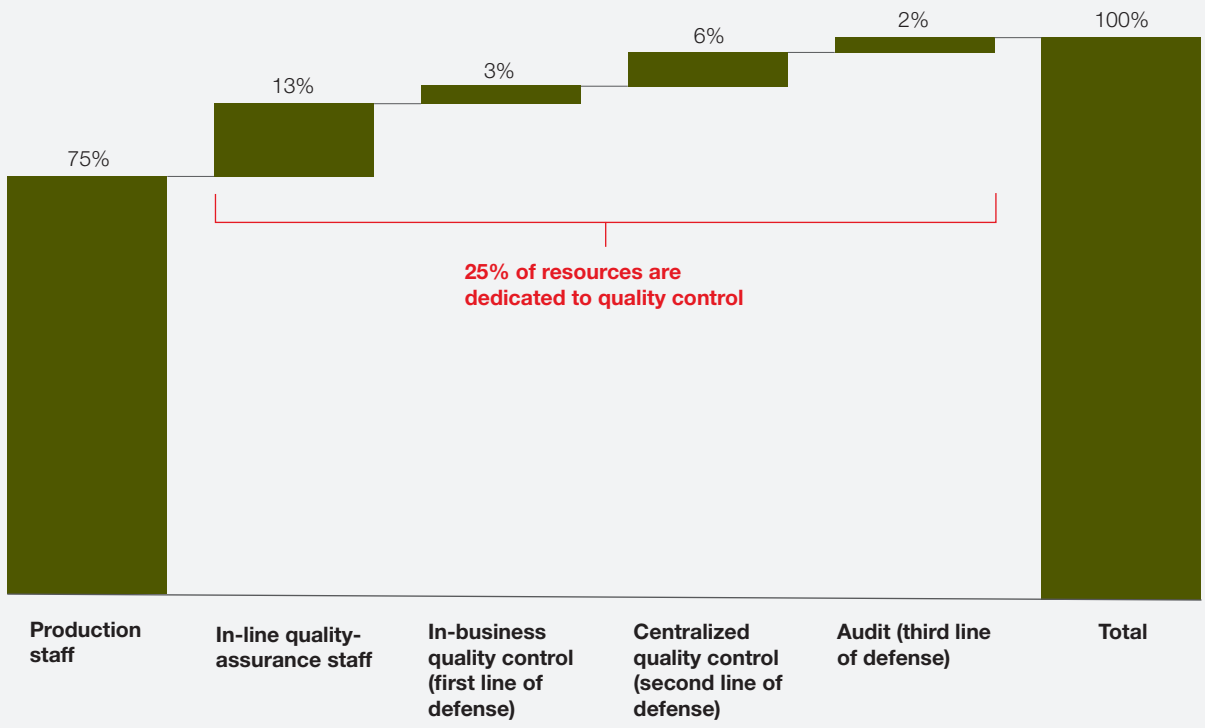
The cost of regulatory compliance in banking rose dramatically in the years after the financial crisis. Some of the increase came from investment in technology, but most of it was—and remains—driven by additional staff. The crisis triggered numerous critical control failures that required immediate remedy. Institutions responded, appropriately enough given the urgency, by adding layers of control. An idea of what resulted can be seen in a typical example. At a large universal bank, a quarter of one business unit's resources is now dedicated to control, significantly reducing the share focused on the business (Exhibit 1). While the exact numbers will vary by institution and business unit, what's certain is that more resources than ever before are being dedicated to testing, monitoring, and other oversight responsibilities—at the expense, given budget limits, of production resources.

The investments have magnified industry resilience and improved the quality of risk management. The high cost, however, is now coming into focus. At many financial institutions, business, compliance, and risk practitioners are beginning to question the sustainability of the resource-intensive approach to managing compliance risks. We believe they are asking the right question. Banks are still adding layers of control as the remedy of choice for compliance issues. The result is an unwieldy "system" of overlapping controls that is difficult to automate and does not address the true root

Exhibit 1

More resources than ever before are being dedicated to testing, monitoring, and other oversight responsibilities.

Breakdown of FTEs[1] across lines of defense,[2] US banking example



[1] Full-time equivalents.
[2] Figures may not sum, because of rounding.

causes of risk. Arising issues are approached one at a time and in isolation; remediation efforts are inadequately measured and tracked.

Fragmented efforts, manual processes, mountains of data

We analyzed the time spent on remediation at one global financial institution according to the importance (materiality) of the issue. We found that first- and second-line compliance staff were spending 80 percent of this time on issues of low or moderate materiality, and only 20 percent on critical high-risk issues. The issues were approached individually, according to an "issue log" with thousands of entries. Unsurprisingly, separate remediation initiatives and audit reports were often directed at the same processes and had the same underlying causes. These could have been addressed systematically, but individual projects did not have the budget to take that on. Only when the institution took an enterprise-wide view did the case for IT investment become clear.

The status quo approach to compliance does not allow for an integrated view across the enterprise. The approach to risk assessment is fragmented: some risks are covered by multiple assessments and others not at all. Nor does a consistent

understanding of the material risks emerge, as the varying standards of materiality and testing produce conflicting results across the organization. Compliance, activities relating to banking secrecy and anti-money laundering (BSA/AML), operational risk, third-party risk, and other assessments are performed frequently by separate teams applying different approaches, and much effort is expended in reconciling the outputs. At one large financial institution, we found that business leadership teams are required to participate in 20 or more risk-assessment activities annually, led by the various control functions. Yet despite all this labor, top management still cannot obtain a reliable view of the institution's biggest compliance exposures nor on the state of controls governing them.

Many leading institutions have tried to shift compliance frameworks toward a more risk-based approach. They have struggled to escape an orientation to procedural adherence and refocus on residual risk (outcomes). Metrics present another challenge. Rather than forward-looking measures of risk, many are ill defined and generate data with unclear implications. As mountains of details pile up, critical exposures can get lost easily. Legacy controls remain in use as new metrics are added. Many intermediate controls and testing can be removed, however, as a recent efficiency effort at a bank's consumer business demonstrated. The needed solution (expanded sample-based quality-assurance testing on executed affidavits) was simpler, less time consuming, and more effective in disclosing material exposures. And it was less costly than the existing haphazard system.

The value in sustainable compliance

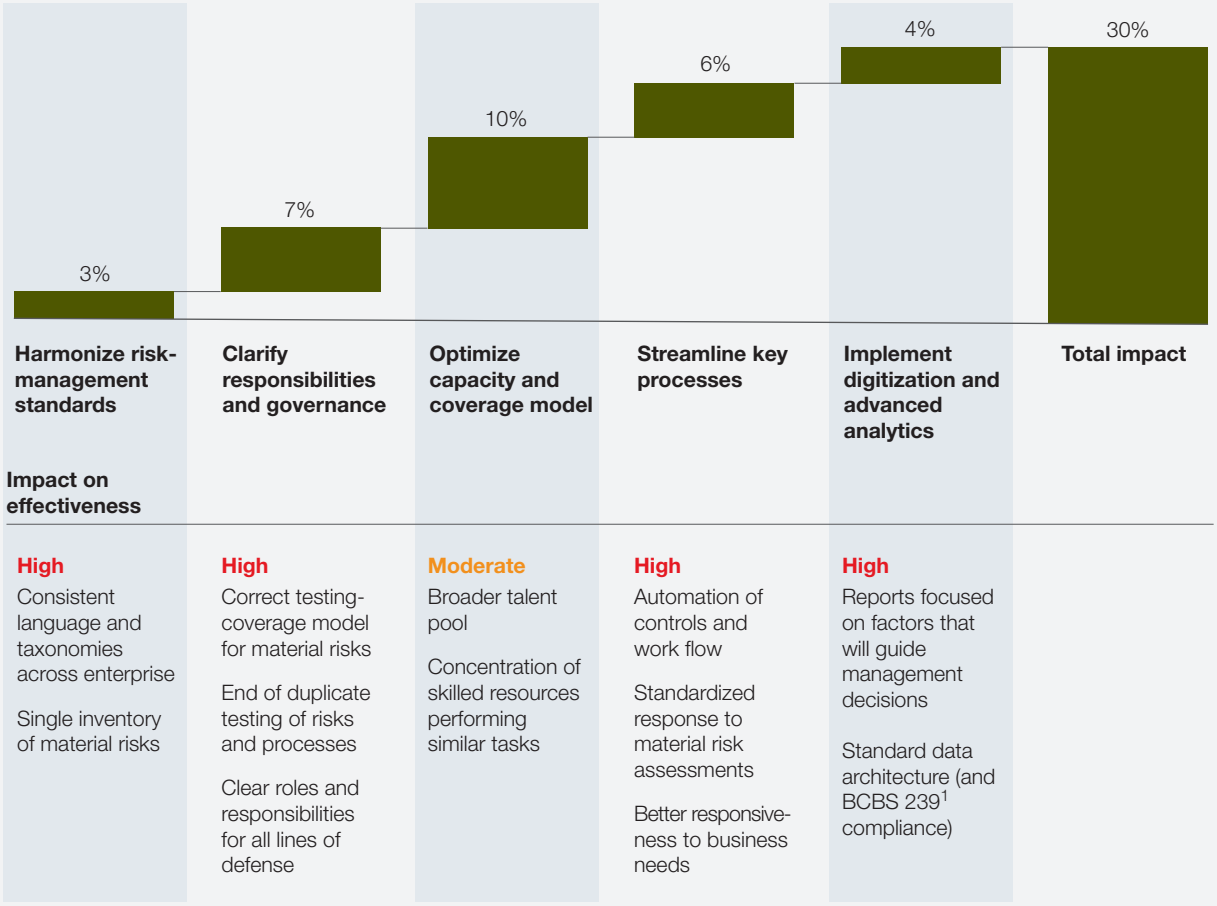
The aim of a sustainable compliance program is to improve the bank's risk profile through a more effective and efficient compliance function focused on the most important risks. The approach both centers on material risk and eliminates inefficient activities. In our experience, it can free up to 30 percent of the compliance function's capacity (Exhibit 2). The size of the opportunity depends on the starting point of the bank: leaner institutions will benefit from effectiveness improvements, while institutions with heavier quality-assurance, control, and audit structures will additionally benefit from meaningful efficiency savings.

One global financial institution recently developed a set of initiatives to free up 20 percent of capacity in its risk and compliance functions. The starting point was organizationally heavy: the two second-line functions accounted for one-third of corporate function expenses. The resource footprint was 95 percent concentrated in high-cost metropolitan areas with very competitive talent markets. At the same time, effectiveness was inadequate, as evidenced by a growing backlog of regulatory issues and audit findings. Risk-management standards, including taxonomies and tolerances, varied across and within lines of defense; "shadow" testing and monitoring activities were being performed by business lines (the so-called one-and-a-half line of defense); and modeling, analytics, and reporting activities were fragmented across the first and second lines.

The improvement program prioritized initiatives that enhanced the effectiveness of compliance and risk-management activities and their efficiency, to achieve a sustainable operating model to support future growth. Better effectiveness was sought by taking a proactive approach to help the business manage material risks. Rather than reacting to issues, the bank would diagnose root causes and translate regulations into operational requirements. Effectiveness was further fostered through timely and adequate transparency into the state of risks and controls, and increased confidence that no material risk would be left unattended. The functions became more efficient through the automation of tasks and controls and easier access to qualified talent. The resource footprint was optimized, aligning it with

Exhibit 2

A program for sustainable compliance can free up to 30% of the function's capacity, improving the effectiveness of risk management.



[1] Basel Committee on Banking Supervision's regulation number 239.

business and strategic needs. Resource allocation could then focus on material risks, boosting staff productivity. Nonessential work was minimized, including the remediation of low-materiality risks. Testing, reporting, and other activities were rationalized across the three lines of defense; duplication, especially in the control functions (such as remediation tracking and risk identification and assessment), was largely eliminated.

Building it: Seven steps to sustainable compliance

Compliance practitioners point out that compliance activities are triggered by regulatory requirements and by how well businesses manage regulatory risks. Regulatory demands, they argue, are outside the control of the compliance function, while the adroit management of regulatory risks takes time to mature. In our view, the key to sustainable

compliance is how well the compliance function responds to these demands. Below we lay out seven practical steps that institutions can take to move closer to sustainable compliance.

1. Transform frontline units into a true first line of defense.

At many institutions, frontline units have "outsourced" a significant portion of their compliance responsibilities to the second line of defense, relying on the compliance function for everyday compliance-related business and control decisions. At other institutions, both lines of defense are involved in similar activities, leading to duplication and fragmentation of effort. These two faulty approaches are avoided when roles and responsibilities are appropriately defined. There is real value in having a strong first line of defense handling everyday business and in-line control activities. The role of the second line varies based on the type of compliance requirements. Some regulations can be translated into a set of clear operational requirements—this is called "rules-based compliance." Other regulations, such as consumer protections, reflect regulatory intent for a desired outcome. This is called "principles-based compliance," which does not easily convert into specific operational and control requirements.

For rules-based compliance, the second line needs to define clear standards and shift in-line execution and approval (such as consumer disclosures) to the first line of defense. For principles-based compliance, some decisions (such as the suitability of marketing materials) need to be embedded in the first line with adequate training, certification, and monitoring. Conduct risk in retail banking, for example, will present challenges in defining first- and second-line roles and testing and monitoring responsibilities. The compliance function will need to clearly articulate regulatory requirements for disclosures, adverse action, advertising, and privacy—and then provide technical expertise as business lines translate those requirements into operational procedures, practices, and controls. Compliance also needs to define requirements for training and certification (including in general areas such as product design and usage and fair and nondiscriminatory treatment), and ensure that they are met by all relevant stakeholders. The execution of control, such as authorizing accounts or approving new products, should, however, be embedded in the first-line processes. The second line will focus on independent approval and risk-based testing to ensure that controls do indeed work as intended.

As the second line, the compliance function defines and monitors control standards; the complementary role for the first line is to manage those controls more strategically. Accordingly, the control office in each business unit organizes how the front line manages its control environment—the front line reviews the business setup against the controls in the context of the inherent risk profile and business complexity. When global banks streamline their business footprint (for example, by offering products across markets or the customer portfolio), the related business processes and systems become essential in managing the inherent risk profile.

2. De-risk and reengineer business and compliance processes.

The demand for compliance resources can be significantly reduced by reengineering labor-intensive activities for core compliance processes, such as onboarding or transaction approvals. For control breaches, root-cause analysis is critically important. This will ensure that the true underlying drivers will be revealed for effective, lasting remediation. Further similar breaches—and the consumption of further resources, such as the addition of more checkers—are eliminated by the automation and redesign of the exposure areas. An

additional important measure is the development of consolidated risk-assessment requirements across control functions for key business decisions. This way, duplicate functional controls—such as legal, BSA/AML, information security, and compliance requirements for new clients—can be eliminated and businesses freed from repetitive requests.

For one wealth-management company, automation of know-your-customer (KYC) controls reduced the turnaround time for the new-customer-onboarding process from five or six days for the most complex institutional accounts to 24 hours. The cost of KYC was reduced by more than 70 percent and the customer experience dramatically enhanced. These savings of time and money were possible because the institution tackled KYC requirements, along with credit-process digitization, as an integrated reengineering and automation program. The initiative was built on the understanding that the end-to-end process is no faster than its weakest link—which is often the compliance requirements.

3. Optimize the compliance operating model.

The compliance resources needed to support the business units can be configured most effectively and efficiently by consolidating subject-matter expertise and core activities in centers of excellence and utilities. This will help ensure that the best expertise is applied across channels in business-unit-facing compliance teams. Additionally, the opportunity in optimizing the location strategy for compliance is often sizable. A new look at location could lead to lower structural costs for compliance and offer access to global talent markets to tackle the challenges posed by talent scarcity in traditional locations. A diversified geographic footprint also ensures greater resilience in the face of adverse business or market events.

4. Focus on what matters.

Compliance with laws, rules, and regulations is viewed by banks as a zero-tolerance activity. Nevertheless, the time spent on each compliance demand must be differentiated according to the bank's highest sensitivities and biggest risks in noncompliance. Time and resources, that is, should be allocated to the risks that matter most. Usually at the top of the list are finance laws and customer and market conduct.

Detailed adjustments can be made in the frequency of testing and sample sizes, depending on the level of inherent exposure in a given operational area. Moreover, testing and remediation activities can be risk-ranked and embedded in resource- and investment-allocation processes. Compliance priorities can then be regularly reassessed to account for new risks, defective controls, and business or regulatory changes.

Ongoing prioritization based on risk requires that organizations objectively measure residual risk exposures and know where in the business process controls can potentially fail. Understanding where the critical breakpoints occur in business processes and having a manageable set of quantitative, forward-looking metrics for each process breakpoint are critical capabilities. For risks that are difficult to quantify (such as internal conduct or fair and responsible banking), banks can develop qualitative risk markers. Trends in staffing levels or changes in business processes and technology often correlate with increased risk. Even if quantitative metrics that directly measure residual risk cannot be defined, qualitative tracking of these trends can alert the institution about potentially increased exposure. With AML compliance, for example, some exposures can be measured through quantitative key risk indicators, while others will require qualitative risk markers (Exhibit 3).

5. Actively manage controls and management-information systems.

The portfolio of controls needs to be actively managed over the life cycle of each control. Old

Exhibit 3

The effectiveness of anti-money-laundering controls can be measured by quantitative key risk indicators or qualitative risk markers.

KRI example Risk marker

Requirements	Key risk indicators (KRIs) or risk markers	Residual risk	Test questions
Customer risk assessment	New customers not risk-rated appropriately or in a timely manner	**Medium**	Customer due-diligence requirements obtained and risk appropriately rated? If high risk, was customer added to high-risk log?
	High-risk customers not reviewed appropriately or in timely manner		
Report filing	Customer-transaction reports (CTRs)	**High**	Was assessment of money-laundering risk completed in time?
	Monetary-instrument logs		
	Suspicious-activity reports (SARs)		
Customer identification program (CIP)	New customers not provided with CIP notice at or before account opening	**Low**	
	New accounts with inadequate verification of identity		
	Existing customers without timely, complete, or correct due-diligence review		
Employee incentives	Reporting forms (SARs, CTRs, CTR exemptions) completed by the same employee who made the decision to file the reports or grant the exemptions	**Medium**	**Risk marker** indicates misaligned incentives due to lack of segregation of duties
	Volume of CTRs in relation to volume of exemptions (did additional exemptions significantly reduce CTR filings?)		
	Growth in higher-risk operations[1] without proportional increase in CTRs and SARs		**Risk marker** indicates operations are outgrowing capabilities of compliance program (training, onboarding, monitoring)

[1] Higher-risk-customer examples: foreign financial institutions, deposit brokers, cash-intensive businesses, nongovernment organizations. Higher-risk-product examples: ATMs, private banking, foreign-correspondent accounts, trade finance, foreign exchange.

Source: FDIC, BSA/AML Office of Foreign Assets Control regulation; Federal Financial Institutions Examination Council, *BSA/AML Examination Manual*

controls, testing strategies, and management-information systems (MIS) should be discontinued quickly when no longer needed or when deemed ineffective. Clearing away unneeded controls saves compliance and business resources and helps ensure that material risks are not missed. Many controls are redundant or obsolete—such as reports for a particular issue that no longer exists. Others have been added to old processes where underlying problems have not been remediated.

The result is layers of detective controls but few preventative controls. For many activities, controls are overabundant and it is unclear which are the key controls that truly make a difference. A bank can have hundreds of mostly weak controls in its trading chains without understanding that 20 are the most important (and should be perfected and tightly monitored to mitigate risk). Finally, controls are often ineffective because they are insufficiently understood and consequently undermanaged (for example, supervisors may not understand their roles and control responsibilities).

Markets businesses are a particularly challenging area for managing controls. These involve many frontline and middle- and back-office units, as well as risk and finance. We have encountered situations where more than 500 controls are in place, from supervisory controls in the front office to extensive reconciliation and reporting controls. A source of the challenge is the separation between units where risks emerge and those in charge of the controls. For example, frontline conduct risk may arise from ill-defined trader mandates or trade and booking data structures, while control responsibility rests with middle- and back-office units. These units, like compliance or control and settlement, might react by adding layers of control without identifying and addressing root causes upstream.

By rationalizing the control portfolio, most banks will be able to reduce monitoring and testing activities significantly. The remaining controls should then be automated, where this is possible (such as system checks or work flow). In-line quality controls, such as document-quality tollgates, can replace manual checkers for controls that cannot be fully automated.

For example, according to a legacy requirement of a consumer business unit at one bank, post-underwriting quality control of all new loan applications was performed by both an internal quality-control team and external attorneys. This triple-checking was replaced by quality tollgates much earlier in the process and automated data pulls that prevented errors. That eliminated most of the rework and expensive back-and-forth communications by attorneys, production, and the quality-control team.

6. Optimize testing and monitoring activities.

Duplication and overlap should also be eliminated from testing and risk-assessment programs, including BSA/AML, operational risk, IT risk, and first-line-of-defense activities. Furthermore, monitoring and testing standards need to be aligned with compliance standards in the first line of defense. These should be clearly tied to the inventory of material risks, associated key risk indicators, risk markers, and MIS. These measures will provide a clear line of sight to the risks the organization should focus on, what is being measured, and how the information will be used to make management decisions and prioritize resources.

Having eliminated overlap, banks can streamline the remaining testing and monitoring activities. For rules-based compliance, subjective assessments can be replaced with objective measures of residual risk—actual defect rates for critical regulations. Meanwhile, manual testing methods should, where possible, be replaced with system-driven exception reporting, such as timeliness and accuracy of customer disclosures based on time stamps and figures in the system of record. Advanced analytics can be deployed to analyze financial, operational, and control performance and identify patterns and hot spots. This level of automation of manual tasks can provide an early warning of failing controls, obviating headaches down the road. For monitoring and testing activities requiring manual intervention, a testing utility can be created to standardize tests and improve load balancing. This will help ensure that capacity is utilized efficiently and according to target quality standards.

7. Effectively manage supervisory and audit issues.

At many banks, remediation of supervisory and audit issues accounts for a large part of the compliance budget and the related change-the-bank budget. In most cases, banks handle supervisory and audit issues individually. Each major finding results in a separate project, and little thought is given to related control issues and root causes. In our experience, the attendant costs of this approach can be significantly reduced by moving to a more integrated portfolio-management approach.

Projects need to be managed on two dimensions: the underlying issues and the affected business areas. Supervisory issues related to client onboarding in the commercial-banking business unit, for example, need to be consolidated to avoid duplicating enhancements of core business processes. Effective KYC management for global banks in fact requires a centralized, cross-division view of customers and their business activities. Without this view, suspect activities could escape detection, or inconsistent client onboarding approaches and decisions may result. To address related BSA/AML issues, furthermore, banks will likely require a comprehensive and integrated approach to control design, to avoid uncoordinated technology efforts.

Supervisors rightly value an adequate focus on the root causes of issues. Banks that have this focus are able to design changes to core business processes that stop issues from arising in the first place. When issues are addressed individually, the solution is often to put in place additional layers of manual controls. Root-cause analysis helps an institution become more resilient in its business environment while reducing reliance on costly manual controls.

Where manual controls are still required to plug an existing gap, banks need to develop plans to automate them and/or redesign the underlying business process. Appropriate cost-benefit analysis should accompany such plans and help prioritize automation projects across the portfolio of remediation activities. Many banks would also benefit from comprehensive management reporting to measure the cost and effectiveness of remediation activities and make the best possible use of subject-matter experts and technology budgets to "buy down" the risks.

Effective remediation governance—with clear responsibilities and effective implementation monitoring—can also reduce complexity and lower costs. This means clearly delineating responsibilities for all remediation activities among the compliance function, business lines, and other control functions.

■ ■ ■

The cost of regulatory compliance in financial services has spiked over the past decade. In particular, resources in the first and second lines of defense have expanded dramatically. As a result, the industry has become more resilient and the quality of risk management has improved. The current resource-intensive approach to managing compliance is not, however, sustainable in the long run. While the demand for compliance activities is largely out of banks' control, these seven practical steps can optimize how banks respond to that demand and allow meaningful progress toward a sustainable compliance function over time. ■

Piotr Kaminski is a senior partner in McKinsey's New York office, **Daniel Mikkelsen** is a senior partner in the London office, **Thomas Poppensieker** is a senior partner in the Munich office, and **Kate Robu** is a partner in the Chicago office.