McKinsey&Company

Piotr Kaminski
Kate Robu

A best-practice model for bank compliance

Risk January 2016

Tighter compliance regulations have challenged financial institutions in a variety of ways. Yet those who adapt best may enjoy a distinct competitive advantage.

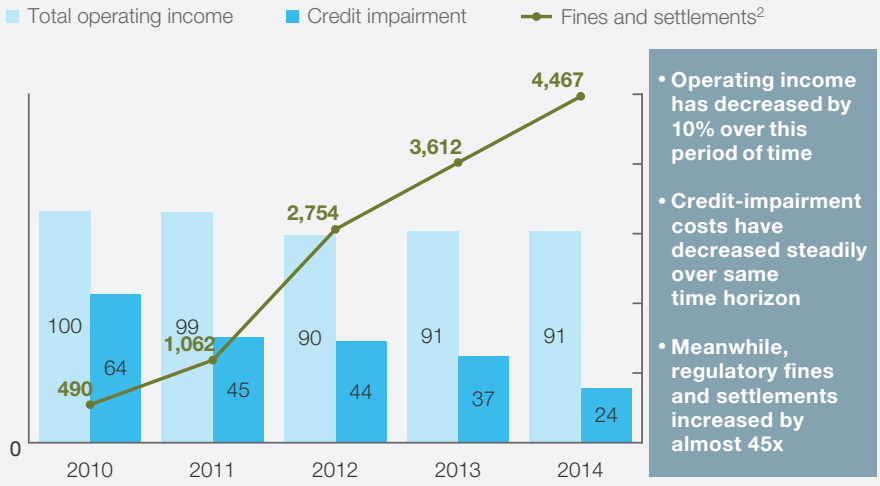
Compliance risk has become one of the most significant ongoing concerns for financial-institution executives. Since 2009, regulatory fees have dramatically increased relative to banks' earnings and credit losses (Exhibit 1). Additionally, the scope of regulatory focus continues to expand. Mortgage servicing was a learning opportunity for the US regulators that, following the crisis, resulted in increasingly tight scrutiny across many other areas (for example, mortgage fulfillment, deposits, and cards). New topics continue to emerge, such as conduct risk, next-generation Bank Secrecy Act and Anti-Money Laundering (BSA/AML) risk, risk culture, and third- and fourth-party (that is, subcontractors) risk, among others. Even though a lot of work has been done to respond to immediate pressures, the industry needs a more structural answer that will allow banks to effectively and efficiently mature their risk-and-control frameworks to make them more robust and sustainable over time.

The traditional compliance model was designed in a different era and with a different purpose in mind, largely as an enforcement arm for the legal function. Compliance organizations used to promulgate regulations and internal bank policy largely in an advisory capacity with a limited focus on actual risk identification and management. However, this model has offered a limited understanding of the business operations and underlying risk exposures, as well as of how to practically translate regulatory requirements into management actions. Even if a compliance testing program was established, it frequently borrowed heavily from the late-20th-century operational-risk playbook by emphasizing a bottom-up, subjective process of control testing versus a more objective, risk-based monitoring of material residual risks. Frequently, business managers are left to their own devices to figure out what specific controls are required to address regulatory requirements, typically leading to a buildup of labor-intensive control activities with uncertain effectiveness. Many banks still struggle with the fundamental issues of the control environment in the first line of defense such as compliance literacy, accountability, performance incentives, and risk culture. Finally, compliance activities tend to be isolated, lacking a clear link to the broader risk-management framework, governance, and processes (for example, operational-risk management, risk-appetite statement, and risk reporting and analytics). More often than not, the net result is primarily a dramatic increase in compliance-and-control spend with either limited or unproved impact on the residual risk profile of a bank.

Exhibit 1

Since 2009, regulatory fees have increased dramatically relative to banks' earnings and credit losses.

Performance of 20 large US and EU universal banks,[1] 2009–14, indexed to 2009 value (ie, value in 2009 = 100)



[1]Calculated using company annual reports and press clippings from 2009 to 2014. Coverage includes top 20 European and US global systemically important banks (universal banks only) by assets.
[2]Amounts include paid fines and settlements only; does not include provisions, such as payment protection insurance in the case of UK banks.

McKinsey&Company | Source: SNL Financial; McKinsey analysis

An emerging best-practice model for compliance in banking needs to rely on three core principles to address these challenges.

1. An expanded role of compliance and active ownership of the risk-and-control framework

In most cases banks need to transform the role of their compliance departments from that of an adviser to one that puts more emphasis on active risk management and monitoring. In practice it means expanding beyond offering advice on statutory rules, regulations, and laws and becoming an active co-owner of risks to provide an independent oversight of the control framework.

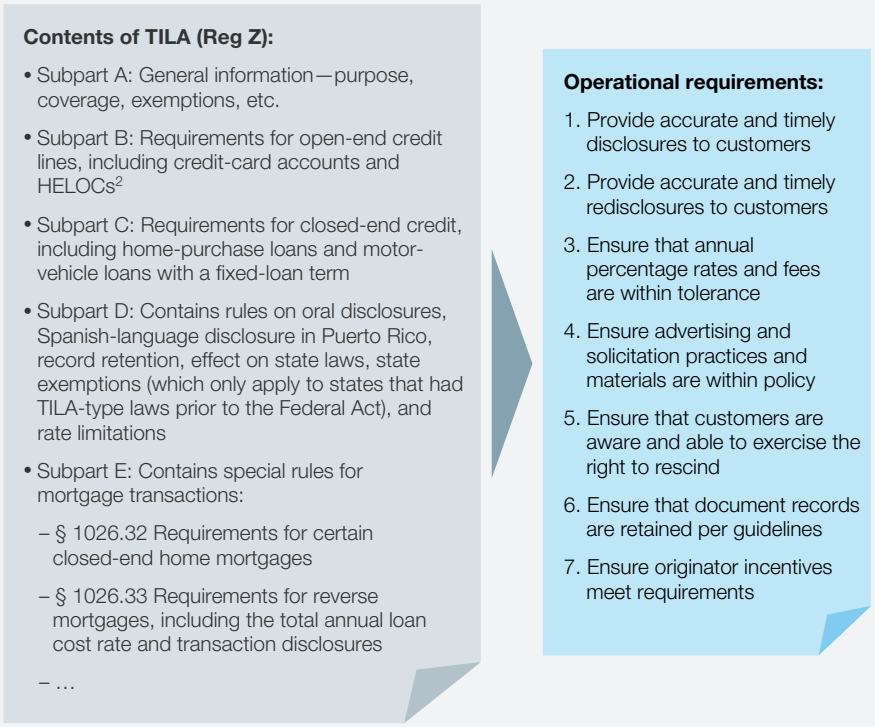
Given this evolution, responsibilities of the compliance function are expanding rapidly to include the following:

- Generating practical perspectives on the applicability of laws, rules, and regulations across businesses and processes and how they translate into operational requirements (Exhibit 2)
- Creating standards for risk materiality (for example, definition of material risk, tolerance levels, and tie to risk appetite)
- Developing and managing a robust risk identification and assessment process/tool kit (for example, comprehensive inventory of risks, objective risk-assessment scorecards, and risk-measurement methodology)

Exhibit 2

Compliance is now expected to provide practical perspectives on how regulations translate into specific operational requirements.

Example: Numerous TILA[1] subparts can be distilled into 7 major operational requirements



[1]Truth in Lending Act.
[2]Home equity line of credit.

McKinsey&Company

- Developing and enforcing standards for an effective risk-mediation process (for example, root-cause analysis and performance tracking) to ensure it addresses root causes of compliance issues rather than just "treating the symptoms"
- Establishing standards for training programs and incentives tailored to the realities of each type of job or work environment
- Ensuring that the front line effectively applies processes and tools that have been developed by compliance
- Approving clients, transactions, and products based on predefined risk-based rules
- Performing a regular assessment of the state of the overall compliance program
- Understanding the bank's risk culture and its strengths as well as potential shortcomings

Risk culture has a special place in the compliance playbook. Indeed, most serious failures across financial institutions in recent times have a cultural root cause leading to heightened regulatory expectations. Elements of "strong" risk culture are relatively clear (albeit not always explicitly articulated) and include timely information sharing, rapid elevation of emerging risks, and willingness to challenge practices; however, they are difficult to measure objectively. Use of tools such as structured risk-culture surveys can allow for a deeper understanding of nuances of risk culture across the organization, and their results can be benchmarked against peer institutions to reveal critical gaps. Consequently risk culture can be actively shaped, monitored, and sustained by committed leaders and organizations.

Effective execution of these expanded responsibilities requires a much deeper understanding of the business processes by compliance. There are a few practical ways to achieve this:

- Incorporating process walk-throughs into the regular enterprise compliance-risk assessments (for example, facilitated workshops with first line and second line to assess inherent risk exposures and how they affect business processes)

- Implementing a formal business-change-management process that flags any significant operational changes (for example, volumes, products, workflows, footprint, and systems) to the second line

- Developing a robust tool kit for objectively measuring risk (for example, quantitative measurement for measurable risks, risk markers for risks harder to quantify, common inventory of risky outcomes, and scenario analysis and forward-looking assessments)

Finally, the design of the compliance function's operating model is becoming increasingly important. Thus, it demands a shift from a siloed, business-unit-based coverage to a model where business-unit coverage is combined with horizontal expertise around key compliance areas, such as BSA/AML; unfair, deceptive, or abusive acts or practices (UDAAP); mortgage (across all mortgage businesses); third-party and others.

2. Transparency into residual risk exposure and control effectiveness

One of the traditional industry practices for the second line's engagement with the business has been to identify "high-risk processes" and then to identify "all the risks" and "all the controls" that pertain to each of them. This approach, however, falls short of creating a real and comprehensive transparency into material risk exposures and often becomes a merely mechanical exercise.

First, the lack of an objective and clear definition of a "high-risk process" frequently leaves this decision to the discretion of business lines, which can lead to the omission of risks that are critical from a compliance-risk standpoint but deemed less significant from a business standpoint (for example, a low-volume collections process can seem an insignificant part of the overall business portfolio but can be a critical area for regulatory compliance). This approach

also suffers from inconsistencies. As an example, an account-opening process may be deemed high risk in some retail units but not in others.

Second, the pursuit of documenting virtually "all risks" and "all controls" implies a significant amount of work and actually limits the first line's ability to go deep on issues that truly matter, producing lengthy qualitative inventories of risks and controls instead of identifying material risk exposures and analyzing the corresponding process and control breakpoints and root causes.

The new approach focused on residual risk exposures and critical process breakpoints ensures that no material risk is left unattended and provides the basis for truly risk-based, efficient oversight and remediation activities. It addresses these challenges by directly tying regulatory requirements to processes and controls (that is, through the mapping of risks to products and processes), by cascading material risks down to the front line in a systematic and truly risk-based way, and by defining objective (and whenever possible quantitative) key risk indicators (KRIs) in the areas where the process "breaks" and creates exposure to a particular risk.

Thus, as Exhibit 3 illustrates, there are typically numerous controls associated with every regulatory requirement throughout a given business process. Testing all of these controls consumes tremendous organizational time and resources. Each control is documented and its level of effectiveness qualitatively assessed (although the definition of "effectiveness" is often ambiguous and varies from person to person). Unfortunately, the overall control-effectiveness score resulting from this exercise is only loosely correlated with the outcome—it's not unusual to see critical audit findings in areas where the majority of controls have been deemed effective.

In contrast, the new approach starts by defining which risks apply to a given business process and identifying where exactly in the process they occur (known as "breakpoint analysis"). Informed by the identified process breakpoints, one can then design KRIs that directly measure the residual risk exposure. This approach leads to far fewer items to test (in our example, two KRIs versus seven controls) and much more robust insights into what the key issues are. Moreover, it provides the essential fact base to guide and accelerate the remediation process and resource allocation.

3. Integration with the overall risk-management governance, regulatory affairs, and issue-management process

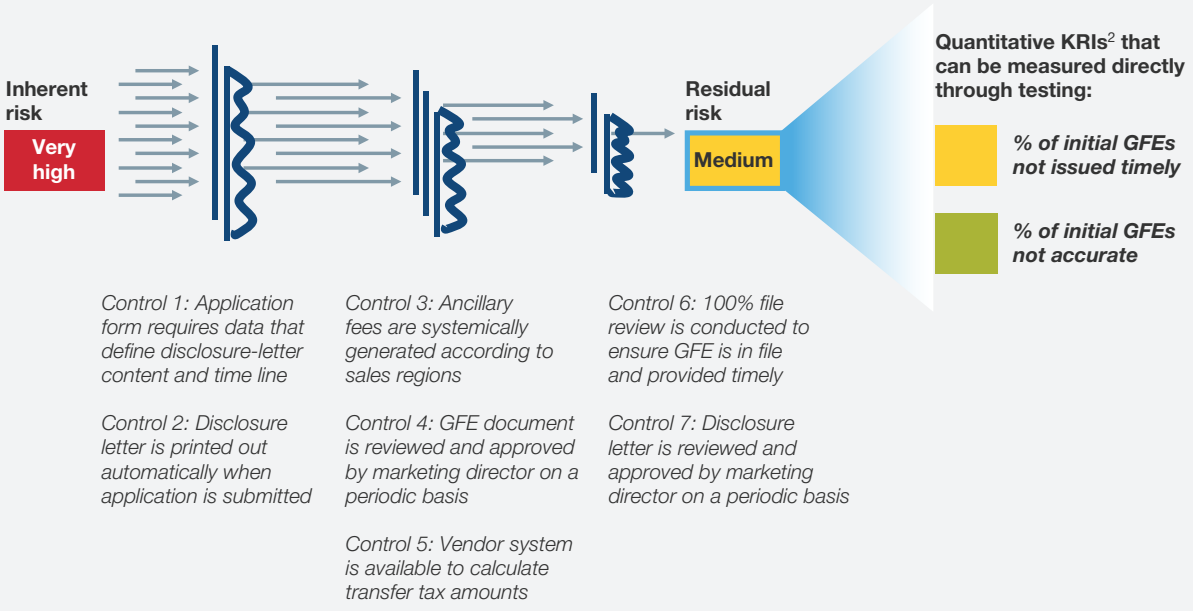
Compliance risks are driven by the same underlying factors that drive other banking risks, but their stakes are higher in the case of adverse outcomes (for example, regulatory actions that can result in restriction of business activities and large fines). Therefore, it's only fitting that a modern compliance framework needs to be fully integrated with the bank's operational-risk view of the world.

Integrating the management of these risks offers tangible benefits. First, it ensures the enterprise has a truly comprehensive view of its portfolio of risks and visibility into any systemic issues (for example, cross-product, cross-process), and that no material risk is left unattended.

Exhibit 3

Focus on residual risks versus individual controls leads to greater efficiency and effectiveness of the risk-identification and assessment processes.

Regulatory risk: Good-faith-estimate (GFE) disclosures in mortgage[1]
Business process: Delivery of disclosure letters to customers at time of application



- Traditional compliance approach calls for ongoing testing of each of 7 controls embedded in business process
- Monitoring KRIs for residual risk vs testing numerous individual controls results in much more efficient (fewer items to focus on) and effective (due to objective measurement) risk-identification and assessment processes

[1]Real Estate Settlement Procedures Act (§ 1024.7).
[2]Key risk indicators.

McKinsey&Company

Second, it lessens the burden on the business (for example, no duplicative risk assessments and remediation activities) as well as on the control functions (for example, no separate or duplicative reporting, training, and communication activities). Third, it facilitates a risk-based allocation of enterprise resources and management actions on risk remediation and investment in cross-cutting controls.

The following practical actions can help the bank firmly integrate compliance into the overall risk-management governance, regulatory affairs, and issue-management process:

- Develop a single integrated inventory of operational and compliance risks
- Develop and centrally maintain standardized risk, process, product, and control taxonomies
- Coordinate risk assessment, remediation, and reporting methodologies and calendars (for example, ensure one set of assessments in cross-cutting topical areas like third-party risk management; ensure consistency of compliance monitoring and testing activities with quality-assurance/quality-control activities in operational risk)

- Define clear roles and responsibilities between risk and control functions at the individual risk level to ensure there are no gaps or overlaps, particularly in "gray areas" where disciplines converge (for example, third-party risk management, privacy risk, AML, and fraud)
- Develop and jointly manage integrated training and communication programs
- Establish clear governance processes (for example, escalation) and structures (for example, risk committees) with mandates that span across risk and support functions (for example, technology), and that ensure sufficient accountability, ownership, and involvement from all stakeholders, even if issues cut across multiple functions
- Consistently involve and timely align senior compliance stakeholders in determining action plans, target end dates, and prioritization of issues and matters requiring attention
- Establish a formal link and coordination processes with government affairs

To address this integration effectively, financial institutions are also considering changes to the organizational structure and placement of the compliance function. Exhibit 4 lays out the three archetypes of compliance organizations in banks. Migration of compliance to risk organization (that is, archetype B) is a recent trend among global banks, which previously had compliance reporting to legal (that is, archetype A). This new structure reinforces the view of compliance as a risk similar to operational risk and as a control rather than advisory function, and is meant to facilitate an integrated view across all risk types. A few banking institutions have elevated compliance to a stand-alone function (that is, archetype C), positioning it similar to internal audit, with clear separation from business, thus significantly raising its profile but also creating the need for stronger coordination with the operational-risk function.

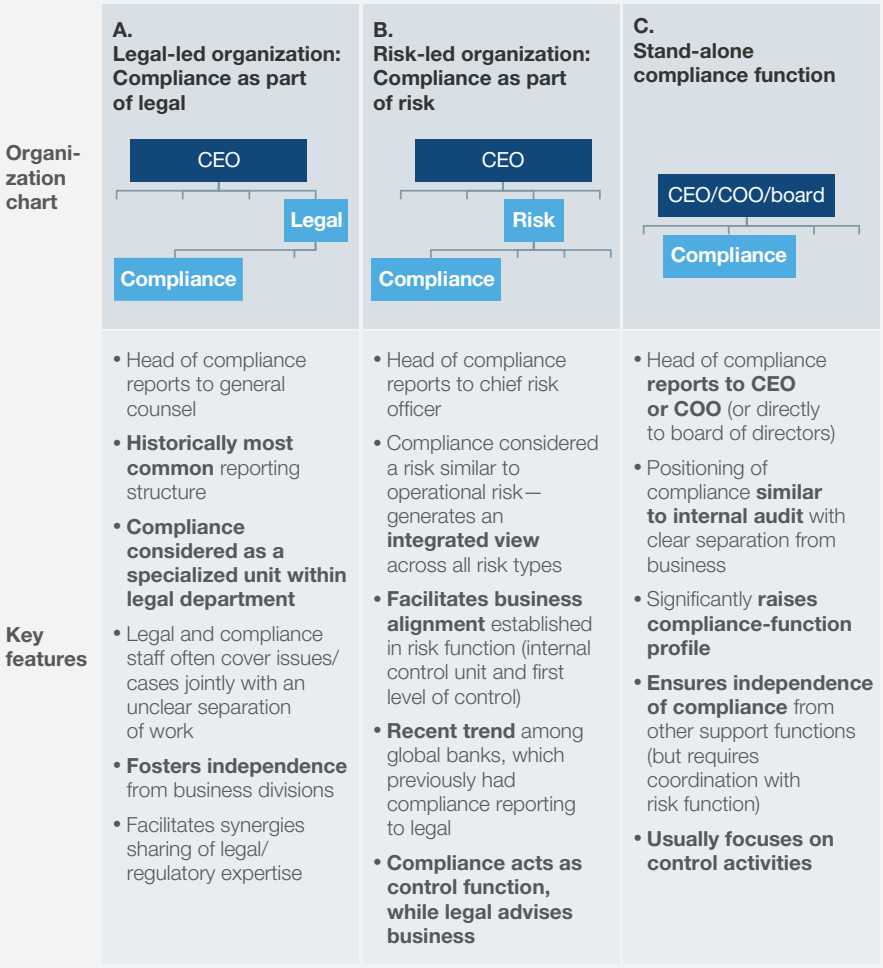
Measuring progress—outcomes that matter

The three principles outlined above imply a multifaceted transformation of the compliance function. The scope and complexity of this transformation create a real risk of "missing the forest for the trees." We have found it helpful to apply the following ten-point scorecard to measure progress on this journey:

1. Demonstrated focus on the role of compliance and its stature within the organization
2. Integrated view of market risks with operational risk
3. Clear tone from the top and strong risk culture, including evidence of senior-management involvement and active board oversight
4. Risk ownership and independent challenge by compliance (versus "advice and counsel")
5. Compliance operating model with shared horizontal coverage of key issues and a clear definition of roles versus the first line of defense

Exhibit 4

There are several common archetypes for compliance organizations.



McKinsey&Company

6. Comprehensive inventory of all laws, rules, and regulations in place to drive a risk-based compliance-risk-assessment program

7. Use of quantitative metrics and specific qualitative risk markers to measure compliance risk

8. Compliance management-information systems providing an integrated view of risks and reflecting a common risk taxonomy

9. Evidence of the first line of defense taking action and owning compliance and control issues

10. Adequate talent and capabilities to tackle key risk areas (for example, BSA/AML, fiduciary risk) and a working knowledge of core-business processes (for example, mortgage servicing).

Assuming one point for each of these requirements, a bank with a low score (for example, four to five points) may require a significant transformation. Banks can maximize the impact of the transformation by rigorously measuring progress against desired outcomes. Audit should

play an important role in this process, providing an independent view of program status and effectiveness with respect to commonly agreed-upon transformation objectives.

Regulatory compliance has undoubtedly affected banks in a variety of challenging ways, increasing the cost of service and sometimes making the delivery of great customer experiences more difficult. However, as the regulatory environment evolves, we see a major opportunity for the compliance function to get ahead of the curve by implementing targeted changes to its operating model and processes, and thus delivering a better quality of oversight while at the same time increasing its efficiency. Banks that successfully make this shift will enjoy a distinctive source of competitive advantage in the foreseeable future, being able to deliver better service, reduce structural cost, and significantly de-risk their operations.

Piotr Kaminski is a director in McKinsey's New York office, and **Kate Robu** is an associate principal in the Chicago office.