Unfortunately, there are no off-the-shelf formulas for compliance risk management. The complexities of each compliance issue and the unique circumstances of every bank make understanding compliance risk management challenging. It is our purpose to clarify this task by offering some easy-to-use concepts for bringing compliance risks into focus, employing examples that highlight common compliance issues.

A bank’s compliance program is an essential component of the institution’s overall risk management framework. As regulatory expectations continue to increase, the challenge is to successfully implement a compliance program that is a proactive component of the institution’s risk management culture and imbedded in the institution’s operating units.

A compliance risk management program should identify potential events that may affect the bank and determine how the institution will effectively manage risk based on its risk appetite and strategic direction, taking into consideration anticipated operational and market changes. Appropriate mitigating controls must be developed and implemented as needed after identified risks have been comprehensively assessed, potential impact to the bank has been evaluated, and the effectiveness of existing controls has been determined. In developing and implementing regulatory compliance programs, financial institutions are wise to utilize a risk-based versus rule-based approach, focusing compliance resources on minimizing the greatest risks to ensure that the risk taken is the risk intended.
In developing and implementing regulatory compliance programs, financial institutions are wise to utilize a risk-based versus rule-based approach, focusing compliance resources on minimizing the greatest risks to ensure that the risk taken is the risk intended.
Included in an effective compliance risk management program are a governance structure appropriate for the bank’s activities that demonstrates a management commitment to sound compliance risk management practices; compliance resources reasonable for the business activities performed; policies and procedures that are maintained to ensure consistent application of laws; and compliance training, reporting, and communication processes. These elements, along with others supported by senior leadership, compliance officers, business lines, and corporate partners serve to identify key compliance risks and develop and implement controls to mitigate them.

At the outset, it is important to address two common misconceptions about compliance risk management. First, short of deciding to go out of business, no bank will ever eliminate compliance risk. Second, there is no such thing as “taking the risk” and intentionally disregarding regulatory requirements. Compliance with regulations is expected, and while not all regulations are zero-tolerance, intentional or willful disregard of any regulations, even if the ramifications of violations seem insignificant, can result in extensive detrimental consequences.

With these two general misconceptions covered, the following aims to define compliance risks, discuss identification of risks within a bank, and offer some specific suggestions on how a bank can assess its specific risks.

**Defining Compliance Risk**

While there may be slight variances depending upon a bank’s circumstances, consider the following as a possible overall definition of compliance risk:

The adverse consequences that can arise from systemic, unforeseen, or isolated violations of applicable laws and regulations, internal standards and policies, and expectations of key stakeholders including customers, employees, and the community, which can result in financial losses, reputation damage, regulatory sanctions, and, in severe cases, loss of franchise or rejected mergers and acquisitions.

Effective management of compliance risk can also possess the following positive business benefits:

- A strong compliance program speaks to organizational integrity, a building block of ethical corporate culture.
- An ethical corporate culture helps build a strong reputation with customers, shareholders, employees, and communities.

**Consequences of Noncompliance**

Financial loss—whether in the form of civil damages in a class action lawsuit for truth-in-lending finance charge errors, fines for missing OFAC-prohibited wire transfers, costs associated with privacy violations, or the expense incurred due to refilling inaccurate Home Mortgage Disclosure Act (HMDA) data, just to mention a few—warrants first mention in defining compliance risk. In many banks, consumer-lending compliance may incur the greatest costs due to complicated truth-in-lending regulations, where reimbursements to customers are likely should something go wrong. Anti-money laundering (AML) compliance is another area where financial implications are obvious, with several multimillion-dollar fines recently assessed for deficient programs. In addition to lawsuits and fines, financial ramifications in compliance matters include associated costs such as the implementation of new systems, hiring consultants and lawyers, and printing correct disclosures.

Of course, the risk does not end with the potential costs for violations and the expenses sustained in fixing them. Due to the nature of the financial services business, which
requires institutions to maintain the confidence of customers, creditors, and the general marketplace, the reputational risk posed by noncompliance is particularly critical because it has the potential to negatively affect the profitability and ultimately the viability of the bank. Obvious examples are seen in AML and predatory lending, where a bank can suffer significant damage to its reputation for publicized violations or civil lawsuit settlements and, in extreme cases, have its senior executives testify on C-SPAN before Congress about the institution’s compliance inadequacies. A damaged reputation can take years to repair and result in lost business opportunities. While a pristine compliance reputation may not translate to revenue enhancement, a poor one can be exceptionally destructive.

Compliance risk also impacts a bank’s reputation with regulatory agencies. Even if its deficiencies are not publicized, a poor compliance examination record can create a never-ending cycle of intense compliance exams, often leading to the discovery of additional violations. Repeat violations—even for seemingly minor issues such as inaccurate paid outside of closing (POC) Real Estate Settlement Procedures Act (RESPA) disclosures, missing branch signs, or incorrectly completed notice-of-hold forms—can be especially disturbing to examiners. While examiners may not identify all regulations as equally important, there is an expectation that every bank will make a good-faith effort to ensure compliance with all of them, especially when errors have previously been detected. Banks that fail to do so will likely have poor relationships with their regulators, which may result in greater compliance costs or formal enforcement orders.

Persistent poor regulatory compliance examination ratings can have severe ramifications. As one example, the USA PATRIOT Act added AML compliance to Community Reinvestment Act (CRA) as potential merger and acquisition impediments. A poor AML examination within a holding company can, as a result, prevent a bank from pursuing an acquisition or, in a worst-case scenario, lead to the loss of the bank’s charter.

**Identifying Compliance Risk**

The consequences of compliance failures include financial, reputation, and regulatory factors; what combination of events triggers these results? While risk exists in virtually every aspect of a bank’s business, risks should not be weighted equally. For example, potential systemic truth-in-lending finance charge errors would probably rank above POC RESPRA omissions with respect to defining an institution’s overall compliance risk and therefore they warrant greater attention in the compliance program. Similarly, the maintenance of a deposit account for a shell bank would have far more significant ramifications than the missed filing of a single currency transaction report (CTR). On the other hand, an isolated truth-in-lending violation caused by a failure to obtain a customer credit insurance acknowledge-
not be used by launderers, but rather because the immediacy of funds transfers, their international capabilities, and the attention given them by bank examiners has made them a high risk product. Deposit products, too, can have varied inherent compliance risk; the complexities of advertising and disclosing multiple interest rates on tiered money market accounts raise far more potential truth-in-saving issues than passbook savings accounts. It is imperative that compliance officers understand the differences in the compliance risks of the products their banks offer.

Compliance officers must also take into consideration the bank’s target markets. As with products, an important factor in some compliance areas may be whether the business’s target clientele is retail or commercial, which can eliminate many (but not all) consumer compliance issues for commercially oriented business units. Within these categories, further risk analyses can be made, such as separating private banking from general retail banking with respect to AML risk and perhaps retail lending risks, where customized private bank mortgage lending can raise significant documentation challenges not present in standardized consumer loans, unless, of course, the standard consumer loans are targets at the “sub prime” market. Within the commercial bank, real estate lending, with potential flood insurance requirements, might warrant a higher risk exposure than asset-based lending. Obviously these examples are not standardized, and there can be situations where the risk profiles of certain businesses within a bank can be affected by other issues. The compliance officer must consider each business within the bank, understanding its products, its customers, and their transactions.

Compliance risks are also associated with new business initiatives, such as new products or changes to existing products, mergers and acquisitions, new systems, and marketing campaigns. While in some cases the assessment of these risks might be covered while considering transaction, product, or business level, in other cases the initiative may warrant separate analysis, particularly if it is a major project for the institution that crosses business lines or involves significant changes or additions to the bank’s business profile.

Following the evaluation of each business’s compliance risks, it is necessary to determine the bank’s overall risk profile. This is a key component of the risk process, as it may serve as the basis upon which the bank will allocate limited compliance and technical resources to mitigate risk exposure. The compliance officer (or, depending upon the compliance infrastructure of the institution, another person familiar with the business) should document the risks of each business unit, focusing on the various components of the risk equation (financial, reputation, regulatory) and the relevant regulations, and balancing them against their transactions, products, and targeted customers. The bank can then identify whether any of its businesses trigger substantial compliance risks that, when compared to financial factors such as revenue or earnings, suggest that the overall contribution of that business might be outweighed by these potential risks.

For example, if a bank has a small foreign correspondent banking business that features three payable-through-account relationships that yield little revenue but are high AML risks, the bank might decide to terminate these relationships. More likely, the risk assessment will allow management to understand where its compliance risk exposure resides, and to allocate sufficient resources to manage them. If completed properly, this “bottom up” approach to compliance risk will enable each business to understand its unique risks and provide bank management with the full picture of compliance risks within the organization.

**Assessing Compliance Risk**

When identified, risks must be assessed. There are a variety of tools that can assist a compliance officer in this task, some measuring compliance risk on a periodic basis, others flagging changes to the profile based on key business developments. Some banks use general business risk profiles as risk management tools for assessing all categories of risks throughout the organization. These risk profiles have separate sections for credit, liquidity, market, and other risk disciplines and include a compliance risk section for the assessment of the business’s compliance risk system.

If a bank uses this approach, its compliance officer must be involved in the process by either directly documenting the risks of each business, or approving documentation produced by another person responsible for the risk assessment. The process enables the business to inventory its products and their transactions, along with variables such as the targeted customers, geographic concerns, and other material information related to the applicable regulations. Following the inventory, the business would determine the potential financial, reputation, and regulatory risks these factors raise for the business. The risk profile might also include the processes used to manage these risks. If used properly, the business risk profile process provides an excellent opportunity to document a business-by-business assessment of compliance risks.

A separate compliance risk assessment may be conducted for each business in the bank, either alternatively or as a supplement to the business risk process. A standalone compliance risk assessment would follow the same general approach as the compliance component of the business risk profile, perhaps in more detail. In some cases, a separate risk assessment covering a particular compliance area, such as AML, is appropriate (especially with respect to the “risk-based” requirements for CIP verification). In any event, the initial mission should be to assess compliance risks at the business level, in as detailed a manner as possible.

Given the dynamic nature of banking, a point-in-time compliance risk assessment could easily become stale.
If completed properly, this “bottom up” approach to compliance risk will enable each business to understand its unique risks and provide bank management with the full picture of compliance risks within the organization.

relatively quickly. Compliance risks associated with major business initiatives must therefore be part of the planning and implementation process. If a bank has a formal project-planning infrastructure, compliance risk identification assessments should be part of the process. This can be included as a documented component of the business initiative, preferably identifying both the compliance risks and the management processes employed, if applicable, for any new or increased risks triggered by the initiative. The business risk profile should also be changed if the initiative has a material impact on the overall compliance risk. While many initiatives raise the degree of risk, others—such as a major upgrade to a loan documentation system that automates a manual APR calculation process—may reduce it.

The business risk profiles should roll up to a bank-level compliance risk profile. As with business risk profiles or assessments, this can be a component of an integrated risk assessment process, a separate compliance assessment, or a combination that carves out particular compliance areas for separate evaluation. The bank-level risk profile should weigh the respective risks of each business, highlighting particularly significant risk exposures as well as management processes. This will enable management to evaluate the relative costs associated with a business against its potential rewards. As with the business-level process, the bank-level assessment should be a dynamic document that reflects material changes based on major business initiatives, taking into account that the bank level might differ from the business level.

A quarterly self-assessment (QSA) is one example of a risk management assessment measure. A QSA is designed to evaluate the level of a bank’s compliance program and assist in identifying risk exposure by examining the following eight fundamental components of compliance risk management: policy and procedure, performance and management, identification and prioritization of risk, monitoring and tracking of compliance issues, reporting and communication, training programs and professional proficiency, management commitment, and infrastructure effectiveness. This process of assessing the management of risk is as critical to successful risk management as the assessment of risk itself. Ultimately, it is a bank’s efficiency at managing risk and the strength of its compliance program that will enable the bank to appropriately respond to and mitigate identified risks.

The QSA requires compliance officers to evaluate the effectiveness of their compliance programs by responding to prescribed assessment questions—for example, is their resource commitment adequate to effectively administer all required compliance tasks? Responses can be tabulated according to a scale, with the low end representing a program that needs improvement and the high end indicating that a strong program is in place. In completing the QSA, a compliance officer may identify the program’s efficiencies and weaknesses as well as help assess the bank’s overall risk exposure.

While there is no hard and fast formula for calculating compliance and assessing risk, there are a variety of key risk indicators. In light of today’s regulatory environment and increased scrutiny, it is important that we utilize a risk-based approach in managing compliance. Moreover, it is important that we elevate compliance beyond adherence to regulation through basic functions, to be incorporated as an essential element in risk management culture. Only through careful evaluation and regular assessment of risks can we manage compliance and be assured that the risk taken is the risk intended.

About the Authors

Michael D. Kelsey is PNC Financial Group’s director of retail and wholesale bank compliance as well as its corporate anti-money laundering compliance officer. He joined PNC in 1985 and has held a number of positions in its legal and compliance departments. He currently serves on the ABA Compliance Executive Committee, writes and speaks frequently on money laundering and other compliance issues, and is a member of the Widener University School of Law adjunct faculty in Wilmington, Delaware. Mr. Kelsey became a member of the Delaware Bar in 1983 and lives in Wilmington with his family. He can be reached by telephone at (302) 429-1775 or via e-mail at michael.kelsey@pnc.com.

Michael Matossian, CPA, CMA, CRP, joined Fifth Third Bank as chief compliance officer in October 2003. He previously worked as SVP and director of regulatory risk management and director of anti-money laundering and BSA officer at Wachovia Corporation, spent 10 years working for a “Big 4” public accounting firm, and served two years with the Office of the Comptroller of the Currency (OCC). Mr. Matossian serves on the ABA Compliance Executive Committee and on the BAI Risk Management Advisory Committee. He also participates on several national task forces addressing compliance matters. He holds the following certifications: Certified Public Accountant, Certified Management Accountant, Certified Fraud Examiner, Certified Risk Professional, and Certified Anti-Money Laundering Specialist. He can be reached by telephone at (513)-534-7323 or via e-mail at michael.matossian@53.com.