JOURNAL OF TAXATION and REGULATION of FINANCIAL INSTITUTIONS

Navigating the Evolving Risk Management Landscape: Considerations for Financial Institutions

Financial institutions face unique challenges in risk management. Not only are they exposed to traditional business risks, but also to those inherent in the business of banking—for example, credit risks, interest rate risks, and liquidity risks. Financial institutions operate in a heavily regulated environment that creates compliance risks of its own, and failure to manage these risks to the satisfaction of regulators may result in enforcement actions and significant reputational harm. Additionally, public policy considerations have increasingly required financial institutions to take on responsibilities not strictly relevant to business and banking, such as combating terrorist financing and other forms of money laundering. As a result, it is critical that financial institutions implement comprehensive Enterprise Risk Management programs designed to identify, monitor, and minimize risk and create a corporate culture in which risk management efforts are considered on an equal basis with other strategic efforts.

BRIAN C. MCCORMALLY, CHRISTOPHER L. ALLEN, AND HELEN E. MAYER

Risk management is a familiar concept to financial institutions. Regulators have long assessed institutions on their ability to manage risk appropriately, and to a certain degree banking itself is an exercise in risk management. Credit risk, interest rate risk, and liquidity risk, for example, are inherent in the business of banking and must be successfully managed to turn a profit. However, as the financial services sector has expanded in size, complexity, and product offerings, the risks faced by industry participants have expanded as well. Not only must "traditional" risk factors be monitored and managed, but numerous other internal and external risk sources—many of which, in the absence of government mandates, would not be a bank's concern at all—must be identified and mitigated to avoid agency enforcement actions, including potentially severe civil and criminal penalties and the accompanying reputational damage. This new reality is reflected in the growing importance of "enterprise risk management," or "ERM," which focuses on the development of a top-down approach to risk management.

The past decade has witnessed an increased formalization and centralization of risk-management practices and expectations, particularly for large organizations. For example, in 2004, the New York Stock Exchange adopted governance rules requiring the audit committees of listed firms to oversee management's risk oversight practices. In 2008, Standard & Poor's began incorporating the strength of a nonfinancial company's ERM processes into its credit ratings analysis in a wide range of industries. In 2009, the Securities and Exchange Commission expanded its oversight-related proxy disclosure requirements to provide shareholders more information about the board's role in ERM.[1] These steps not only require affirmative implementation

Brian C. McCormally is a partner, and Christopher L. Allen and Helen E. Mayer are associates, at Arnold & Porter LLP, Washington, DC, in the firm's Financial Services Practice Group. The authors may be contacted by email, respectively, at Brian.McCormally@aporter.com, Christopher.Allen@aporter.com, and Helen.Mayer@aporter.com.

[1] Mark S. Beasley et al., Comm. of Sponsoring Org. of the Treadway Comm'n., "Developing Key Risk Indicators to Strengthen Enterprise Risk Management: How Key Risk Indicators Can Sharpen Focus on Emerging Risk," at III (December 2010), available at http://www.coso.org/documents/COSOKRIPaperFull-FINALforWebPostingDec110_000.pdf.

JOURNAL OF TAXATION and REGULATION of FINANCIAL INSTITUTIONS

of ERM programs but provide for transparency in such programs to assist in monitoring, at least with respect to public companies. While many financial institutions were already subject to, or were at least encouraged to act by, these requirements, it was not until 2010 that the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) created statutory ERM requirements explicitly for financial institutions.[2]

By virtue of the central role they play in the economy, financial institutions are particularly vulnerable to internal and external risks associated with their operations. Some risks are obvious. In addition to the credit, interest rate, and liquidity risks noted above, all depository institutions are exposed to general market risk and are particularly susceptible to fluctuations in investment markets. They are also exposed to the risks associated with information technology and the management of personal or private information. More recently, depository institutions have been placed on the front line of the fight against terrorist financing and money laundering activity. As a result, even though a depository institution is not a law enforcement operation, its failure to root out wrongdoing may expose the institution to significant liability. Further, on a business level, depository institutions must increasingly assess their products to determine not only whether those products comply with the letter of the law, but also whether consumers may be harmed by them, potentially exposing the institution to consumer protection violations. Finally, today's depository institutions face the challenge of coping with these and other risks in a highly regulated environment in which a single systemic compliance issue can expose the institution to agency enforcement actions for restitution and penalties, and both the institution and its parent company to significant reputation and litigation risk.

Although the avoidance of an enforcement action may be at the forefront of a board's mind when it considers implementing or modifying an ERM program, the ultimate goal of any ERM program must be to instill a corporate culture in which risk management efforts are considered on an equal basis with other strategic efforts.

This article will discuss ERM issues generally and focus on the unique challenges facing financial institutions. We first set out a definition of ERM and how Congress has set up statutory ERM requirements through the Dodd-Frank Act, and then summarize the regulators' expectations, which will arise principally through their supervisory review of the institution. Next we describe the process of setting up a risk management program, including where responsibility should be placed, and what processes should exist and discuss emerging trends in ERM as it relates to financial institutions.

Financial institutions of all sizes should be mindful of both the Dodd-Frank Act's ERM requirements and the regulators' expectations. Although the Dodd-Frank Act's risk provisions are applicable only to large banking entities, they are a valuable guidepost for all banking entities for several reasons. First, they provide a window into the regulators' mindset when considering robust risk management practices. Second, the new provisions and other ERM best practices are critical to proactively avoiding enforcement actions or complying with an enforcement action already in place. As any bank officer knows, enforcement actions or even lesser regulatory criticisms can create severe reputational and litigation risks. Although the avoidance of an enforcement action may be at the forefront of a board's mind when it considers implementing or modifying an ERM program, and the key features discussed herein are ones an institution may use to demonstrate compliance with a regulator's risk management expectations, the ultimate goal of any ERM program must be to instill a corporate culture in which risk management efforts are considered on an equal basis with other strategic efforts.

WHAT DOES ENTERPRISE RISK MANAGEMENT MEAN?

ERM in General. Broadly speaking, ERM requires a business entity to develop an organization-wide, top-down approach to identifying and managing risks throughout the entity's operations. The Committee of Sponsoring Organizations of the Treadway Commission, a private sector initiative dedicated to developing frameworks and guidance on enterprise risk management, has defined ERM as

> a process, effected by an entity's board of directors, management, and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within the risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.[3]

Successfully implementing an ERM requires not only that risks be mitigated, but also that they be identified

[2] See 12 U.S.C. § 5325.

[3] Beasley et al., supra note 1.

Journal of Taxation and Regulation of Financial Institutions

in the first place. This effort requires a comprehensive understanding of both the operations of the enterprise and the markets in which the enterprise is active, and how these various pieces interact to increase (or decrease) risk for the organization as a whole.

ERM in the Banking Context. Regulators have also spoken publicly about the nature of ERM in the banking context. Then-Acting Comptroller of the Currency Julie Williams explained the concept in a 2005 speech at the Federal Reserve Bank of Chicago:

> We look at whether a bank has an environment for sound decision-making that includes effective structural governance and a system of checks and balances to identify, monitor and control the risks to which the organization in subject.
>
> . . . [P]art of that environment is whether the organization's incentives recognize and reward the corporate values and culture that the company wants to promote.
>
> . . . [W]e can and will notice and comment on whether a banking organization has a corporate organizational framework, and policies or practices that support—or undermine—sound corporate values and an ethical climate within the organization. It is our experience that if such values and the *ethos* of the organization are not strong, institutional soundness and a bank's good name and reputation can suffer in unpredictable ways.[4]

As alluded to above, Dodd-Frank Act Section 165 sets out statutory ERM requirements for bank holding companies of a certain size and character. The Board of Governors of the Federal Reserve System (the Board) is responsible for establishing the detailed standards. The Dodd-Frank Act's provision is, in part, a response to two reports by the Senior Supervisors Group (SSG), undertaken during and shortly after the financial crisis. The SSG found critical deficiencies in the then-current risk management practices of banking entities. As the Board explained, SSG found that "business line and senior risk managers did not jointly act to address a company's risks on an enterprise-wide basis; business line managers made decisions in isolation and at times increased, rather than mitigated, risk; and treasury functions were not closely aligned with risk management processes, preventing market and counterparty risk positions from being readily assessed on an enterprise-wide basis."[5]

Risk Committee of Bank's Board. Section 165 is an effort to address these deficiencies in risk management of banking entities. Under the Board's proposed implementing rule issued earlier this year,[6] publicly traded nonbank covered companies and publicly traded bank holding companies with total consolidated assets of $10 billion or more will be required to meet certain standards regarding their risk management practices. First, a banking entity must establish a Risk Committee of its board of directors. At a minimum, the Risk Committee must have three outside directors and one director with risk management expertise commensurate with the company's capital structure, risk profile, complexity, activities, size, and other appropriate risk-related factors. The larger and more complex a banking entity is, the greater the regulators' expectation that additional members of the Risk Committee will have risk-management expertise. Under the Board's proposed rule, the Risk Committee of a large banking organization would also have to be chaired by an independent director, as that term is defined in federal securities law.[7] The Risk Committee should meet at least once a month and should have a formal, written charter approved by the board setting forth the Committee's mission, authority, and responsibilities. As necessary, the Committee should advise the board about oversight of the bank's risk, including credit risk, market risk, interest rate risk, liquidity risk, information technology risk, and compliance risk.

The Risk Committee should meet at least once a month and should have a formal, written charter approved by the board setting forth the Committee's mission, authority, and responsibilities.

Chief Risk Officer. Second, a banking entity must establish or enhance its Risk Management Department by designating an executive to serve as Chief Risk Officer (CRO). The CRO should report directly to, and have direct access to, the board and the Risk

[4] Julie Williams, Acting Comptroller of the Currency, Office Comp. Currency, Remarks Before the Conference on Bank Structure and Competition, Federal Reserve Bank of Chicago (May 6, 2005), available at http://www.occ.treas.gov/news-issuances/speeches/2005/pub-speech-2005-45.pdf.

[5] Bd. of Governors of the Fed. Reserve Sys., "Enhanced Prudential Standards and Early Remediation Requirements for Covered Companies," 77 Fed. Reg. 594, at 622 (Jan. 5, 2012) (to be codified at 12 CFR pt. 252).

[6] Id.

[7] See 17 CFR § 229.407.

JOURNAL OF TAXATION and REGULATION of FINANCIAL INSTITUTIONS

Committee. Generally speaking, the CRO should be tasked with managing a banking entity's risk profile on an enterprise-wide level by:

- Allocating delegated risk limits and monitoring compliance with such limits;
- Establishing appropriate policies and procedures relating to risk management governance, practices, and risk controls;
- Developing appropriate processes and systems for identifying and reporting risks, including emerging risks;
- Managing risk exposures and risk controls; monitoring and testing risk controls;
- Reporting risk management issues and emerging risks; and
- Ensuring that risk management issues are effectively resolved in a timely manner.

Comprehensive, Enterprise-Wide Program. Third, a banking entity must of course develop a comprehensive ERM program that operates on an enterprise-wide basis. A banking entity's ERM program must not only conform to industry best practices, but must also facilitate compliance with corrective actions undertaken by regulators.

In the event an enforcement action is sought, regulators will likely view positively an institution's implementation of a risk management program that is reasonably commensurate with its risk profile, even if in the eyes of the regulator the program fell short.

Although these requirements apply to organizations $10 billion and larger, they provide helpful guidance for institutions of all sizes in preparing risk management programs. These standards, coupled with the additional agency guidance discussed below, provide a roadmap to assist organizations of all sizes in implementing ERM.

BEYOND THE BASICS: OVERVIEW OF REGULATORS' EXPECTATIONS

Although the statutory requirements of ERM may be new, ERM's relevance in the regulatory enforcement context is well-established. If a financial institution develops and fosters a robust ERM program, it may prevent an enforcement action from ever arising. In the event an enforcement action is sought, regulators will likely view positively an institution's implementation of a risk management program that is reasonably commensurate with its risk profile, even if in the eyes of the regulator the program fell short. Moreover, from a practical standpoint, having the framework in place will facilitate an institution's incorporation of additional risk-mitigation factors if required to do so.

Over the past several years, financial regulators through their public statements have provided a window into their expectations of bank ERM programs. Those regulators have repeatedly emphasized five areas: effective structural governance, robust and independent internal audit functions, consistent flow of risk-related information to the highest levels of the institution, instilling a strong corporate culture, and early identification of risks. The regulatory emphasis on each is discussed below.

Effective Structural Governance. Regulators have indicated that one of the key structural components of a robust ERM program (at least for large banking organizations) is having some form of risk management function and accountability in each business line.[8] In her 2005 speech, Acting Comptroller Williams explained that OCC examiners

> will note what activities and risks exist within a line of business and would be sensitive to the quality of risk management for how that business is conducted. Does the line of business risk-assess the activities and transactions it conducts, and is the quality of risk management commensurate with the level of risk taken? Does it apply more diligence and tighter controls in its high-risk areas? What external indicators are taken into consideration to identify risks? In a retail line of business, examiners might begin by looking at the institution's customer complaint function—an excellent window on the bank's commitment to the quality of its customers' banking experience. The best companies have quality assurance programs in place that track and analyze their customer complaint experience and flag unusual trends. And what becomes of that information? Are managers held accountable for acting on the information and improving performance? What process exists within the business line to check to verify what follow-up has occurred?[9]

Further, regulators also look for a strong, well-placed risk management compliance function. Structurally, regulators will look to see whether the institution's risk management function (1) is properly resourced, (2) has adequate stature and influence within the organization, and (3) has adequate access to the institution's senior management and board.[10]

[8] Williams, supra note 4.

[9] Id. at 3.

[10] Id. at 2.

Journal of Taxation and Regulation of Financial Institutions

Regulators will also notice the way the institution's risk management structure has functioned in the past:

> Has the compliance function been effective in protecting the bank by identifying practices that fail to comply with law or regulation? Are activities that fall into gray areas that are not clearly noncompliant also flagged? Is that information being brought to the attention of business line or enterprise-wide risk managers, who are in a position to take appropriate and decisive action?[11]

In assessing the adequacy of the structure of a financial institution's risk management program, regulators will look for these key components to be satisfied.

Robust and Independent Internal Audit Function. Regulators closely monitor the structure of a financial institution's internal audit function, in particular the degree to which audit testing of the institution's internal controls is conducted for financial management and key business lines.[12] For example, one Board Governor noted that a bank's wire transfer activities and loan administration functions are often targeted for review.[13] Further, regulators will be looking to ensure the independence of the audit reporting line. In measuring independence, regulators may look to the internal audit staff's size, whether the unit is headed by individuals "of the appropriate rank and stature within the organization to give that function the credibility and weight that its recommendations need."[14] Further, regulators look to ensure the internal audit unit is not subject to "cost pressures that might compromise its effectiveness. . . ."[15] Of course, regulators will also look to ensure that a financial institution has external auditors with the appropriate competence and independence.[16]

Consistent Flow of Risk-Related Information. Another metric regulators use to examine the effectiveness of a financial institution's ERM program is how risk-related information flows through the organization. In particular, regulators will look to see whether the information reaches senior management and whether and under what circumstances information reaches the Audit Committee, Risk Committee, and Board of Directors. Further, regulators will evaluate what managers and committees do with the information received—whether they probe the representations they receive, whether information is "capped off" by senior management so that the board does not receive it, and whether senior management is open with regulators when supervisory issues arise.[17] According to Julie Williams, the OCC "believe[s] that most bankers will make good decisions if they have good information—from their own risk control processes and from their regulator—and that bad decisions are more likely than not a result of incomplete, unduly influenced, misleading, or erroneous information."[18] Thus, regulators focus on ensuring that risk-related information flows accurately and appropriately through the financial institution.

Strong Corporate Culture. Several regulators have also noted that any system of risk management would be incomplete "if the organization [itself] is not grounded in a sound corporate culture and value system understood by all its employees."[19] According to OCC's then-Chief National Bank Examiner Timothy Long, a financial institution's corporate culture must include and encourage "mechanisms that allow business line and risk managers to elevate concerns to appropriate levels of management and to ensure the timely resolution of those concerns."[20] Regulators may also look to compensation programs to determine whether employees are rewarded inappropriately, or whether compensation supports the behaviors an organization wants to encourage.[21] Of course, regulators are also mindful that the attitude of senior management—i.e., the "Tone at the Top"—can greatly influence whether risk-management practices are truly put into motion in a financial institution.[22] It is therefore critical not only that the upper echelons of the organization publicly support the ERM effort to all employees, but also that their individual interactions reinforce senior management's and the board's commitment to ERM.

[11] Id.

[12] Id.

[13] Susan Schmidt Bies, Member of the Bd. of Governors of the Fed. Reserve Sys., "A Bank Supervisor's Perspective on Enterprise Risk Management, Remarks Before the Enterprise Risk Management Roundtable" (Apr. 28, 2006), available at http://www.bis.org/review/r060502d.pdf.

[14] Williams, supra note 4, at 3.

[15] Id.

[16] Id.

[17] Id. at 4.

[18] Id.

[19] Id. See also "Lessons Learned in Risk Management Oversight at Federal Financial Regulators," (testimony of Timothy W. Long before the United States Banking, Housing, and Urban Affairs (March 18, 2009)), available at http://banking.senate.gov/public/index.cfm?FuseAction=Files.View&FileStore_id=d92ff037-4d3b-4b9e-bdb8-1d9f8af40eb0); Bies, supra note 13.

[20] Long, supra note 19, at 12.

[21] Williams, supra note 4, at 5.

[22] Id. at 6.

JOURNAL OF TAXATION and REGULATION of FINANCIAL INSTITUTIONS

Early Identification of Risks. Additionally, regulators have stressed the need for financial institutions to be proactive in identifying the risks associated with their operations. In the product context, Mr. Long noted that the OCC expects institutions to conduct "appropriate due diligence at the front-end, before products are offered, to ensure that all risks have been appropriately considered and can be effectively identified, managed and controlled."[23] Naturally, early identification of risks can only be effective if the financial institution has in place metrics to identify all types of risks associated with its operations, whether the risk is internal or external.

BUILDING AN ERM PROGRAM

As the public statements of regulators indicate, an appropriate risk management framework begins with the proper structure. Once a financial institution builds the structure and assigns responsibilities appropriately, it can begin assessing and monitoring risks on an enterprise-wide basis. In particular, the institution can begin developing "Key Risk Indicators," discussed more fully below, which will permit it to evaluate risks on a forward-looking basis.

The board should encourage a culture in which all employees are invited to identify potential risks and notify management of their existence, as opposed to simply relying on internal audit or risk management to find and report them.

Responsibilities of the Board. A financial institution's board has the primary responsibility for setting a Tone at the Top that promotes open communication of risks, escalation of problems to higher levels in the bank, and discourages excessive risk-taking. A board is also responsible for the following:

- *Overall risk strategy:* The board is responsible for directing the success of the institution, including approving and overseeing the implementation of the institution's strategic objectives, risk strategy, and corporate governance. In the area of risk management, the board is responsible in particular for setting the institution's risk appetite.[24] In doing so, the board should consider, among other questions, the following: (1) Are there specific risks the institution is not prepared to accept? (2) How much earnings volatility is the institution willing to accept? (3) To what extent is the institution willing to expand its product, customer, or geographic coverage? (4) What amount of risk is the institution willing to accept on new initiatives to achieve a specified return on investment?[25] The board's monitoring of the institution's ERM must be an ongoing process rather than a one-time event (and indeed, through regular reevaluation of risk management approaches, an institution may identify business lines where it has reduced risk *too much*, and thus maximize returns by reviewing its policies regularly).[26]
- *Policies for risk, risk management, and compliance:* In addition to setting an institution's overall risk appetite, the board is also responsible for implementing generally applicable risk management and compliance policies. In order to infuse ERM into the culture of the institution, communications from the board should be clear and consistent. The board should require regular training for employees of each business unit.[27] Moreover, the board should encourage a culture in which all employees are invited to identify potential risks and notify management of their existence, as opposed to simply relying on internal audit or risk management to find and report them.[28]
- *Internal Controls System:* The board must also put in place a robust internal audit function to ensure compliance with the institution's risk management policies (as discussed before, external auditing is also a critical function). The internal audit function should be responsible for evaluating the effectiveness of the institution's risk management and compliance functions on an individual business line and enterprise-wide basis.[29] Internal audit

[23] Long, supra note 19, at 12. (Mr. Long further noted that "At the OCC, approval of new or novel banking activities is predicated on the bank having sufficient risk management controls in place.")

[24] Basel Committee on Banking Supervision, "Principles for Enhancing Corporate Governance," at 7-8 (Oct. 2010), available at http://www.bis.org/publ/bcbs176.pdf.

[25] Comm. of Sponsoring Org. of the Treadway Comm'n, Strengthening Enterprise Risk Management for Strategic Advantage, at 7 (2009), available at http://www.coso.org/documents/COSO_09_board_position_final102309PRINTandWEBFINAL_000.pdf.

[26] Mark L. Frigo & Richard J. Anderson, Comm. of Sponsoring Org. of the Treadway Comm'n, "Embracing Enterprise Risk Management," at 7 (Jan. 2011), available at http://www.coso.org/documents/EmbracingERM-GettingStartedforWebPostingDec110_000.pdf; see id.

[27] Id.

[28] Basel Committee on Banking Supervision, supra note 24, at 22.

[29] Id. at 23.

Journal of Taxation and Regulation of Financial Institutions

must be staffed to a level commensurate with the institution's size, complexity, and activities, among other risk-related factors. The unit must have sufficient resources to operate independently. Further, the unit must be headed by individuals with the appropriate rank and stature to give the function credibility within the institution. Internal audit must also have open access to the board and senior management.

- *Corporate Governance Framework:* The board is responsible for the allocation and monitoring of authority and responsibilities within an organization. In particular, the board should provide oversight of senior management, including monitoring senior management's activities, meeting with senior management regularly, and ensuring that senior management's knowledge and expertise remain appropriate given the nature of the business and the institution's risk profile. The board is also responsible for organizing itself into the necessary committees, including a Risk Committee for large banking organizations.[30]
- *Compensation:* The members of the board involved most actively in overseeing the compensation system should be outside directors. The board should ensure that no compensation framework encourages risk-taking in excess of the institution's risk appetite (e.g., significant reductions in business line income after risk adjustment should result in reduced compensation). In particular, the compensation of the CRO and other risk management officials should not be substantially tied to business line revenue, given that such ties could compromise their independence.[31]
- *Resources:* The board should ensure that the organization, including the Risk Committee of the board and the CRO, have access to sufficient resources to carry out their responsibilities fully. Such resources could include, for example, access to outside business and legal consultants with expertise in risk management as needed.

Risk Committee. As discussed above, the board should establish a Risk Committee of the board that has several responsibilities and characteristics, including the following:

- *Advising the board:* The Risk Committee should be responsible for developing and advising the board on the institution's overall current and future risk appetite and strategy. Once adopted by the full board, the Risk Committee should be responsible for overseeing senior management's implementation of that strategy. In advising the board, the Risk Committee should undertake a careful analysis of all risks facing the institution.[32]
- *Independence:* The Risk Committee should be made up primarily of the board's outside directors. At least one director should have risk management expertise commensurate with the company's capital structure, risk profile, complexity, activities, size, and other appropriate risk related factors. Most institutions should consider having an independent director chair the Risk Committee, and larger banking organizations may be required to do so.
- *Charter:* The Risk Committee should have its own charter that sets forth its mandate, scope, and working procedures.[33]
- *Communication and recordkeeping:* The Risk Committee should maintain open communication, both formal and informal, with the full board and with senior management.[34] Further, the Risk Committee should maintain appropriate records of its deliberations and decisions.[35]

The role of the Chief Risk Officer should be distinct from other executive functions and business line responsibilities.

Chief Risk Officer. The CRO position of a financial institution should have the following characteristics:

- *Structure:* The CRO should have sufficient stature, authority, and seniority within the organization to ensure that issues raised by the CRO receive the necessary attention from the board, Risk Committee, senior management, and the business lines.[36]
- *Independence:* The CRO should report directly to the board and its Risk Committee and should have direct access to both. The role of the CRO should be distinct from other executive functions and business line responsibilities. The CRO should not serve as the Chief Operating Officer, the Chief Financial Officer, or the chief auditor. In smaller institutions in which resource restraints make overlapping responsibilities necessary, the overlapping

[30] Id. at 5.
[31] Id. at 25.
[32] Id. at 13.
[33] Id. at 12.
[34] Id. at 13.
[35] Id. at 12.
[36] Id. at 18.

JOURNAL OF TAXATION and REGULATION of FINANCIAL INSTITUTIONS

roles should be compatible with the individual's role as CRO.[37]
- *Communication and recordkeeping;* The CRO should meet regularly with the board. All interactions should be documented appropriately.

Enterprise-Wide Risk Assessment and Monitoring. Once a financial institution has the proper risk management framework in place, it can begin assessing and monitoring enterprise-wide risks through a top-down review of those risks that could be most significant to the institution. Each institution should consider doing so by developing Key Risk Indicators. An idea promoted by COSO, Key Risk Indicators mirror Key Performance Indicators.[38] Whereas Key Performance Indicators are used to evaluate whether the institution met its various goals on a look-back basis in a variety of areas, including risk management, Key Risk Indicators will allow the institution "to better monitor potential future shifts in risk conditions or new emerging risks so that management and boards are able to more proactively identify potential impacts on the organization's portfolio of risks."[39]

Periodic inter-business line discussions can help ensure that cross-business line risks are appropriately identified, and help avoid "siloing" within the organization.

For example, one Key Risk Indicator for a financial institution's commercial lending portfolio might be the percentage of commercial building vacancies in the institution's geographic lending area. An increase in commercial vacancies, of course, could be an early sign of future losses in the institution's commercial lending portfolio. Once alerted to this possibility by the Key Risk Indicator, an institution can act proactively to mitigate losses in its portfolio.[40]

In conducting a top-down review of risk, institutions may, as necessary:

- List the major risk categories to which the institution is exposed and discuss exposures to each category which, if not managed properly, could endanger the institution's strategic objectives.[41]
- Consider prioritizing or ranking the risks identified.[42]
- Develop Key Risk Indicators in each risk category to enable the board and senior management to monitor potential shifts in risk conditions and proactively address any material changes. In making this calculation, the board must consider the risks themselves, the probability and impact of each risk, and the speed with which each risk could manifest.[43]
- Convene periodic inter-business line discussions to ensure that cross-business line risks are appropriately identified. Such interaction will help avoid "siloing" within the organization.
- Regularly monitor risk concentrations and exposures.
- Inevitably, certain risks will not be identified or fully mitigated and losses will ensue. It is critical that the institution use such incidents as an opportunity to evaluate how the loss or oversight occurred and to strengthen the ERM program moving forward.

EMERGING ERM TRENDS

The focus of regulatory supervision is ever-evolving, particularly in the risk management context. Although risks of all sizes must be given due consideration in any ERM, certain risks may warrant special attention in light of recent enforcement trends by the federal banking agencies. We believe the following areas should be priorities for financial institutions:

- *Bank Secrecy Act/Anti-Money Laundering Compliance:* Since the events of September 11, 2001, U.S. law enforcement has increasingly enlisted banks in the fight against terrorist financing, narcotrafficking, and other illegal flows of money. The past 10 years have demonstrated that significant administrative actions and civil and criminal liability can result from failure to comply with BSA/AML requirements, and BSA/AML compliance will undoubtedly continue to be an examination focus for the foreseeable future.[44]
- *Unfair, Deceptive, and Abusive Acts and Practices (UDAAP):* Following a perceived lapse in consumer protection efforts, the federal banking agencies have shown increased interest in protecting the public from potentially harmful products and services. The Dodd-Frank Act's creation of the

[37] Id. at 18.

[38] Beasley et al., supra note 1.

[39] Id. at III.

[40] Example adapted from John Behringer, "Using Key Risk Indicators to Recover, Improve or Maintain Institutional Performance," at 7 (McGladrey & Pullen 2011), available at http://mcgladrey.com/pdf/wp-using-key-risk-indicators.pdf.

[41] Beasley, supra note 1, at 4-5.

[42] Id. at 5.

[43] Id.

[44] Ralph Sharpe & Meredith Boylan, "Operational Risk: Increased Regulatory Focus on BSA/AML Compliance and Third-Party Relationships," 25(6) J. Tax'n & Reg. Fin. Insts. 41 (July-Aug. 2012).

Consumer Financial Protection Bureau, empowered with broad authority to regulate the manner in which consumer financial products and services are offered to the public, is the latest manifestation of this trend. Financial services providers should give careful consideration to how their products and services could result in consumer harm, confusion, or abuse, and ensure that steps are taken to monitor for and prevent such outcomes.

- *Fair lending:* The recent home mortgage crisis renewed concerns over whether lenders were properly monitoring for potential disparities in how protected classes were treated in the mortgage lending process. Even alleged discrimination by independent third-party mortgage brokers became the responsibility of wholesale lenders, despite the fact that the lenders themselves had not discriminated. Although this outcome was driven as much by political expediency—the brokers themselves had largely closed up shop or were otherwise judgment-proof—as by true culpability, the experience demonstrates that the mere fact that a counterparty is an independent contractor does not eliminate risk for the bank.
- *Information management/privacy:* Well-publicized breaches of customer financial information are a consistent reminder to financial institutions of the importance of putting in place robust information management and protection systems. Each financial institution should have in place both a management system as well as a contingency plan in the event of a breach.

In seeking to address these and other areas of risk, it is important to note that complying with the four corners of the law in one area (for example, compliance with Regulation Z's Truth in Lending provisions, or Regulation E's Electronic Funds Transfers provisions) may not protect a financial institution from liability in another (such as a UDAAP claim). Every financial institution should be cognizant of these emerging risk areas in developing and adapting their ERM program and must be creative in assessing the risks they may entail.

CONCLUSION

Risk Management is as much art as science. As news reports frequently demonstrate, financial institutions of all sizes occasionally fail to detect the risks faced by the institution and must suffer the consequences for such oversight. Ultimately, while no risk management program will be able to avoid fully 100 percent of the risks faced by an institution, the fact that the institution has an ERM program in place will help mitigate the losses that result and any collateral impact, including agency enforcement actions, civil and criminal penalties and reputational harm. ■