The Role of Risk Management and Compliance in Banking Integration

Geoffrey P. Miller
NYU School of Law, geoffrey.miller@nyu.edu

Follow this and additional works at: https://lsr.nellco.org/nyu_lewp

Part of the Administrative Law Commons, Banking and Finance Law Commons, Business Organizations Law Commons, Law and Economics Commons, and the Organizations Law Commons

Recommended Citation
https://lsr.nellco.org/nyu_lewp/391
The Role of Risk Management and Compliance in Banking Integration

Geoffrey P. Miller

Abstract: This article explores an important but little studied dimension of the ongoing transformation of banking markets: the growth of risk management and compliance as key governance functions and the focus on risk as a foundation stone for regulatory strategy. The developments in risk and compliance are in part mandated by government regulation, but also reflect practices and norms developed in the private sector. Parallel developments reflecting convergence of norms and practice are observed in banking markets around the world.

* * *

Europe is engaged in an experiment unprecedented in world history: can independent nations – even if linked by significant legal, economic, and social ties – merge their financial systems into a true banking union? Policymakers in Europe are working diligently to achieve that goal. Spurred by the financial turmoil of 2007-2009 and its aftermath, Europe has created a network of regulatory institutions including the Single Supervisory Mechanism, the European Systemic Risk Board, the European Banking Authority, the Single Resolution Mechanism, and the European Stability Mechanism. Acting individually and in concert, these bodies are working to enhance the integration of financial markets in the euro area.

Important as these developments are, they are not the only factors at work. Changes in best practices in the management of banking institutions have also had a major impact in the in the current trend towards harmonization of banking in the euro area. Although promoted in important ways by regulatory authorities, these practice changes have their root in broader developments: a movement which emphasizes risk and compliance as key elements in the governance of banking enterprises. These

---

1 Stuyvesant Comfort Professor, NYU Law School; Co-Director, Program in Corporate Compliance and Enforcement. I thank Danny Busch, Guido Ferrarini, and Roel Theissen for helpful comments.
developments, moreover, are even more international in scope than the move towards
European banking integration: the growth of risk management and compliance is
occurring on both sides of the Atlantic – in the United States as well as Europe, in South
as well as North America, in parts of Asia, and elsewhere. Arguably the treatment of risk
and compliance at banking firms is one of the most successful examples of an
international framework for control of banking institutions -- even though the applicable
rules are not embodied in any single statute, code, or regulatory action.

This article identifies key aspects of this enhanced focus on risk and compliance.
The paper argues that financial institution regulation is experiencing a risk revolution and
identifies some of the important drivers of that development. In particular, the article
discusses the widespread acceptance of enterprise risk management; dramatic
enhancements to the roles and responsibilities of internal and external auditors; the
emergence and empowerment of the office of Chief Compliance Officer; and the growth
of risk-based approaches to examination and supervision. The article concludes by
offering some thoughts for why systems both in Europe and elsewhere seem to be
converging on risk management and compliance as keys to best practices in financial
institution governance.

The risk revolution in financial institution regulation

Over the past decade, financial institutions on both sides of the Atlantic have
experienced what might be called a “risk revolution” -- a far-reaching change in
governance and management that significantly upgrades considerations of risk within
systems of internal and external controls. Before discussing specific aspects, it is useful
to identify some of the key drivers that have produced this development. While the
causes of a phenomenon this extensive can never be fully identified, the following have played a role:

1. Finance economists have invented powerful and sophisticated techniques for modeling risk within firms. Key advances include the capital asset pricing model, which predicts the price of a financial asset based on a few simple variables; the Black-Scholes option pricing model, which predicts the price of options; Value-at-Risk methodologies, which predict the performance of investment portfolios under stressed conditions and which facilitate simple methodologies for control at the level of the trading desk; and various corporate default models (Altman’s “Z” being one of the earliest and best-known) which predict the likelihood that a borrower will fail to meet its obligations under a bond or other debt instrument. Each of these models -- and many others -- has been thoroughly integrated into the day-to-day management of banks through computerized models and reporting and control systems.

2. It would be hard to overstress the importance of the Basel Committee on Banking Supervision, which through its risk-based capital regulations has directed attention to the systematic analysis and management of risk. The Basel framework was a breakthrough insofar as it highlighted the importance of risk -- first the risk in a bank’s portfolio and off-balance sheet activities and, later, market and operational risk. The emphasis on risk contained in the Basel capital adequacy rules had a large impact on the thinking of banks, bank regulators and financial market participants generally.

3. The corporate frauds uncovered during the late 1990s and early 2000s raised public concerns about the processes of internal control which seemed to have broken down at firms such as Enron, Worldcom, Global Crossing, and Adelphia in the United
States and Parmalat and Royal Ahold in Europe. How was it that these companies, which appeared on the surface to have maintained the requisite procedures and safeguards, were capable of engaging in massive fraud and illegality? Many concluded that internal controls were inadequate and that, to prevent such frauds in the future, it was desirable to upgrade the control environment. The Sarbanes-Oxley Act of 2002 (SOX) responded to these concerns. It requires corporate officers to certify that they are "responsible for establishing and maintaining internal controls;"\(^2\) and requires management and the external auditor to report on the adequacy of the company's internal control on financial reporting.\(^3\) SOX gave central importance to the concept of internal controls as mechanisms for managing the risk of misstatements in financial reporting.

4. The crisis of 2007-2009 convinced many that financial risk at banks had been poorly controlled in the years that led up to the crisis. The light of hindsight revealed that many financial institutions invested too much of their assets in subprime mortgage-backed securities and other assets whose value was tied to the U.S. housing bubble. Some of these investments were highly complex instruments (such as collateralized debt obligation securities) whose risk profile was only vaguely understood by the traders who bought and sold them. But it was not only financial institutions that misjudged these risks; rating agencies and regulators were at least as far off in their estimates. In retrospect, it appeared that had risk assessment and risk management been better in all these institutions, the crisis could have been mitigated or avoided. The current emphasis on risk management reflects that assessment and seeks to ensure that the disaster of 2007-2009 does not recur.

5. A variety of influential committees and quasi-governmental bodies have offered advice about the advantages of risk management, especially through the implementation of effective internal controls. Important among these is the Committee of Sponsoring Organizations of the Treadway Commission (COSO), which formulates best practice standards which have been widely adopted in the financial world. One pillar of the COSO framework for internal control is “risk assessment”: the process by which the organization identifies and evaluates material risks to its operations, both internal (e.g., a fraud committed by senior officers) or external (e.g., changes in market prices).

* * *

These and other events and developments have contributed to the phenomenon discussed in this paper – namely, the greatly enhanced emphasis on risk and risk management in the structure of systems of internal and external control at financial institutions. The following sections discuss key institutions or functions where this emphasis on risk has had a major impact.

**Enterprise risk management**

Not too long ago, banks managed risk though what by today’s standards might seem like fairly primitive techniques. Five elements were distinctive of the “old” risk management approach:

1. Risk management was distributed throughout the institution along business lines. The commercial loan department managed the risk of the commercial loan

---

The mortgage department managed the home loan portfolio, the trading desk managed the bank’s trading book, the trust department, if one existed, managed the risk of the bank’s fiduciary accounts and so on. There was little coordination between departments.

2. Risk was conceived of as downside risk -- that is, the risk of something bad happening, weighted by the costs to the organization if the risky event occurred. Upside risk -- the risk of something good happening -- was not considered to be a risk at all and was not integrated into the risk management function.

3. Risk management was not transparent, either to investors, to regulators, or even to the board of directors. Different managers defined their objectives differently, reported their department’s risk profile and performance with different metrics, and failed to systematically track existing or potential threats.

4. Risk was principally managed through insurance or hedging transactions that transferred risk to others. Internal mitigation strategies were less frequently used. The idea of a business line “accepting” a risk -- that is, consciously conducting an activity knowing that it presents an unhedged risk of loss -- was not widely employed.

5. Overall, the technical task of risk management -- as opposed to the management of strategic or business risks -- was given a relatively low priority by senior managers and the board of directors.

Each of these features of the “old” risk management has given way to a somewhat different approach. The approach has many names, but the currently favored label is “enterprise risk management.” The idea of enterprise risk management is not fully

---

understood, even by those prone to use it most frequently; but the term is always used in a positive sense, as indicating a progressive, modern, state-of-the-art system far superior to what had gone before. Key features of enterprise risk management include the following:

1. Risk is evaluated and managed on an enterprise-wide basis. Rationales for centralizing risk management include the following.

   First, if risk is distributed across business lines with no central authority, an important aspect of an organization’s functioning will not be properly controlled. Rational risk management requires centralized direction in order that the enterprise as a whole may follow a well-defined, objective and rational set of objectives with respect to risk.

   Second, the distributed approach raises problems of overlap and gap. Sometimes an activity that an individual manager might consider to pose excessive risk, when viewed from the perspective of a single business line, turns out not to be particularly problematic from the standpoint of the enterprise as a whole, either because the risk is *de minimis* in light of the enterprise’s overall operations or because the negative results anticipated from a risk in one part of the organization are offset by positive results elsewhere. In other cases, a risk not considered problematic by the business line managers may in fact represent an unacceptable degree of risk for the organization as a whole because it is pervasive within the organization. Risks may also fall in the gap between the portfolios of business line managers and, accordingly, not be considered at all within the framework of the old risk management (examples could be certain forms of reputational or operational risk).
Third, the distributed approach creates potential agency costs. American bankers are familiar with the term “IBGYBG” -- “I’ll be gone you’ll be gone.” The idea is that two parties to a transaction may engage in a deal that both know to be ill advised, simply because neither of them plans to be around when the negative consequences of their action come to be experienced. Originators of subprime mortgages acted this way when they solicited mortgage loans during the mid-2000s from borrowers they knew could not repay. Arguably the originators did not particularly care about the borrower’s ability to repay because they were compensated for originating the loan, not for its subsequent performance, and by the time the loan went into default it would have been transferred to a special purpose entity and sold to the public as part of a mortgage backed security.

Enterprise risk management facilitates the correction of these problems. This approach allows the board of directors to establish a risk appetite for the bank as a whole, based on systematic analysis of the institution’s overall objectives. Problems of gap and overlap are mitigated because risk in the organization as a whole is overseen by a risk department headed by a chief risk officer enjoying rights of the “C-Suite” -- substantial discretion and rights of direct report to the CEO or a committee of the board of directors. Agency costs can be mitigated, although not eliminated, if the enterprise risk management system tracks performance of investments after the officer responsible for the initial decision ceases to be directly responsible for its outcome.

2. Risk is no longer exclusively conceived of as downside risk. Instead, enterprise risk management employs the more sophisticated corporate finance concept which defines risk as the distribution of outcomes, good or bad. In practice, the commitment to a two-tailed concept of risk is often honored in the breach, because as a
practical matter people have always been and will remain more worried about the chance something bad will happen than about the chance something good will happen. Nevertheless, maintaining the two-tailed approach serves a salutary purpose because if a bank’s performance is outside of risk tolerances, even on the positive side, this is a potential danger sign indicating that risk is not fully controlled.

3. Enterprise risk is more transparent than its predecessor. This is not to say that enterprise risk systems in banks are fully transparent even today. Far from it: enterprise risk management systems may employ loosely defined concepts, set tolerances on the basis of poorly considered assumptions, and remain confidential documents that are not available to investors or other interested parties. Nevertheless transparency has increased under enterprise risk management.

Most importantly, the board of directors of large, publicly traded banks is responsible for establishing a formal “risk appetite” document which identifies key risks and sets metrics and tolerances for measuring inherent risk and the residual risk that remains when mitigation and control strategies are implemented. The term “risk appetite” is evocative, and also apt. Like our appetite for food, banks can be said to desire risk -- not for its own sake, but rather because a satisfactory return on investment cannot be achieved without the acceptance of a certain level of risk. As risk increases, however, the bank’s appetite for risk becomes sated; at some point the bank affirmatively dislikes and wishes to reduce its risk profile. Here again the analogy is appropriate: when we are hungry a slice of pizza is delicious; but once we have had a slice or two, eating any more becomes affirmatively unpleasant. The risk appetite and its associated “dashboard” -- a chart or suite of charts that contains key metrics and tolerances and
reports on current and historical performance -- is the key tool for enhancing transparency at the level of senior management and the board of directors.

The creation of risk departments headed by chief risk officers also enhances transparency. The CRO is responsible for ensuring that the board’s risk appetite is implemented throughout the organization and for monitoring the metrics of the appetite to ensure that no items are approaching the tolerance limits. The CRO is thus a central repository of information regarding risk in the organization as well as a principal source of information for the board or board risk committee.

4. Enterprise risk management does not contemplate that risk will principally be managed through insurance or hedging. Instead, once an inherent risk is identified, the risk manager considers available options for controlling or mitigating the risk. Risks are controlled when the organization implements systems of internal controls designed to prevent the risk from coming to pass; risks are mitigated when the institution adopts strategies such as insurance or hedging which reduce the impact of the event if it occurs. The risk manager also evaluates the residual risk that remains when control or mitigation strategies are implemented. The resulting analysis is complex, involving the intellectual equivalent of simultaneous equations; but the objective is simple: the risk manager seeks, at reasonable cost, to bring risks within the tolerance framework set by the board’s risk appetite.

5. Enterprise risk management upgrades the attention given to risk issues by senior officers and the board of directors. This attention may be reflected institutionally by the establishment of a board-level risk committee and an executive risk office headed
by the chief risk officer. It is reflected in practice by the amount of board and management time devoted to issues pertinent to risk.

Bank regulators have enthusiastically embraced the idea of enterprise risk management. Senior officials of regulatory agencies promote the idea at conventions of bankers, and regulatory guidance frequently assumes that banks have robust enterprise risk management systems in place. The Basel Committee on Banking Supervision, in particular, approves and endorses the idea of enterprise risk management for the integrated control of all risks facing a banking institution. These days, major banks on both sides of the Atlantic operate systems of enterprise risk management; if they did not they would likely receive an unwelcome letter from their regulator informing them that their procedures are not up to par.

Perhaps the most important enterprise risk-management activity for the banking industry is the use of stress tests, mandated for larger banks both in the United States and in Europe. The stress test process can be complex, but the essence is simple. The bank creates a model of its operations which responds to inputs of variables representing

---


conditions in the economy and in financial markets. Stress scenarios are developed which test how the bank will perform under progressively adverse conditions; these may be supplied by the regulators or devised by the bank as part of its internal control processes. The bank “passes” the test if under the stressed scenarios it maintains a level of solvency and liquidity deemed satisfactory by the regulators or the bank. It is obvious that stress tests of this sort implement a strategy of risk management: they provide an assessment of the risk posed to the institution by possible adverse future conditions.

**Internal audit**

Complementing the discipline of enterprise risk management is a focus on risk-based internal audit. Here, again, practices have changed over the past decades. At one time internal audit used a “check-the-box” approach, under which locations, products, practices or processes were selected every year and evaluated according to a predetermined set of audit criteria. The check-the-box approach had virtues of consistency and reliability, but was increasingly seen as inefficient and unresponsive to changes in the organization. Under the older approach the same units would be audited over and over again, regardless of whether they posed significant risk. Meanwhile, because the check-the-box approach was known to the business line manager, it was possible to “game” the system by engaging in questionable activities in areas that the manager knew would not be audited.

The modern approach to internal audit is explicitly risk-based. The chief audit executive performs a risk assessment of the organization and rates the elements in the audit universe based on the assessment. Units deemed to present higher risk are audited

---

more frequently, and with higher intensity, than units deemed to pose lower risk.

Alternatively, the audit executive may perform a risk assessment of the extent to which audit units are well-controlled by the business line managers under the organization’s system of internal controls. This “systems-based” approach faces the difficulty that internal audit is not specialized in understanding the constraints and objectives faced by managers who set internal controls. It also requires internal audit to engage in a normative evaluation of the control environment, which can be considered to be above internal audit’s “pay grade.” Nevertheless this approach has advocates for the obvious reason that a risk-assessment of internal controls, if performed accurately, should generate a better understanding of the firm’s risk profile than an assessment that excludes consideration of internal controls. Systems-based auditing is sometimes presented as an alternative to risk-based audit, but it is in fact still a risk-based approach, albeit one that focuses on different risks (risks of breakdown in internal controls rather than risks inherent in the business process).

The scope, process, and timing of internal audits are determined by the initial risk assessment. The head of internal audit prepares an annual audit plan which is presented to the audit committee of the board of directors for approval. The audit plan identifies the auditable units, identifies whether and when they will be audited during the year, and budgets staff and resources to each audit. Ideally, the head of internal audit will disclose to the members of the audit committee the methodology which she used to make the risk assessment that underlies the audit plan, as well as the rationale for assigning risk levels to each audit unit.
The risk-based feature of internal audit makes the internal audit department a participant in implementing the organization’s enterprise risk management strategy, since the auditing process provides information as to whether the line managers are controlling risk within the institution’s risk appetite. In the case of banks, however, the oversight of risk has migrated largely to the specialized risk office, leaving internal audit in a secondary (but still important) role in this respect.

A subtle question concerns where internal audit gets its risk assessment. On the one hand the head of internal audit is not a professional risk manager. She is probably not trained in risk management and may lack the comprehensive overview of the firm’s business strategies and evolving threats that is necessary for a fully informed risk assessment. These considerations suggest that the audit executive could “borrow” the risk assessment from the chief risk officer or another official charged with identifying and overseeing risk on an enterprise-wide basis. On the other hand there are problems with allowing the head of internal audit to “outsource” the risk assessment to someone else. Outsourcing the assessment deprives the company of a potentially independent evaluation of risk which can improve the accuracy of the company’s approach; limits the independence of internal audit which is crucial to its role as the “third line of defense;” and discourages internal audit from thinking proactively about risk or utilizing information obtained during the audit process to update the risk assessment. For these reasons internal audit may be tasked with developing its own risk-assessment. However, as a practical matter the audit department’s risk assessment will inevitably be informed by the views of others in the organization.
Bank regulators in the United States encourage the risk-based approach to internal audit. The Comptroller of the Currency, the regulator of federally-chartered depository institutions, has this to say:

The OCC, with the other federal banking regulators, encourages risk assessment and risk-based auditing for all banks. Risk assessment is a process by which an auditor identifies and evaluates the quantity of the bank’s risks and the quality of its controls over those risks. Through risk-based auditing, the board and auditors use the results of the risk assessments to focus on the areas of greatest risk and to set priorities for audit work.¹¹

The Comptroller specifically requires that the internal audit department of banks under it supervision conduct a risk assessment as part of the audit process:

A control risk assessment (or risk assessment methodology) documents the internal auditor’s understanding of the institution’s significant business activities and their associated risks. These assessments typically analyze the risks inherent in a given business line, the mitigating control processes, and the resulting residual risk exposure of the institution. They should be updated regularly to reflect changes to the system of internal control or work processes, and to incorporate new lines of business.¹²

As to responsibility for risk assessment, the Comptroller recognizes that internal audit must work with line department managers in evaluating risks and functions. Ultimately, however, the development of the risk assessment and the assignment of risk scores is the responsibility of internal audit, in consultation with the audit committee; the department is not supposed to borrow the risk assessment from others.¹³

**External audit**

A similar process has occurred in the activities of external auditors. The symbolism here is the green visor. At one time green visors were as emblematic of the

---

¹³ Comptroller’s Handbook, Internal and External Audits 17-18 (2003); Interagency Policy Statement on the Internal Audit Function and its Outsourcing 4 (2003) (“the audit committee should ensure that efforts to coordinate these monitoring functions do not result in the manager of internal audit conducting control activities nor diminish his or her independence with respect to the other risk monitoring functions.”)
external auditor as slide rules were of engineers. External audit would pore over the company’s books according to a preformed audit plan, and test processes and functions and transactions across the audited entity’s business lines without any adjustment for risk.

Over the past decades, the green visor approach has given way to an approach that is explicitly based on risk. Under the risk-based approach, the external auditor attempts to gain a global understanding of the audited entity and its business and regulatory environment in order to identify risks that may cause a material misstatement in financial reports. The auditor assesses these risks in order to devise an audit plan that responds the areas of greatest concern, taking account of nature of the risks, the nature and efficacy of internal controls, and the level of audit evidence required to support an audit finding. Based on the risk assessment, for example, the external auditor may identify the matters to be tested and the nature of the tests performed, the timing of the audit, the need or lack of need for experts in a particular topic, and the degree to which the auditor relies on the tests that are performed -- among other things.

The risk-based approach to external audit is often described as a “top-down” strategy. In a top-down approach, the auditor starts with company-level controls and moves on to significant accounts at the financial-statement level, finally drilling down to review specific processes and transactions. Part of the rationale for the top-down approach is that the examination of company level controls may reveal areas of risk that call for more intensive scrutiny at later phases of the audit.14

Auditing standard No. 2 of the Public Company Auditing Oversight Board (PCAOB), the U.S. regulator of public company auditors, implements the top-down

14 This concept is not unique to external audit: it is also widely used by bank regulators and also -- but to a limited extent -- by internal audit as well.
concept. It contemplates that the auditor will focus first on company-level controls, then move on to significant accounts at the financial statement level, significant processes, risks of error or fraud, and key controls designed to prevent mistakes or misconduct.

The risk-based approach to external audit is standard procedure in the United States and Europe as well as throughout the financial world. U.S. bank regulators encourage and expect that external auditors will utilize a risk-based approach, although they do not mandate a risk-based approach in as direct a way as they use with internal audit.\textsuperscript{15}

**Compliance**

Like the other activities discussed in this paper, the compliance function has experienced dramatic changes. At one time compliance was a bit of a backwater in firms. People working in compliance were treated with a certain amount of disdain by traders or managers, who viewed them as an annoying impediment to the important work of making a profit. In some firms being assigned to the compliance department was the career equivalent of exile to Siberia. The task of the compliance department was conceived as making sure that people followed the rules, without regard to the potential risk of violations. A compliance officer was charged with making sure that forms had been filled out and procedures followed. Someone has to make sure that a trader has signed the conflict of interest form; although the head of the business line may have the initial responsibility to obtain these signatures, the compliance department had to make sure that

\textsuperscript{15} Comptroller’s Handbook, Internal and External Audits 32 (2003) (external audit should provide “information useful to directors and management in maintaining a bank’s risk management processes”); id. at 48 (external auditors should report to bank examiners on the “[r]esults and conclusions of risk assessments”).
the business line manager is doing her job. The compliance function, in other words, had elements of the “check-the-box” approach once popular in the audit field.

Compliance today has features inherited from this older approach, but the role of compliance departments has changed. The head of compliance has enjoyed a significant upgrade in prestige, power, and compensation. Banks these days are likely to designate the head of compliance as a member of the “C-Suite” by conferring the title “chief compliance officer” or equivalent. The upgrade is partly for show, in that a bank is well-advised to demonstrate a commitment to compliance if it wishes to reassure the regulators that it is not up to anything. But the upgrade also reflects a genuine increase in authority -- embodied in enhanced autonomy, increased budgets and staff, rights of access to meetings, and reporting lines to the chief executive officer or a committee of the board of directors.

Associated with this increased authority is a change in strategy. Today, while compliance officers still make sure forms are submitted, the compliance function itself has moved towards a risk-based approach. The compliance officer performs a risk assessment of the organization, focusing on the areas that are of special interest to compliance -- that is, potential violations of laws or company standards. For example, in an international bank, the officer might identify money laundering and sanctions regulations as areas of special risk and allocate extra resources to these areas while reducing the attention paid to other areas deemed to present lower risk of violations. Often, this task is assisted by vendors who themselves promote and encourage a risk-based approach to compliance management.
The risk-based approach to compliance faces a conceptual obstacle in that the official attitude of many institutions is one of “zero tolerance” for compliance violations. If no compliance violation is acceptable, the identification and acceptance of compliance risk seems out of place. The rhetoric of zero tolerance never comported with reality if it meant that all violations need to be prevented. In practice there is a tradeoff between the frequency and severity of violations and the amount expended on compliance. Any attempt to eliminate all violations would be prohibitively costly. Nevertheless, the zero tolerance idea exerted a restraining influence on the development of risk-based approaches to compliance.

These misgivings are increasing being forgotten. Although regulators rarely say so publicly, they now recognize that compliance is, in effect, one aspect of risk management. The Basel Committee on Banking Supervision put the matter as follows:

“[t]he purpose of the compliance function is to assist the bank in managing its compliance risk, which can be defined as the risk of legal or regulatory sanctions, financial loss, or loss to reputation a bank may suffer as a result of its failure to comply with all applicable laws, regulations, codes of conduct and standards of good practice. . . . Compliance risk is sometimes also referred to as integrity risk, because a bank’s reputation is closely connected with its adherence to principles of integrity and fair dealing.”

Accordingly, in the view of the Basel Committee, the very definition of compliance in banks is essentially one of risk management:

[Compliance is] an independent function that identifies, assesses, advises on, monitors and reports on the bank’s compliance risk, that is, the risk of legal or regulatory sanctions, financial loss, or loss to reputation a bank may suffer as a result of its failure to comply with all applicable laws, regulations, codes of conduct and standards of good practice . . . .

---

17 Id. at ¶ 10.
Risk-based approaches are now standard in compliance departments, and are strongly encouraged by the regulators. The U.K. Financial Services Authority, for example, approved of such a risk-based compliance program in its consent agreement with the insurance firm AON Ltd settling charges that AON had failed to exercise due care to prevent its agents from bribing foreign officials. As a factor mitigating the penalty imposed for the alleged violation, the FSA took note that AON had:

“designed and implemented a new global anti-corruption programme that includes a policy limiting the use of third parties. Aon Ltd has also implemented robust risk-based procedures that control and restrict the circumstances in which staff may make payments to Overseas Third Parties, particularly in high risk jurisdictions. . . . The new policy . . . generally prohibits the use of third parties whose only service to Aon is to assist in the obtaining and retaining of business solely through client introductions in countries where the risk of corrupt practices is anything other than low.”

Supervision and examination

The risk revolution has profoundly influenced how financial institution regulators approach the task of supervising banks. Supervisors once used an approach similar to the “check-the-box” strategy of internal and external audit. Mr. Carter, the examiner in Frank Capra’s movie “It’s a Wonderful Life,” would have arrived at the bank equipped with a list of items to check in the files and would have systematically gone through the list regardless of whether there was any significant risk that a particular item would pose a problem. More recently, the check-the-box approach has fallen into as much disfavor with the bank regulators as it has with auditors.

In place of the “bottom-up” approach traditionally used, regulators now favor risk-based supervision, which begins with a “top-down” analysis of the risks that the

---

19 Id. at ¶ 2.5.
regulator deems to be present in the organization -- in other words, a risk assessment. The regulator then devotes supervisory resources to those areas considered to present the greatest regulatory concern -- processes and products posing a risk to safety and soundness and areas where legal violations are likely to occur. The regulator uses the risk analysis to determine the type of examinations to schedule, the frequency with which examinations occur, and the makeup of the examination team.

The Basel Committee on Banking Supervision promoted the use of risk analysis in its revised “Core Principles for Effective Banking Supervision,”20 issued as a consultative document in 2011 and designed, in part, to address the “significant risk management weaknesses and other vulnerabilities” in financial institutions that came to light during the financial crisis of 2007-2009.21 Principle 8 of the new framework adopts a risk-based supervisory strategy. An “effective system of banking supervision” requires supervisors to engage in a “forward-looking assessment of the risk profile of individual banks and banking groups,” and “identify, assess and address risks emanating from banks and the banking system as a whole.”22

Principle 15 of the Basel supervisory principles carries the importance of risk and risk management into the operations of the banking institutions. It requires banks to “have a comprehensive risk management process (including effective Board and senior management oversight) to identify, measure, evaluate, monitor, report and control or mitigate all material risks on a timely basis and to assess the adequacy of their capital and

20 Basel Committee on Banking Supervision, Consultative Document -- Core Principles for Effective Banking Supervision (December 2011).
21 Id. p.2.
22 Id. p.29.
liquidity in relation to their risk profile and market and macroeconomic conditions.”

The required approach is one of enterprise risk management: The bank should take an “integrated bank-wide perspective” of the bank’s risk exposure, encompassing the bank’s individual business lines and business units. Where a bank is a member of a group of companies, the risk management framework should also cover the risk exposure across the banking group.

Virtually all financial institution regulators base their activities on a risk analysis. The Single Supervisory Mechanism approach to supervision is risk-based, taking account of both the degree of damage which the failure of an institution could cause to financial stability and the possibility of such a failure occurring. The intensity of supervision depends, in substantial part, on the SSM’s judgment as to the risks posed by different institutions and sectors. The ECB explains the rationale as follows: “Such a risk-based approach ensures that supervisory resources are always focused on the areas where they are likely to be most effective in enhancing financial stability.” Risk analysis is also incorporated in European banking regulation through consultations between the Single Supervisory Mechanism and the European Systemic Risk Board, a body commissioned with assessing risks to the financial sector.

Risk is also a key factor in the European Union’s implementation of the Basel III guidelines. The Capital Markets Directive adopted in 2013 (CMD4) directs supervisors

23 Id. p.40.
24 Id. p.40 n.53.
25 Id.
27 See id. at 19 (“close cooperation between the ECB and the ESRB and the development of information flows is mutually beneficial: it improves the ESRB’s ability to effectively identify, analyse and monitor EU-wide systemic risks, while the SSM may take advantage of the ESRB’s expertise, which goes beyond the banking sector and covers the entire financial system, including other financial institutions, markets and products.”).
to enhance risk management at banks and other credit institutions. Paragraph 54 provides that “In order to address the potentially detrimental effect of poorly designed corporate governance arrangements on the sound management of risk, Member States should introduce principles and standards to . . . promote a sound risk culture at all levels of credit institutions and investment firms and enable competent authorities to monitor the adequacy of internal governance arrangements.”28 Paragraph 57 calls on independent directors to exercise a credible challenge to management to satisfy themselves that “systems of risk management are robust and defensible;”29 and boards as a whole should devote sufficient time to understand the implications of the institution’s risk strategy.30 Risk management considerations are nearly ubiquitous in this enactment; they appear also in discussions of board diversity (¶ 60), executive remuneration (¶ 62-68). Drilling down to specific requirements, the technical criteria require, among other things, that significant institutions host board-level risk committees composed of independent directors (Art. 76 ¶ 3), which must have adequate access to information on the risk situation of the institution and to the risk management function and to external expert advice (id. ¶ 5). Further, the institutions must operate an executive-level risk operation headed by a senior officer who may report to the board or a board committee and who may not be summarily removed by other executives (id. ¶ 5),

Enhanced focus on risk and compliance is also manifest in the technical standards and rules developed by the European Banking Authority. The EBA is charged with responsibility to identify and analyze trends, potential risks and vulnerabilities stemming from the micro-prudential level with the aim of ensuring the orderly functioning and

---

29 Id. ¶57.
30 Id. ¶58.
integrity of financial markets and the stability of the financial system in the EU.\textsuperscript{31} The EBA publishes a semi-annual Risk Assessment Report\textsuperscript{32} and an associated risk dashboard which summarizes the main risks and vulnerabilities in the banking sector, focusing on key risk indicators among a sample of EU banks.\textsuperscript{33} The EBA also deals extensively with internal controls. Its High Level Principles of Risk Management, published in 2010, sets forth best practices for financial institutions in the risk management area.\textsuperscript{34} More recently, the EBA’s Guidelines on Internal Governance deal extensively with issues in risk management such as risk culture, alignment of remuneration with risk appetite, a risk management framework, board-level risk committees, and management-level risk control activities.\textsuperscript{35} The Guidelines also encourage banks to institute robust compliance functions, headed by “a person responsible for this function across the entire institution and group (the Compliance Officer or Head of Compliance).”\textsuperscript{36}

**Reasons for convergence**

Why has this remarkable degree of convergence occurred in the approach to risk management and compliance? The reasons are no doubt complex, but the following factors appear to have played a role:

1. Large banks are truly international in scope. To a substantial degree, all of these institutions face similar problems in coping with the challenges of surviving in the world financial market. Being similarly situated, it is perhaps not surprising that they

\textsuperscript{34} European Banking Authority, High-Level Principles of Risk Management
\textsuperscript{36} Id. ¶ 28.
have adopted similar coping strategies -- or that their regulators have encouraged them to do so.

2. Because of their international scope, large banks are subject to the authority of multiple regulators. This can create a ratchet effect in that the standards of risk management and compliance imposed by the most rigorous regulators are likely, as a practical matter, going to be adopted by the bank to govern its operations world-wide. It would not make sense for a bank to use one system in part of the world and another in a different part: because risk management and compliance today operate at the enterprise level, a strategy imposed by any country where the bank does substantial business is likely to become the norm for all others.

3. The financial crisis of 2007-2009 profoundly affected banks in both the United States and Europe. It is not surprising that banks on both sides of the Atlantic responded by greatly upgrading their risk management operations -- since it was obvious that failures in risk management had contributed substantial to the disaster of those years.

4. In part as a consequence of the financial crisis, bank regulators today communicate and cooperate with one another as never before. How one important country regulates risk management and compliance is likely, therefore, to exercise a substantial influence on how other countries do so, leading to the development of a high degree of consensus across regulators.

Conclusion

This paper has explored aspects of risk management and compliance in banks in the United States and Europe. I have attempted to demonstrate that the past few decades have witnessed a revolution in the treatment of risk characterized by a significant upgrade
in the importance of risk analysis at all levels of internal and external control and by the explicit incorporation of risk assessments in the structure of all control activities. This revolution has occurred on both sides of the Atlantic, and indeed throughout the world, and has generated a remarkable degree of convergence among different regulatory systems. Aspects of this revolution can be observed at the level of corporate governance with the growth of enterprise risk management, in internal and external audit, in the compliance function, and in regulatory supervision and examination. The convergence of practices and standards appears to be due to several factors: the inherently international scope of large bank operations; the ratchet effect under which the rules implemented by the country with the most demanding regulations are likely to be adopted by banks for all their operations worldwide; the shared impact of the financial crisis of 2007-2009; and the tendency of bank regulators to cooperate and consult across borders.