2 of 2 DOCUMENTS

The Banking Law Journal

2016 The Banking Law Journal
Volume 133, Number 1 The Banking Law Journal January 2016

2016-133-1 The Banking Law Journal § 1.01

§ 1.01 Enterprise Risk Management: Where is Legal and Compliance?

Thomas C. Baxter, Jr., and Won B. Chai n*

This article proposes a flexible approach to integrating the legal and compliance functions of an organization into its enterprise risk management framework. Existing guidance on the role of legal and compliance is often too rigid, leading to misallocation of responsibilities and duplicative efforts. In contrast, leveraging of past practice and existing expertise would help avoid common pitfalls in the implementation of a risk management framework and preserve unique benefits.

The recent financial crisis underscored the importance of effective risk management at banks, bank holding companies and other financial institutions. In 2008, Chairman Ben Bernanke noted that significant deficiencies in risk management had contributed to the crisis and concluded that "improvements in banks' risk management will provide a more-stable financial system by making firms more resilient to shocks." n1 This diagnosis echoed the observations of a 2008 report by the Senior Supervisors Group, an organization comprised of domestic and international regulatory authorities, which identified certain risk management practices that affected the ability of firms to withstand market turmoil. n2 The Financial Crisis Inquiry Commission, a bipartisan federal commission created to examine the causes of the financial crisis, made similar findings in 2011, declaring that "dramatic failures of corporate governance and risk management at many systemically important financial institutions were a key cause of this crisis." n3 These authorities, however, did more than simply reiterate the importance of risk management, which supervisors had been calling attention to long before the crisis started. n4 They identified specific individual practices that had either failed during the crisis or contributed to it.

Such precise observations foreshadowed more detailed guidance to come. Most notably, the Office of the Comptroller of the Currency ("OCC") in 2014 published its heightened standards for risk management, developed in direct response to the risk management failures the agency observed at covered institutions during the financial crisis. n5 Generally applicable to insured national banks and certain entities with over $50 billion in average total consolidated assets, these standards contain extensive risk management structure and practice requirements supplemented by compliance deadlines and documentation rules. The guidelines also list the responsibilities for each proposed line of defense--front line units that "own" risk; independent risk management that identifies, monitors and controls risk; and internal audit

that ensures compliance with regulatory guidelines and the appropriateness of overall risk management--to function within the broader risk management framework of the covered institution. n6

The OCC's commendable effort, however, can be supplemented with guidance on a more fundamental issue. The agency's guidelines list requirements for an effective, properly implemented risk management framework, but largely leave to firms the difficult task of integrating their existing functions into the framework being prescribed by regulators and other authorities. This omission can result in significant tension and uncertainty if a proposed rule is in conflict with current practice or if the implementation of an abstract recommendation is overly burdensome or costly. The OCC encountered this difficulty during the public comment phase for its heightened standards, when industry respondents challenged the agency's placement of Legal in the first line of defense and spurred the OCC to revise its position. n7

In particular, two functions--Legal and Compliance--present a unique conundrum for risk management because of their history and current role in many organizations. To overcome this challenge, supervisors and firms must rethink the interaction of Legal and Compliance with a risk management framework. The practical examples discussed below demonstrate the numerous subtleties underlying the appropriate treatment of these functions, and show that using an all-encompassing universal approach to integrating Legal and Compliance into an enterprise risk management framework may be suboptimal. Best practice in this area should not only follow the principle of flexibility, but actively be firm-specific and sensitive to the unique history and operations of the institution in question. Otherwise, the implementation of any best practices may fall prey to foundational flaws in the enterprise risk management framework.

THE SCOPE OF ENTERPRISE RISK MANAGEMENT

Enterprise risk management, as described by the Committee of Sponsoring Organizations of the Treadway Commission ("COSO"), is "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 its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives" (emphasis added). n8 This definition serves as a starting point for the creation of many risk management frameworks. Firms, however, need not interpret the phrase "across an enterprise" to require changes in every aspect of their operations. The purview of an enterprise risk management framework should not be conflated with what operations an organization must modify when implementing the framework.

Unfortunately, this distinction can be lost when an enterprise risk management framework is applied to an organization's Legal and Compliance functions. In such cases, firms often attempt to ensure that every function at an organization is covered in one way or another by the framework, such as by placement in a particular line of defense. Supervisors and other authorities can fall victim to the same tendency. As mentioned above, the OCC in its proposing release to the heightened standards placed Legal in the first line of defense, only to change course in response to adverse public comment and leave Legal outside the confines of any particular line. A recent white paper from COSO attempted to map the various principles from COSO's framework for internal control (incorporated by reference into its guidance on enterprise risk management) to the three lines of defense. n9 As part of this effort, the authors noted that typical second-line functions included expertise groups such as Legal and Compliance, in apparent contrast to the initial instincts of the OCC. n10 Such contradictions are significant because the placement of Legal and Compliance into one line of defense or another can directly impact the role these functions play in identifying and managing risk. Commenters on the OCC's heightened standards highlighted such concerns by noting that placement of Legal in the first line of defense might affect its independence, mischaracterize its risk ownership, and force non-lawyers to make legal decisions. n11

The pitfalls of forcing Legal and Compliance into a theoretical right place in an enterprise risk management framework also extend to the subject matter often associated with these functions. Definitions by supervisory authorities can serve as guideposts for thinking about the various types of risk, but can also present challenges for those implementing a risk

management framework without specialized expertise in the relevant topics. The Board of Governors of the Federal Reserve System ("Board") defines legal risk as the risk that "arises from the potential of unenforceable contracts, client lawsuits, or adverse judgments to disrupt or otherwise negatively affect the operations or condition of [an institution]." n12 Drawing upon a definition used by the Basel Committee on Banking Supervision, the Board characterizes compliance risk as "the risk of legal or regulatory sanctions, financial loss, or damage to reputation resulting from failure to comply with laws, regulations, rules, other regulatory requirements, or codes of conduct and other standards of self-regulatory organizations applicable to the [institution]." n13 Although these two definitions appear to focus on distinct concepts, closer scrutiny shows the categories are not mutually exclusive. A strategic breach of contract, for example, appears to implicate a legal risk associated with "the potential of unenforceable contracts" or "client lawsuits," but also seems similar to the "legal or ... financial loss" associated with compliance risk, especially if the breach in question involved a regulatory commitment, such as a provision in an acquisition agreement to use best efforts to obtain all required regulatory approvals. Furthermore, strategic breach could also probably result in reputational risk, which the Board defines as "the potential that negative publicity regarding an institution's business practices and clients, whether true or not, could cause a decline in the customer base, costly litigation, or revenue reductions." n14

Under these circumstances, attempts by an observer without specialized knowledge to parse out applicable risks will be vulnerable to misidentification and the pitfalls associated with incorrect risk assessments, such as misallocated resources. At the same time, the risks discussed above present unique issues because they are often paired with immediate repercussions or irreversible effects, such as statutes of limitation or regulatory deadlines. Failures in risk assessment for these risks can also create knock-on effects, such as collateral consequences associated with a statutory or regulatory violation. Yet the approach of identifying legal or compliance risk in every event would render the definition of such risks meaningless, which ultimately leaves managers implementing risk management frameworks with the unenviable challenge of delineating *a priori* the scope of legal, compliance and related risks which are inherently difficult to identify.

CASE STUDIES

These uncertainties about the role of Legal and Compliance and their associated risks become even more apparent in several applied examples. First, consider a case in which Compliance, in close coordination with a firm's technology function, develops a program that prevents transfer of funds to certain specially designated persons. The program, however, has a serious flaw that fails to sequester multiple funds transfers effected in violation of an economic sanctions regulation. As an initial matter, the transfers would have occurred as part of a firm's day-to-day operations, and hence appear to fall under operational risk, which the Board describes as arising from "the potential that inadequate information systems, operational problems, breaches in internal controls, fraud, or unforeseen catastrophes will result in unexpected losses." n15 There are, however, alternative ways to characterize the risk event. Rather than just operational risk, the regulatory sanctions that will follow the inappropriate transfers seem like a compliance risk. At the same time, the negative publicity associated with revelations of these transfers to sanctioned entities carries an aspect of reputational risk. Furthermore, for some firms, such as those already under a deferred prosecution agreement, the follow-on sanctions and regulatory consequences associated with the subject transfers might be the most significant and damaging to the business. For others, such as those in which industry confidence and public trust are vital to continuing operations, the reputational harm might be the most worrying. The "right" assessment with respect to the type of risk, even if the fact pattern stays the same across firms, is not clear.

This categorization dilemma extends to the roles of the functions involved. On the one hand, Compliance's direct involvement in the development of the program seems to make it similar to a front line unit. If Compliance, on the other hand, only oversaw the technology function's development of the program by providing information on the current state of rules, it seems to be acting in an expertise and oversight capacity, which would traditionally be associated with the second line of defense. One possible response to this quandary, similar to the one used by the OCC when queried about the position of Compliance by public comments, n16 is to note that Compliance can have roles in multiple lines of

defense based on the particular facts and circumstances of its activities. This solution, however, provides little guidance to a firm tasked with responding to a particular situation. It superficially solves the issue of categorizing the risk and the place of Compliance (by saying it is everywhere), but does not give guidance on how to operationally address the issue at hand, as manifested under a particular set of circumstances at a specific firm.

An alternative approach is to avoid forcing Compliance, as a general matter, into a particular line of defense (or all lines of defense) and permit each organization to use a risk management framework that accommodates (rather than replaces) the way in which the Compliance function and its associated risks currently fit into the organization. Mandating that Compliance be uprooted and transplanted into a pre-determined spot within a three lines of defense model, or asserting that it be divided and individual pieces placed in all three lines, seems needlessly rigid. As demonstrated by the public comment to the OCC's heightened standards, in which "[s]everal commenters ... expressed varying views on whether compliance should be considered a front line unit, independent risk management, internal audit, or a different organizational unit," n17 different organizations can reach different reasonable conclusions, and risk management frameworks should be flexible enough to incorporate such variations. A way to visualize this approach is to consider the risk management framework as something that will be laid over the organization as it exists. Compliance will not, under this view, need to fit within a particular place in the framework; instead, the framework lies on top of the organization and Compliance lies beneath.

The same principle applies to Legal and its role in the risk management framework. Imagine that a financial institution is selling credit default swaps and, in response to customer demand, the executive selling the swaps asks Legal to include a provision entitling counterparties to receive cash collateral if the issuer of the credit default swaps is downgraded. The role of Legal in this scenario again seems to implicate multiple types of risk, and variations on the hypothetical--such as having an external counsel draft the provision in question or having the executive draft the provision himself--throw into relief the different methods by which a rational enterprise risk management framework could approach the issue. Most notably, the example highlights how Legal is *sui generis*, not only by virtue of its existing unique responsibilities but also because the lawyer is subject to a historical professional code of conduct.

For instance, suppose that independent risk management--the second line of defense--becomes aware of the cash collateral provision in the contracts and challenges the business owner about the provision's propriety. Suppose further that risk management asks Legal to explain how the provision works, and that a fair explanation would show just how risky these instruments can be. Could the business owner block Legal from assisting risk management, based on a theory that the lawyers did this work for the business? The simple answer is "no." Although Legal worked for the executive in drafting the provision, Legal performed this task in support of the business area that is marketing the credit default swaps. The business area owns the risk of the swaps, and the business area is the first line of defense. Legal, in contrast, represents the organization as a whole, not an individual constituent thereof. Moreover, every lawyer is bound by a standard of professional judgment independence that stands apart from any mandates associated with an enterprise risk management framework. Under these circumstances, simplifying the role of Legal to fit into a particular line of defense--such as declaring that it is a front line unit because it acted as an agent of the executive requesting the provision--is detrimental to the overall risk management enterprise. Doing so would replace principles of corporate representation and professional independence--which benefit from a lengthy statutory, judicial and self-regulatory history--with the potentially untested dictates of a newly developed risk management framework.

The example above also illustrates one of the unique features of Legal within a corporate organization. In drafting the language of the credit default swap, Legal was taking direction from the business area (the first line of defense) and performed a key support service for that area. When the independent risk management function contacted Legal and asked it to explain how the cash collateral feature of the credit default swaps actually worked, Legal was assisting the second line of defense in carrying out its challenge function. If queried about the provision by any other corporate constituencies, Legal will again likely lead discussion of the language it helped to draft. In this way, Legal often performs different and varied functions as a general resource for an entire organization and potentially all three lines of defense. Such a utility function reinforces the rationale for allowing Legal to operate outside the confines of any

particular line of defense--it needs to have the flexibility to move around, and business units may rely upon the existence of that flexibility in their own operations.

These considerations become even more apparent when Legal is directly involved in the management of a risk affecting the firm. Imagine, for example, that the company is faced with a "bet-the-company" lawsuit that could result in crippling damages. Most firms in such circumstances will retain outside law firms to act as counsel in the litigation. In such cases, Legal's oversight of outside counsel's day-to-day management of the litigation, in which Legal requests status updates, makes estimates of potential damages, and monitors aggregate potential effects on the firm, appear to give it challenge responsibilities typically associated with the second line of defense. At the same time, the strategic consultations between the firm's outside counsel and Legal, which are required by a lawyer's professional code of conduct, n18 would give Legal responsibilities--such as determining the permissibility of settlement; the aggressiveness of a filed motion; or the appropriateness of adding litigation resources--that could directly affect the nature and extent of the risk involved. Lastly, Legal will have its own direct reporting responsibilities to the board of directors and other officers of the firm, which may ask about the details of the strategy selected, the sufficiency of risk management for the particular litigation, and any other matters of interest relating to the case. In a three lines of defense model, which operates in part on the concept of checks and balances across each of the lines, a function that participates in the creation of a risk, manages that risk for the organization, and reports on the status of both the risk and its management to the board of directors and other officers, seems inconsistent with the basic architecture. For a function that acts as a general utility for the firm and performs its responsibilities with the benefit of professional conduct rules tailored for such difficult balancing, however, the task is both natural and familiar.

For the next example, imagine if a financial institution proposes to alter marketing materials for one of its financial products to decrease the appearance of risk in the product, such as by using an illegible font for a key disclosure or including a potentially misleading chart. These inappropriate actions carry with them a significant reputational risk if such deceit is discovered and publicized. On its face, this scenario does not involve any direct actions by Legal or Compliance, but the nature of the proposal would likely prompt a firm to consult these functions anyway. The General Counsel and Chief Compliance Officer are often best-placed to respond as voices of caution and as sources of conscience for the firm. n19 Furthermore, executives at the firm are likely to undertake such consultations as a matter of habit and past practice. Under these circumstances, these salutary communications should not be stifled by the iron cage of an enterprise risk management system that limits the purview of Legal or Compliance to a specific line of defense or a closed universe of narrowly tailored responsibilities. Both Legal and Compliance have developed significant expertise in their history of being consulted in such gray situations, and a risk management system should not inhibit these roles in the name of structural purity.

Lastly, consider a case in which Legal and Compliance professionals through their regular interactions with business units become aware of a senior manager that regularly instructs his employees to "do what whatever it takes" to meet project goals, rates the performance of his subordinates based solely on their revenue generation capability, and constantly cajoles his employees to think of ways to "make the system work for them." Supervisors after the financial crisis have increasingly focused on the necessity of a strong ethical culture as a prophylactic against financial crime (as well as formal enforcement actions and other punitive measures). n20 Here, the senior manager is most likely not yet in breach of any legal or regulatory requirements, and may not even be in violation of any of the firm's policies. For purposes of the risk management framework, it is also unclear what, if any, risk currently exists. The supervisor's behavior may encourage an employee to collude with colleagues at other banks, lead to employee dissatisfaction and retention problems, or possibly persist with no discernible effect. Yet an observer is unlikely to consider continuation of such behavior acceptable, and the dictates of a risk management framework should not hinder potential informal efforts to resolve the situation. In this case, providing flexibility to Legal and Compliance not only permits these functions to work more effectively for the risk management enterprise, but also fills potential gaps that a framework may otherwise leave unaddressed. From a cost/benefit perspective, the machinery associated with documented risk identification, measurement, re-assessment and follow-up may not be necessary or appropriate for all cases, and the risk management framework should permit Legal and Compliance--which are two functions with natural access to information and

expertise in providing guidance to business units--to proactively identify and correct potential problems that the framework may overlook or wait to address.

THE "LAY OVER" APPROACH

Firms should look at an enterprise risk management framework for what it is--a framework for developing a discipline that enables the identification, monitoring, and management of risks with effective accountability. This framework can be taken and laid over the organization as it already exists. In an existing organization, pursuant to historical and tested practice, compliance professionals and lawyers will already be working alongside other risk professionals, and the effective operation of their current state should not be disrupted for the sake of the new, especially when doing so entails notable drawbacks.

The prior examples demonstrate that attempts to force Legal and Compliance to fit the confines of a new framework can result in confusion of responsibilities, loss of existing expertise by Legal and Compliance, and unnecessary changes in a firm's internal procedures. In practice, Legal and Compliance already know well the scope of their responsibilities, are experts in their respective fields, and have established methods of communication and collaboration within a firm. These advantages should support the introduction of a risk management framework, not be supplanted by it.

As a case in point, in 2008 the Federal Reserve Bank of New York created a new independent risk management function led by a Chief Risk Officer. This risk function, however, neither displaced the Compliance function that had existed since 2005 nor did it supplant the Legal function that had existed since the Bank opened approximately 100 years ago. The risk management framework was laid over the pre-existing legal and compliance functionality, integrating the expertise and responsibilities that they had already developed, to facilitate a harmonious operation of the whole. Expectations for enterprise risk management should not only permit such flexibility, but actively embrace it as a guiding principle. At no point in the Bank's restructuring did anyone suggest that the Office of General Counsel should be moved to the second line of defense and should report up to the Chief Risk Officer. Similarly, the Chief Ethics and Compliance Officer of the Bank continued to report up to the General Counsel. A long history of collaboration between Legal and Compliance had already cultivated and strengthened compliance risk management within the organization. Consequently, there was no burning platform to move the Chief Ethics and Compliance Officer to the second line of defense, or to have the Chief Ethics and Compliance Officer report to the Chief Risk Officer.

One concern associated with permitting Legal and Compliance to remain independent of any line of defense is that these functions might currently be malfunctioning in some way that prevents their harmonious integration with a new risk management framework. Such a criticism, however, argues in favor of rehabilitating these individual functions to meet current expectations, and would not justify their wholesale restructuring. If Legal and Compliance at a firm create problems when being integrated into an enterprise risk management framework, the solution is to fix those problems, rather than to change the way these functions fit within the structure. This would be the classic "rearrange the deck chairs on the Titanic" approach.

For example, an organization where Compliance reports to the General Counsel might try to move Compliance so that, going forward, it reports to the Chief Risk Officer. Often, the justification for such a move is a perception that the General Counsel lacks "independence," and will likely act as an advocate of the business owner. If the General Counsel, however, is in fact acting as an advocate of the business owner, then the General Counsel has failed to live up to the General Counsel's ethical duty, which is to represent the organization. n21 The solution should be to replace the General Counsel rather than move the Compliance function. This simple scenario reveals the diagnostic value of the integration exercise. By forcing a firm to scrutinize the functions that Legal and Compliance currently perform, and thoughtfully consider how those functions support or detract from the proposed risk management exercise, a firm can identify current weaknesses, such as underlying staffing or cultural problems, that might otherwise not come to light if one set of responsibilities is simply swapped out for another without any consideration of existing duties and performance.

Another possible concern is that giving Legal and Compliance flexibility in the risk management framework would inappropriately empower these groups at the cost of other functions. Firm-specific flexibility, however, does not mandate increased authority or discretion for Legal and Compliance. For example, although traditionally associated with the third line of defense, Internal Audit at some institutions may have de facto responsibilities across (and outside of) all three lines of defense in a manner similar to that of Legal and Compliance. n22 Internal Audit instead of Compliance may oversee or propose the development of technology programs--such as systems used to monitor internal firm processes--or Internal Audit at some organizations may act as the corporate conscience and resolve day-to-day matters. Under these circumstances, forcing Legal and Compliance to take on expanded new responsibilities may be just as disruptive to the organization as inappropriately limiting them to a particular line of defense. The proposed approach is to permit an enterprise risk management framework to be organization-specific with respect to Legal and Compliance. The guiding principle is effectiveness based on unique past experience, regardless whether such an approach results in expanded or contracted responsibilities for any particular unit within the firm.

The proposal for flexibility does come with certain costs. In the beginning, it may be more costly for a firm to survey its existing functions and incorporate their expertise into a risk management framework rather than simply assign responsibilities from the ground up. In particular, firms will have the challenging task of harmoniously integrating a risk management framework with Legal and Compliance, which by their nature have multi-faceted duties and complex risk management responsibilities. The diagnostic value of such a survey, the ability to benefit from past experience, and the other advantages of flexibility in risk management, however, would justify the cost at most firms. Similar to a problem in ethical culture, a seemingly minor gap or limitation in a risk management framework could one day result in significant future repercussions, and discovering potential problems early in the framework's development would be preferable to discovering them during a crisis.

An enterprise risk management framework does not need to comprehensively re-tool all risks and functions within an organization. It does not need to fix what is not broken. Some functions--such as Legal and Compliance--may have achieved efficient handling of their responsibilities, and the framework (as well as any guidance to implementing it) should not require that this status quo be upset. At the same time, the enterprise risk management framework should not operate as a wall that prevents functions that are not directly modified by it from contributing to the overall risk management effort. Legal and Compliance may be *sui generis*, but their responsibilities have important synergies with the duties associated with the three lines of defense and other parts of an enterprise risk management framework. Ultimately, the final form of the framework should reflect organization-specific characteristics, and there may be good reason to restructure Legal and Compliance at certain firms. Some authorities have caveated their standardized recommendations with a principle of flexibility. n23 More than just an outlet for permitting exceptions, however, this concept of organization-specific flexibility should be actively recommended for at least the Legal and Compliance functions. Every organization is unique, and so is the role played in each by the General Counsel and Chief Compliance Officer. These officers have already integrated themselves into the organization's risk management, whether or not a formal risk management framework is in place. Given that the risk management framework is a relatively new innovation, and given that Legal and Compliance are very well established in most financial institutions, it is logical to make the most of what is already there and not to be disruptive.

Return to Text

FOOTNOTES:

(n1)Footnote *.

Thomas C. Baxter, Jr. is general counsel and executive vice president and Won B. Chai is an attorney for the Federal Reserve Bank of New York. The views expressed here are solely those of the authors and are not necessarily shared by the Federal Reserve Bank of New York or any other component of the Federal Reserve System. The authors may be contacted at thomas.baxter@ny.frb.org and won.chai@ny.frb.org, respectively.

(n2)Footnote 1. Ben S. Bernanke, Chairman, Bd. of Governors of the Fed. Reserve Sys., Risk Management in Financial Institutions, Remarks at the Federal Reserve Bank of Chicago's Annual Conference on Bank Structure and Competition, Chicago, Illinois (May 15, 2008).

(n3)Footnote 2. Senior Supervisors Group, Observations on Risk Management Practices during the Recent Market Turbulence (2008), https://www.sec.gov/news/press/2008/report030608.pdf. *See also* Senior Supervisors Group, Risk Management Lessons from the Global Banking Crisis of 2008 (2009), https://www.sec.gov/news/press/2009/report102109.pdf.

(n4)Footnote 3. Financial Crisis Inquiry Commission, The Financial Crisis Inquiry Report (2011), http://fcic-static.law.stanford.edu/cdn_media/fcic-reports/fcic_final_report_full.pdf.

(n5)Footnote 4. *See, e.g.*, Board of Governors of the Federal Reserve System, SR 97-24 (SUP), Risk-Focused Framework for Supervision of Large Complex Institutions (1997).

(n6)Footnote 5. 12 C.F.R. Part 30 (Appendix D) (2015).

(n7)Footnote 6. This "three lines of defense" framework has also been codified in guidance issued by organizations such as the Institute of Internal Auditors. The Inst. of Internal Auditors, The Three Lines of Defense in Effective Risk Management and Control (2013), http://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%2

(n8)Footnote 7. Department of the Treasury, Office of the Comptroller of the Currency, OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches; Integration of Regulations; Final Rule, 79 Fed. Reg. 54518, 54525 (Sept. 2014) .

(n9)Footnote 8. Committee of Sponsoring Organizations of the Treadway Commission, Enterprise Risk Management--Integrated Framework: Executive Summary (2004), http://www.coso.org/ERM-IntegratedFramework.htm.

(n10)Footnote 9. Douglas J. Anderson & Gina Eubanks, Leveraging COSO Across the Three Lines of Defense (2015), http://www.coso.org/documents/COSO-2015-3LOD-PDF.pdf.

(n11)Footnote 10. *Id.* at 6.

(n12)Footnote 11. Department of the Treasury, Office of the Comptroller of the Currency, OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches; Integration of Regulations; Final Rule, 79 Fed. Reg. 54518, 54524 (Sept. 2014) .

(n13)Footnote 12. Board of Governors of the Federal Reserve System, Bank Holding Company Supervision Manual, Sec. 2010.11.2.2, (2015), http://www.federalreserve.gov/boarddocs/supmanual/bhc/bhc.pdf.

(n14)Footnote 13. *Id.* at Sec. 2124.07.

(n15)Footnote 14. *Id.* at Sec. 2010.11.2.2.

(n16)Footnote 15. *Id.*

(n17)Footnote 16. Department of the Treasury, Office of the Comptroller of the Currency, OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches; Integration of Regulations; Final Rule, 79 Fed. Reg. 54518, 54529 (Sept. 2014) .

(n18)Footnote 17. *Id.*

(n19)Footnote 18. American Bar Ass'n, Model Rules of Professional Conduct, Rule 1.4, (2013) ("A lawyer shall ... reasonably consult with the client about the means by which the client's objectives are to be accomplished.").

(n20)Footnote 19. Ben W. Heineman, Jr., General Counsel are One Conscience of the Company (2013), http://www.law.harvard.edu/programs/corp_gov/articles/Heineman_CorpCon_01-24-13.pdf. *See also* Ben W. Heineman, Jr., The General Counsel as Lawyer-Statesman (2010), https://clp.law.harvard.edu/assets/General_Counsel_as_Lawyer-Statesman.pdf ("The essence of being a lawyer-statesman is to move beyond the first question--'is it legal?'--to the ultimate question--'is it right?' ").

(n21)Footnote 20. *See, e.g.*, Thomas C. Baxter, Jr., Exec. Vice Pres. and Gen. Counsel, The Rewards of an Ethical Culture, Remarks at the Bank of England, London (Jan. 20, 2015).

(n22)Footnote 21. American Bar Ass'n, Model Rules of Professional Conduct, Rule 1.13, (2013) ("A lawyer employed or retained by an organization represents the organization ... .").

(n23)Footnote 22. The Inst. of Internal Auditors, The Role of Internal Auditing in Enterprise-wide Risk Management (2009), http://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Role%20of%20Internal%20Auditing%20in%20Enterprise

(n24)Footnote 23. *See, e.g.*, Douglas J. Anderson & Gina Eubanks, Leveraging COSO Across the Three Lines of Defense (2015), http://www.coso.org/documents/COSO-2015-3LOD-PDF.pdf ("Because every organization is unique, organizations may have sound reasons for defining roles and responsibilities differently.").