THE EVOLVING ROLE OF COMPLIANCE

MARCH 2013

The Evolving Role of Compliance

I. The Enhanced Prominence of Compliance

A. Introduction

In 2005, the Securities Industry Association issued a White Paper on the Role of Compliance that provided an extensive account of the role that the Compliance Department plays in support of securities firms' efforts to develop and maintain an effective overall compliance program.[1] Because Compliance is historically a creature of evolution rather than prescriptive legislative or regulatory requirements,[2] the Compliance function continues to develop over time in response to changes in market operations, business practices and new regulatory mandates.

Since the publication of the 2005 White Paper, the securities industry has experienced change unmatched in the recent history of financial services. The 2008 financial crisis has been the catalyst to much of this transformation. For instance, in the United States, lawmakers and regulators have realigned or expanded their authority over many aspects of the financial industry, and extensive new rulemaking will continue to alter or limit business activities. Substantial changes also have been triggered by the natural evolution of the securities business, such as the globalization of business activities, the reshaping of business support through outsourcing and off-shoring, and the rapid adoption of new technology in the form of trading, communications and other systems. The confluence of business evolution and the consequences of the financial crisis have led to additional developments, including the adoption of more standards and rules of cross-border and extraterritorial applicability and an increased focus on cost discipline.

These changes to the context in which Compliance operates tell only part of the story of the increasingly complex world that the Compliance officer inhabits. The Compliance officer role itself has moved to center stage. As one Securities and Exchange Commission ("SEC") official explained, the financial crisis revealed "the need for stronger independence, standing and authority among a firm's internal risk management, control and compliance functions."[3] Most prominent among legislative initiatives, the Dodd-Frank Wall Street Reform and Consumer Protection Act (the "Dodd-Frank Act") addresses these concerns by assigning significantly increased responsibilities to Compliance and by requiring closer involvement of Compliance with day-to-day business operations and decisions.[4]

---

[1] This White Paper refers generally to the "securities industry" or "industry," and to "securities firms" or "firms." We use these terms to refer to the securities, investment banking, brokerage and related fields. A copy of the Securities Industry Association, *White Paper on the Role of Compliance* (Oct. 2005) ("2005 White Paper"), is attached as Appendix A. The Securities Industry Association was the predecessor entity to the Securities Industry and Financial Markets Association ("SIFMA").

[2] *See generally*, O. Ray Vass, *The Compliance Officer in Today's Regulatory Environment*, Practicing Law Institute: Corporate Law and Practice Course Handbook Series, Broker-Dealer Institute, 49, 55 (Nov. 12, 1987) [hereinafter Vass, *The Compliance Officer*].

[3] Carlo V. di Florio, Director, Office of Compliance Inspections and Examinations ("OCIE"), U.S. Securities and Exchange Commission, Remarks at the Compliance Outreach Program (Jan. 31, 2012).

[4] Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, H.R. 4173, 124 Stat. 1376 (July 21, 2010) [hereinafter Dodd-Frank Act]. *See also* European Securities and Markets Authority

In addition to these new developments, important issues identified in the 2005 White Paper still exist today: the multiple and at times inconsistent responsibilities of Compliance, which have since expanded; the relationship and increased interdependence of Compliance with other control functions; and the related yet distinct roles of management and Compliance. This last issue has become more complicated by rulemaking and recent enforcement actions that focus on Compliance and its role.

This White Paper discusses the evolving role of the Compliance function in securities firms in light of these changes and explores the challenges that firms and their Compliance professionals currently face on a daily basis. This White Paper also offers recommendations to assist senior management, regulators and Compliance itself in defining the appropriate role of Compliance in an increasingly complex and variable environment. In that regard, we believe that the interests of senior management, regulators and Compliance should be balanced, so that Compliance is sufficiently resourced and independent. We also encourage Compliance to foster strong relationships and open lines of communication with business managers so issues are properly escalated and addressed, and with regulators so that the development of rules, regulations and regulatory examination programs has the benefit of meaningful Compliance input. Ultimately, we believe the Compliance function will be most effective and its role in firms will be the strongest when senior management, regulators and Compliance collectively define a role for Compliance that is appropriate given the realities of the securities industry and the operation of Compliance.

B. New Expectations and Demands on Compliance and Compliance Officers

Compliance in securities firms is an independent control function that provides advice, training and education regarding financial services regulation to business units and senior management, and that undertakes to monitor and review business activities with respect to such regulation. Compliance protects firms by partnering with other control functions and working with management to ensure that potential regulatory risks and liabilities are identified, escalated and appropriately addressed. In providing these services, a strong Compliance function is critical to sound business practices and a firm's ability to instill a culture of compliance.

The quickly shifting business and regulatory landscape today requires Compliance to evolve at an accelerated pace. For instance, Compliance traditionally focused on the industry and regulatory goals of assuring customer protection and fair treatment as well as enhancing market integrity. However, the 2008 crisis elevated concerns about risk, especially systemic,

---

("ESMA"), *Guidelines on Certain Aspects of the MiFID Compliance Function Requirements (Final Report)* (July 2012) (providing guidelines for creating compliance policies and procedures, and for effectively monitoring and testing compliance programs); International Organization of Securities Commissions ("IOSCO"), *Objectives and Principles of Securities Regulation*, at 11 (June 2010) ("Market intermediaries should be required to establish an internal function that delivers compliance with standards for internal organization and operational conduct, *with the aim of protecting the interests of clients and their assets and ensuring proper management of risk*, through which management of the intermediary accepts primary responsibility for these matters.") (emphasis added).

financial and other risks, to a new prominence,[5] and Compliance officers have begun to adapt to this change in regulatory priorities. In that regard, Compliance has had to develop new subject matter expertise and skill sets that are quite different from those needed to address issues relating to customers and markets. Even in the more traditional areas of Compliance focus, the emergence of new technology and global business models – to name just two developments – have dramatically changed business operations, the services and products available to customers, and the very manner in which firms interact with their customers. While these developments create new opportunities and efficiencies in the markets, they also have exposed firms to new vulnerabilities and risks and highlighted the need for Compliance to have the expertise, understanding, skill and resources to identify, escalate and appropriately address these risks.[6]

C. Compliance, Management and Regulators—New and Continuing Challenges

The interactions between Compliance and senior management and between Compliance and regulators illustrate the complex responsibilities of Compliance in maintaining an independent and effective role in firms. Senior management has always been, and remains, responsible for setting a "tone at the top"[7] demonstrating that compliance is to be taken seriously and that all employees must play an active role in sustaining a "culture of compliance" in a firm.[8] In that regard, senior management is responsible for creating and defining a sufficiently

---

[5] With financial and other oversight responsibility over securities firms, securities regulators have always had an interest in the risk profile of individual firms. Regulators exercise such oversight through various mechanisms, such as the formulation and enforcement of net capital and customer protection requirements, and Compliance often has advisory and related responsibilities in these areas.

[6] At an event for chief compliance officers during which he discussed the present and future importance of Compliance, SEC Chairman Christopher Cox emphasized the responsibility of senior management to identify and address the needs of Compliance, including the need to staff Compliance functions appropriately:

> Now more than ever, companies need to take a long-term view on compliance and realize that their fiduciary responsibility requires a constant commitment to investors. That means sustaining their support for compliance during this market turmoil, and beyond it as well.
>
> Today, when the future is uncertain, when markets are unstable, when investor confidence is shaken, this is the time – more than ever – when we need a powerful voice for compliance.

Christopher Cox, Chairman, U.S. Securities and Exchange Commission, Address to the 2008 CCOutreach National Seminar (Nov. 13, 2008).

[7] Carlo V. di Florio, Director, OCIE, U.S. Securities and Exchange Commission, Speech at Private Equity International's Private Fund Compliance (May 3, 2011) ("But beyond just implementing good policies and procedures, our examiners assess the culture of the firms that they examine, beginning with whether management is setting a tone at the top of the organization that fiduciary and regulatory obligations are to be taken very seriously. We are interested in seeing that senior management and boards (where a board structure exists) are engaged and taking responsibility for oversight, of compliance and of risk management generally.").

[8] *See* Stephen M. Cutler, Director, Division of Enforcement, U.S. Securities and Exchange Commission, Speech at Second Annual General Counsel Roundtable: Tone at the Top: Getting it Right (Dec. 3, 2004) ("[I]f CEOs were themselves breaking the law, then they couldn't have been setting a particularly melodious tone [at the top]. . . . Violations of the securities laws are very frequently the product of both individual failings and a deficient corporate culture.").

resourced Compliance function to assist the firm in complying with applicable laws, rules and regulations.[9]

For sound reasons, Compliance traditionally has acted as an advisory and control function that does not have supervisory authority over business functions. Balanced, impartial advice is more likely to come from Compliance professionals who are not business supervisors and who do not have a direct financial stake in business decisions. Compliance advises business units and senior management regarding a firm's regulatory obligations and the firm's compliance program. Compliance also exercises its control function through various monitoring and testing activities. Compliance must find a way to build a relationship of trust with the business while remaining independent and capable of executing the control aspects of its role.[10] Extensive new regulations coupled with budgetary constraints mean that many firms have asked Compliance to assume greater responsibilities and to be more actively involved in advising business activities with limited resources. Thus, with individuals taking on more responsibilities and in combined roles, Compliance's ability to maintain both trust in its advisory capacity and independence in its control capacity remains a challenging objective for firms and the industry as a whole.[11]

A new influence on the business-Compliance relationship comes from the regulators whose expectations also shape the manner in which Compliance professionals perform their daily functions. While Compliance has always sought to maintain a constructive and open relationship with regulators, new regulations, such as those requiring self-reporting or certifications, place increased pressure on Compliance.[12] Such expectations further challenge the ability of Compliance to be an effective advisor to business personnel and can discourage business personnel from using Compliance in its advisory capacity. New regulations requiring Compliance to be more actively involved in a broader set of business activities also create the risk, as illustrated by recent enforcement actions, that regulators will hold Compliance

---

9 *See* National Association of Securities Dealers ("NASD") Rules 3010 ("Supervision") and 3012 ("Supervisory Control System"). NASD was the predecessor entity to the Financial Industry Regulatory Authority ("FINRA").

10 Vass, *The Compliance Officer*, *supra* note 2, at 58.

11 The integration of Compliance's advisory and control roles has significant advantages. For instance, the control function benefits from an understanding of the business that is best obtained from and through the lens of a regulatory-sensitive advisor, and the advisory function becomes more refined by having an unfiltered understanding of how things can and have gone wrong.

12 New requirements from the Commodity Futures Trading Commission ("CFTC") require the Chief Compliance Officers ("CCOs") of certain entities to certify, under penalty of law, that compliance reports are accurate and complete. *See infra* note 44 and accompanying text (discussing the CFTC CCO certification process). Additionally, FINRA Rule 4530 now requires firms to report certain internal findings of wrongdoing where the firm "concluded or reasonably should have concluded" that a violation of applicable laws, rules, regulations or standards of conduct may have occurred. *See infra* note 81 and accompanying text (discussing FINRA Rule 4530).

accountable for supervisory failures in the business units that Compliance advises.[13] That risk may in turn hinder a firm's ability to develop a clearly defined, knowledgeable, integrated and robust Compliance function.[14]

Compliance's relationships with senior management and with regulators may involve competing or conflicting expectations, and this also may have the effect of unnecessarily constraining Compliance's contribution to a firm's regulatory compliance efforts. For instance, regulators, and prosecutors,[15] appropriately see Compliance as an important control function that can help identify, escalate and report wrongdoing if it does occur. At the same time, Compliance's strongest contribution may be to help the business shape appropriate standards and adopt practices that promote the right behaviors from the very start. To do so, Compliance must be structured in a way that encourages senior management to seek out Compliance as an advisory resource. This, in turn, encourages Compliance to look for affirmative opportunities to influence outcomes and provide responsible advice, while retaining and executing its crucial control function. A well-informed and engaged Compliance function that is involved in these multiple ways ultimately benefits firms, their customers and the industry as a whole.

Acknowledging Compliance's various opportunities to contribute to a firm's regulatory compliance efforts and achieving a greater consensus on the extent and limits of Compliance's responsibilities are crucial to minimizing differences in expectations and allowing Compliance to act without undue uncertainty as to its own obligations. This White Paper will now examine those roles and responsibilities and some of the challenging issues that arise in defining and assessing them.

---

[13] *See supra* note 11 and accompanying text (discussing new requirements that have the effect of causing Compliance to become more closely involved in business activities). Separately, two recent enforcement cases illustrate the potential liability of Compliance officers. In one case, the CCO of a registered broker-dealer settled charges for failure to supervise where the SEC staff alleged that, had the CCO followed firm procedures and reviewed customer accounts and correspondence, he "likely would have prevented and detected [] violations of the securities laws" and cured red flags related to unauthorized trading in customer accounts. *In re Manuel Lopez-Tarre*, Exchange Act Release No. 65391, Admin. Proc. File No. 3-14562 (Sept. 23, 2011). In a separate matter, a Compliance employee, who was not the CCO or an officer of similar capacity, was tasked with establishing a firm's policies and procedures for its capital markets practice. Although senior management is ultimately responsible for enforcing a supervisory system, the employee was nonetheless penalized for failure to supervise because she allegedly failed to establish, maintain and enforce a supervisory system that was reasonably designed to satisfy Regulation SHO. *Susan Margaret Labant*, Letter of Acceptance, Waiver and Consent, FINRA No. 2008013127802 (Aug. 19, 2011).

[14] Daniel M. Gallagher, Commissioner, U.S. Securities and Exchange Commission, Remarks at "The SEC Speaks in 2012" (Feb. 24, 2012) ("Deterring such engagement is contrary to the regulatory objectives of the Commission, and I am concerned that continuing uncertainty as to the contours of supervisory liability for legal and compliance personnel will have a chilling effect on the willingness of such personnel to provide the level of engagement that firms need—and that the Commission wants. In resolving this uncertainty, we should strive to avoid attacking or penalizing the willingness of compliance and legal personnel to be fully involved in firms' responses to problematic actors or acts.")

[15] *See, e.g.,* U.S. SENTENCING GUIDELINES MANUAL § 8B2.1 (2011) (outlining the basic requirements of compliance and ethics programs designed to remedy harm from criminal conduct).

II. Defining the Role of Compliance

A. Generally Defining Compliance and Allocating Responsibilities

The duties of Compliance must be clearly defined and distinguished from duties of the business as well as those of other risk and control functions. The scope of duties may differ to a degree from firm to firm and even within a firm, where they may align differently for distinct business lines, products or services, and reflect different legal entity structures and global geographic considerations; but in any event, the duties should be clearly stated.[16] In allocating duties, firms must protect Compliance's independence in order to mitigate conflicts of interest and exposure to potential liability. For instance, Compliance's advice should not be subject to the approval of senior management, Compliance personnel should be solely responsible for accomplishing Compliance-oriented tasks, rather than requiring such tasks to be performed in tandem with business personnel, and Compliance should have sufficient tools and expertise (including, as necessary, technology or business experts) to fulfill its responsibilities.

B. Coordination with Business Units and Control Groups

As discussed above, the role of Compliance as an advisor to the business on regulatory compliance risks brings business, Compliance and other control functions together. This can create the possibility for misunderstanding, both inside and outside the firm, of the advisory role because Compliance is typically aligned with business units to advise on the regulatory aspects of business activities and decisions, and with other control groups to assist in risk monitoring and governance.

1. Coordination with Business and Firm Committees

In the framework of risk governance, senior management plays the primary role with coordinated support from Compliance and other control and support functions.[17] Although Compliance professionals should neither exercise final decision-making authority on business issues nor engage in supervisory activities, coordination and engagement with business units and

---

[16] For this purpose, firms should seriously consider adopting a mission statement that describes the overall goals of Compliance and the means by which the goals will be achieved. While Compliance mission statements ordinarily are not extremely detailed, they give a clear and broad picture of Compliance's goals (*e.g.*, "working with business and other control functions to reflect the firm's values and to remain compliant with applicable laws, rules and regulations") and the primary means used to achieve those goals (*e.g.*, "by providing advice, training and monitoring with respect to financial services regulation to business units and senior management"). Mission statements can be an effective tool to set out the standards and expectations to which Compliance can be held accountable.

[17] In a commonly applied framework of risk governance, there are three "critical lines of defense": (i) the business and senior management, which manage and supervise risk; (ii) Compliance and other support functions (*i.e.*, Ethics and Risk), which implement programs to monitor, test and escalate risks; and (iii) Internal Audit, which provides independent verification and assures that effective controls are in place. *See, e.g.*, Carlo V. di Florio, Director, OCIE, U.S. Securities and Exchange Commission, Remarks at the Compliance Outreach Program (Jan. 31, 2012); *see also* Jamie Symington, Financial Services Authority Enforcement & Financial Crime Division, Final Notice, sent to UBS AG, London, 25 Nov. 2012 (in a case involving a rogue trader and a substantial monetary loss to UBS AG, the Financial Services Authority analyzed the components and role of the firm's three lines of defense).

senior management are essential.[18] The level of coordination varies by firm, but Compliance professionals must be mindful that if they make, or are viewed to be responsible for, business or managerial decisions, they may exceed the scope of a Compliance mandate and take on business or supervisory liability.

One situation where Compliance should be particularly careful in how its role is delineated is when it interacts with, and within, firm committees. Many firms delegate responsibility and authority to various committees, and certain statutes and regulations also require the use of committees for specific functions.[19] Committees have a broad range and variety of mandates. Some committees are advisory only in nature; others are decision-making bodies with either intermediate or final effect. Additionally, some committees address narrow proposals presented to them, while others choose, or are required, to fashion broader results and remedies. Small firms may have very few committees, whereas large firms may delegate authority to multiple committees and sub-committees to accommodate geographically or organizationally dispersed business units and personnel. As greater emphasis is placed on compliance issues, many firms request or require the representation or participation of Compliance on one or more committees. While this involvement contributes to a firm's compliance program and risk management, it also can present distinct challenges.

Front-office committees, such as the Executive, Management and Operating Committees, retain a great deal of authority and control. These committees generally decide issues that influence a firm's overall operation and direction, such as compensation, hiring and firing, and business expansion. Representation on, or participation in, front-office committees by a Compliance professional is beneficial because it encourages senior management to seek Compliance's input on important business decisions and provides Compliance with direct access to important information. In this regard, Compliance's representation on or participation in firm committees generally enhances a firm's culture of compliance; however, this representation or participation does not change Compliance's core functions: control and advice. To promote Compliance's important participation at this level of firm governance, and absent an express mandate or agreement to the contrary, Compliance professional participation on committees should not be viewed as indicative of the exercise of managerial or supervisory activity. This should be the case even where a committee requires or allows Compliance officers to record votes on matters. A determination by Compliance to approve, or to not object to, a particular activity or decision is not an exercise of supervisory control.

In contrast to front-office-centered committees, Compliance also may be involved in control-related committees that review or advise business and operational endeavors.

---

[18] Carlo V. di Florio, Director, OCIE, U.S. Securities and Exchange Commission, Remarks at CCOutreach National Seminar (Feb. 8, 2011) ("to be effective, compliance and ethics programs cannot exist in silos . . . [t]hey need to be imbedded in the business process and at the table when strategic decisions are being made and new products are being developed.").

[19] *See, e.g.*, NASD Rule 2711(d) (requiring that committees set research analysts' compensation); FINRA Rule 3130 (requiring a firm to submit its annual certification of compliance and supervisory processes to its board of directors and audit committee, or equivalent); Securities and Exchange Act of 1934 ("Exchange Act") Section 10A (requiring an issuer to maintain an audit committee, or equivalent); Exchange Act Section 10C (requiring an issuer to maintain a compensation committee).

Compliance's involvement is beneficial here too, because participation in a general Risk Committee facilitates Compliance's ability to escalate broad, firm-wide issues, such as those related to anti-money laundering ("AML") or conflicts of interest procedures, to senior management. Working with or as part of specific Risk Committees, such as Credit Risk, Operations Risk or Technology Risk, allows Compliance professionals to advise on specialized areas involving unique regulatory considerations. Similarly, participating in or advising other control-related committees, like a Disciplinary, Conflicts of Interest or Ethics Committee, allows Compliance professionals to advise on specific issues that affect the compliance program. As with front-office committees, Compliance professionals should be mindful of the risks associated with performing functions that could be viewed as managerial or supervisory.[20]

2. Coordination with Other Control Groups

As the 2005 White Paper observed, Compliance often carries out control functions in conjunction with other control groups and, accordingly, must coordinate with those groups on an ongoing basis.[21] This need for coordination has increased as regulators have broadened their focus on the overall compliance, risk and control framework in firms. Since firms allocate responsibilities and resources differently, the overlap and convergence of Compliance, Legal, Internal Audit and Risk present distinct challenges and highlight the need to define clearly the role of each of these functions. The considerations that apply to Compliance's relationship with other control groups parallel those relating to Compliance's involvement on firm committees. In both instances, if firms provide clarity and assign accountability, and regulators accept reasonable though varying approaches, Compliance can contribute its expertise and perspective without unnecessary concern about liability for business or risk management decisions that they do not in fact control.

a) Compliance-Legal Relationship

Managing the relationship between Compliance and Legal, which advises and represents a firm regarding legal issues, is important, particularly if they share responsibilities, resources or staff. For instance, privilege issues may arise if Compliance professionals are also lawyers who provide legal advice to the firm since such advice may not be privileged if it is rendered solely from a Compliance perspective.[22] Additionally, regardless of how clearly a firm defines the line between Compliance and Legal, there will be instances where roles and responsibilities converge, and it may be difficult to determine whether an employee acted in a Compliance or Legal capacity. This often occurs when Compliance and Legal collaborate to, among other things: (i) conduct internal investigations; (ii) respond to regulatory examinations and inquiries;

---

[20] Daniel M. Gallagher, Commissioner, U.S. Securities and Exchange Commission, Remarks at "The SEC Speaks in 2012" (Feb. 24, 2012) ("However, one must carefully weigh the consequences of full voting membership in light of the substantial benefits of being a valued but non-voting advisor to the board or committee. I have personal experience with this issue and I believe that non-voting lawyers and compliance officers can be fully effective voices in those forums.").

[21] In some firms, the relationship between Compliance and other control groups may go beyond mere coordination, as Compliance may actually report to another control group or into another control structure.

[22] Firms must clearly communicate to Compliance and Legal personnel that lawyers' communications may be privileged if they relate to advising the firm and that the privilege belongs to, and can only be waived by, the firm. *See Upjohn Co. v. United States*, 449 U.S. 383, 396-97 (1981).

(iii) handle customer complaints; (iv) draft disclosures and filings; (v) draft policies and procedures; (vi) interpret rules and regulations and assess their applicability to existing business practices; and (vii) advise on the regulatory requirements associated with new business initiatives, products and services. In that regard, it is important that Compliance and Legal create a protocol to establish when an employee is acting in a Compliance or Legal capacity (or under the direction of Legal) to ensure that applicable laws, rules and regulations are satisfied and privileges are maintained. A formal protocol is advisable to establish what otherwise may be a cumbersome after-the-fact determination.

b) Compliance-Internal Audit Relationship

Internal Audit reviews business activities and controls to identify risks and to determine whether a firm's internal policies and procedures are satisfied. Although Internal Audit performs an independent verification function, it may seek assistance from Compliance in identifying and understanding policies and procedures. For instance, Internal Audit and Compliance may coordinate to review and test select business activities as well as a firm's supervisory control system.[23] In addition to reviewing and testing the effectiveness of supervisory systems, Internal Audit also conducts independent reviews of the Compliance function and program. Accordingly, although their roles and purposes differ, it is important that firms maintain distinct, though coordinated, Compliance and Internal Audit functions.

c) Compliance-Risk Management Relationship

While Compliance focuses on identifying, assessing, escalating and mitigating regulatory risk as well as reputational risk, in many firms, other distinct risk management lines work closely with business units and others to identify and control specific risk exposures related to business risks, such as market, credit, liquidity, funding, other financial, operations and transaction processing, and information security risks. Compliance may assist risk management and business units in identifying risk and contribute information to a firm's overarching operational risk management structure. However, Compliance should not have responsibility for deciding, executing or overseeing the steps necessary to reduce or manage specific risks primarily assigned to other risk management functions or to the business itself.

C. Compliance and Supervision: Enforcement of Existing Standards

The discussion of Compliance involvement with firm committees described one instance where the line between compliance and supervision can be unclear. Our 2005 White Paper focused on this core consideration – where supervision and compliance each begin and end – and set out our thinking in detail.[24] Traditionally, Compliance maintains the compliance program and advises business units and senior management, whereas senior management is ultimately responsible for a firm's overall supervisory and compliance obligations. Line supervisors oversee business operations and have the authority to control employee behavior (*e.g.*, by hiring and firing powers) as a means of satisfying applicable laws, rules and regulations. What appears to have changed recently is the view of enforcement authorities of Compliance's role—changes

[23] Specifically, Compliance and Internal Audit may work together to satisfy the obligations of NASD Rule 3012 ("Supervisory Control System").

[24] *See* 2005 White Paper, attached as Appendix A, at 9-13.

not based in legislative mandate or rule interpretation by rulemaking bodies, but by differing and more expansive views of Compliance responsibilities relative to management's supervisory responsibilities. Compliance personnel have been named in some recent enforcement actions alleging that their performance of Compliance functions constitutes business or supervisory activities.[25]

It is sometimes unclear when regulators will deem the performance of Compliance functions to be supervisory activities, thereby exposing Compliance to the risks associated with being deemed a supervisor. However, three theories have emerged: control, affect and blended. Under the "control" theory, the power to control an employee's conduct – by hiring, firing or otherwise disciplining the employee – may cause a Compliance officer to be deemed a supervisor.[26] The broader "affect" theory provides that exercising any authority to affect the conduct of an employee whose behavior is at issue may cause a Compliance professional to be deemed a supervisor.[27] These two theories existed at the time of the 2005 White Paper, and Compliance professionals have been held liable under both theories for failure to supervise with respect to the misconduct of an employee whom they were deemed to supervise.

A new third theory that emerged from a recent SEC enforcement case combines the "control" and "affect" theories to create a farther-reaching standard. Under this blended theory, Compliance professionals may be liable as supervisors simply if they are viewed as authoritative, that is, if their recommendations on an issue are generally followed by business personnel. Like the "affect" theory, this new theory presents a deeply problematic view. Compliance should be influential and affect the decision-making of supervisors, but influence does not equate with control. Because the SEC case propounding this view was ultimately dismissed,[28] the precise point at which the performance of Compliance activities would cause a Compliance professional to be deemed a supervisor remains unclear.

---

[25] *See supra* note 13 and accompanying text (discussing recent enforcement matters against Compliance personnel alleging failure to supervise various business activities).

[26] *In re Arthur J. Huff*, Exchange Act Release No. 29017 (Mar. 28, 1991) ("*[T]he most probative factor that would indicate whether a person is responsible for the actions of another is whether that person has the power to control the other's conduct*. This view is supported by the common meaning of the term 'supervision,' when used in the employment relationship to which the statute refers and by the statutory language 'subject to his supervision' which also seems to emphasize control.") (emphasis added).

[27] *In re John H. Gutfreund*, Exchange Act Release No. 31554 (Dec. 3, 1992) ("[D]etermining if a particular person is a 'supervisor' depends on whether, under the facts and circumstances of a particular case, that person has a *requisite degree of responsibility, ability or authority to affect the conduct of the employee whose behavior is at issue*.") (emphasis added).

[28] In a recent appeal to the SEC, the Commissioners were evenly divided on whether allegations were established that a general counsel tasked with Compliance and Legal duties failed to reasonably supervise a broker. Because of this deadlock, the case was dismissed. In an initial decision, an administrative law judge ("ALJ") found that the general counsel had the requisite degree of responsibility, ability or authority to affect the conduct of the broker and was therefore a supervisor. However, the ALJ determined that he was not guilty of failure to supervise because he acted reasonably by speaking with the broker and attempting to escalate red flags to senior management. Due to the SEC's dismissal, the point at which the performance of compliance functions constitutes engaging in supervisory activities remains unknown, creating the potential for similar, future actions against Compliance and Legal personnel. *See In re Theodore W. Urban*, SEC Admin. Proc. File No. 3-13655, Initial Decision Release No. 402 (Sept. 8, 2010), *dismissed by* Exchange Act Release No. 66259 (Jan. 26, 2012).

As pointed out recently by an SEC Commissioner, the danger posed by this uncertainty is that "robust engagement on the part of legal and compliance personnel raises the specter that such personnel could be deemed to be 'supervisors' subject to liability for violations of law by the employees they are held to be supervising" and that "the Commission's position on supervisory liability for legal and compliance personnel may have had the perverse effect of increasing the risk of supervisory liability in direct proportion to the intensity of their engagement in legal and compliance activities."[29] Currently lacking clear and uniform guidance, Compliance must attempt to determine for itself the degree of authority or involvement in business activities that is appropriate for its professionals. Even if it articulates clear and detailed delineations of supervisory and compliance obligations, Compliance remains vulnerable to after-the-fact judgments that, despite such articulated policies and procedures, its actions are to be deemed an exercise of supervisory authority and an assumption of supervisory responsibility and liability. This possibility discourages Compliance involvement in critical decision-making and is the unacceptable status quo for the industry and for Compliance professionals today.

We urge regulators to work with Compliance professionals to develop reasonable standards for determining when the performance of job functions constitutes supervisory, rather than Compliance, activities.[30] In that regard, we believe such standards should recognize the difference between a strong, independent control function and a business line supervisory function. Where firms have established a framework setting forth the roles and responsibilities of Compliance, we believe regulators should recognize and respect that framework and assess the performance of Compliance functions within such framework.

D. Expanding and Competing Regulatory Expectations

Compliance must address numerous rules and regulations, including those promulgated by Congress, self-regulatory organizations ("SROs"), government agencies, state regulators and financial regulators.[31] Even a single financial product may be subject to the requirements of multiple regulators and regulatory schemes.[32] Not only must firms spend significant resources harmonizing, rationalizing and meeting various regulations, but they are also exposed to liability

---

[29] Daniel M. Gallagher, Commissioner, U.S. Securities and Exchange Commission, Remarks at "The SEC Speaks in 2012" (Feb. 24, 2012). *See also* Daniel M. Gallagher, Commissioner, U.S. Securities and Exchange Commission, Keynote Address at Investment Adviser Association Investment Adviser Compliance Conference 2012 (Mar. 8, 2012) ("[W]e should strive to avoid attacking or penalizing the willingness of compliance and legal personnel to be fully involved in firms' responses to problematic actors or acts. To put it simply, if a firm employee in a traditionally non-supervisory role has expertise relevant to a compliance matter, that employee shouldn't fear that sharing that expertise could result in Commission action for failure to supervise.").

[30] Daniel M. Gallagher, Commissioner, U.S. Securities and Exchange Commission, Keynote Address at Investment Adviser Association Investment Adviser Compliance Conference 2012 (Mar. 8, 2012) ("We must strive to ensure that failure-to-supervise liability never deters legal and compliance personnel from diving into the firm's real-world legal and compliance problems.").

[31] These requirements subject Compliance to a range of standards from a flexible "reasonable" approach to stricter requirements carrying criminal penalties.

[32] For instance, securities futures products are jointly regulated by the CFTC and SEC. Swaps transactions may be subject to the rules of the SEC, CFTC and/or the Board of Governors of the Federal Reserve ("Federal Reserve Board"), if swap entities are banks or systemically important financial institutions ("SIFIs").

on multiple fronts since being penalized by one regulator may cause other regulators to bring actions for the same issue.[33]

While Compliance functions of securities firms traditionally focus on satisfying securities laws and regulations, regulators – including securities regulators – increasingly expect the Compliance mandate to cover a much broader range of compliance and control issues.[34] For instance, both regulators and Congress have created new obligations for firms to identify and mitigate broad conflicts of interest.[35] Congressional and regulatory focus has also expanded regulation and the application of regulatory requirements to a wider spectrum of activities and personnel, including those employees who do not directly interact with customers, handle customer funds or securities, or otherwise engage in securities activities.[36] New disclosure and recordkeeping rules, while intended to promote market transparency and integrity, have created new duties for Compliance and increased its accountability for any inaccuracies. These obligations have expanded the Compliance mandate significantly beyond its traditional scope.

Similarly, the expectations of non-securities regulators have also begun to affect the Compliance mandate in securities firms. In particular, the Federal Reserve Board's guidance on compliance programs is increasingly influencing the securities industry even though many securities firms are not affiliated with bank holding companies. This guidance emphasizes the importance of a strong Compliance function that is focused on implementing a firm-wide, global approach to risk management and oversight—a much broader mandate than that traditionally

---

[33] Regulators often enter arrangements to share information with each other related to enforcement actions. *See* FINRA Rule 8210(b)(1)-(2) ("staff may enter into an agreement with a domestic federal agency, or subdivision thereof, or foreign regulator to share any information in FINRA's possession for any regulatory purpose set forth in such agreement . . . for the purpose of an investigation, complaint, examination, or proceeding").

[34] At this juncture, compliance with non-financial services laws and regulations, such as those related to tax, accounting, environmental issues, general employment, occupational health and safety related human resources and legal risks (*e.g.*, negligence and contractual obligations), are not typically the responsibility of Compliance.

[35] Congress clearly illustrated its intent in the preamble to the Dodd-Frank Act. This explains that the act is intended "[t]o promote the financial stability of the United States by improving accountability and transparency in the financial system, to end 'too big to fail,' to protect the American taxpayer by ending bailouts, to protect consumers from abusive financial services practices, and for other purposes." Dodd-Frank Act, *supra* note 4, Preamble. *See also* Prohibition Against Conflicts of Interest in Certain Securitizations, Exchange Act Release No. 65355, at 4 (Sept. 19, 2011) (proposing a rule that would "make it unlawful for a securitization participant to engage in any transaction that would involve or result in any material conflict of interest between the securitization participant and any investor in an ABS that the securitization participant created or sold.").

Additionally, several agencies, including the SEC, Federal Reserve Board, Office of the Comptroller of the Currency and Federal Deposit Insurance Corporation ("FDIC") (collectively, "Agencies"), proposed a detailed rule applying to banking entities and certain nonbank entities that, if adopted, would prohibit and restrict proprietary trading and certain interests in, and relationships with, hedge funds and private equity funds (the "Volcker Rule"). The rule would also prohibit material conflicts of interest that arise in connection with certain trading activities. Prohibitions and Restrictions on Proprietary Trading and Certain Interests in, and Relationships With, Hedge Funds and Private Equity Funds, 76 Fed. Reg. 68,846, 68,893 (Nov. 7, 2011) [hereinafter *Volcker Proposal*].

[36] FINRA Rule 1230, adopted in 2011, requires operations personnel to be qualified and licensed in order to engage in operational activities related to, among other tasks: client on-boarding; account maintenance; trade confirmations and customer statements; and posting entries to books and records. *See* FINRA Rule 1230. Prior to Rule 1230, employees did not have to be qualified and licensed to perform many activities that now fall under the rule.

given to the Compliance functions of securities firms.[37] The guidance also states that a firm's board of directors "should review and approve key elements of the organization's compliance risk management program and oversight framework."[38] Finally, the guidance endorses the principles of the Basel Committee on Banking Supervision ("Basel Committee"), which require firms to adhere to ten principles that guide the operation and function of Compliance.[39]

Firms also encounter competing and, in some cases, conflicting regulatory demands, particularly if they operate in multiple markets or jurisdictions or employ dual-hatted employees.[40] A prime example is the role of the chief compliance officer ("CCO"), who traditionally heads Compliance and is responsible for maintaining an effective compliance program. Depending on a firm's products and services, the CCO may be subject to various overlapping requirements set out in the Exchange Act,[41] the Investment Advisers Act of 1940 ("Advisers Act"),[42] FINRA rules[43] and the Commodity Exchange Act,[44] among others. If the

---

[37] *See* Federal Reserve Board, *Compliance Risk Management Programs and Oversight at Large Banking Organizations with Complex Compliance Profiles*, SR 08-8/CA 08-11 (Oct. 16, 2011) [hereinafter Federal Reserve Board, *Compliance Risk Management Programs*].

[38] *See* Federal Reserve Board, *Compliance Risk Management Programs*, *supra* note 37.

[39] *See* Federal Reserve Board, *Compliance Risk Management Programs*, *supra* note 37 ("The principles in the Basel compliance paper have become widely recognized as global sound practices for compliance risk management and oversight, and the Federal Reserve endorses these principles."). The Basel Committee released ten principles addressing the Compliance function within banks. At a high level, the principles address four main areas: (i) responsibilities of the board of directors for Compliance; (ii) responsibilities of senior management for Compliance; (iii) Compliance function principles (*e.g.*, independence, resources and responsibilities); and (iv) cross-border and outsourcing issues. *See generally*, Basel Committee on Banking Supervision, *Compliance and the Compliance Function in Banks* (Apr. 2005).

[40] Coordinating with affiliated entities, even if only in a very limited capacity such as for clerical or ministerial support, also may pose the risk that regulatory examiners may request the affiliate's internal documentation and may want to review the affiliate's risk and compliance programs.

[41] The CCO often develops or assists in the development of policies and procedures designed to comply with various requirements of the Exchange Act, including Section 15(g) (information barriers) and Rules 17a-3 and 17a-4 (recordkeeping and retention). If adopted, Exchange Act Rule 15Fk-1 would create specific requirements for the CCOs of security-based swap dealers, including, among others: reporting directly to the board of directors; reviewing the firm's compliance program; establishing, maintaining and reviewing written policies and procedures reasonably designed to achieve compliance with Section 15F of the Exchange Act; and consulting with the board of directors to resolve conflicts of interest. SEC Proposed Rule, Business Conduct Standards for Security-Based Swap Dealers and Major Security-Based Swap Participants, Exchange Act Release No. 64766 (June 29, 2011).

[42] Advisers Act Rule 206(4)-7 requires registered investment advisers to designate a CCO and to establish a Compliance function that includes internal policies and procedures and a method for annual review.

[43] FINRA Rule 3130 obligates firms to designate a CCO, or multiple CCOs, with expertise and ultimate responsibility for Compliance functions, including assisting in the preparation of annual certifications of Compliance and supervisory processes, and otherwise maintaining and running a firm's compliance program.

firm conducts financial or securities-related business outside of the United States, Compliance and the CCO also must satisfy non-U.S. regulatory requirements.[45]

III. The Evolving Role of Compliance in Firms

The securities industry has a core connection to the world's economic well-being and, as illustrated by the financial crisis and ensuing regulatory response, the importance of stable and viable markets has never been more apparent. The regulatory response, including the implementation of the Dodd-Frank Act, has broadened the role of Compliance beyond its traditional focus on broker-dealer compliance issues.[46] Compliance functions have assumed greater responsibility as the complexity of securities firms and their operations has increased exponentially.[47]

A. Key Factors Impacting the Operation of the Compliance Function

1. Expansion of Complex Business Models

Securities firms and their operations have grown much more complex in recent years. New technology and a general increase in globalization have dramatically changed many business lines, services and products at both large and small firms. These factors also have led to new methods for assessing markets and trading strategies, which in turn have driven financial products and strategies to become more specialized and complex. For instance, high speed

---

[44] The Commodity Exchange Act now imparts criminal penalties on CCOs if certified compliance reports are later found to be inaccurate. Commodity Exchange Act Sections 4s(k) and 5b(i)(3)(B)(ii) (CCOs must certify "under penalty of law, the compliance report is accurate and complete"). New CFTC rules require that the CCOs of registered derivatives clearing organizations have "the full responsibility and authority to develop and enforce, . . . appropriate compliance policies and procedures." CFTC Final Rule, Derivatives Clearing Organization General Provisions and Core Principles, 76 Fed. Reg. 69,333, 69,341 (Nov. 8, 2011). Other new CFTC rules address a firm's business conduct and will require the closer integration of CCOs with business units to review and approve certain business and suitability determinations. CFTC Final Rule, Business Conduct Standards for Swap Dealers and Major Swap Participants with Counterparties, RIN 3038-AD25 (Feb. 17, 2012).

[45] Being subject to both U.S. and foreign regulations may be particularly challenging if the requirements do not align. For instance, the German financial regulator Bundesanstalt für Finanzdienstleistungsaufsicht ("BaFin") released a circular in 2010 providing minimum requirements for Compliance regarding conduct, organization and transparency. The circular delineates the duties of Compliance and specifically states that Compliance must be independent and advise operational departments, and that CCOs should be appointed for terms of at least 24 months to bolster such independence. However, the circular also states that Compliance should be involved in supervising and evaluating a firm's procedures, which may actually cause Compliance professionals to be considered line supervisors under U.S. requirements. BaFin, Circular 4/2010 (WA), Minimum Requirements for the Compliance Function and Additional Requirements Governing Rules of Conduct, Organization and Transparency (June 7, 2010).

[46] In some areas, obligations have even shifted away from employees and toward firms and their Compliance functions. *See, e.g.*, Order Approving Proposed Rule Change to Adopt FINRA Rules 1010 and 2263 in the Consolidated FINRA Rulebook, Exchange Act Release No. 60348 (July 20, 2009) (increasing requirements on firms to register and license their employees, while reducing the obligations of individual employees).

[47] Like securities firms, regulators have had to enhance their processes and staffs to better address increasingly complex products, transactions and markets. The SEC Division of Enforcement recently established five specialized units to develop expertise in high-priority areas and to keep pace with the private sector. Robert Khuzami, Director, Division of Enforcement, U.S. Securities and Exchange Commission, Remarks at SIFMA's Compliance and Legal Society Annual Seminar (Mar. 23, 2011).

electronic trading, the creation and sale of non-traditional structured products, the use of cross-product hedging strategies and similar concepts are now becoming standard practice in the securities industry. As discussed below, the globalization of business has increased the demands on Compliance as the requirements of multiple jurisdictions must be taken into consideration. Similarly, as major broker-dealers have become part of bank holding companies, bank regulators have increasingly become involved in compliance matters that had previously been the province only of securities regulators.

a) Globalization of Business

Global business structures and cross-border activities expose U.S. firms to risks from both regulatory and operational perspectives. In today's global markets, many firms engage in activities in non-U.S. markets and/or with non-U.S. customers and market participants, which may expose them to increased legal and regulatory risk if their Compliance functions lack comprehensive knowledge of regulatory requirements that may have no comparable U.S. counterpart. As a result, U.S. firms are challenged to develop compliance programs that comply with relevant non-U.S. requirements, while their global counterparts face similar, reciprocal challenges.

In many ways, the globalization of business has increased the complexity of the securities industry. Now, issues with one country's economy or regulatory regime, or of the largest financial services firms, can quickly spread to the entire industry or the global economy as a whole. The close ties between various, geographically dispersed global economies and markets emphasize the need for greater cooperation among regulators to better identify, address and prevent industry-wide risks.

b) Influence of New and Changing Technology

The development and increased use of new technology in the securities industry both assist Compliance and other control functions engaging in surveillance in performing their duties and present them with new challenges and risks. For instance, the availability of advanced technology has automated and streamlined many business processes at securities firms. Workflow tools allow middle and back-office personnel to provide invaluable support to business units in a short amount of time, while reducing overhead and capital costs by employing fewer personnel. Similarly, new risk control, trade monitoring and electronic communication surveillance tools have increased the scope and effectiveness of many compliance programs.[48] These tools allow Compliance to facilitate and streamline its activities while reducing the human resources necessary to run an effective compliance program.

At the same time, firms must support efforts by Compliance and other control functions to keep pace with the rapid development of highly complex systems, some of which permit firms and customers to effect transactions at higher speeds or to access a multitude of information in real-time. Since the 2005 White Paper, the increased use of technology has led to a much higher

[48] Regulators have recognized the availability of electronic monitoring solutions, but they have declined to specifically endorse the use of any particular tool. Joint guidance from the New York Stock Exchange and FINRA explained that, while the use of electronic solutions will not alleviate a firm of its compliance burden, such solutions may assist Compliance in monitoring electronic communications. FINRA, *Notice to Members 07-59: Review and Supervision of Electronic Communications*, at 12-13 (Dec. 2007).

volume of market transactions, requiring firms to take on greater responsibility monitoring, capturing and maintaining vast amounts of data.

Firms must regularly take into account the availability of new technology and assess any impact the technology may have on compliance programs.[49] Compliance professionals also must assess whether particular solutions comply with applicable regulatory requirements as well as a firm's own policies and procedures. Although the introduction of new technology may assist business activities as well as the performance of Compliance activities, firms must be mindful of any collateral impact that the technology may have, including the creation of new potential risks, and should consider partnering Compliance with other risk management or control functions to understand and assess any such impact. For instance, new trade monitoring systems must be tested to confirm that they appropriately identify and escalate improper trading activity and that they draw from all relevant trade data feeds. Any change or upgrade in systems creates the risk that data feeds into and out of the particular system will be disrupted.

In recent years, the internet and the use of personal communications devices, such as smart phones, have revolutionized not only the way in which securities firms engage in business, but also how they communicate with customers, potential customers and even internally. The development and widespread use of new forms of electronic communications, including social media, pose particular challenges to business supervisors, Compliance and other control functions. While regulations and related guidance generally direct firms to focus only on an employee's business, as opposed to personal, activities,[50] firms must now consider communications that occur outside of the workplace.[51] In addition, the global nature of the internet poses challenges to the implementation of the regulatory and compliance requirements of specific jurisdictions.

c) Outsourcing Arrangements

Outsourcing arrangements are used by numerous securities firms to support back and middle-office operations, as well as Compliance and supervisory functions.[52] Outsourcing arrangements include the use of third-party service providers as well as the affiliates of a

---

[49] Compliance functions also must account for the way in which regulatory and jurisdictional borders become blurred, if not entirely nonexistent, by new technology. For instance, internet sites and web-based technology that are accessible in multiple jurisdictions and/or that are shared by multiple affiliated entities present distinct challenges.

[50] FINRA, *Regulatory Notice 11-39: Social Media Websites and the Use of Personal Devices for Business Communications*, at 2 (Aug. 2011) [hereinafter *Regulatory Notice 11-39*] ("The obligations of a firm to keep records of communications made through social media depend on whether the content of the communication constitutes a business communication."); FINRA, *Regulatory Notice 10-06: Social Media Websites*, at 2 (Jan. 2010) [hereinafter *Regulatory Notice 10-06*] ("This Notice only addresses the use by a firm or its personnel of social media sites for business purposes."). FINRA has not defined what constitutes a business versus a personal communication.

[51] Similarly, and equally troubling, a firm may be exposed to liability due to the actions of non-employee, third-parties that interact with the firm's social media. FINRA has explained that third-party posts to a firm's social media page may, in certain circumstances, be considered a communication of the firm. *See Regulatory Notice 10-06*, *supra* note 50, at 8-9.

[52] Middle and back-office operational support may be required to register as operations professionals under FINRA Rule 1230. *See, e.g.*, *supra* note 36 and accompanying text.

securities firm.[53] Senior management often favors outsourcing as a means of increasing efficiencies and reducing costs by centralizing common functions in one entity, whether an affiliate or third-party. For instance, certain core Compliance functions of securities firms that are part of multi-service financial institutions have traditionally been centralized and "outsourced" to affiliates.

Many firms address the use of outsourcing arrangements in their compliance programs to ensure that such arrangements are adequately supervised and subject to appropriate policies and procedures. However, outsourcing will continue to challenge business supervisors, Compliance and regulators, as novel arrangements and new technology support a greater degree of integration among dispersed personnel and operations.[54]

2. Structure of Compliance in Diverse Business Models

Compliance functions vary considerably depending upon a firm's size, the nature and complexity of its activities, its geographic reach and other factors. The business and organizational structures that securities firms utilize each present unique challenges. At the outset, the role of the CCO must be clearly defined, regardless of whether a firm has a small Compliance function with one CCO, utilizes a matrix reporting system, has multiple CCOs, or has one or more dual-hatted CCOs. Each of these models requires that reporting lines and responsibilities are documented and detailed so that personnel understand their duties and, when necessary, the process for escalation.[55] Clear roles and reporting lines are especially important for large firms where core Compliance functions, resources and systems may be shared across multiple business lines or affiliates, including those operating in different countries and those that permit associated persons to engage in private securities transactions or outside business activities.

---

[53] Proposed FINRA Rule 3190 clarifies that a "third-party service provider" includes "any person controlling, controlled by, or under common control with a member, unless otherwise determined by FINRA." *See* FINRA, *Regulatory Notice 11-14: FINRA Requests Comment on Proposed New FINRA Rule 3190*, at 11 (Mar. 2011) [hereinafter, *Regulatory Notice 11-14*].

[54] In 2005, NASD addressed the use of outsourcing arrangements that, until recently, constituted the primary guidance on outsourcing. NASD discussed the outsourcing of covered activities, or those activities requiring qualification and registration if performed directly by a broker-dealer, and explained that such activities cannot be performed by an unregistered entity. Covered activities "include, without limitation, order taking, handling of customer funds and securities, and supervisory responsibilities." NASD, *Notice to Members 05-48: Outsourcing*, at 5 n.2 (July 2005). That guidance, as well as a 2011 FINRA rule proposal, provides that while firms may outsource certain activities that support supervisory and Compliance functions, they cannot delegate away their responsibility for these functions. *See id.* at 4 (in an outsourcing arrangement, "the ultimate responsibility for supervision lies with the member.") and *Regulatory Notice 11-14*, *supra* note 53, at 3-4. The 2011 rule proposal, if adopted, will require firms to establish written procedures that address outsourced functions performed by third-party service providers. Such procedures would have to provide for ongoing due diligence by the firm to determine: (i) whether the provider is capable of performing the outsourced activities; and (ii) for any outsourced activity, whether the firm itself can comply with applicable securities laws, regulations and rules.

[55] The reporting lines through which Compliance escalates potential issues vary by firm and each reporting model impacts how Compliance interacts with, and may be influenced by, senior management. For instance, some firms require Compliance to escalate issues to the CEO or to a Chief Risk Officer, while others instruct Compliance to report to the General Counsel or to an Audit Committee.

The overall structure of Compliance also must be clearly defined. Instead of prescribing a specific organizational structure for Compliance functions, regulators appropriately have permitted firms flexibility[56] to account for varying business models, sizes and resources.[57] Such flexibility is necessary because no single Compliance structure could be used for each of the following business models: single-business broker-dealers; dual-registered broker-dealer/investment advisers; international integrated financial services organizations; and holding company structures with multiple affiliated businesses housed in separate legal entities. At one end of the spectrum, a single-business broker-dealer may employ several securities professionals and one Compliance officer; whereas, at the other end, an international integrated financial services firm may use a self-contained Compliance function with dozens of professionals at the holding company level and additional Compliance staff housed in individual business lines or countries.

Additionally, Compliance may be organized in various ways, including in a centralized or a divisional manner. A centralized function houses all Compliance personnel in one department that monitors all aspects of a firm's business. However, some firms find it impractical or undesirable to have one Compliance function to focus on all of the competing, and in some cases conflicting, requirements and expectations of the laws and regulations applicable to different business units and legal entities. A divisional function uses dedicated Compliance personnel to provide support to each of a firm's business units, in different countries where the firm operates or in separate legal entities. When using a divisional structure, communication and coordination among the various facets of Compliance are essential, and the functions and responsibilities of each component of Compliance should be documented.

3. Resource Limitations

As the role of Compliance evolves to account for changes to the industry and related regulatory regimes, many Compliance functions have taken on greater responsibility and accountability with, at times, limited resources to do so. This strains Compliance's ability to remain current on developments that may affect the performance of its functions. This is particularly true in light of heightened regulatory requirements, some of which call upon Compliance to utilize dedicated technology resources and staff to monitor systems and electronic communications. While many firms continue to face increased capital costs and constraints on profitability, senior management must ensure that Compliance is sufficiently resourced so that it

---

[56] Regulatory flexibility permits firms to tailor Compliance functions to their unique operations. Where internal conflicts may arise, Compliance should have another channel (*e.g.*, a "dotted" reporting line) through which it can escalate issues. Additionally, the U.S. Sentencing Guidelines suggest that firms create a mechanism that allows employees to anonymously report, or to seek guidance on, potential wrongdoing. U.S. SENTENCING GUIDELINES MANUAL § 8B2.1(b)(5) (2011).

[57] Financial services firms, including non-U.S. firms, have argued that requiring a specific organizational structure "would be neither practical nor necessary because of the significant diversity" of firms. Rather, firms should be allowed to create organizational structures according to general principles, such as "size, geographic dispersion, internal culture, regulatory environment of the firm; different regulatory requirements applicable to banks and broker-dealers; nature, scale, complexity of the business and risks undertaken." Technical Committee of International Organization of Securities Commissions ("IOSCO"), *Compliance Function at Market Intermediaries, Final Report*, at 28-29 (Mar. 2006).

can accomplish the goals and tasks to which it is assigned.[58] Likewise, new regulatory requirements should account for small firms with fewer staff and recognize that all firms have finite resources to satisfy a broad range of requirements.

B. New Challenges and Developments to Core Compliance Functions

The traditional functions of Compliance were discussed in our 2005 White Paper. Although Compliance continues to perform these functions, emerging trends have caused its focus to become more diffuse and have altered the manner in which it performs many of these functions. Following the financial crisis and a series of highly publicized financial frauds, there has been constant pressure on Compliance to broaden the scope of its coverage and to take a more hands-on role in business operations.[59] In many cases, Compliance must account for new risks, such as those related to dealings with third-parties.[60] This Section addresses the manner in which Compliance's traditional functions have been affected by new and enhanced regulatory requirements and expectations.

1. Advisory

a) Coverage of Technology, Finance and Operations

In addition to the traditional advisory role that Compliance has with respect to front office activities, Compliance increasingly advises middle and back-office units, such as technology, finance and operations, on the application of various regulations to new systems and technologies. Firms have an increasing need to employ Compliance professionals with technical knowledge and experience who can support these units, particularly given recent statements from regulators and regulatory staff reflecting greater concern about technology issues,[61] including, among others, data protection and privacy. While dedicated Compliance professionals with such

---

[58] Senior SEC staff has reminded firms of their "legal obligation to maintain an adequate compliance program reasonably designed to achieve compliance with the law," when considering reductions and cost-cutting measures. Lori A. Richards, Director, OCIE, U.S. Securities and Exchange Commission, Open Letter to CEOs of SEC-Registered Firms (Dec. 2, 2008). Director Richards also explained that by fulfilling their regulatory obligations, firms can restore and bolster public confidence in the markets, and their "[p]roviding adequate resources to compliance programs and functions and ensuring that CCOs and compliance personnel are integrated into the activities of the firm are essential to that process." *Id.*

[59] Even the SEC has revised its operations to better address financial fraud and prevent the recurrence of future financial crises. Mary Schapiro, Chairman, U.S. Securities and Exchange Commission, Testimony Before the H. Subcommittee on Financial Services and General Government (Mar. 17, 2010) (explaining that the SEC revised its practices and examination process in response to, and to account for, "ever-changing Wall Street practices and lessons learned from the Madoff fraud.").

[60] The unlawful actions of third-parties with whom firms have close ties may expose the firms to potential liability and reputational harm. For instance, the web of consultants, firms and other third-parties used in insider trading rings has resulted in numerous investigations that, at times, involve parties that were only tangentially related. Notably, the investigation into Raj Rajaratnam, a hedge fund manager at Galleon Management Group LP, continues to spawn innumerable third-party civil and criminal proceedings. *See* SEC Press Release 2011-233, SEC Obtains Record $92.8 Million Penalty Against Raj Rajaratnam (Nov. 8, 2011).

[61] *See, e.g.*, FINRA, *2012 Regulatory and Examination Priorities Letter* (Jan. 31, 2012) (discussing trends and changes in regulatory priorities, and the numerous, specific areas on which FINRA examiners will focus in 2012, including the use of technical systems); *see also infra* Section III.B.4.b.

expertise can assist Firms in reducing potential liability in these areas, Compliance must be cautious about avoiding supervisory responsibility when advising these units as regulators are increasingly seeking to bring failure to supervise actions in connection with back-office violations.[62]

b) Conflicts of Interest

Partly triggered by the Dodd-Frank Act[63] and partly the result of new enforcement attention,[64] Compliance has been given an enhanced role in firms' processes for addressing conflicts of interest. While firms have struggled with identifying and managing conflicts of interest for many years,[65] the integration of Compliance into the process is relatively new. In this role, Compliance helps identify and escalate conflicts issues to senior management who, as supervisors, are responsible for resolving the issues.[66] Although Compliance may define a process for escalating or recommending steps for managing or eliminating conflicts, the final management or resolution of a particular business conflict is more appropriately the role of business supervisors.

c) Risk Assessments

In the wake of the financial crisis, regulators consider Compliance an important resource for firm-wide risk assessments. As discussed above, at many firms, Compliance reviews risk controls and performs an independent, broad assessment of a firm's general regulatory risk and, in some cases, reputational risk, while other risk management functions focus on specific credit, finance and operational risks. When firms conduct broad-based risk assessments, Compliance should participate and provide advice on the assessment of regulatory risk.

---

62 *See, e.g., In re AXA Advisors, LLC*, Exchange Act Release No. 66206 (Jan. 20, 2012) (penalizing a broker-dealer for failure to review and supervise redemptions of variable annuities and the account activities of registered representatives on extended disability leave); *In re Wunderlich Sec., Inc.*, et al., Exchange Act Release No. 64558 (May 27, 2011) (penalizing a broker-dealer/investment adviser for, among other things, charging "excessive fees to numerous advisory clients in thousands of separate transactions" that were "primarily due to back-office errors"); *In re Busacca*, Exchange Act Release No. 63312 (Nov. 12, 2010) (upholding penalties against a former president of a broker-dealer for failure to supervise back-office operations with respect to an ineffective third-party computer program used for books and records and customer statement purposes); *E*Trade Clearing LLC*, Letter of Acceptance, Waiver and Consent, FINRA No. 2007009471101 (May 5, 2010) (E*Trade consented to a censure, fine and findings that it committed various back-office failures, including those related to transaction processing, transmission of account statements and segregation of positions).

63 The Dodd-Frank Act, *supra* note 4, amended the Commodity Exchange Act to require CCOs to describe firms' conflict of interest policies as part of the annual certification. *See* Commodity Exchange Act Section 4s(k)(3)(A)(ii).

64 *See SEC v. Goldman, Sachs & Co.*, No. 10 Civ. 3229 (S.D.N.Y. filed Apr. 16, 2010).

65 Stephen M. Cutler, Director, Division of Enforcement, U.S. Securities and Exchange Commission, Remarks Before the National Regulatory Services Investment Adviser and Broker-Dealer Compliance/Risk Management Conference (Sept. 9, 2003) ("The historical success of the financial services industry has been in properly managing [] conflicts, either by eliminating them when possible, or disclosing them. In the long run, treating customers fairly has proven to be good business.").

66 In some firms, Compliance may initially escalate conflicts to a Conflicts Committee that focuses exclusively on creating and maintaining a process for identifying and resolving conflicts of interest.

d) Follow-Up

Not only must Compliance consider the quality of the advice that it provides to business personnel, but in certain instances such as when it becomes aware that significant advice is not being followed, it must also take appropriate measures to follow-up on the advice that it has given. In that regard, Compliance, like all control functions, must take reasonable follow-up action (*e.g.*, escalation) when it identifies red flags. Recent cases, such as *Urban*, show that regulators may not consider a Compliance officer's duties to have been fully discharged once he or she has provided advice. As a follow-up to giving advice, Compliance must determine if it is necessary to escalate an issue through a clearly documented escalation process to senior management or to a higher authority in the firm. Because the facts and circumstances of a particular issue may create internal conflicts of interest for decision-makers, any escalation procedure should consider alternative reporting lines. In any event, it is important to note that follow-up by Compliance is not a substitute for senior management's ownership of supervisory responsibility.

2. Policies and Procedures

The Compliance function advises business principals responsible for establishing and maintaining policies and procedures for a firm's front office, support and control functions, while taking into account a vast array of regulatory rules and requirements related to these functions.[67] While the traditional standard is that policies and procedures should be "reasonably designed to achieve compliance with applicable securities laws and regulations,"[68] recent regulatory actions do not appear to acknowledge this standard. The "reasonably designed" standard, which is reflected in many securities laws and regulations, permits flexibility to allow firms to tailor their policies and procedures to their unique business models.[69] However, some new proposals would introduce exceedingly detailed and burdensome requirements for firms.[70] Going forward, regulators and firms must consider how to meet new requirements while

---

[67] *See, e.g.*, Written Supervisory Procedures Checklist, FINRA, http://www.finra.org/Industry/Compliance/Registration/QualificationsExams/MemberFirms/HowtoBecomeaMember/P009839.

[68] NASD Rule 3010(a) ("Each member shall establish and maintain a system to supervise the activities of each registered representative, registered principal, and other associated person that is reasonably designed to achieve compliance with applicable securities laws and regulations, and with applicable NASD Rules").

[69] *See supra* Part III.A.2 (addressing flexible business structures and reporting lines); *see also* Exchange Act Section 15(g) (formerly 15(f)) ("Every registered broker or dealer shall establish, maintain, and enforce written policies and procedures *reasonably designed, taking into consideration the nature of such broker's or dealer's business*, to prevent the misuse in violation of this title, or the rules or regulations thereunder, of material, nonpublic information by such broker or dealer or any person associated with such broker or dealer") (emphasis added).

[70] *See generally Volcker Proposal*, *supra* note 35. Before the Volcker Rule was proposed, the Financial Stability Oversight Council ("FSOC") released a study in which it recommended that the Agencies "compel banking entities to develop and integrate into current compliance regimes a new, specifically-tailored program of policies, procedures and other controls designed to ensure adherence to the Volcker Rule and facilitate supervision." FSOC, *Study & Recommendations on Prohibitions on Proprietary Trading & Certain Relationships with Hedge Funds & Private Equity Funds*, at 33 (Jan. 2011). The study also recommended specific requirements for internal policies and procedures, and for internal quantitative and other controls. *Id.* at 33-34.

recognizing that different business activities may be governed by competing, and sometimes conflicting, regulatory schemes.[71]

3. Education and Training

Employee education and training have long been components of the compliance program. Recently, and largely in connection with the Dodd-Frank Act, regulators have developed, proposed and adopted new rules and regulatory requirements at an unprecedented pace. This pace has strained the resources of regulators, while creating extraordinary challenges for Compliance. Not only must Compliance stay current on new and quickly changing requirements, but it also must consider how to address each new requirement in a firm's policies and procedures and how to effectively educate and train employees on the requirements. New third-party education programs, including those that use electronic training tools instead of live sessions, though useful, may not be sufficient for all firms, given variances in business models, sizes and resources. From a practical point of view, Compliance also must consider how to avoid training fatigue, which impacts the ability of employees to retain and utilize any newly received information, while simultaneously increasing the amount of training that each employee receives.

4. Compliance Surveillance

As part of a firm's surveillance structure, Compliance functions generally spend significant resources and time on designing and implementing surveillance systems related to financial services regulations. Effective systems now address a very wide range of activities, including the handling of customer funds and accounts, internal and external communications, the use of social media by licensed employees, and overall compliance with the myriad of regulatory rules and requirements that apply to securities firms and their activities.[72] The cost of designing and staffing effective surveillance functions is very high, while the resources available to individual firms to meet the extensive expectations and requirements of regulators are often limited.

a) Designing an Effective System

While firms generally have some flexibility and latitude when designing their surveillance systems, there are certain elements that all systems must address. For instance, each system must have a method for monitoring and testing the adequacy and performance of the system itself, including any system changes or upgrades, and for ensuring the adequacy of credit

---

[71] The expectations of the SEC, FINRA and the Federal Reserve about the Compliance function in firms serve as a prime example of competing regulatory regimes. Where the SEC and FINRA may penalize a firm or its Compliance officers for broadly performing activities or exercising authority that may constitute supervisory functions, the Federal Reserve encourages firms to take a broad, global approach to Compliance and risk management. *See, e.g.*, Federal Reserve Board, *Compliance Risk Management Programs*, *supra* note 37.

[72] Some systems are designed and used by Compliance to conduct surveillance, while others are designed with Compliance's assistance but used by business units and other control functions for surveillance purposes.

and market risk controls.[73] In designing an effective system, firms must consider both the marginal benefits of a particular surveillance system, including the significance of the risks that it will be designed to detect, and the costs of such system. This consideration is complicated by the potential liability associated with designing an effective system, given recent rules that require the CCO or CEO, under advisement of the CCO, to certify as to the adequacy of internal systems and controls.[74]

b) Implementing an Effective System

From a resource perspective, the greatest burdens on firms are often those related to implementing effective surveillance systems – for use by Compliance as well as by business supervisors and other control functions – in the face of changing technology and regulatory expectations. These challenges are compounded by a dramatic increase in new communications platforms and devices that allow employees to engage in both business and personal communications and to store and transmit vast amounts of data from any location. As a result, firms must determine how to effectively monitor all forms of electronic media and how to create and retain records of all communications.[75] Increasingly, enforcement actions are tied specifically to the use of electronic and social media and, undoubtedly, firms will continue to struggle with how to most effectively monitor and limit such dynamic, rapidly evolving modes of communication.[76]

The growing use of algorithmic trading strategies, which is closely tied to a sharp rise in high frequency and high speed trading, also creates significant challenges for firms' ability to monitor trading activity. The Chairman and CEO of FINRA has expressed concern in the ability of firms to monitor and manage algorithmic trading, explaining that "[i]t is not okay to simply allow algorithms to continue to operate without evaluating their results and their impact, their incremental changes over time and how they work in periods of excessive volatility."[77] Rather, firms are expected to both understand and develop testing that can adequately address the risks posed by the use of algorithms.[78] In this regard, because Compliance often lacks the technical

---

[73] SEC Final Rule, Risk Management Controls for Broker-Dealers with Market Access, 75 Fed. Reg. 69,792, 69,801 (Nov. 15, 2010) ("effective controls with respect to financial risk incurred on exchanges and ATSs must be automated and applied on a pre-trade basis").

[74] *See* FINRA Rule 3130 (requiring CEO certification of a firm's compliance and supervisory processes on an annual basis; CEOs are required to meet with the firm's CCO at least once within the 12 months preceding the certification); *see also supra* note 44 and accompanying text (describing new CFTC rules regarding annual CCO certifications).

[75] *Regulatory Notice 11-39, supra* note 50, and *Regulatory Notice 10-06, supra* note 50, provide guidance on the use of social media by registered broker-dealers and their employees. Notably, the guidance recognizes resource and personnel constraints that firms face when implementing effective monitoring and surveillance programs that address the use of social media and that are capable of capturing and retaining records of social media activities.

[76] *See, e.g., Jenny Quyen Ta*, Letter of Acceptance, Waiver and Consent, FINRA No. 2010021538701 (Sept. 29, 2010) (penalizing an individual for investment recommendations posted on a social media website).

[77] Richard G. Ketchum, Chairman and CEO, FINRA, Remarks at the Security Traders Association Annual Conference (Oct. 13, 2011).

[78] *Id.*

expertise to scrutinize the design and operation of algorithmic trading strategies, business line supervisors should be responsible for verifying the operation of algorithms and similar tools. [79]

Compliance functions also must address heightened regulatory requirements regarding firms' relationships and interactions with customers. For instance, a recent proposal to require broker-dealers to assume a fiduciary standard when they provide individualized investment advice, if adopted, may require Compliance to develop more extensive surveillance to test whether business supervisors are performing their duties and whether registered representatives are appropriately interacting with customers. Similarly, recently adopted suitability and "know your customer" rules further complicate firms' obligations to maintain effective surveillance programs by expanding the applicability of the suitability rule to recommended investment strategies and hold recommendations, and increasing the customer information attributes requiring consideration when making a recommendation.[80] These requirements are extremely time and resource intensive.

5. Business Unit Compliance: Review and Testing

As noted in the 2005 White Paper, Compliance also undertakes "look back" reviews of a business unit or function over time, often across multiple activities. These look back reviews are different from the Compliance surveillance activities, discussed above, which focus on contemporaneous or near-contemporaneous views of business activity and often activities of a high volume nature.

Recently, certain regulators have increased their focus on the manner in which Compliance conducts reviews of this nature. The details of these review programs have traditionally been left to the thoughtful discretion of Compliance, and look back reviews have been viewed as one component of a firm's toolkit for an overall and effective compliance program, or more recently, as we discuss later, as one component of a comprehensive risk assessment process. To the extent that regulators are concerned with the independence of Compliance in reviewing these business units (because Compliance also advises them), it should be noted that there are numerous oversight mechanisms that have been, and continue to be, used to address any such concern. These oversight mechanisms include, among others, Internal Audit reviews, division of responsibilities within Compliance, and oversight of Compliance's own management.

It is important to note that these reviews are in many instances designed to be secondary to the business' own system of supervisory reviews. Accordingly, in assessing the robustness of a Compliance program, there should not be a presumption that all areas of business activity should be subject to such a Compliance review. Rather, such reviews arise from (or are part of)

---

[79] European Securities and Markets Authority ("ESMA") has recognized that Compliance should be responsible for providing clarity to business supervisors on a firm's regulatory obligations and policies and procedures so that improper activities can be detected, rather than mastering the technical properties of a trading system or algorithm itself. ESMA, *Guidelines on Systems and Controls in an Automated Trading Environment for Trading Platforms, Investment Firms and Competent Authorities (Final Report)*, at 12 (Dec. 22, 2011).

[80] FINRA Rules 2090 ("Know Your Customer") and 2111 ("Suitability") collectively require that firms use "reasonable diligence" when servicing customer accounts and when determining the suitability of particular investments.

an assessment of the firm's risks and go forward as part of a selective, risk-based plan—a resource-mindful approach increasingly utilized by regulators themselves. These "look back" reviews are one of many controls – which are all discussed in this White Paper – among the full array used in conjunction with any particular business activity or business line.

As firms increasingly add testing initiatives and programs to more traditional reviews of business units undertaken by Compliance and by other control functions, some regulators now require firms to document and to notify the regulator after the firm has concluded, or reasonably should have concluded, that the firm or one of its employees violated any regulatory requirement.[81] FINRA staff, for instance, has indicated that the adequacy of a firm's processes to identify and, where appropriate, self-report violations of securities laws, rules and regulations, will be a primary focus during routine examinations of FINRA member firms.[82] This will likely lead to more examinations of firms' Compliance testing programs and more requests for information related to methodologies employed in internal audits and reviews.

6. Dedicated Compliance Functions

Compliance's "Control Room" has traditionally focused on compliance with Section 15(g) (formerly 15(f)) of the Exchange Act, which requires broker-dealers to have policies and procedures that prevent the misuse of confidential information, certain trading rules, like Regulation M, and beneficial ownership reporting requirements, such as Section 13(g). Recently, the Control Room's mandate at some firms has grown to encompass activities such as chaperoning, conflict clearance and privacy regulations. For instance, some firms have centralized assessments related to Foreign Corrupt Practices Act ("FCPA") and/or AML obligations in a Compliance unit to ensure that these assessments are standardized and thorough, given the high degree of potential risk that these provisions present. The use of centralized Compliance functions varies by firm and often depends upon the level of geographic dispersion of a firm's offices and personnel.

7. Registration, Licensing and Employment-Related Functions

Engaging in "the business of a broker-dealer," including providing investment or securities recommendations or effecting securities transactions for customers, is the main trigger for registration as a broker-dealer with the SEC and applicable regulators.[83] Over time,

---

81 Firms must promptly report to FINRA when they "concluded or reasonably should have concluded that an associated person of the member or the member itself has violated any securities-, insurance-, commodities-, financial- or investment-related laws, rules, regulations or standards of conduct of any domestic or foreign regulatory body or self-regulatory organization." FINRA Rule 4530(b). Although former New York Stock Exchange ("NYSE") Rule 351 required NYSE member firms to self-report violations of "any provision of any securities law or regulation, or any agreement with or rule or standards of conduct of any governmental agency, self-regulatory organization, or business or professional organization, or [] conduct which is inconsistent with just and equitable principles of trade or detrimental to the interests or welfare of the [NYSE]," this provision did not apply to NASD or FINRA member firms that were not also NYSE member firms. Thus, FINRA Rule 4530, which became effective in July 2011 and replaced similar provisions in NYSE Rule 351, applied to FINRA member firms the requirement to self-report certain internal findings for the first time.

82 FINRA, New FINRA Reporting Requirements Rule Webinar (July 20, 2011).

83 Exchange Act Sections 3(a)(4)-(5) and 15(a)(1).

regulators, such as FINRA, greatly broadened licensing and registration categories. As a result, firms face greater administrative and operational costs.[84] Other new requirements relate to specific functions and require that the employee performing the function – even back and middle-office functions – be properly qualified by examination and licensed.[85] Centralizing registration and licensing may reduce risk by ensuring that a single group tracks and manages all registrations and licenses, and allowing the business and human resources functions, upon which the registration function is dependent, to contribute their information to a single source.

8. Internal Inquiries and Investigations

Effective compliance programs include policies and procedures that address the identification and escalation of red flags, as well as a process for disciplining employees who violate firm policies or applicable laws, rules and regulations. A process for conducting internal inquiries and investigations is necessary to resolve red flags. As regulators continue to define the proper role of Compliance professionals in the escalation and disciplinary process, Compliance must consider when its active involvement with management on these issues may cross the line into supervisory activity. Absent guidance from regulators, firms will continue to struggle with these issues for the foreseeable future.

9. Regulatory Examinations and Investigations

Regulators routinely examine firms to ensure that they satisfy applicable laws, rules and regulations, but for many firms, handling the increasing number of requests from multiple regulators has placed Compliance and other resources under tremendous strain. Regulatory requests for information have become increasingly data-intensive and often call for analytical components and conformance with detailed format requirements. Compliance must effectively monitor and track all requests and respond with the requested materials or information in the regulator's allotted timeframe, which may be only a matter of days, to avoid incurring penalties. Timeliness and accuracy of a response is vital to avoid charges of lack of cooperation. The involvement of multiple regulators has also created the risk that any penalty or wrongdoing identified by one regulator may quickly escalate into additional, parallel investigations by other regulators.

---

[84] For instance, research analysts, equity traders and investment bankers are now subject to licensing requirements for their specific functions. *See, e.g.,* NASD Rule 1050(b) (requiring registration as a research analyst if a firm employee is "primarily responsible for the preparation of the substance of a research report or whose name appears on a research report"); *and* NASD Rule 1032(f) and (i).

[85] Even the performance of many traditional middle and back-office functions, such as client on-boarding, now requires that employees are Series 99 licensed. FINRA Rule 1230. FINRA Rule 1230.06 exempts from registration as operations professionals those employees whose activities are solely clerical or ministerial in nature. Clerical and ministerial activities traditionally include administrative activities, such as sending sales literature.

10. Promoting a Culture of Compliance

Senior management is ultimately responsible for promoting a culture of compliance in a firm, and a close working relationship with the Compliance function greatly assists this task.[86] Requirements that CEOs and CCOs certify the accuracy of compliance reports further exemplify the need to bolster the business-Compliance relationship.[87] This can be achieved by clearly memorializing the role of Compliance in a firm's policies and procedures and by defining a reporting structure for supervisory, accountability and escalation purposes. Such an approach lays the groundwork for a strong culture of compliance within a firm.

To further promote a culture of compliance, some firms establish an Ethics function that supports senior management and works closely with Compliance.[88] The Director of the SEC's OCIE has commented that integrating ethics into a firm's compliance program is beneficial both to risk management and to operating an efficient Compliance function.[89] A strong Ethics function may assist firms in promoting honest, fair business practices.[90] While some firms have a combined Ethics/Compliance function, others maintain a separate Ethics function that has a distinct mandate,[91] such as drafting a Code of Conduct that outlines the responsibilities and expectations of firm personnel. Compliance is always in a position to advocate and support a strong Ethics function and Code of Conduct

While firms are taking various measures to promote their cultures of compliance, certain new provisions under the Dodd-Frank Act threaten to be a countervailing force that impedes

---

[86] *See* Carlo V. di Florio, Director, OCIE, U.S. Securities and Exchange Commission, Speech on the Role of Compliance and Ethics in Risk Management, NSCP National Meeting (Oct. 17, 2011) ("Senior management is responsible for reinforcing the tone at the top, driving a culture of compliance and ethics and ensuring effective implementation of enterprise risk management in key business processes.").

[87] While FINRA requires CEO certification, the CFTC requires CCO certification.

[88] *See generally,* Chief Ethics & Compliance Officer ("CECO") Definition Working Group, Ethics Resource Center, *Leading Corporate Integrity: Defining the Role of the Chief Ethics & Compliance Officer ("CECO")* (Aug. 2007) (suggesting "the role that is most appropriate to the corporate CECO such that an organizational ethics and compliance capability can achieve its intended purpose.") [hereinafter *Leading Corporate Integrity*].

[89] *See* Carlo V. di Florio, Director, OCIE, U.S. Securities and Exchange Commission, Speech on the Role of Compliance and Ethics in Risk Management, NSCP National Meeting (Oct. 17, 2011) ("[E]thics is a topic of enormous significance to anyone whose job it is to seek to promote compliance with the federal securities laws. At their core, the federal securities laws were intended by Congress to be an exercise in applied ethics."); *see also SEC v. Capital Gains Research Bureau, Inc.*, 375 U.S. 180, 186-87 (1963) (quoting *Silver v. New York Stock Exchange*, 373 U.S. 341, 366 (1963)) ("'It requires but little appreciation . . . of what happened in this country during the 1920's and 1930's to realize how essential it is that the highest ethical standards prevail'" in every facet of the securities industry.).

[90] Carlo V. di Florio, Director, OCIE, U.S. Securities and Exchange Commission, Remarks at the Compliance Outreach Program (Jan. 31, 2012) ("[A] corporate culture that reinforces ethical behavior is a key component of effectively managing risk across the enterprise. Nowhere should this be more true than in financial services firms today, which depend for their existence on public trust and confidence to a unique degree.").

[91] An Ethics officer's duties may include: overseeing an assessment of organizational risk; establishing objectives for Ethics and Compliance; managing an ethics program; supervising Ethics staff embedded throughout a firm; informing the board of directors and senior management of ethical risks and goals; and implementing a program to monitor the performance and effectiveness of the ethics program. *Leading Corporate Integrity, supra* note 88, at 2.

cooperative efforts within firms. For instance, whistleblower provisions provide a financial reward of up to 30% of penalties and recovered funds to individuals who provide regulators with original information that leads to an enforcement action with sanctions of $1 million or more.[92] These new rules may undermine Compliance's cooperative and remedial efforts and weaken relations between Compliance and business units if individual employees are incentivized to contact regulators, rather than work with Compliance.[93]

11. Chaperoning Function

Serving as an intermediary to internal business communications is not part of the traditional role of Compliance, and the increasing tendency of regulators to turn to Compliance to chaperone such communications as well as communications between firm personnel and experts and/or issuers creates distinct challenges and concerns. In this role, the Compliance professional is charged both with preventing inappropriate information (*e.g.*, material nonpublic information) from being conveyed and inappropriate conduct (*e.g.*, pressuring a research analyst to change a research rating) from occurring. Some of these arrangements inject Compliance into business interactions where Compliance professionals may lack the specific, seasoned business expertise and experience to be effective chaperones.[94] In many instances, this role is more effectively and appropriately executed by business supervisors, and the use of Compliance for this function is an ineffective use of limited firm resources.

12. Compliance Program Assessment—Addressing Emerging Trends

In light of numerous regulatory initiatives and requirements, a firm's compliance program and policies and procedures must be continuously reviewed and revised to ensure that they are current and address all applicable rules and regulations as they are adopted. As new requirements or trends in the priorities of regulators emerge, firms must constantly consider updates to existing business activities and Compliance structures and programs much more frequently than in the past. This requires firms to commit significant resources in terms of time, personnel and money. Firms also must prepare for more in-depth regulatory examinations as FINRA and other SROs strive to ensure that the firms comply with all new requirements.

IV. Observations and Recommendations on the Role of Compliance

Multiple forces have shaped the evolution of the Compliance role since 2005. New regulatory requirements and an overall shift in focus toward greater accountability and control have posed new and significant challenges to Compliance functions and their personnel. While many of these challenges cannot be easily addressed, we conclude by offering some general

---

92 SEC, Final Rule, Implementation of the Whistleblower Provisions of Section 21F of the Securities Exchange Act of 1934, 76 Fed. Reg. 34,299 (June 13, 2011).

93 New whistleblower rules and heightened requirements for firms to self-report internal findings of misconduct may result in firms losing the mitigation of penalties due to cooperative efforts with regulators in the course of an investigation.

94 For instance, a lack of transactional experience may mean that a Compliance professional is unable to "speak the language" of business personnel and, therefore, may misinterpret some aspect of the transaction and fail to identify misconduct.

recommendations to assist firms, Compliance and regulators in fostering a cooperative environment and, ultimately, a more effective role for Compliance.

A. Reconciling the Expectations of Compliance with the Role of Compliance

There is no single solution to reconcile the expected role of Compliance professionals, as viewed by regulators and senior management, with the challenges and realities that they regularly encounter in performing their functions. Generally, regulatory and business interests must be balanced while taking into account the manner in which Compliance's traditional role can be applied to evolving markets and new legal and regulatory obligations. We believe that clearly defined expectations of the Compliance role and strong and cooperative, yet balanced, relationships among the business units and senior management, regulators and Compliance, are essential to shaping the proper role of Compliance moving forward.

1. Business Units and Senior Management

Senior management is responsible for establishing and maintaining a firm's Compliance function and for encouraging a culture of compliance across all levels and departments of a firm. Senior management must ensure that the Compliance function is sufficiently staffed and resourced, in light of a firm's size and business, so that it can satisfy applicable regulatory obligations. We urge senior management to clearly define and memorialize the role and responsibilities of Compliance in a way that allows Compliance to exist and operate independently and without undue pressure from any business unit or other control function. Senior management should also continue to remind employees that "compliance" is the responsibility of all employees and not just Compliance professionals. This message not only bolsters the effectiveness of the Compliance function, but it also enhances the overall culture of compliance at a firm.

Business personnel should be encouraged to seek the advice of, and maintain open lines of communication with, Compliance. Only a cooperative effort will build a foundation of trust between Compliance and business units and enhance a firm's overall culture of compliance by, ultimately, encouraging ethical, responsible and honest business practices.

Although close, cooperative relationships with Compliance are beneficial, senior management must be mindful that they should not assign supervisory or managerial responsibilities to Compliance. Supervisory powers should rest with senior management and line supervisors and should not be delegated, even in limited ways or on a temporary basis, to Compliance. In that regard, the Compliance function should retain the ability to challenge or reject any authority or responsibility that is improperly delegated to it.

2. Regulators

When reviewing Compliance functions within firms, regulators should be aware of, and focus on, the role agreed to and ordinarily undertaken by Compliance professionals.[95] Active involvement in advising business personnel should not transform Compliance professionals into business personnel or line supervisors.[96] Similarly, while a job title (*e.g.*, Compliance Trading Supervisor) or isolated, good faith attempts by a Compliance professional to assist other risk and control areas may be relevant factors in determining the potential liability of a Compliance professional, they should not be determinative. Rather, when senior management or line supervisors are ultimately accountable for overseeing business activities and employees, potential supervisory liability should not be shifted to Compliance.

Regulators should also keep in mind that regulations that effectively deputize Compliance professionals as their agents may eventually weaken the role of Compliance. For instance, a strictly enforced self-reporting regime may have the effect of reducing the effectiveness of Compliance professionals by deterring senior management and other employees from seeking the advice and input of Compliance. This, of course, frustrates the very purpose of Compliance.

We urge greater cooperation and coordination among different regulators, and also among regulators, senior management and Compliance professionals, to work toward greater consistency with regard to the expectations that each group has of Compliance and its functions. To that end, we suggest that regulators, when applying and enforcing new rules and regulations to the securities industry, should consider whether Compliance professionals are being expected to perform oversight roles where they lack the specialized business expertise or supervisory authority within a firm to carry out those responsibilities.

3. Compliance Professionals

The CCO and other Compliance leadership must recognize the consequences that result when Compliance steps out of its traditional role by acting in a supervisory, managerial or similar capacity. Compliance must build a strong relationship with senior management and take a proactive part in ensuring that its role and functions are clearly defined so that it is able to identify and address pressure to expand its activities into supervisory or other roles that are not core to Compliance functions. Compliance professionals should also escalate concerns about gaps in the oversight and control environment to senior management in a timely and appropriate manner, instead of simply trying to fill the gaps themselves.

---

[95] For instance, in assessing potential liability against a Compliance function or an individual Compliance officer for failure to supervise, regulators should consider whether Compliance or the individual under investigation expressly agreed to exercise delegated supervisory authority. Compliance and Compliance personnel should not be held liable for supervisory failures when they are clearly acting within the scope of the Compliance mandate.

[96] *See* Daniel M. Gallagher, Commissioner, U.S. Securities and Exchange Commission, Remarks at "The SEC Speaks in 2012" (Feb. 24, 2012) ("[F]irms and investors are best served when legal and compliance personnel feel confident in stepping forward and engaging on real issues. An overbroad interpretation of 'supervision' risks tacitly deputizing as a supervisor, with concomitant liability, anyone who becomes actively involved in assisting management in dealing with problems. Deterring such active involvement will erode investor confidence in firms, to the detriment of all.").

Compliance leadership and the CCO should encourage strong relationships and open lines of communication with regulators, so that Compliance can assist regulators on a range of matters, including the designing of effective rules, regulations and examination programs that appropriately account for Compliance's proper functions, role in firms, and capabilities and resources.

B. Conclusion

In summary, as new technology, new services and products, and global business models develop at an ever-increasing pace, it is critical that Compliance, senior management and regulators work together to effectively identify, escalate and address risks, and to account for the growing prevalence and complexity of business and outsourcing issues. Without such alignment, it will be difficult for Compliance to respond efficiently to rapidly changing financial markets and related regulatory obligations, as well as the issues described in this White Paper that have persisted since the publication of our 2005 White Paper. By balancing their interests and expectations of the Compliance function, Compliance, senior management and regulators will be able to protect the integrity of the securities industry and financial markets, while promoting good, sound business practices. We hope that this White Paper encourages dialogue among, and enhances the understanding of, regulators, senior management, business personnel and others with respect to the responsibilities and role of Compliance in securities firms.

Acknowledgments

Under the overall direction of SIFMA's Executive Committee, this White Paper was developed by a working group comprised of members of SIFMA's Compliance and Regulatory Policy Committee, the SIFMA Compliance & Legal Society, and Gerald Baker, an Executive Director with the SIFMA Compliance & Legal Society. In addition to the significant time and effort supplied by SIFMA staff and SIFMA membership, we wish to acknowledge the valuable assistance provided by Yoon-Young Lee and Jeremy Moorehouse of WilmerHale, outside counsel for this matter.

Working Group

R. Gerald Baker, SIFMA Compliance & Legal Society

Pamela Cavness, Edward Jones

Scott Cook, Charles Schwab & Co., Inc.

David A. DeMuro, AIG

Louise Guarneri, Credit Suisse

John Ivan, Bank of America Merrill Lynch

Scott Kursman, Citigroup Global Markets Inc.

Yoon-Young Lee, WilmerHale

Jacqueline LiCalzi, Morgan Stanley

Christopher Mahon, AllianceBernstein

James McHale, E*TRADE Financial

Jeremy Moorehouse, WilmerHale

Jill Ostergaard, Barclays

Richard Paley, W.P. Carey Inc.

Howard R. Plotkin, RBC Capital Markets

John Polanin, Macquarie Holdings USA Inc.

Claire Santaniello, Pershing LLC

Kevin Zambrowicz, SIFMA

New York | Washington | www.SIFMA.org