



Securities Industry Association

120 Broadway - 35 Fl. • New York, NY 10271-0080 • (212) 608-1500, Fax (212) 968-0703

1425 K Street, NW • Washington, DC 20005-3500 • (202) 216-2000, Fax (202) 216-2119

www.sia.com, info@sia.com

July 15, 2005

Mr. Philippe Richard
IOSCO Secretary General
Oquendo 12
28006 Madrid
SPAIN

Re: Public comment on *Compliance Function at Market Intermediaries*.

Dear Mr. Richard:

Thank you for giving the Federal Regulation Committee of the Securities Industry Association (“SIA”)¹ the opportunity to comment on the above-captioned consultation report (the “Consultation Report” or “Report”). Broker-dealers in the United States have devoted significant resources over many years in developing robust compliance programs, both to fulfill regulatory requirements and as a good business practice. We applaud the International Organization of Securities Commissions (“IOSCO”) for undertaking this initiative to assist market intermediaries to increase the effectiveness of their compliance programs.

This letter will offer the perspective of broker-dealers in the United States concerning practical issues that the Consultation Report poses for us. We recognize that it is a challenging task to issue statements of general principle extrapolated from the laws of many nations. Our comments are intended to identify for you aspects of the Consultation Paper that may be inconsistent with, or impractical from the perspective of, practices or requirements in the United States, or that do not reflect the nature of compliance functions as they are generally understood in the securities industry in the United States.

¹ The Securities Industry Association brings together the shared interests of nearly 600 securities firms to accomplish common goals. SIA’s primary mission is to build and maintain public trust and confidence in the securities markets. At its core: Commitment to Clarity, a commitment to openness and understanding as the guiding principles for all interactions between investors and the firms that serve them. SIA members (including investment banks, broker-dealers, and mutual fund companies) are active in all U.S. and foreign markets and in all phases of corporate and public finance. According to the Bureau of Labor Statistics, the U.S. securities industry employs nearly 800,000 individuals, and its personnel manage the accounts of nearly 93-million investors directly and indirectly through corporate, thrift, and pension plans. In 2004, the industry generated an estimated \$227.5 billion in domestic revenue and \$305 billion in global revenues. More information about SIA is available at: www.sia.com.

Overview and Summary.

The role and purpose of the compliance function in the United States is rapidly changing and expanding, as it is in other nations. For example, the National Association of Securities Dealers (“NASD”) recently issued a set of new rules detailing a host of new process requirements and standards for broker-dealers’ compliance efforts.² Other initiatives by the SEC and state regulators have also recently changed the compliance landscape.³ These changes prompted SIA’s Compliance and Legal Division to recently issue an extensive White Paper on the Role of Compliance (“White Paper”). The White Paper, a copy of which is attached to this letter, focuses on many of the issues raised in the Consultation Report. In particular, the White Paper discusses the scope and responsibilities of compliance departments in U.S. broker-dealers, and the distinctions between (a) general efforts by firms designed to achieve compliance with securities regulatory obligations, and the specific functions of compliance departments in support of those goals, as well as (b) management’s responsibility to supervise, and the monitoring and surveillance role of compliance departments. Because of the diversity of the broker-dealer community in the United States, in terms of size, resources, and lines of business, both the White Paper and United States regulators recognize that regulatory requirements for broker-dealer compliance programs have to be flexible.

In our responses to the individual questions posed by the Consultation Report we seek to emphasize four key points.

1. We urge IOSCO to adopt a principles-based approach to the requirements for a compliance function. This approach should focus on the characteristics of a sound compliance organization as opposed to cataloguing prescriptively specific requirements or steps that firms

² The new NASD initiatives include, *inter alia* (1) a new rule requiring member firms to designate one or more principals to establish, maintain, and enforce a system of supervisory control policies and procedures that test and verify that the member’s supervisory procedures are reasonably designed to comply with applicable securities laws and NASD rules, *see* Rule 3012, NASD Notice to Members (“NTM”) 04-71, (October 2004), (2) a new rule requiring the Chief Executive Officer (“CEO”) certify annually that the member “has in place processes to establish, maintain, review, test, and modify written compliance policies and written supervisory procedures reasonably designed to achieve compliance with” applicable securities regulations, *see* Rule 3013, NTM 04-79 (November, 2004), as well as requiring each firm to name a Chief Compliance Officer (“CCO”) and for the CCO to meet at least annually with the CEO and other senior management, and (3) more stringent in-house inspections for members’ offices, *see* Rule 3010(c). *See also* NYSE Rule 342 (establishing similar requirements).

³ *See, e.g.*, 68 Federal Register 74714 (Dec. 24, 2003) (Securities and Exchange Commission’s (“SEC”) adoption of new rule 38a-1 under the Investment Company Act and new rule 206(4)-7 under the Investment Advisers Act to require, *inter alia*, that all funds and advisers have adequate written compliance policies and systems for reviewing those policies; Joint Research Settlement between the SEC, National Association of Securities Dealers (“NASD”), New York Stock Exchange (“NYSE”) and the New York State Attorney General (information available at http://www.sec.gov/spotlight/global_settlement/consultlist.htm) (highly detailed regulatory undertakings by several major broker-dealers as part of an enforcement settlement concerning conflicted research).

must take. We believe that in many respects this will address the need for flexibility described above, as well as the following issues.⁴

The Consultation Report tends to blur the distinction between the overall compliance function and the role of a compliance department. For U.S. broker-dealers, the overall compliance function encompasses many control functions that are not typically housed within the compliance department, but instead necessarily reside in other areas of the firm, particularly legal, internal audit, financial control and risk management. In addition, firms may have dedicated compliance departments for certain businesses, or in the case of firms that have multiple regulators, there may be different compliance departments to address the requirements of each regulator. Other than question 2, there is no explicit recognition anywhere in the Consultation Report of the fact that the compliance function is typically fulfilled by more than one arm of a firm, with groups outside of the compliance department exercising a control function.

A related issue is the Consultation Report's view of the independence of the "compliance function." While we fully agree with the principle stated in Topic 3, the suggestion that the "compliance function . . . should report to the board of directors or senior management" unnecessarily limits the flexibility that a firm should have in organizing how it fulfills the compliance function in light of its size, business structure and resources. As noted above, a broker-dealer is likely to have its compliance function divided among the compliance department, the legal department, internal audit and other departments. Some of these departments may report through other units with compliance functions, while others may report directly to the board or senior management. For example, in some firms the compliance department may report to the legal department, while in others the compliance department may report to the chief executive. Either arrangement should be acceptable to regulators, because under either the overall compliance function is able to "operate on its own initiative, without improper influence from other parts of the business."

2. Compliance and supervision are distinct and separate concepts in the regulatory scheme in the United States, which provide that the supervisors in the business are responsible for implementing and enforcing all firm policies and procedures.⁵ Except in rare instances, having compliance responsibility should not imply having supervisory responsibility. The Consultation Report recognizes this in principle (a) under Topic 2, yet it conflates the two in some places, especially Appendix A.

⁴ We note that the Basel Committee on Banking Supervision has adopted such a principles-based approach for the recommendations contained in its paper, 'Compliance and the compliance function in banks' (April 2005). We respectfully suggest that consistency of approach with the Basel Committee paper be considered.

⁵ "The NASD Board of Governors recognizes that supervisors with business line responsibility are accountable for the discharge of a member's compliance policies and written supervisory procedures." IM 3013, 69 Fed. Register 46603, at 46604 (August 3, 2004). *See also* White Paper at 5.

3. The Consultation Report appropriately defines the role of the "compliance function" under principle (b) of Topic 1, yet in several other places it describes the role of compliance as being "to ensure" compliance with all applicable legal requirements. It would be more consistent with Topic 1 principle (b), and more consistent with U.S. law, to describe the role of the compliance function as being to develop and implement systems and procedures reasonably designed to achieve compliance. This clarification is critical to make the Consultation Report both internally consistent, and consistent with well-established supervisory principles and regulatory standards in the United States.⁶ Moreover, as a practical matter, firms need to deploy surveillance resources in a risk-based and cost-effective manner, and any implication to the contrary could create unrealistic expectations by regulators or investors.

4. In at least one place the Consultation Report references as part of the "compliance function" an obligation to have processes to "protect the firm from any liability arising from abuses committed by its customers." This suggested obligation stretches well beyond existing U.S. law. Highly invasive procedures would have to be devised to monitor any aspect of customers' conduct that might conceivably create some liability for the broker-dealer, and these procedures might raise fresh concerns about customer privacy. Due to the elastic and uncertain boundaries of civil liability in the United States, it is unrealistic to think that a broker-dealer could ever design a system that would be certain to catch every type of customer behavior that might create liability exposure for the broker-dealer.

This requirement is especially troubling with regard to "structured finance" transactions with corporate customers, since developing systems to monitor the compliance of sophisticated counterparties with any applicable foreign or domestic law or regulation would be even more prohibitively difficult than for other types of customers. The net effect would be to deter broker-dealers from entering into any structured finance transactions. While a very few of these types of transactions have been the subject of well-publicized abuses and law enforcement actions in the United States, the vast majority serve very legitimate economic functions and provide critical liquidity and risk exposure protection.

Responses to Questions.

1. Do you agree with the definition and description of the scope of a compliance function? Please explain.

Answer: *Scope of the Term "Compliance Function."* SIA agrees that the definition of "compliance function" as stated on page 6 of the Consultation Report is appropriate, as far as it goes, to characterize the overall objective of a firm in seeking to achieve compliance with securities regulatory requirements. However, we see at least three respects in which the definition could go farther or be more explicit.

⁶ For example, NASD Rule 3013(b) requires an annual certification from the chief executive officer of each broker-dealer that the firm has in place policies and procedures "reasonably designed to achieve compliance with applicable NASD rules, MSRB rules and federal securities laws and regulations."

First, except for the risk management function, the Consultation Report does not explicitly recognize that these compliance functions can, and usually do, reside in several locations within a firm in addition to the compliance department. It is important to note that the “compliance function” must be fulfilled by more than one arm of a firm. Depending on a firm’s size, organizational structure and type of business, both Compliance Department reporting lines and the allocation of compliance-type functions can vary. Consequently, it is not uncommon for professionals outside a Compliance Department to have responsibility for many of the “Compliance Functions” to which the Consultation Report refers. For example, as a matter of practice, oversight of a firm’s activities relating to the firm’s financial controls and compliance with regulatory financial reporting requirements usually reside with the broker-dealer’s Controller, Chief Financial Officer or Treasurer, and may be reviewed by the Internal Audit Department. Similarly, a member firm’s systems and procedures for assuring compliance with margin regulations and the clearance and settlement process is typically the responsibility of the firm’s Chief Operations Officer. In addition to the compliance department and risk management department, other groups that typically carry “compliance functions” include the comptroller’s or treasurer’s office, the legal department, the credit, finance, internal audit and operations departments, and in some firms the human resources department. In addition, in many firms, control function officers with specific monitoring and surveillance or financial control responsibilities are often located within individual business units.⁷

Second, the definition and description also does not draw a clear distinction between the compliance function and supervision. As explained in the White Paper, there is a huge difference between the role of the Compliance Department and its personnel, and the overall broad firm responsibility ‘to comply’ with applicable rules and regulations. “The Compliance Department plays an integral support function for firm compliance programs, but only senior management and business line supervisors are ultimately responsible” for the effectiveness of the firm’s compliance program.⁸

Third, the definition and description does not recognize education as a compliance function, along with identifying and preventing violations of regulatory requirements.

Mechanisms Regarding Customer Activity. SIA respectfully disagrees with one aspect of the description of the scope of a compliance function, the statement on pages 6-7 that “[a] compliance function of a firm should also have mechanisms in place to protect the firm from any liability arising from abuses committed by its customers.” Broker-dealers in the United States have a well-established obligation to “know their customers,” as well as an obligation, imposed on all U.S. financial institutions, to look for and report on potential money-laundering activity.

⁷ A discussion of the roles and interrelationships between many of these groups is contained at pages 16-19 of the White Paper.

⁸ White Paper at 20.

U.S. law also clearly proscribes broker-dealers from colluding with customers to violate the law.⁹ However, the above-quoted statement is much broader, suggesting an open-ended surveillance/investigatory obligation of customer behavior, including behavior away from the broker-dealer, in case that customer's behavior in some respect could give rise to "any liability" for the broker-dealer because of any "abuses committed" by a customer. Due to the fluid scope of private civil liability in the United States,¹⁰ it will be difficult for a U.S. broker-dealer to rule out any prospect of liability for almost any conceivable transgression that a customer might commit that touches in some way upon the customer's account or relationship with the firm. Putting "mechanisms in place to protect the firm from any liability arising from abuses committed by its customers" is therefore unrealistic, and even if it were achievable would be extremely intrusive for customers, giving rise to a host of potential privacy concerns.

This suggestion is particularly troubling with regard to structured finance transactions. These transactions provide an important source of capital and liquidity for many capital- and credit- intensive financial products and operations, and are also an important complement to risk management tools. Especially since they involve sophisticated counterparties, a customer's compliance with applicable accounting, disclosure, tax and other legal requirements for these transactions is generally the responsibility of that customer, its management and advisers. As noted above, there will seldom be complete *a priori* certainty that a customer's failure to meet one of these legal requirements might not create some type of legal exposure for the broker-dealer counterparty. If as a consequence of that uncertainty, a broker-dealer must design and implement "mechanisms" to monitor its client's compliance with every conceivable applicable regulatory obligation, the costs and practical obstacles would be such that financial institutions or their client companies may curtail otherwise legitimate complex structured finance activities for which financial institutions cannot practically or cost-effectively satisfy the responsibilities proposed.

2. What is the relationship between the compliance function and risk management function? For example, is the compliance function part of or separate from the risk management function; and if they are separate, how do they interact when dealing with compliance issues?

Answer: As this question implies, there is an overlap between the compliance function and the risk management function. Compliance risk has become an integral part of a firm's overall risk management program, and therefore compliance functions may be seen as integral to the

⁹ The SEC has, among other powers, administrative authority to suspend or revoke the registration of a broker-dealer that "has willfully aided, abetted, counseled, commanded, induced or procured" the violation by another person of any of the federal securities laws. Exchange Act Section 15(b)(4)(E).

¹⁰ The vast majority of customer accounts in the United States are held at broker-dealers that are national in scope, and therefore subject to the separate and varying legal liability standards and regulatory requirements of 50 states, in addition to federal regulatory requirements.

organization's program for risk management.¹¹ Consequently, the White Paper recommends that Compliance Departments "should be alert to risk issues and, if identified, bring them to the attention of Risk Management and work with them in developing remediation steps."¹² Similarly, the risk management function should be informed of compliance risk issues identified by either the legal or internal audit departments. Generally, the role of the compliance function is to assist in development of policies and procedures designed to comply with regulatory requirements and to monitor and advise on the effectiveness of those policies and procedures. Risk management, which is typically closer to the business side, should help harmonize business practices, plans and objectives with these policies and procedures.

It is also important to note that the risk management function is often subdivided between specific activities, such as trading and financial exposure, as well as enterprise-wide risks.¹³ These roles may each have their own individual relationships with the compliance function.

3. Should a specific organizational structure for compliance be prescribed? Please explain.

Answer: No. The compliance function is shared among various units of a firm, and the appropriate structure will vary greatly according to the size, resources and business needs of a particular firm, as well as the different regulatory requirements applicable to banks and broker-dealers. Compliance departments within firms will have different structures for these same reasons. Compliance departments may report to the legal department, risk management function or directly to the chief executive, and may operate in a centralized manner, across functional lines or across business units, or be divided according to business unit. For this reason, regulators in the United States have avoided prescribing structure or reporting lines. The internal audit department rather than the compliance department may review other departments that handle elements of the "compliance function," such as the unit that handles regulatory financial reporting.

These illustrations demonstrate that firms need flexibility to design compliance structures that match their individual size and business model. For this reason, we are concerned that the suggestion in Topic 3 that the "compliance function . . . should report to the board of directors or senior management" will result in regulators becoming hostile to arrangements such as these noted above, even though they have evolved due to the practical requirements of individual firms and have proven effective. The critical point is that officers with ultimate responsibility for

¹¹ Risk management assessment is now being carried out as part of the SEC's examination program. See Mary Ann Gadzialla, Remarks Before the 5th Annual Regulatory Compliance Conference for Financial Institutions (Sept. 24, 2003).

¹² White Paper at 19.

¹³ There are areas (e.g., management, audit and operations) that can carry out both compliance and risk management functions).

compliance functions should have direct access to the Board or senior management, since those individuals bear ultimate responsibility to see that compliance functions are carried out.¹⁴

4. Are there any essential roles, responsibilities or activities for the compliance function that should be mandated or otherwise identified by regulators?

Answer: There are a large number of compliance functions that are required by regulators in the United States, and that we believe should be universally required. These include: education and training, insider trading monitoring, trade surveillance, anti-money laundering functions, data privacy, net capital and financial responsibility compliance. Of these, education and training stands out as a key role for the Compliance function: to be proactive in addressing legal and regulatory developments and to assist senior management of the firm in preventing possible violations by raising awareness within the firm of applicable legal and regulatory requirements.

It is important to stress that not all of these compliance functions necessarily belong in the compliance department, and that other units bear primary responsibility for many of these compliance functions, as described in Answer 1 above.

5. Please identify responsibilities other those described above that are carried out by the compliance function at market intermediaries.

Answer: Other responsibilities of the compliance function (though not necessarily the compliance department)¹⁵ that are not specifically identified in the Consultation Report (although perhaps implicit in some of its discussion) include:

- Education and training to keep business personnel and other employees apprised of policies, procedures, and regulatory requirements. This training should involve both regularly scheduled updates as well as additional sessions on an as-needed basis to implement new policies or procedures or to communicate recent regulatory developments. The format of this training should be flexible, and can include web-based or other electronic training modules as a supplement to in-person training, as well as enhanced training on an as-needed basis for business unit supervisors as well as for new hires;
- Licensing and registration of the firm and its registered personnel are another common compliance function, together with the related role of advising senior management on

¹⁴ Both the NYSE and the NASD require annual compliance reports to the CEO, and the NASD requires an annual certification from firms' chief executive officers as to compliance. See NYSE Rule 342, NASD Rule 3013.

¹⁵ As noted in our response to question 1, many compliance functions may be fulfilled by more than one arm of a firm. For example, education and training may involve personnel from human resources, the legal department or business management, in addition to, or instead of, the compliance department. Likewise, licensing and registration may not necessarily be performed by a compliance department, but might instead involve the legal department or human resources department.

disciplinary issues, including terminations.¹⁶ Some of these functions may be performed jointly by the compliance department and human resources department;

- Internal inquiries and investigations are a critical compliance function that is not explicitly addressed in the Consultation Report. This role can be played by any or a combination of several control functions within a firm, including the compliance department, the legal department, internal audit or other control areas. These inquiries sometimes involve the use of third parties such as law firms or forensic accounting experts if deemed necessary by senior compliance personnel;
- Monitoring and surveillance of business units to identify potential issues is another important area of the compliance function. This monitoring applies to, among other things, handling of customer accounts, proprietary trading, and employee-related trading and communications; and
- Participating in industry committees and working groups organized by industry trade associations such as SIA, or self-regulatory organizations such as the NYSE or NASD.

Several additional responsibilities of the compliance function are discussed throughout our White Paper. Many of these functions can be shared between different departments of the firm that exercise control functions.

6. How and when should the compliance function be responsible for managing compliance risk?

Answer: See answer 9 below.

7. Are there any practical concerns for requiring documentation of policies and procedures for smaller, less complex, market intermediaries? Please explain. If policies and procedures should be documented, what degree of detail should regulators expect to see for smaller, less complex, market intermediaries?

Answer: See answer 9 below.

8. Please describe the level of accountability for compliance at your firm for each of the following: board of directors, senior management, designated compliance officer, business unit personnel, where applicable. For example, in the case of the failure to establish proper procedures to prevent sales practices violations, who would be accountable and what would be the extent of their accountability? Please explain your answers.

¹⁶ In relation to this function, we are concerned with the statement on page 8 of the Consultation Paper that one aspect of the compliance function is to “enforce” compliance policies and procedures. It might be more accurate to state that the compliance function advises senior management on the enforcement of policies and procedures, since the final authority to determine disciplinary sanctions against personnel, including termination, resides with senior management, not with the compliance function.

Answer: See answer 9 below.

9. Do you distinguish among responsibility, accountability and liability? Please explain.

Answer: We will answer questions 6-9 collectively, since they are all closely related. The role of the compliance function is to assist in designing compliance policies and procedures and to monitor, test and advise on the effectiveness of those policies and procedures, rather than to “manage” compliance risk. The responsibility for managing (i.e., implementing and supervising) all aspects of the compliance function belongs to senior management.

Documentation of policies and procedures needs to be flexible in light of the resources available to firms of varying sizes. A single compliance manual may be appropriate for a smaller, less complex firm, while a larger firm with multiple business lines might require separate documentation of differing policies among different business units or different geographic units. No single prescription for how best to organize documentation of policies is appropriate. The goal for every organization must be to strive for no gaps between the procedures put in place and the regulatory requirements that apply, and to update these procedures as necessary, but different approaches work best depending on the size, structure and business lines of the organization.

Responsibility refers to an individual’s duties within an organization. Accountability concerns how an organization tracks the performance of those duties and imposes consequences for successfully or unsuccessfully performing them. Liability refers to the regulatory or other legal consequences that can follow when responsibility or accountability break down. Responsibility can be delegated within a firm, and firms should be given wide latitude to delegate responsibility for compliance functions as they see best (as discussed in more detail in answer 1), but accountability and liability cannot be delegated.¹⁷ Within a broker-dealer, these terms can be applied as follows: the board of directors and senior management are ultimately accountable, with respect to the entire firm. Business unit managers have accountability with respect to their particular units. Compliance officers are responsible for creating policies and procedures that are reasonably designed to achieve compliance. They are not generally responsible for implementation of these policies and procedures (except for specific policies where the compliance department has a specific role as executor) and some responsibility for monitoring implementation of the policies (often shared with business units).

10. Should a senior officer be designated for the day-to-day compliance responsibility? Please explain.

Answer: Yes. In the United States, NASD Rule 3013 now requires firms to designate a chief compliance officer. However, senior management has the ultimate responsibility for establishing

¹⁷ For example, under the federal securities laws there are well-established principles of control person and supervisory liability, which cannot be delegated from those who are potentially subject to that liability. *See, e.g.*, Section 15, Securities Act of 1933, Section 20, Securities Exchange Act of 1934.

and maintaining a firm's overall compliance effort.¹⁸ This is appropriate, since business line managers have the responsibility to oversee business operations, and the authority to control employee activity to achieve compliance with applicable regulatory requirements. In this regard, the Consultation Report should recognize the central role of senior management in ensuring an effective compliance program. For example, the statement on page 8 of the Report that the compliance function should "enforce effective compliance policies and procedures" could create the false impression that compliance personnel have the authority to discipline all other firm personnel. The ability to terminate or otherwise discipline employees is held by senior management, although compliance personnel often play an important advisory role on such discipline. Therefore, it would be more accurate to say that the compliance function "advises on the enforcement" of compliance policies and procedures.

11. What requirements relating to independence and ability to act are relevant to a small firm?

Answer: Allowances should be made for businesses that are owned or operated by just a few people. For example, the NASD permits the compliance function to be performed by the business owner/principal if a firm only has one such person. Regulators can ensure proper sales and business practices in a "one person" type environment in the same fashion they do for larger organizations - routine audits. It may be necessary or preferable for the audit cycle to be more frequent in this type of scenario to allay the fears and special challenges presented by self-compliance. Due to the size of the firm, the audits should be fairly short in term. In addition, at smaller firms the Chief Compliance Officer may have additional responsibilities.¹⁹ However, supervisors cannot supervise themselves.

12. In cases where individuals perform both business and compliance activities, should they be allowed to supervise their own business activities? If so, how can the regulators ensure that they supervise their own business activities in an objective manner?

Answer: We agree that individuals performing both business and compliance activities should not have compliance responsibilities for their own business activities. This follows from the general principle that compliance should not report to a business unit.²⁰ However, the term "supervision" requires some refinement. There is an important distinction between having compliance responsibility and having overall business responsibility. The NASD, for example, has taken pains to note that compliance responsibility and business line supervision are separate

¹⁸ See note 5, *supra*. Recently adopted NASD Rule 3012 requires that member firms designate and specifically identify one or more principals who will establish, maintain, and enforce supervisory control procedures that test and verify that the member's supervisory procedures are sufficient.

¹⁹ See White Paper at 3-4.

²⁰ *Id.* at 3.

concepts, with the latter “accountable for the discharge of a member’s compliance policies and written supervisory procedures.”²¹

13. Are the means for implementation of independence set out above sufficient to achieve independence? Please explain.

Answer: SIA largely agrees with the definition of compliance independence stated in Topic 3. Specifically, we agree that the compliance function should operate on its own initiative, without improper influence from other parts of the business, and that it should have direct access to the board of directors and senior management. However, as detailed in our response to question 3, we question the statement that the compliance function “should report to the board of directors or senior management.”

We also agree with the following points from the narrative discussion:

- (a) the budget for the compliance function and compensation for compliance personnel, while linked to the performance of the firm as a whole, should not be directly dependent on the financial performance or revenues of a specific business line, product or transaction overseen by that compliance function or employee;
- (b) compliance personnel should have access to any employees, records and other information necessary to carry out their responsibilities; and
- (c) compliance personnel should have unrestricted access to the board of directors and senior management to discuss significant compliance matters.²²

We do not understand the meaning of the statement “The independence of the compliance function may also be undermined if the tenure (i.e., prospects of staff, position) of compliance personnel is dependent on the business lines.” If this means that independence is compromised if promotion decisions about anyone involved in compliance functions over a particular business unit can be made or influenced by that unit, we fully agree. If it means that compliance personnel are immune from hiring or wage freezes, or even layoffs and salary reductions, due to a downturn in the firm’s overall business lines, then this statement is in conflict with the prior statement that compliance compensation can be dependent on the firm’s overall performance.

As noted in our response to question 11, barring an individual from exercising compliance oversight of his her business activities is entirely appropriate.

²¹ See IM 3013, note 17, *supra*.

²² A necessary caveat is that the access should be reasonable, and that allowances should be made for a “reporting up” obligation, so that procedures can be in place for junior staff inside departments with compliance responsibilities to report their concerns up a supervisory chain within their department. See Standards of Professional Conduct for Attorneys Appearing and Practicing Before the Commission in the Representation of an Issuer, 17 C.F.R. Sec. 205.1 *et seq.*

14. How do you ensure that compensation of compliance personnel is not subject to undue influence? Please explain.

Answer: Firms should have processes in place, subject to regulatory examinations, reasonably designed to assure that there is no undue influence by business units on any aspect of the performance of compliance personnel. However, input from business colleagues may be solicited as part of the appraisal process for compliance personnel in order to better assess how well a compliance officer is performing his or her advisory function.

15. What are the appropriate qualifications for compliance personnel?

Answer: General standards for qualification of key compliance personnel, including appropriate testing and continuing education requirements, should be established by regulators. In addition, due to the specialized and complex nature of many aspects of the securities business, firms should have the flexibility to set additional requirements for different categories of compliance personnel to meet their individualized compliance needs. Qualifications will vary based on function. While qualification examinations for some compliance functions (such as general compliance supervisors, and research supervisors) currently exist, we do not believe that further specific qualifications need to be set by regulators.

16. Should the qualifications vary depending on functions, responsibility or seniority?

Answer: Yes. Regulatory testing may vary for some compliance functions as noted in answer 15, but beyond this firms are likely to have their own very specific and tailored qualification requirements for particular compliance roles.

17. How do you evaluate the adequacy of courses and training for compliance personnel?

Answer: The NASD and NYSE both have continuing education requirements.²³ Typically, a firm's compliance department will contribute to the development of the firm element of these requirements, and especially the training for compliance personnel. In addition, some firms have a dedicated position for compliance training, and part of this job function includes evaluating the adequacy of courses, including soliciting feedback from course participants.

18. Who, within or external to a market intermediary, is best placed to assess the effectiveness of the compliance function? Please explain.

²³ NASD Rule 1120, NYSE Rule 345A. In addition, there are a wide variety of educational events sponsored by the NASD, *see, e.g.*, http://www.nasd.com/web/idcplg?IdcService=SS_GET_PAGE&nodeId=591 (NASD Institute at Wharton) and the NYSE, *see, e.g.* <http://www.nyse.com/regulation/howregworks/1101074878245.html>. In addition, SIA – most notably through its Compliance and Legal Division's annual three-day conference -- sponsors numerous compliance and regulatory seminars and conferences each year with heavy participation by industry regulators, nearly all of which are focused on providing professional compliance education for the industry, *see, e.g.*, <http://www.siacl.com/events.html>, (current list of Compliance and Legal Division events), <http://www.sia.com/conferences/> (current list of SIA conferences).

Answer: Within each firm, senior management is best placed to perform this function, since senior management has the ultimate authority and responsibility to create and maintain systems and procedures reasonably designed to assure compliance. In addition, a periodic external assessment of the compliance function is desirable. Regulators are in a position to add another dimension to senior management's understanding of the effectiveness of its firm's compliance function by advising the firm of how various aspects of its compliance function compare to other firms of similar size and business profile. Senior management and regulators do not have identical stakeholders. Hence, it is appropriate that they have independent responsibility to assess the effectiveness of the compliance function at a firm.

19. What should be the role of an external party in assessing the effectiveness of a compliance function?

Answer: See answer 22 below.

20. What are the practical concerns of requiring an external party to conduct periodic assessment of a compliance function?

Answer: See answer 22 below.

21. What should be the scope and frequency of the assessment by an internal party and/or external party?

Answer: See answer 22 below.

22. Please identify the methods of monitoring that are the most effective from your perspective and explain why.

Answer: Since questions 19-22 are closely related, we will answer them collectively. Regarding an external review, the White Paper endorses an independent assessment of a broker-dealer's compliance department, and the Internal Audit Division of SIA has published a guide for conducting such reviews. In addition, there is a regulatory requirement that broker-dealers submit to an annual audit of their compliance with financial responsibility rules.²⁴ With regard to internal assessments, both the NASD and NYSE require firms to conduct annual assessments of their compliance programs, and the NASD requires that a firm's chief executive officer certify annually that the firm has processes in place to maintain and review compliance procedures and policies.²⁵

Apart from these areas, a private external audit of the effectiveness of the compliance function is generally not necessary, since that is a function that the SEC, NYSE, NASD and

²⁴ Exchange Act Rule 17a-5(d).

²⁵ See, e.g., NASD Rule 3010 and NYSE Rule 342 (annual assessments), NASD Rule 3013 (annual certification).

other federal as well as state regulators perform through their examination programs.²⁶ The role of these regulators is to examine whether firms have established and maintained policies and procedures reasonably designed to achieve compliance with applicable regulatory requirements. These examinations should be conducted on a frequent basis, based on regulators' judgment of potential risks. Where multiple regulators have oversight of a broker-dealer, it is critical that they coordinate their examination programs and share information to avoid unnecessary duplication and inefficient use of both regulatory and internal compliance resources.

Whether an assessment is conducted by a regulator, a private third party or by firm personnel, it is appropriate to make the assessment based on an evaluation of where the greatest risks to investors or the markets may lie from potential compliance shortfalls. This is important to enable the assessment to have the maximum benefit and avoid wasting compliance or regulatory resources.

The types of monitoring that are most effective depend on the function being monitored. Monitoring activities that might be used include direct interaction with the business unit, review of marketing materials, physical observations of a trading floor, pre-clearance of certain trades, review of internal reports generated by control functions, and various types of surveillance such as review of exceptions identified through real-time or post-transaction analysis.

23. What factors are indicative of a strong compliance culture and a weak compliance culture? Please explain.

Answer: A strong compliance culture is set from the top of the organization. Senior management and the board of directors must demonstrate strong support for the importance of the compliance function to the firm and clearly prioritize compliance goals. Some indicia of a strong compliance culture include:

- Clear communication of compliance priorities to all employees by senior management;
- Sufficient resources devoted to build effective compliance systems;
- Creating incentive structures that reward compliant behavior and penalize behavior that sacrifices compliance principles;
- For firms that have complex organizations or multiple business lines, ongoing reviews of potential conflicts of interest among business lines, products and services, including the effectiveness of systems or procedures to manage or remove those conflicts;
- A willingness on the part of compliance personnel to identify problems independently, work on appropriate solutions to problems that are identified,

²⁶ In addition, broker-dealers are often part of financial institutions subject to examination by other federal agencies, such as the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, the Commodity Futures Trading Commission, and, with regard to some types of asset management advisers, the Department of Labor.

- Active participation in industry trade groups such as SIA that provide an opportunity to share best practices, discuss emerging issues, and help shape effective regulatory policy;
- Giving personnel with compliance responsibilities regular and unfettered access to senior management;
- Having procedures and processes in place to enable the compliance function to operate independently; and
- Having sufficient resources devoted to compliance activities.

24. Are there other means for implementation that we should consider?

Answer: We recommend that the Consultation Report should note that one appropriate means for implementation is to adopt a risk-based strategy of prioritizing compliance procedures, policies and controls so that those that are most critical to protecting customer assets, reducing the firm's financial exposure or fulfilling other important objectives as articulated by regulators receive greater attention than other procedures, policies and controls. Such strategies serve to deploy compliance resources more effectively to maximize compliance.

25. Please identify the specific issues that arise for the compliance function of a market intermediary if it is operating in more than one jurisdiction.

Answer: One common concern is the potential for conflicts among the requirements of different jurisdictions, leading to inefficiency or customer confusion. For example, many jurisdictions have conflicting requirements for disclosures about potential conflicts on research reports, resulting in firms either having to produce separate reports on the same issuer tailored to different jurisdictions, or issue a single research report with a raft of disclosures so dense that the overall document might have little utility for investors. Another common concern is the uncertain extraterritorial reach or effect of some regulatory requirements. Various national regulators have different standards for the threshold of activity with investors in a jurisdiction that triggers that jurisdiction's licensing, examination, or other regulatory requirements.

This dissonance between regulatory requirements is steadily becoming a larger issue as financial services firms become more global in scope. It will require continuing and deepening discussions among regulators around the world to ensure that differences between jurisdictions in regulatory treatment are minimized.

While regulators and firms jointly face these important challenges in the globalized financial services markets, the compliance function of market participants face other challenges as well in day-to-day multi-national operations. One challenge is staying abreast of changes in local regulations, especially in jurisdictions where regulatory changes are not always as transparent or easy to ascertain as they are in other jurisdictions. A second is understanding how local markets operate and how investors in those markets use different products. A related challenge is to have

compliance function personnel in each jurisdiction who have facility with the language spoken in that jurisdiction.

26. What are the effective means to ensure that you or your related entities are complying with securities regulatory requirements in all jurisdictions you and your related entities operate? For example, local and/or centralized compliance function?

Answer: We respectfully question the premise that the goal of a compliance function is to “ensure” compliance with any jurisdiction, since as noted in our overview and summary above, it is misleading and inconsistent with U.S. law to suggest that compliance can ever be a guarantor against any regulatory violations.

There is no single “right” model for designing adequate compliance in all jurisdictions, and firms need flexibility to design a structure that works for their relative sizes of operations in various jurisdictions, and their varying ability to implement effective oversight from another jurisdiction. As a general matter, there will be a need to hire some local or regional compliance staff in the jurisdictions in which the firm does business, particularly with regard to legal advisors. Firms take many different approaches regarding the allocation of responsibility between local personnel and regional or global compliance personnel, and no one approach can be said to be superior to another for all firms.

Conclusion.

Thank you for giving us the opportunity to respond to this important Consultation Report. Please feel free to contact George Kramer of the SIA staff at 202-216-2047, or gkramer@sia.com, if you have any questions about this letter or would like more information.

Sincerely,

Carlos M. Morales
Chair, SIA Federal Regulation Committee

Attachment

cc: Ethiopis Tafara, Director, SEC Office of International Affairs
George Lavdas, Senior Special Counsel - International, SEC Division of
Market Regulation
Ira D. Hammerman, General Counsel - SIA