COMPLIANCE FUNCTION AT MARKET INTERMEDIARIES

FINAL REPORT

A REPORT OF THE
TECHNICAL COMMITTEE OF THE
INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS

MARCH 2006

Preamble

The IOSCO Technical Committee Standing (TC) published for public consultation in April 2005 a Consultation Report on *Compliance Function at Market Intermediaries.*[1] The Consultation Report set out a number of supplementary principles with measures for implementation to assist market intermediaries to increase the effectiveness of their compliance function. Following the receipt of comments by the public, the IOSCO Technical Committee Standing Committee on the Regulation of Market Intermediaries revised the Consultation Report and the IOSCO Technical Committee approved the final Report during its February 2006 meeting.

[1] Available at: http://www.iosco.org/library/pubdocs/pdf/IOSCOPD198.pdf.

Key terms

In this report, the following terms are used with the following meaning:

Compliance function: The term "compliance function" is used as a generic reference to refer to the range of roles and responsibilities for carrying out specific compliance activities and responsibilities.

Governing authority: The term "governing authority" is used to refer to, for example, the board of directors, the general partner of a partnership, the supervisory board in jurisdictions that have a dual board structure, and the board of auditors. In some countries, the board of directors has the main, if not exclusive, function of supervising the executive body (e.g. senior management, general management) so as to ensure that the latter fulfils its tasks. For this reason, in some cases, it is known as a supervisory board. This means that the board has no executive functions. In other countries, by contrast, the board has a broader competence in that it lays down the general framework for the management of a firm. Furthermore, in some countries, there is an additional statutory body which audits the directors' execution of their duties.

Senior management: The term "Senior management" means the persons who direct the business of the market intermediary.

Reporting / Notification: The term "Reporting" is used to refer to reporting within a market intermediary. The term "Notification" refers to reporting externally to third parties, such as regulators. See topics 1 and 2 for discussion on reporting obligations and topic 6 for discussion on notification obligations.

Policies and procedures: The term "policies and procedures" is used in a general sense to include, among other things, procedures for supervision and procedures on required and prohibited activities. Some market intermediaries have different sets of policies and procedures for different purposes or for different users. For example, some intermediaries may have one set of policies and procedures that outline guidelines with respect to required and prohibited actions under the regulatory framework, a second set that outlines the supervisory structure for the business units, and a third set that describes the activities of the compliance function.

I. Introduction

The purpose of this paper is to review existing IOSCO principles and establish broad supplementary principles in the area of compliance. Compliance is intrinsic to the operations of market intermediaries because they must have systems or processes in place to help ensure that they are complying with all applicable laws, codes of conduct and standards of good practice in order to protect investors and to reduce their risk of legal or regulatory sanctions, financial loss, or reputational damage.[2]

Market intermediaries should conduct themselves in a way that protects the interests of their clients and helps to preserve the integrity of the markets.[3] They must comply with all regulatory frameworks in which they operate. Compliance with securities laws, regulations and rules[4] (referred in this paper as "securities regulatory requirements") is part of the essential foundation of fair and orderly markets as well as investor protection. It is equally important, however, that firms develop a business "culture" that values and promotes not only compliance with the "letter of the law," but also a high ethical and investor protection standard.

Market intermediaries have become more innovative on how they structure their businesses in order to maximize profits and provide different services to their clients. For example, there has been unbundling of services to clients, partnering with other firms to meet all the needs of their clients, and outsourcing to other parties. The complexity of their business has increased, making the burden of the compliance responsibility heavier. To be compliant with all laws, regulations and rules has become both increasingly important as well as more challenging.

Although different jurisdictions may have different approaches and policies to help ensure compliance with their securities regulatory requirements, they share a common belief that the compliance function at market intermediaries plays an essential role in preventing possible misconduct and in promoting ethical behavior, which in turn can contribute to fair and orderly markets and investors' confidence in the markets. Moreover, compliance is not the responsibility solely of those performing an official "compliance function." It is a matter for which the firm and all its employees have responsibility.

In this Report, we have avoided, to the extent possible, referring to internal structures (such as Departments) recognizing the diversity of size and type of securities firms and have used the term "compliance function" as a generic reference to the range of roles and responsibilities for carrying out specific compliance activities and responsibilities.

---

[2] IOSCO. Objectives and Principles of Securities Regulation. May 2003: Section 12.5.
[3] IOSCO. Objectives and Principles of Securities Regulation. May 2003: Section 12.5.
[4] These include laws, regulations and rules promulgated by the legislature, regulators and self-regulatory organizations (SRO).

Principle 23 of the Objectives and Principles of Securities Regulation for market intermediaries states that:

> Market intermediaries should be required to comply with standards for internal organization and operational conduct that aim to protect the interests of clients, ensure proper management of risk, and under which management of the intermediary accepts primary responsibility for these matters.

Although IOSCO acknowledges that the internal organization of a market intermediary will vary according to its size, the nature of its business and the risks it undertakes, the market intermediary should still have a compliance function. Specifically, IOSCO notes that a market intermediary's compliance with securities regulatory requirements and internal policies and operating procedures and controls should be monitored by "a separate compliance function".[5]

In addition, the Methodology for Assessing Implementation of the IOSCO Objectives and Principles of Securities Regulation supporting Principle 23 focuses on management and supervision and internal controls, and their roles in a market intermediary's compliance. It considers accountability, adequate internal structure and controls, and monitoring of the effectiveness of the procedures and controls as key issues.[6]

* * *

Given the increased focus on compliance by regulators in different jurisdictions, the TC prepared this paper to set out a number of supplementary principles to Principle 23 with means for implementation to assist intermediaries to increase the effectiveness of their compliance function. This report is based on a survey of current regulatory requirements in the jurisdictions of SC3 members, supplemented by the comments received on the consultative version of this report. Since IOSCO members only have jurisdiction over the securities activities of market intermediaries, this Report places the focus on the securities regulatory requirements of these intermediaries. However, IOSCO expects market intermediaries to comply with all applicable regulatory requirements. It should also be noted that, to the greatest extent practicable, the principles set forth in this report are consistent with those developed by the Basel Committee,[7] since banks are also involved in the securities markets and subject to securities regulation.[8] The principles set forth in this paper are intended to be sufficiently flexible to adapt to the nature, scale and complexity of a market intermediary's business and operations, and in particular according to the level of risk that the firm's activities entail, both for the financial system

[5] IOSCO. Objectives and Principles of Securities Regulation. May 2003: Section 12.5

[6] See items 1, 2 and 7 of the Key Issues section in the IOSCO's Methodology for Assessing Implementation of the IOSCO Objectives and Principles of Securities Regulation (October 2003).

[7] Basel Committee on Banking Supervision. *Compliance and the compliance function in banks* (April 2005). Available at: http://www.bis.org/publ/bcbs103.pdf

[8] In addition, some countries have applied Basel principles, which are aimed at internationally active banks, to other categories of market intermediary.

as a whole and for the firm's clients. Even where a market intermediary has a small operation with a simple business, it should consider the appropriateness of adopting the means for implementation outlined under each principle.

II. Principles and comments

Topic 1: Establishing a Compliance function

Principles:

(a) Each market intermediary should establish and maintain a compliance function.

(b) The role of the compliance function is, on an on-going basis, to identify, assess, advise on, monitor and report on a market intermediary's compliance with securities regulatory requirements and the appropriateness of its supervisory procedures.

In this paper, "compliance function" is used as a generic reference to the aggregate of roles and responsibilities for carrying out specific compliance activities and responsibilities. The expression does not intend to denote any particular organizational structure, recognizing the diversity of size and type of securities firms. The definition is similar to the definition of "compliance function" for banks by the Basel Committee. Although a market intermediary has a compliance function that is responsible for carrying out specific activities, compliance is the responsibility of everyone within the firm.

Other than *monitoring* for compliance with securities regulatory requirements, a compliance function should also engage in the *identification* and *prevention* of violation of these securities regulatory requirements. This is the pro-active role of the compliance function. For example, a compliance function may be involved when considering new business lines. In this case, the compliance function will be involved in compliance risk management. Compliance also speaks to the culture and ethics of a market intermediary, and is an important tool in managing the risk of legal or regulatory sanctions, financial loss, or reputation damage resulting from violation of regulatory requirements. Where a firm has obligations to report or prevent abuses by customers, the compliance function should also have mechanisms in place designed to assist the firm in meeting those obligations.

Market intermediaries range in size from one person firms to multi-national organizations, and they may conduct a simple business offering limited services and products or multiple businesses of significant complexity. A market intermediary should consider the nature, scale and complexity of its business and the risks it undertakes when establishing its compliance function, including:

- The products and services it offers;
- The characteristics of its clients, for example retail or institutional;
- The structure and diversity of its operations (including the geographical spread of and the regulatory requirements applicable to its operations); and
- The number of people that it engages to conduct its business.

To the extent it is permitted by legal requirements, market intermediaries operating as part of a financial conglomerate may centralize their compliance function taking into account the business operations and compliance systems established by the parent company or other entities within the conglomerate (hereafter referred to as centralization[9]).

In larger firms, the activities generally performed by the compliance function may not necessarily be fulfilled by the compliance department but by other departments, such as legal or financial control and risk management departments. In addition, market intermediaries may choose to organize their compliance function in dedicated compliance units for certain businesses. In larger firms too, reporting to senior management or the governing authority may be done directly or via other control functions such as risk management (see topic 2).

The expectations of regulators with regards to the scope, structure and activities of the compliance function will not be the same for full service market intermediaries that conduct complex businesses and for smaller market intermediaries that conduct a single service.

Means for Implementation

(a) An effective compliance function should have the necessary authority and resources[10] to properly discharge its functions.

(b) The scope, structure and activities of the compliance function should be proportionate to the nature, scale and complexity of a market intermediary's business. The compliance function should generally perform the following:

(1) Identify the regulatory requirements imposed on the market intermediary;

(2) Establish, communicate, monitor and enforce effective compliance policies and procedures to address regulatory requirements;

(3) Provide information to the governing authority and/or senior management on applicable laws and regulations to assist them with their compliance responsibilities, in particular with their responsibilities for managing compliance risk;

(4) Provide assistance, guidance and/or training to business units and staff in relation to compliance;

[9] In some jurisdictions this concept is referred to as consolidation of the function rather than centralization.
[10] Some larger market intermediaries may consider using technology or automating their process to increase the efficiency of the compliance function. For example, some firms may have systems designed to highlight unusual activities and to track outstanding compliance matters.

(5) Report periodically to the governing authority and senior management on the market intermediary's overall compliance with securities regulatory requirements and internal compliance policies and procedures, including significant breaches; and

(6) Where required by law or regulation, notify regulators, in a timely manner, of any material breach by the firm of securities regulatory requirements; where notification is not required by law or regulation, notify, when appropriate, the regulators of any misconduct by the firm and the firm's actions with respect to such misconduct, including efforts to prevent future violations.

(c) Roles and responsibilities need to be clear and identified whether the compliance function resides in one department or in different parts of the organization.

(d) The mandate of the compliance function should be communicated to appropriate individuals within the firm; and depending on the size and nature of the business, should have formal documented status.

(e) The market intermediary should encourage staff to consult with compliance personnel regarding compliance with securities regulatory requirements. For this purpose, staff should be made aware of how to consult with the compliance function.

Topic 2: Role of Senior Management and the Governing Authority

Principles:

(a) It is the role of senior management to establish and maintain a compliance function, and compliance policies and procedures designed to achieve compliance with securities regulatory requirements.

(b) The governing authority should obtain adequate assurance that senior management is carrying out this role effectively.

This principle deals with the role of senior management and the governing authority, but is not intended to address their legal liability, which may vary depending on the jurisdiction.

Where there is an obligation on a firm, the firm will need to organize its internal affairs to enable it to meet this obligation. As explained below, how firms do this is primarily a matter for the firm, but the regulator will be interested in these internal arrangements and will want to have confidence that they are effective.

In this paper, we set out certain features which regulators regard as particularly important, because they indicate that compliance with regulatory requirements is afforded appropriate priority by the firm.

Business units also have a role with respect to compliance, such as monitoring their compliance with applicable controls, policies and procedures, in order to conduct their operations in accordance with regulatory requirements. They are assisted by those performing the compliance tasks.

Those performing the compliance activities and responsibilities assist senior management by identifying issues, making recommendations, and implementing the solutions chosen by senior management. They also assist the governing authority through presentation, directly or indirectly through senior management, of information regarding compliance so that the governing authority can perform its oversight function.

Due to differences in their size and internal organization, market intermediaries will employ different structures to ensure compliance with securities regulatory requirements. Placing responsibility on the senior levels of management enables accountability and promotes a compliance culture, by ensuring that the compliance function is given a proper level of attention within the organization and that appropriate resources are devoted to the compliance function.

Means for Implementation

(a) Senior management[11] should consider the following:

- Designating a senior officer, who has the appropriate competence, to have the day-to-day responsibilities for the intermediary's compliance with securities regulatory requirements,
- Being available to compliance personnel to discuss material compliance issues,
- Assessing on a regular basis the overall compliance of the market intermediary, including its adherence to internal compliance policies and procedures and the effectiveness of its compliance function,
- Ensuring that any compliance issues are resolved effectively and expeditiously, and
- Ensuring that compliance improvements and new policies and procedures may be implemented effectively.

(b) The governing authority should periodically obtain relevant information from senior management, or independently from the compliance function, on the overall effectiveness of the compliance function including any material issues within the firm.

(c) Senior management should directly oversee the scope, structure and activities of the compliance function[12] to ensure that the compliance function is carrying out its mandate.

(d) Senior management should encourage the business units to consult with the compliance function with respect to their operations when appropriate.

(e) The compliance policies and procedures of a market intermediary should identify procedures to be followed when breaches of securities regulatory requirements or internal policies are detected, such as:

- methods for identifying breaches,
- steps to be taken when a breach is identified,
- parties (internal or external) to be notified when a breach occurs and the time frame within which the breach must be reported,
- measures to be taken to correct the breach and to ensure that it does not reoccur, and
- methods for keeping records of breaches.

[11] In small firms, senior management may also be the governing authority.

[12] The senior management may delegate certain activities of the compliance function to a designated senior officer, but retain oversight responsibilities.

Topic 3: Independence and Ability to Act

Principle:

The compliance function should be able to operate on its own initiative, without improper influence from other parts of the business, and should have access to senior management and/or, as appropriate, to the governing authority.

Independence of the compliance function is critical to ensuring that the governing authority and the senior management, who are ultimately responsible to regulators, receive accurate and unbiased reports on the market intermediary's compliance with securities regulatory requirements. Although legal frameworks vary according to jurisdictions and may lead to various types of sharing of responsibilities between senior management and the governing authority, independence of the compliance function will be strengthened through the existence of internal procedures that seek to ensure that either senior management or the governing authority, as appropriate, are promptly made aware of any significant compliance matters (see topic 2).

Independence means that a compliance function should be able to operate without improper or undue influence by other parts of the business. Improper influence is mitigated by providing the compliance function with the authority and resources (including human resources) to carry out their responsibilities, and by allowing them access to all levels of the organization. In addition, to help ensure that a market intermediary can hire and retain highly qualified compliance personnel, their compensation and opportunities for advancement should not be directly dependent on the success of a specific business line, product or transaction.

Regulators need to recognize, however, the difficulty of achieving complete independence for the compliance function in the smallest firms. In the smaller firms, there may be an overlap between senior management who trade or provide advice and the compliance function. In such a case, procedures are required to prevent conflicts of interest or other problems regarding the performance of their compliance responsibilities.

Means for Implementation[13]

(a) To achieve independence, the budget for the compliance function and compensation for compliance personnel should not be directly dependent on the financial performance or revenues generated by a specific business line, product or transaction; however, the compensation for compliance personnel may be dependent on the performance or revenues of the firm as a whole. The compliance budget should receive sufficient resources to enable compliance personnel to carry out their responsibilities effectively. The independence of the

[13] The following are examples of methods that are used by firms to ensure independence.

compliance function may also be undermined if promotion of compliance personnel is dependent on the performance of a particular business line.

(b) Compliance personnel should have the ability on their own initiative to communicate with any employees and to obtain access to records or other information necessary to carry out their responsibilities, including the ability to conduct investigations of possible breaches of securities regulatory requirements or the internal compliance policies and procedures.

(c) Compliance personnel should have unrestricted access to senior management and, as appropriate, to the governing authority to discuss significant compliance matters.

(d) In cases where individuals perform both business and compliance activities, they should not be supervising their own business activities. In two-person firms, each person should review each other's responsibility. In one-person firms, where such firms are allowed by legislation, independence of the compliance function is to be addressed by regulators in the way they see fit, for example by reviewing such firms more frequently because of their risk profile, or by requiring the use of an independent external body for carrying out of the compliance tasks.

Topic 4: Qualification of Compliance Personnel

Principle:

Staff exercising compliance responsibilities should have integrity, an understanding of relevant rules, the necessary qualifications, industry experience and professional and personal qualities to enable them to carry out their duties effectively.

Staff exercising compliance responsibilities should have the skills, knowledge and expertise necessary for the discharge of their responsibilities or tasks. In addition to formal qualifications, the main requirement should be the ability of compliance staff to perform their role, which may be gained by reason of experience rather than through only study. In addition to technical knowledge of relevant rules, compliance staff should understand the nature of the business within which they operate. Certain personal qualities and soft skills are also important, examples of these include analytical skills, communication skills and problem solving skills. The requisite competency for compliance staff will depend on the range of regulation and business activities that are their responsibility.

Means for Implementation

Market intermediaries should consider imposing upon persons responsible for compliance activities the following requirements:

(a) Completion of relevant courses and/or training prior to accepting compliance responsibilities;

(b) Knowledge and experience prerequisites concerning securities regulatory requirements, which may be confirmed by successful completion of prescribed examinations;

(c) Continuing education requirements; and/or

(d) Relevant work and industry experience.

Topic 5: Assessment of the Effectiveness of the Compliance Function

Principles:

(a) Each market intermediary should periodically assess the effectiveness of its compliance function.

(b) In addition to any internal evaluations, the compliance function should be subject to periodic external review. Such reviews may be conducted by independent third parties, such as external auditors, SROs or regulators.

In order to help ensure that a compliance function is adequately identifying, assessing, advising on, monitoring and reporting on the market intermediary's compliance with securities regulatory requirements, its effectiveness should be periodically assessed. As part of an assessment, a market intermediary should determine whether it has assigned responsibility for all necessary compliance functions, and that the compliance function overall is coordinated and operates effectively. Such a determination may be particularly important when responsibility for compliance functions are dispersed through an organization, and may also be required by regulatory considerations.

The responsibility for compliance lies primarily within the firm, with external parties providing a useful independent assessment of the compliance function. Internal and external parties play complementary roles to ensure effective assessment.

The roles of external parties such as regulators or auditors will differ depending on the objectives and scope of the assessment and the differing jurisdictional rules or requirements.

Parties that provide assessments should utilize information and resources effectively to assess, detect, and correct any compliance problems that could cause harm to investors, while attempting to minimize the burden on the firm being examined. Establishing the scope of the assessment beforehand facilitates an efficient use of resources during the review and reduces unnecessary duplication of work done in previous reviews. However, a party performing an assessment must be free to follow up on any findings they may make during an examination or to extend the scope of the review, even if it leads into areas not included in the originally intended scope of the examination.

A minimum scope or frequency of assessment cannot be prescribed due to differences in risk levels of securities firms and regulatory resources across jurisdictions. However, periodic assessments are necessary.

Means for Implementation

(a) The policies and procedures and controls put in place to identify, assess, monitor and report on compliance with regulatory requirements should be evaluated.

(b) The effectiveness of the compliance function should be reported to the governing authority and/or senior management, by either the designated senior officer responsible for compliance or by individuals independent from the compliance function.

(c) Any deficiencies of the compliance function should be addressed in a timely manner. Where appropriate, additional training should be provided to compliance personnel.

(d) The internal or external party performing the review of the compliance function should generally establish the scope of the review before commencing the review in order to effectively use information and resources both within the market intermediary and within the reviewing party. However, a party performing the assessment must be free to follow up on any findings they may make during a review or to extend the scope of the examination, even if it leads into areas not included in the originally intended scope of the review.

Topic 6 Regulators' Supervision

Principles:

(a) Regulators' supervision of market intermediaries should include the assessment of the compliance function, taking into account the intermediary's size and business.

(b) Regulators should take steps to encourage market intermediaries to improve their compliance function, particularly when the regulators become aware of deficiencies. In addition, regulators should have the authority to bring enforcement actions, or other appropriate disciplinary proceedings, against market intermediaries relating to their compliance function.

Monitoring the organization put in place by market intermediaries for compliance and the performance of the compliance function may allow regulators to identify weaknesses in a market intermediary before a serious problem arises. In such circumstances, regulators would then be in a position to require the necessary enhancements.

The manner in which regulators supervise their market intermediaries may differ. Some regulators may choose to conduct regular examinations of their intermediaries to assess the effectiveness of their compliance function. Other regulators may choose to supervise their market intermediaries using a risk-based approach. In the latter case, the frequency and the scope of a regulator's examination may depend on a number of factors, such as the number of complaints filed against an intermediary and the compliance history of the intermediary. Alternatively, some regulators may, in part, rely on SROs to directly regulate and monitor the compliance function at market intermediaries. Lastly, regulators may also require their market intermediaries to notify them of significant breaches of securities regulatory requirements and/or customer complaints. These regulators believe that this approach allows them to assess the overall compliance of an intermediary, and thus, the effectiveness of its compliance function.

Means for Implementation

Regulators could consider the following measures, taking into consideration the size of the firm, the complexity of its business, including the type of risk it has to face, and the firm's compliance history:

(a) Direct examination, by the regulator, of the compliance function of a market intermediary at the time of license application;

(b) Direct examination, by the regulator, of the compliance function as part of the general on-site inspections of market intermediaries, which may be conducted either on a regular basis or pursuant to a risk-based approach;

(c) Direct examination, by the regulator, of the internal policies and operational procedures and controls of market intermediaries and subsequent amendments;

(d) Examination of a market intermediary, including its compliance function, by external auditors appointed by the market intermediary, and the forwarding of the results of the examination to the regulator;

(e) Examination by SROs, either on a periodic or "for cause" basis,[14] of market intermediaries;

(f) Periodic self-assessment and/or certification[15] by the governing authority and/or senior management of market intermediaries, which should be filed with the regulators for review; and

(g) Revising and re-examination of the compliance function where issues had previously been identified with the firm about the operation of the function.

The above examinations may cover: the adequacy of the firm's policies and procedures, the structure of the compliance function (such as the degree of independence and lines of reporting), human and material resources dedicated to the compliance function, qualifications and fitness of the person(s) responsible for compliance, and possible or mandated measures taken to address deficiencies previously identified.

[14] SROs are, in turn, examined by the regulator, in order to assess the adequacy of the SROs' supervision and examinations of market intermediaries.

[15] Some jurisdictions do not support sole reliance on self certification.

Topic 7 Cross-border compliance arrangements

Principle:

Where market intermediaries operate on a cross-border basis, the compliance function must understand the applicable laws in each jurisdiction in which the market intermediary operates, and take steps to help ensure that it has the necessary personnel and expertise to comply with them.

As market intermediaries undertake business in jurisdictions outside their home country, they may face new issues for compliance. Geographic separation means that supervision may not be as direct. There is the potential for inconsistencies and omissions in the way in which compliance may be undertaken for activities outside the home jurisdiction. This may increase the potential for errors and compliance risk, yet it is important that the compliance function operate effectively in relation to all the activities of the firm wherever those activities occur. For the sake of simplicity, market intermediaries often choose to adopt the more stringent standard.

For the compliance function to be effective we expect that there should be identification of who is responsible for what components of the function. As stated in Topic 1, some market intermediaries that operate on a cross-border basis may organize their compliance function taking into account the business operations and compliance systems established by other entities within the group. Details of the accountabilities for performing that function should be clearly set out for all involved in the compliance function. Where the compliance function may be split between personnel in two or more jurisdictions there is need for clear identification of responsibilities.

As firms' activities are dynamic and local events may prompt changes in the operations of a firm, periodic review of the compliance arrangements is important to ensure that the compliance function continues to be appropriately involved in the activities of the firm whether or not being undertaken inside or outside the home jurisdiction.

Means of Implementation

It is expected that where the compliance function is involved in the oversight of activities of the market intermediary outside the home jurisdiction, the firm should clearly identify the responsibilities and accountabilities of the personnel involved in the applicable activities in order to avoid gaps and unnecessary inconsistencies. This may involve:

- Identifying the compliance obligations that need to be met in relation to the activities of the firm that are being undertaken outside its home jurisdiction;
- Identifying the responsibilities of the relevant compliance personnel in the home jurisdiction and the other jurisdiction to seek to ensure that all activities being conducted in the other jurisdiction are subject to appropriate oversight by the compliance function;

- Identifying the reporting and accountability lines for relevant compliance staff responsible for the compliance function;
- Undertaking periodic review of the securities firm's activities and the compliance function outside the home jurisdiction. This review should seek to ensure that the current compliance obligations and responsibilities applicable outside the home jurisdiction are appropriate given the nature scope and scale of the firm's activities as they evolve over time. A review from time to time may involve the audit of the performance of the compliance function to ensure that the operations are being undertaken in accordance with the documented procedures; and
- Having ready access to details of the relevant compliance obligations applicable to the activities of the firm outside the home jurisdiction, such as laws, regulations and policies issued in the jurisdictions in which the market intermediary is engaged in business.

Topic 8 Outsourcing of the Compliance Function

Some market intermediaries may consider outsourcing certain compliance tasks to third party service providers. The market intermediaries, however, still retain full legal liability and accountability to the regulator for any and all functions or tasks that they outsource to a service provider. IOSCO has issued a report on *Principles on Outsourcing of Financial Services for Market Intermediaries*, which sets forth a framework that is designed to assist intermediaries in determining the steps they should take when considering outsourcing activities. This report can be found on the IOSCO website at http://www.iosco.org/pubdocs/pdf/IOSCOPD187.pdf.

Annex

IOSCO Consultation Report on Compliance Function at Market Intermediaries Summary of Comments and Response

Compliance with securities laws, regulations and conduct of business rules is part of the essential foundation of sound and orderly markets. It is also a key element of investor protection. Although jurisdictions may have different approaches and policies to help ensure compliance with their principles, rules and regulations, they share a common belief that the compliance function at intermediaries plays an essential role in preventing possible misconduct and regulatory breaches and in promoting ethical behaviour. Recent enforcement actions have highlighted the importance of reinforcing the compliance culture within securities firms. Moreover, in a number of jurisdictions, the existing rules and regulations concerning the compliance function are being reviewed or overhauled. Today, the issue of compliance is much discussed on a domestic as well as on an international level. The Technical Committee Report on Compliance Function at Market Intermediaries (the Compliance Report) contributes to the discussion that is taking place in the international arena. It sets forth and discusses principles that should be considered by all market intermediaries and their regulators to increase the effectiveness of the compliance function at market intermediaries.

I. Background

In January 2004, the IOSCO Technical Committee Standing Committee on the Regulation of Market intermediaries (SC3) submitted a draft project specification to the TC proposing to undertake a project on the compliance function at market intermediaries with the objective of developing, as appropriate, a set of recommendations or principles to enhance the effectiveness of the compliance function and structure at market intermediaries. During its annual conference in Amman, in October 2004, the TC approved the final mandate of SC3. Following this approval, a survey was conducted of the jurisdictions of SC3 members and a summary of the survey was prepared by a compliance drafting subgroup (see Appendix A). The subgroup also prepared a review of other work conducted in this area by other entities such as the Basel Committee[16] and the Committee of European Securities Regulators (CESR).[17]

On the basis of the regulators' survey, SC3 prepared a consultation report that was approved by the TC and published for consultation in April 2005. This report reviewed

[16] Basel Committee on Banking Supervision. *Compliance and the compliance function in banks* (April 2005).

[17] CESR's advice to the European Commission on implementing measures regarding the directive on Markets in Financial Instruments (CESR/05-024c - January 2005).

current IOSCO principles, regulations in member jurisdictions, along with regulatory initiatives. It proposed supplementary principles and raised some issues for discussion. Consultation was closed on 15 July 2005.

Following the receipt of comments by the public, SC3 revised the consultation report. The final Compliance Report was approved by the TC on 7 February 2006. This paper sets forth a summary of the comments received by SC3, its response, and any changes to the principles that have resulted from those comments. The TC has reviewed this summary of comments and has approved its publication concurrent with the release of the Compliance Report.

II Comments and responses on the IOSCO Consultation Report

The TC expresses its sincere thanks for the numerous responses received to the discussion paper, which are representative of a wide spectrum of views, from a geographical point of view as well because of the variety of entities that responded. The TC thanks commentators for their extensive comments and explanations, as well as for the interesting proposals that were often accompanied by references to documents describing initiatives from commentators in the field of compliance. The overall quality of the responses shows the industry's interest in the issues raised by the consultation report. The TC is grateful to commentators for their contributions, which helped clarifying many parts of this paper.

Thirty-two comment letters were received. They came from Europe (thirteen), Asia-Pacific (eight), America (six), Africa (four), as well as from the IOSCO Self-regulatory Organizations Consultative Committee (SROCC). Commentators included industry associations (sixteen), individual affiliate members of IOSCO (six), individual market intermediaries (seven), and other entities such as service providers to market intermediaries (three).

In general, the comments received were favourable. They generally commented that the consultation report highlighted critical compliance issues and helped to assist market intermediaries in increasing the effectiveness of their compliance programs.

A Canadian industry association commended IOSCO for reviewing the compliance initiatives of different regulators, which would help financial intermediaries and markets to better understand international practices and experiences in compliance matters. An Australian industry association noted the inherent challenges in managing regulation emanating from a number of jurisdictions and regulators. In this context, a Canadian firm and an Italian industry association welcomed IOSCO's initiative in the perspective of a harmonised, principle-based approach to the regulation of the compliance function and expressed the wish for such harmonisation at the international level. According to an IOSCO affiliate member this should be accomplished on the basis of the IOSCO principles. Two European industry associations and a Canadian firm suggested that any

requirements by IOSCO should be consistent with those of other regulators, such as the Basel Committee.

All commentators, either in their general comments or in their specific answers, emphasised the need for flexibility and called for high-level principles. Two German industry associations indicated that any new principles relating to the compliance function should accommodate established and effective national compliance systems. They also should not, according to the associations and others, conflict with ongoing regulatory and compliance initiatives such as those of the Basel Committee and the European Commission in the context of implementing measures to the directive on Markets in Financial Instruments. A US industry association was particularly concerned by the difficulties that small or mid-sized firms may face in the context of increasing regulation but recognised the extent to which the TC had sought to consider the characteristics of these firms.

Among the clarifications that were requested,[18] the major one relates to the need to emphasise that compliance is the responsibility of the entire organization and all its employees, and is not the responsibility solely of the compliance personnel. To that end, it was suggested that the paper better distinguish between the market intermediary's overall responsibility for compliance and the duties of the compliance function itself. It was suggested that the compliance function should be better distinguished from the compliance department, and that the paper should include a reference to the need for a strong compliance culture. The Compliance Report will be amended to clarify these points.

---

[18] In particular by the IOSCO SROCC, four industry associations and two market intermediaries.

I. Introduction

C. Definition of the Compliance Function and Scope

Q1: Do you agree with the definition and description of the scope of a compliance function? Please explain.

Comments:

Twenty-nine commentators[19] responded to this question. Fifteen commentators[20] agreed with the definition and scope of the compliance function as proposed by the TC. Of the fourteen commentators that disagreed[21] with the proposed definition and scope, six were of the view that it was too narrow and three thought that it was too broad.

Five of the commentators[22] who believed the proposed definition to be too narrow, indicated that the compliance function should have a pro-active role, including an involvement in strategic and business development decisions of the intermediary. Consequently, the definition should reflect this role of the compliance function. These commentators also indicated that the scope of compliance should not be limited to securities regulatory requirements, but should include other regulatory requirements, industry best practices and internal policies and procedures. Three commentators,[23] who generally agreed with the proposed definition, also recommended that it be broadened.

Of the commentators who believed the proposed definition to be too broad, a UK and a US industry association indicated that certain responsibilities of the compliance function, as included in the proposed definition, are or may be performed by other parties. For example, a US industry association indicated that monitoring and reporting could be performed by an independent auditor or compliance professional.

A Canadian firm noted that the definition and the means for implementation under Topic 1 should be read together in order to reflect the complete scope of the responsibilities of the compliance function.

[19] The twenty-nine commentators include the IOSCO SRO Consultative Committee (SROCC), two IOSCO affiliate members, sixteen industry associations, eight market intermediaries, and two service providers of market intermediaries.
[20] These fifteen commentators include the SROCC, two IOSCO affiliate member, six industry associations, five market intermediaries and one service provider.
[21] The fourteen commentators include nine industry associations, an IOSCO affiliate member, three market intermediaries and one service provider. Four comment letters were received from organizations in Australia (three industry associations and an IOSCO affiliate member), all of which believe that the proposed definition is too narrow.
[22] The five commentators include four industry associations and an IOSCO affiliate member.
[23] The three commentators include two market intermediaries and one industry association.

A Canadian firm and an Australian industry association noted that there was not sufficient distinction between the responsibilities of the board of directors, senior management and the compliance function of a market intermediary

Three commentators[24] expressed concern with the statement that a compliance function should have "mechanisms in place to protect the firm from any liability arising from abuses committed by its customers".

Response:

The TC agrees with the commentators that the compliance function should be pro-active, in particular through providing advice to the business units about strategic decisions or new businesses. The proposed definition includes this element by stating that the compliance function provides advice, i.e. advises, on an intermediary's compliance, and by further elaborating that its responsibilities are not limited to monitoring but include identification and prevention. The TC provided an example of how the compliance function could assist in preventing violation of rules by getting involved in consideration of new businesses. The TC will clarify this aspect of the compliance function's role in the narrative after the definition.

The TC expects an intermediary to comply with all applicable regulatory requirements and its internal policies and procedures. The TC, therefore, expects its compliance function to identify, assess, advise on, monitor and report on the intermediary's compliance with these requirements and the internal policies and procedures. Since IOSCO members only have jurisdiction over the securities activities of market intermediaries, the principles focus on the securities regulatory requirements of these intermediaries. The TC will include an explanation of its expectation in the introduction to the supplementary principles.

The TC does not believe that the definition is too broad. Responses from a majority of commentators confirm this view.

The TC believes that the definition of the compliance function sufficiently captures the overall responsibilities of the compliance function. The means for implementation under Topic 1 serves to provide concrete ways for the compliance function to meet its responsibilities. The TC agrees that the definition and the means should be read together. While the definition does not need to be revised, the TC agrees that these related issues, which were split between the introduction and Topic 1, should be merged into one single part of the Compliance Report.

The TC believes that the Board of Directors and/or senior management of a market intermediary have the responsibility for the intermediary's compliance with securities regulatory requirements, and that the compliance function provides assistance to the Board and/or senior management in fulfilling their responsibility. The developed

[24] They are two industry associations and one market intermediary.

principles intend to reflect this framework. Further discussions on the clarity of the responsibilities of various parties are included under Topic 2. For clarification purposes revisions will be made to the principles and means for implementation.

In order to address the concerns expressed about the statement that a compliance function should have mechanisms in place to protect the firm from any liability arising from abuses committed by its customers, the TC recognises the need to clarify its proposal by a recommendation that, where firms have obligations to report or prevent abuses by customers, the compliance function should have mechanisms in place designed to assist firms in meeting those obligations.

The TC notes that, when developing the draft principles, it reviewed similar recommendations or principles by other international bodies, including the Basel Committee and CESR. The TC understands that, where appropriate, it would be helpful if its recommendations were consistent with those of other international bodies, and believes that they are.

Q 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?

Comments:

Twenty-eight commentators[25] responded to this question. Over half of these commentators[26] indicated that the compliance function and the risk management function at a firm should have a close relationship and should work closely together. Although the other commentators did not explicitly indicate that the two functions should have close interaction, a majority believed that the two functions overlap.

Ten commentators[27] were of the view that the compliance function was part of a firm's overall risk management system, and one commenter did not distinguish between the two functions. Two commentators[28] specifically indicated that a compliance function should use risk management techniques, and one commenter[29] noted that the risk management function should support the compliance function.

[25] The twenty-eight commentators include the SROCC, two IOSCO affiliate members, seventeen industry associations, six market intermediaries, and two service providers.
[26] They are eight industry associations, the SROCC, one IOSCO affiliate member, four market intermediaries, and one service provider.
[27] The ten commentators are eight industry associations and two market intermediaries.
[28] The two commentators are an IOSCO affiliate member and an Australian industry association.
[29] An IOSCO affiliate member.

Seven commentators,[30] however, believed that the compliance function and the risk management function should be separate. Three of them[31] indicated that the compliance function should operate independently.

Three commentators[32] indicated that IOSCO should not prescribe a specific structure or organization of the compliance and risk management functions.

Response:

The comments confirmed the TC's view that compliance and risk management are tools that allow market intermediaries to manage the different risks in their business, and that a compliance function may be involved in managing the risks arising from violation of regulatory requirements. The TC agrees that a specific organizational structure should not be prescribed, however, regardless of the structure, an intermediary's compliance and risk management functions should have a close working relationship. No amendments to the definition and scope of the compliance function are necessary.

Topic 1 – Establishing a compliance function

Topic 1 and the introductory part of the paper on the definition and scope of the compliance function are related. Therefore some comments made under topic 1 also relate to the definition and scope. They are not repeated here.

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

Commentators did not support mandating a specific compliance structure, with the exception of an Italian and a Nigerian firm, who suggested that every intermediary should establish a dedicated and independent unit that would report directly to the CEO.

The majority of these commentators argued that mandating a specific organizational structure would be neither practical nor necessary because of the significant diversity of market intermediaries.[33] They recommended, however, that market intermediaries should be required to clearly establish their organizational structure according to general high-level principles. The way in which these general high-level principles are transposed into a specific organizational structure should be left to the firms.[34] An Australian industry association added that firms should be able to demonstrate that the structures and practices they have put in place are effective by reference to the underlying policy

[30] These seven commentators are four industry associations, two market intermediaries, and an IOSCO affiliate member.
[31] They are two market intermediaries and an industry association.
[32] The three commentators are two industry associations and a market intermediary.
[33] The SROCC, an IOSCO affiliate member, eight industry associations, one market intermediary, and three service providers
[34] The SROCC, two IOSCO affiliate members, seven industry associations, and one market intermediary.

objectives. These commentators explained that firms were better placed to structure their compliance according to their own characteristics: for instance, 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. A Singapore industry association also mentioned the ownership structure of the firm explaining, that "firms which are owned by bank holding companies will have a different compliance structure from those which are autonomously owned". This point of view was shared by a Canadian firm that supported "an approach that would allow market intermediaries, which operate as part of a financial conglomerate, the flexibility to be able to rely on and/or adopt the compliance controls and systems already established by the parent company or other market intermediary within the conglomerate in order to leverage any existing synergies in meeting the regulatory requirements".

Commentators cited several high level principles, which they considered necessary to underpin the organizational structure of compliance. These principles are set forth in the Compliance Report (independence of the compliance function, suitable access and appropriate reporting lines to senior management,[35] independent lines of communication between the compliance function and the Board, adequate human and material resources, formal status within the organization, accountability, right of access to staff and records).

Response:

The comments received confirm the TC's approach, which is to mandate the establishment of a compliance function, without prescribing a specific organizational structure. There is therefore no need to modify the proposed principle or the means for implementation.

The proposed principle addresses commentators' concerns regarding the need for flexibility allowing firms to structure their compliance according to their own characteristics.

However, the proposed factors that may influence the organization of the compliance function have been modified to include a factor that relates to the nature of a firm's business and the regulatory framework to which it is subject. This amendment meets the concern raised by several commentators,[36] that firms' compliance relates to securities regulatory requirements as well as to other requirements (for instance banking supervisors' requirements) and may be split among various functions in the firm (e.g. internal audit and financial control).

[35] A US industry association underlines the need to allow reporting lines from compliance departments not automatically to the board or senior management but rather, according to the structure of the firm, to the legal department or risk management function – see their comment on topic 3.
[36] In particular by a US and UK industry association.

Among the factors that may influence the organization of the compliance function, commentators also recommended including a factor that would refer to the ability of market intermediaries operating as part of a financial conglomerate to benefit from the synergies that are commonly associated with a group. Further to this suggestion, which was also proposed in the context of the structuring of the compliance function in groups operating on a cross border basis (see Topic 7), a survey was conducted of jurisdictions of SC3 members to gain an understanding of whether regulators permit the centralization of the compliance function in a foreign firm legally operating in their jurisdiction, and whether the rules differ for a domestic financial institutional group. Appendix B summarises the questions asked as part of the survey and the responses received. The TC believes that firms should have the flexibility to organize their compliance function as they see fit, and therefore, has not included comments regarding centralization of compliance function in the final Compliance Report.

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

In addition to the principle related to establishing a compliance function, the consultation report proposed some means for implementation that reflect current practices among regulators. These means for implementation include some of the essential roles, responsibilities and activities that the compliance function should generally perform, taking into account the nature, scale and complexity of the firm.

Commentators were asked whether any activity for the compliance function should be mandated or otherwise identified by regulators. Twenty-six provided a response, of which fifteen indicated that roles, responsibilities or activities should be mandated or identified, and eleven indicated otherwise.

The commentators for whom essential roles, responsibilities and activities should be identified and clearly defined by the regulators were the SROCC, seven industry associations, three market intermediaries, three service providers and one IOSCO affiliate member. Four of these commentators, one market intermediary, one industry association, one IOSCO affiliate member and one service provider, indicated that only high level activities should me mandated. Five commentators noted that the list of responsibilities outlined in paragraph b) of the Means for Implementation is adequate. Three respondents (one from Africa, one from the UK and one from the US) noted that local requirements have already sufficiently outlined the responsibilities of the compliance function.

The opposing responses were received from seven industry associations, one IOSCO affiliate member, two market intermediaries and one service provider. For these commentators the structure of the supervisory system established by the firm should not be mandated, instead flexibility was important to take into account the divergent needs of various intermediaries - within a framework of sound and transparent policy principles. One Australian industry association noted that it is more effective to prescribe the outcome that should be achieved.

Some commentators suggested various activities as key to the compliance function, such as being the liaison to the regulators.

Response:

The TC acknowledges the need for flexibility expressed by commentators and estimates that the proposed principles take this concern into account. The means for implementation are provided as an illustration of the different ways by which the principle concerning the establishment of a compliance function may be implemented in various jurisdictions. Therefore, it does not seem necessary to modify the proposed principle as it is consistent with most of the commentators' views. This approach allows intermediaries to operate in various jurisdictions while being able to adapt the characteristics of their compliance function to the firm's specificities.

The TC agrees to supplement the means for implementation in order to include the comments by a US and UK industry association that the activities generally performed by the compliance function do not necessarily belong in the compliance department, and that responsibility for these activities may be shared with other units of the firm. This would be in line with the Basle principles, as well as with the TC's general approach according to which no specific structure for the compliance function should be mandated.

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

Of the twenty-five commentators, five[37] specifically answered that no other responsibilities than those described in the consultation report should be carried out by the compliance function.

Seven commentators[38] referred to their answer to the previous question and thus did not suggest additional responsibilities. Thirteen commentators suggested some additional responsibilities that should be carried out by the compliance function.[39] (Appendix C to this summary provides a list of tasks and responsibilities that may be within the compliance function, created by a combination of tasks indicated by regulators and of tasks indicated by commentators).

[37] One IOSOC affiliate member, two industry associations, one market intermediary and one service provider.
[38] One IOSCO affiliate member, five industry associations and one market intermediary.
[39] SROCC, five industry associations, four market intermediaries and three service providers.

Response:

The TC takes note of the comments by respondents, which do not call into question the approach set forth in IOSCO's general principles, which is generally supported by commentators.

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

Twenty-one responses were received on this question. According to eleven[40] of the commentators, responsibility for ensuring that compliance risks are managed lies with the board and senior management or heads of business units. For them the role of the compliance function is to assist the firm and its senior management in managing compliance risks, but the compliance function should not be seen as being responsible for managing that risk itself.

In contrast, three commentators stated that the management of compliance risks was the sole responsibility of the compliance function. A Singapore industry association and a Nigerian service provider emphasised that managing compliance risks should take a proactive form. For a UK industry association, managing compliance risks was a continuous obligation and responsibility of the compliance function.

Three other commentators[41] stated that firms should be free to organize the risk managing function according to the size of the firm and assign risk management either to the compliance function, or to the firm's senior management or to both functions, according to the nature and the potential financial impact of such risk. For a UK service provider the answer depended on the firm's structure but a liaison between the compliance function and the risk function was necessary "in supporting efforts to identify, assess and mitigate compliance risk. It might also, in certain structures, be beneficial for the compliance function to assess the risk control methodology and documentation produced by the risk function."

Response:

As presently drafted, the means for implementation suggest that, among the role and activities generally performed, the compliance function may also have an advisory and assistance role in the management of compliance risks (see (b) (1), (2) and (3)). This is the view of the majority of commentators.

[40] SROCC, seven industry associations, two market intermediaries and one service provider.
[41] A European and German industry association, and a UK service provider.

Q 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?

All commentators agreed that market intermediaries should adopt documented policies and procedures as required for their type of business, irrespective of size. However, the vast majority[42] underlined the need for flexible requirements so that the procedural documentation may be tailored according to the scale and complexity of the firm's business and in particular according to the level of risk that the firm's activities entail, both for the financial system as a whole and for the firm's clients.[43] Several stressed that the outcomes of the documented policies and procedures were more important than the existence of the documentation.[44] This goal may be reached by establishing principle-based regulation and avoiding overly prescriptive requirements.[45]

In contrast, six commentators[46] did not refer to the size factor: they stated that all firms should be expected to meet the same standards of compliance and to have written procedures.

Concerns were expressed about imposing on small firms detailed documentation obligations[47] and that excessive requirements for documentation could distract a small intermediary from more important tasks.[48]

An IOSCO affiliate member commented that, in its experience "some very large organizations have had very high standards of documentation and poor compliance outcomes, whilst some small organizations have had poor standards of documentation and high compliance outcomes. Hence, the existence of documentation, whilst an indicator of a compliance culture, is not in its own right a decisive indicator of compliance standards."

Response:

As presently drafted, the means for implementation (see (b) (2)) do not prescribe any particular level of detail for policies and procedures to be established by market intermediaries. Therefore, they adequately address the comments received. However, the TC agrees to include some additional text to confirm that the requirements regarding policies and procedures should be tailored according to the scale and complexity of the

[42] SROCC, eleven industry associations, three service providers, three IOSCO affiliate members, and one market intermediary.
[43] Two industry associations, two service providers, one IOSCO affiliate member.
[44] Four industry associations, one IOSCO affiliate member.
[45] A market intermediary, industry association and service provider.
[46] Three market intermediaries, two industry associations and an IOSCO affiliate member
[47] IOSCO affiliate member and a Singapore industry association.
[48] A Singapore firm.

firm's business, and in particular according to the level of risk that the firm's activities entail, both for the financial system as a whole and for the firm's clients.

Topic 2 – Roles and responsibilities of the Board of directors or Senior management

Q 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.

Twenty-two commentators responded to this question. Four commentators indicated that the board of directors is accountable for non-compliance, five indicated that senior management is accountable, and the remainder indicated that both the board and senior management are accountable.

There are differences between jurisdictions, however, in the degree of Board participation in the operational management of the compliance function. For example, a US industry association stated that the responsibility for managing (i.e., implementing and supervising) all aspects of the compliance function "belongs to senior management." A Canadian IOSCO affiliate member concurred. This would also appear to be the case in the UK, where senior management is responsible for the effectiveness of the compliance function, while the board is responsible for making sure that the management is fulfilling its duty. In contrast, a German and an Italian industry association noted that, in their respective countries, the board of managing directors was generally accountable for the overall compliance with applicable laws, rules and regulations. Ontario, the U.S., and Germany require the designation of a chief compliance officer.[49]

An Australian industry association and a Canadian firm noted the ambiguity about the relative roles of the board and senior management and requested that the paper make a clearer distinction between the responsibilities of the board of directors, senior management and the compliance function of a market intermediary.

Response:

The TC acknowledges the need to clarify Topic 2 further to the comments received, in particular with regards to the respective responsibilities of the different parties involved. The TC agrees to clarify the respective responsibilities of the "management bodies" of the firm (governing authority, senior management), while accommodating various legal requirements which may differ across jurisdictions. In addition, the TC also agrees to

[49] In the U.S., an SEC rule requires a registered investment adviser to designate a chief compliance officer, while broker-dealers are subject to NYSE/NASD rules to designate a chief compliance officer.

modify the drafting in order to clarify that compliance is the responsibility of everyone in firm, not only of the governing authority, senior management and compliance staff.

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

Responses were mixed as to whether these three terms are distinguishable. Among those that do find a distinction, an Australian IOSCO affiliate member viewed the compliance function as being *responsible* for the identification, prevention and remediation of the planning and response to the compliance risk; line management was *accountable* for the implementation of actions to manage or avoid compliance risks; and the governing body should be *liable* for the implementation of actions to manage or avoid compliance risks. A German industry association noted a distinction between the three, but that definitions varied widely among jurisdictions. For an Australian industry association responsibility and accountability were interconnected, although liability was distinct. Among those that found no distinction were a Canadian IOSCO affiliate member, a European and a Singapore industry association.

A US industry association, supported by a Canadian firm, stated that responsibility referred to an individual's duties within an organization. Accountability concerned how an organization tracked the performance of those duties and imposed consequences for successfully or unsuccessfully performing them. Liability referred to the regulatory or other legal consequences that could follow when responsibility or accountability break down. Responsibility could be delegated, and firms should be given wide latitude to delegate responsibility for compliance functions as they see best. However, accountability and liability could not be delegated.

Response:

The comments received indicated that legal liability is different from responsibility and accountability. The TC will clarify in the final Compliance Report that the principles deal with the role of the governing authority and senior management within a firm, but not their legal liability.

Q 10: Should a senior officer be designated for the day-to-day compliance responsibilities?

Twenty-five responses were received. Nineteen agree that a senior officer should be designated for the day-to-day compliance tasks, of which four industry associations indicated who should be designated depends on the size of the firm, three commentators[50] stated that the designated officer must have seniority in the firm, for example a board member. According to an IOSCO affiliated member line management should have

[50] One Australian industry association, a Canadian firm and an UK service provider.

responsibilities for the day-to-day compliance, but may rely on senior compliance officer for advice.

Response

The TC notes that a designated compliance officer may not be practical for small firms, and therefore, will not recommend it. The principles as currently drafted already allow firms the flexibility to designate a compliance officer if practical.

Topic 3 – Independence and ability to act

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

Responses concerning the independence of the compliance function in small firms were mixed. For a majority of commentators some flexibility on independence should be allowed as long as the effectiveness of the compliance function does not decline. Some commentators noted that achieving complete independence in small firms, if not impossible, will give rise to additional costs that may serve as a barrier to entry for these small firms. Therefore, a US IOSCO affiliate member recommended consideration of a broader requirement that market intermediaries diligently supervise every aspect of their business, at least for smaller firms. A US industry association made a similar point noting that allowances should be made for firms that are owned or operated by just a few people, consistent with NASD rules that permit the compliance function to be performed by the business owner or principal if a firm only has one such person. A UK industry association suggested that, in cases where the size of the firm did not enable a compliance function which does not carry out some other roles, these extra roles should, where possible, not create unmanageable conflicts of interest. Where genuine independence is not possible due to the small size of the firm, one option would be to use an independent external body to provide the necessary level of independence.

Other commentators, including some members of the SROCC, as well as an Italian and a German industry association, argued that independence requirements should apply equally, regardless of the size of the firm. For example, in the view of an Italian industry association independence of the compliance function cannot be sacrificed due to the size of the firm. Likewise, a UK firm stated that "although the size of the compliance department may be much reduced in a small firm, the requirements relating to independence and ability to act should apply relative."

Response:

The responses to this question suggested that for a number of commentators the principle as currently drafted might not sufficiently take into account the interests of smaller firms. In general, these commentators believe that smaller firms should be allowed to have their compliance function performed by personnel that is also performing business functions. In smaller firms complete independence is often not feasible so that some degree of flexibility should be permitted. In order to accommodate this concern, the TC agrees to add a statement concerning the unique considerations applicable to smaller firms and need for greater regulatory oversight.

Q 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?

Overall, commentators contended that individuals should not supervise any business activities they perform, although responses differed as to how strict such a ban should be. For example, an Australian industry association argued that self-supervision was inadequate because of the inherent conflict of interest that could not be managed in any meaningful way. It stated that "there needs to be an independent monitoring and reporting function." Likewise, a UK industry association stated that compliance personnel should not be involved in the performance of services or activities they monitor and suggested that in smaller firms such issues may be addressed through the use of external auditors.

Other commentators recognised that such a separation may not be possible in small firms and argued that a prescriptive regulatory approach was inappropriate. For example, in SROCC's view a segregation of duties is preferable but not always possible in small firms. Therefore, guidelines should exist to separate functions to help eliminate potential conflicts. A US IOSCO Affiliate member stated that it was "difficult to dictate a 'one size fits all' form of supervision," and a Netherlands industry association suggested that regulators could review the audit reports of internal or external auditors or perform their own regulatory audits to ensure a firm maintained adequate compliance procedures.

Response:

Similar to question 11, a concern was expressed about the need for flexibility for smaller firms. However, other commentators strongly believed that individuals should not be permitted to supervise business functions they perform. On balance, the TC suggests that the text added pursuant to the comments in question 11 concerning the need for flexibility in order to address legitimate issues raised by smaller firms, sufficiently address the additional concerns raised in the responses to question 12.

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

Many commentators stated that the means for implementation are sufficient to achieve independence, especially for large intermediaries, though some suggested improvements. For example, an Australian industry association and an IOSCO affiliate member suggested that the means of implementation should not be prescribed, but that a principle-based approach would be more effective. A UK firm suggested that compliance staff should be able to communicate with all employees and senior management with unhindered access in appropriate circumstances. A Canadian firm suggested adding a requirement that, where possible, there should be a direct reporting line of compliance staff performing oversight duties or having overall responsibility for ensuring compliance outside of the business function. Finally, an Italian industry association did not agree with letter (d) of the means for implementation, which provides for the case where individuals perform both compliance and business functions.

Other commentators disagreed that the means for implementation as currently set out were sufficient. An Australian IOSCO affiliate member, for example, stated that the means for implementation should not be prescribed. While overall expectations can be established, they should not be set out in prescriptive form. An Australian industry association stated the same, noting that a principle-based approach was more effective. A US IOSCO affiliate member stated that it did not view the means for implementation set out in the consultation report as sufficient to achieve independence because of the diversity of market intermediaries.

Response:

The responses to the question raise issues not just concerning the "means of implementation," but the principle itself, since some of the answers to the question suggested that it was inappropriate for the principle to require that the compliance function report to the board or senior management. Others believed that the means for implementation were too prescriptive, and that a principle-based approach would be preferable, given the wide range of business structures that were meant to be covered by these principles.

As currently drafted, however, the means for implementation are rather flexible. The TC has addressed the comments by stating in a footnote to the means for implementation that these are simply examples of methods that are used by firms to ensure independence. Removing the means for implementation would reduce the utility of the principle however, and is therefore not desirable.

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

Most commentators agreed that because of likely conflicts of interest the compensation of compliance personnel should not be tied to the overall performance of the business they monitor. A Canadian firm suggested that in large companies with various business segments compensation may be tied to the performance of the company as a whole, not to the specific results of a particular segment. In companies that do not have diverse segments, compensation for compliance personnel should not be revenue driven. A German industry association suggested fixed compensation schemes for compliance personnel, including definitions of the extent to which compliance personnel participate in the firm's success and bonus plans, to avoid undue influence.

Some of the commentators indicated that while they agreed in principle with the assertion that the compensation of compliance personnel should not be subject to undue influence, this notion should not be taken to extremes. In particular, it was argued that it was appropriate to consult with a compliance officer's business associates regarding the performance of particular individuals, and that it was also entirely appropriate for compliance personnel to share in the overall success of the enterprise.

Response:

The TC notes that subsection (a) of the means for implementation already addresses these issues in some detail and provides appropriate balance. No further revision to the principle or the means of implementation is therefore necessary.

Topic 4 – Qualification of compliance personnel

Q 15: What are the appropriate qualifications for compliance professionals?

For most commentators key qualifications included: practical experience, an understanding of relevant rules and integrity. A Canadian firm suggested that any formal examination should depend on the activities being monitored. Similarly, a German industry association stated that the necessary qualifications depended on the tasks being performed. An Australian industry association advocated "accreditation" rather than "licensing", suggesting that compliance staff should be "internationally transportable." According to an Australian IOSCO affiliate member standards and competence should *not* be determined by the regulator, but rather by "professional bodies." In contrast, a US industry association stated that "general standards for qualification of key compliance personnel, including appropriate testing and continuing education requirements, should be established by regulators." Continuing education was also viewed as important.[51] Eleven commentators noted that other than hard and soft skills, certain personality traits

[51] By six commentators, including the SROCC, three industry associations and two firms.

of compliance personnel were just as important. The relevant soft skills and personality traits include analytical skills, integrity, good questioning mind, communication skills, professional judgment, tact and problem solving skills.

Response:

The TC takes note of and agrees with the suggestions to modify the proposed principle in order to explicitly state that appropriate qualifications also include integrity, understanding of relevant rules, as well as industry experience.

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

The overwhelming number of commentators answered in the affirmative.

Response:

The TC added a statement to confirm that qualification should vary depending on functions, responsibility and seniority.

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

Some commentators suggested the following factors in evaluating the adequacy of courses and training:

- Relevance – whether the content of the training program is relevant to the functions and the needs of the firms whose personnel are participating;
- Emphasis of the course of training;
- Breadth and depth of issues covered;
- Feedback from course participants;
- Work results or compliance examination results of the compliance personnel who attended the course of training;
- Whether training is modified to account for new rules/rule changes;
- Credentials of the trainer.

Response:

The TC notes that the above factors are useful guidance for firms and regulators to evaluate training and courses for compliance personnel.

Topic 5 – Assessment of the Effectiveness of the Compliance Function

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

Twenty-six commentators provided specific answers to this question. There was no general agreement on whether an internal or external party is best placed to perform the requisite assessment. For nine commentators[52] internal and external assessments complement each other. Eight commentators[53] were of the view that external parties were better placed to assess a compliance function's effectiveness. According to three commentators[54] effectiveness should be assessed internally. An Australian industry association and an IOSCO affiliate member were of the view that external versus internal assessment depended on the objective and scope of the review. Three other commentators[55] did not specify who was best placed to make the assessment. A German industry association, on the other hand, indicated that assessments should always be carried out by qualified professionals, without giving preference to certain solutions or structures.

Of the eight supporters of the view that external parties are the ideal candidates to assess the effectiveness of the compliance function, five[56] argued that the regulators or SROs should perform the assessment. An Australian industry association suggested that regulators assess the effectiveness of the compliance function at the time of licensing and on an on-going basis post-licensing through supervision framework such as risk-based approach. An interesting comment from a UK industry association was that clients of a market intermediary would also be able to provide valuable inputs on the effectiveness of the compliance function. At the same time, a US industry association observed the increasing trend of small firms using external parties to support their compliance functions. A UK service provider noted that, with the increase in outsourcing, external parties maybe better placed to perform the assessment because of the lack of expertise in-house.

Of the five commentators that supported internal assessment, three[57] were of the view that since senior management was ultimately responsible for the firm's compliance, it was also responsible for assessing the effectiveness of the compliance function.

Besides comments on the ideal candidate to perform the task of assessment, it is important to note an IOSCO affiliate member's comment that the objectives, constraints and scope of the review had to be clearly thought through combined with the suggestion that industry standard processes and benchmarks for assessment be established. An Australian industry association also noted that compliance was a complex behavioural

[52] Eight industry associations and one market intermediary.
[53] Three industry associations, two market intermediaries, two service providers, and one IOSCO affiliate member.
[54] A market intermediary, an industry association and an IOSCO affiliate member.
[55] SROCC, an Australian industry association and UK service provider.
[56] An IOSCO affiliate member, two market intermediaries, a service provider and an industry association.
[57] An IOSCO affiliate member, and two industry associations.

process and hence reviews had to be undertaken by individuals with practical compliance expertise.

Response:

The TC has considered each of these comments and agrees that responsibility for compliance lies within the firm, with external parties providing a useful independent assessment of the compliance function. It is also important that individuals with practical compliance expertise undertake the compliance reviews. The TC agrees with the majority of the commentators that internal and external parties play complementary roles to ensure effective assessment.

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

Twenty commentators provided specific answers to this question. In general, the commentators noted that the role of an external party includes performing detailed testing of compliance, identifying weaknesses, providing recommendations or guidance on improvement, and imposing sanctions. For instance, two Singapore industry associations shared the view that an external party's role was to identify weaknesses in the existing systems, recommending improvements and highlighting industry's best practices.

For an Australian IOSCO affiliate member the role of an external reviewer depended upon the objectives, parameters, constraints, scope and the desired outcomes of the review. Others pointed out that the level of external oversight was a function of the size of the organization. To illustrate this point, a Canadian firm highlighted that in larger intermediaries, an external party had to focus on broader issues like the overall mandate of the compliance function and a review of the firm's monitoring activities. In contrast, the same external party will be in a position to conduct in-depth procedures and testing in smaller intermediaries.

A UK industry association acknowledged that, although there were multiple roles that external parties could play, these roles should not be made mandatory. In this respect, external auditors play a part in testing compliance critical functions; external lawyers review clients' documentation while consultants benchmark the intermediaries' performances against best practices.

According to some commentators the role of an external party will fall on the regulator. More specifically, an Australian industry association indicated that the regulator's role was to provide guidance on the benchmarks for which regulated entities were to be assessed. For others, like a UK industry association, the regulator's role was to identify regulatory breaches as well as to monitor and supervise the processes and procedures of the intermediaries' compliance function, possibly through means like risk-based supervision approach whereby firms that are classified as higher risk will be visited more frequently than lower risk firms.

Others, like a Netherlands industry association, considered the external party as the external auditor, whose key role was to perform the financial audit as required by law, and whose secondary role was to report on any compliance issues encountered when performing the financial audit. The Netherlands industry association also noted that an external auditor's role should be limited because of their use of a materiality concept and their limited knowledge. According to a US industry association, a private external audit of the effectiveness of the compliance function was unnecessary since the regulator/SRO already performed this function through their examination programs.

Response:

The TC recognises the diversity in opinions with regard to the different possible external parties such as regulators or external auditors. In light of the views that the roles will differ depending on the objectives and scope of the review as well as taking into account differing jurisdictional requirements, the TC will leave the flexibility to decide on the specific role of the external auditors to individual jurisdictions. The TC respects differences in practices among jurisdictions and will not prescribe the specifics of the regulator's role.

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

Twenty-five commentators responded to this question. There were numerous comments, which cited the costs of an external review and the expertise of the external party conducting the review as two primary concerns.

Eighteen commentators[58] noted that costs of external assessments included monetary and time costs, as well as the cost due to disruption to the day-to-day activities of a firm's compliance and business units. For example, during the review a firm's staff may need to spend a considerable amount of time in informational meetings or walking-through processes with the external party. In relation to the costs of an external review, both a Canadian firm and UK industry association pointed out that external reviews would increase the examination burden on companies and could be an "unnecessary duplication" of internal and regulatory audits.

Sixteen commentators[59] were concerned about the expertise and knowledge of external parties. They noted that external parties, for example external auditors, may not have knowledge about the securities industry and the regulations, and may not understand a firm's business to make a reasonable assessment. A Singapore industry association also

[58] SROCC, an IOSCO affiliate member, ten industry associations, three market intermediaries, and three service providers.

[59] SROCC, seven industry associations, four market intermediaries, three IOSCO affiliate members, and one service provider.

noted that the lack of continuity of staff at an external party prevented knowledge transfer and increased cost to a firm. A Nigerian service provider also questioned the trust and integrity of external parties.

Nine commentators[60] were concerned about the quality of an external assessment, due to factors such as inadequate definition of scope and methodology, misunderstanding of the external reviewer's role, inaccessibility of board and senior management, and lack of consistency in assessment. Four commentators[61] suggested that the scope of each review should be clearly defined so that both the external party's and the company's resources could be well allocated during the review. For instance, a German industry association wrote that a clearly defined scope would allow an external assessment "to go into depth without tying up inappropriate resources". An Australian industry association also provided that one of its '*Protocols for Reviewing and Assessing the Adequacy, Effectiveness and Efficiency of Compliance*' include definitions of "who will be relying upon the review", "the scope and limitations of the review" and "the methodology used in the review".

Four commentators[62] noted the conflicts of interest as a practical concern, and three commentators[63] were concerned about the confidentiality of firms' information in external assessments.

In addition, a UK industry association and a UK service provider indicated that regulators should not mandate the use of external parties to assess the effectiveness of the compliance function, except in very rare circumstances. A French IOSCO affiliate member noted that an external review should mainly be an examination of the way a company's compliance function is organized as "assessing the content of the function is solely an internal task". Lastly, a Nigerian firm had no concerns with external assessments provided that the regulators pre-screened the external reviewers.

Response:

The TC notes the commentators' practical concerns. With regard to the costs of an external review and the expertise of the external party conducting the review, the TC recognises that these concerns can vary depending on jurisdictional laws regarding external reviews, if any, and depending on the size and complexity of each company's business. As the principle on "assessment of the effectiveness of the compliance function" does not mandate any specific frequency of external review or any specific external party to conduct the review, the TC believes the principle is worded flexibly enough to account for these practical concerns in different jurisdictions.

[60] Five industry associations, two market intermediaries, one IOSCO affiliate member and one service provider.
[61] An Australian industry association and IOSCO affiliate member and two German industry associations.
[62] SROCC, an Australian IOSCO affiliate member, a Canadian firm and German industry association.
[63] A Nigerian service provider, a Singapore industry association, and a UK industry association.

The TC has also considered the limitations expressed in terms of conflicts of interest and the usefulness of an external party in reviewing the internal compliance function of a company. While the TC understands that an internal party may be better suited to assess certain areas of the compliance function, it remains of the view that there is merit in an independent assessment of the compliance function.

The TC acknowledges concerns that the scope of an examination or inspection should be defined, and that resources should not be inappropriately "tied up." In this regard, we believe that regulators should be well prepared in advance of an examination, and should not inappropriately waste either their or the intermediary's resources. However, regulators must be free to follow-up on any findings they may make during an examination, even if it leads into areas not included in the originally intended scope of the examination. The means for implementation will therefore not be modified.

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

Twenty-seven responses were received for this question. Thirteen commentators[64] suggested a risk-based approach in determining the scope and frequency of assessments. The risk-based approach would be based on factors such as size and complexity of a firm, nature of its business and compliance history. For example, a Canadian firm suggested that the scope and depth of external reviews were based on the size of a firm – increased scope and decreased depth of review for larger firms, but decreased scope and increased depth of review for smaller firms. An Australian industry association also suggested that reviews should be coordinated with the internal audit and risk reviews to minimise disruption to the business.

Ten commentators[65] provided specific suggestions on the frequency and scope of reviews. A German, an Italian and a Netherlands industry association suggested annual reviews; three Nigerian commentators[66] suggested bi-annual internal reviews and annual external reviews; a UK industry association suggested annual internal reviews and bi-annual external reviews, whereas a Singapore firm suggested reviews once every three years. The four Nigerian commentators provided suggestions for the scope of the reviews, of which three[67] suggested that the scope should cover all businesses of a firm, and one[68] suggested that the scope should cover all key issues and concerns to the compliance function.

A US industry association and a US IOSCO affiliate member stated that the scope and frequency of assessments was defined in US regulations, while two Australian industry

[64] Seven industry associations, two IOSCO affiliate members, three market intermediaries and one service provider.
[65] Five industry associations, three market intermediaries, and two service providers.
[66] Two market intermediaries, and one service provider.
[67] Two market intermediaries, and one service provider.
[68] A Nigerian service provider.

associations noted that the company should determine the requirement for internal and external audits, if any. Two European industry associations were of the view that the frequency of reviews should not be prescribed. Specifically, a German industry association pointed out that IOSCO should not prescribe excessively strict rules ahead of possible future developments in the harmonisation of European securities businesses.

Response:

The TC has considered the comments and is of the view that, due to differences in risk levels of companies and regulatory resources across jurisdictions, it will be impracticable to prescribe a minimum scope or frequency of assessment as an IOSCO principle or 'means of implementation'. In light of this, the TC wishes to point out that periodic assessments are appropriate, and that it may be useful, in some circumstances, that their frequency follows a risk-based approach.

Topic 6 – Regulators' supervision

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

Answers to the question on the most effective methods of monitoring were varied. For several commentators the effectiveness of the method(s) to be used depends on the size of the firm, on the complexity of its business, including the type of risk it has to face, on the firm's compliance history, on the function being monitored, or on the degree of standardisation of the transactions to be monitored.[69]

The suggestions mainly referred to monitoring by regulators and SROs, as part of their regular reviews of market intermediaries, or via self-assessment questionnaires. Some commentators also referred to monitoring by external audits and to internal assessments by intermediaries. Monitoring by regulators (and SROs, as the case may be), as part of their regular reviews of market intermediaries, is cited by nearly all commentators.[70]

A Canadian firm suggested that regular reviews of the intermediary's internal policies and procedures by regulators should concern the larger organizations, while more focused reviews should be performed for smaller entities (by the regulator or an external party). An Australian and a US industry association proposed that the regulator should operate on a risk-based approach to prioritise regulatory supervision. A UK industry association is of the opinion that the general supervisory function should be carried out by a regulatory authority with cautious recourse to external auditors, in particular because of the cost that regulators incur when having recourse to external auditors. Four industry

[69] Five industry associations, one IOSCO affiliate member and one market intermediary.
[70] Some answers do not refer (explicitly or implicitly) to monitoring by regulators or SROs (four industry associations and one service provider).

associations also emphasised that regulators should be aware of the cost and disruptive effect of external reviews and encouraged coordination among regulators to avoid coinciding reviews. Furthermore, they urged regulators to share information to avoid duplication and inefficient use of regulatory and internal compliance resources.

As far as self-reporting questionnaires to the regulator are concerned, six commentators[71] found them to be a very effective method of monitoring market intermediaries. To this type of monitoring, some commentators added the reporting of breaches[72] and/or of customer complaints[73] as well as notification to the regulators on significant changes to the Compliance personnel in the companies[74]. However, both a UK and Netherlands industry association were opposed to self-assessment reports to be sent to regulatory authorities. A Netherlands industry association and an IOSCO affiliate member cautioned against the presumption that there was a causal relationship between the number of breaches of securities rules and the effectiveness of the compliance function.

A Nigerian service provider and two European industry associations suggested monitoring by external audits, while a US industry association explained why private external audits were generally not necessary in addition to the various audits, assessments and certification required by the SEC, NASD and NYSE, as well as to the various examination programs conducted by these entities and other federal and state regulators.

Answers that specifically focused on internal assessment of the compliance function by intermediaries included monitoring performed by compliance itself and internal audit. The suggested means included the limited testing of compliance rules as well as the use of statistical sampling checks against a defined test matrix, which, in serious cases, may lead to a review of a wider process that would seem susceptible of failure.

A European industry association proposed assessment and monitoring of the compliance function by internal and external auditors (via review of compliance policy and procedures and their adequacy).

As examples of monitoring activities (whether conducted by a regulator, a private third party or the firm personnel), a US industry association cited direct interaction with the business unit, review of marketing material, physical observations of a trading floor, pre-clearance of certain industries, 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.

[71] Three market intermediaries, two industry associations and one IOSCO affiliate member.
[72] SROCC, an IOSCO affiliate member.
[73] A Singapore firm.
[74] A Singapore industry association.

Response:

The TC takes note of the suggestion by several commentators that the effectiveness of the monitoring method(s) to be used by regulators depended on several factors that could be listed in the means for implementation.

Topic 5 has been modified to reflect the encouragements to regulators and SROs to avoid duplication of reviews and inefficient use of regulatory and internal compliance resources.

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

Several commentators[75] answered that compliance was part of the culture of the entire organization and that it was somewhat misleading to single out the compliance culture as if it were separate from the organization's culture. Two Australian and one US industry associations noted that a strong compliance culture was best established from the top of the organization. Several factors have been put forward by commentators as indicative of a strong compliance culture (see appendix D).

Response:

The TC shares the view of commentators regarding the importance of compliance culture in firms.

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

Most commentators did not suggest additional means (either by answering no, or by not answering the question), some of them pointing at the costs.[76]

Response:

No amendment to the principles is necessary. The TC notes that how regulators supervise their intermediaries will be determined locally by each jurisdiction.

[75] Three industry associations, two IOSCO affiliate members and one market intermediary.
[76] A UK service provider and a European industry association.

Topic 7 – Cross Border issues

Q 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.

Twenty-one commentators responded to this question. They generally indicated that there was a tension between promoting uniformity of a compliance function and accommodating particular ways in which an activity is undertaken or regulated in another jurisdiction. Most commentators characterised the problem in terms of consistency, and in some cases, compatibility of requirements, including addressing differing regulatory standards, as the primary issue for the compliance function of a market intermediary operating in more than one jurisdiction. Differences were variously described as "slight" or "subtle", but sometimes "obvious" or "dissonant" or even "conflicting". Two specific examples were given by the industry as illustrations of the problem: differing disclosure requirements for research analysts' reports dealing with conflicts of interests[77] and differing privacy requirements leading to a situation where information cannot be disclosed in one jurisdiction but must be disclosed in another.[78] The consultative paper did not request comments on proposed regulatory solutions to issues arising for the compliance function in the cross border context. Nonetheless, two of the twenty commentators suggested that the solution to the challenge of complying with different laws was for "national regulators [to] recognize overseas regulatory regimes that have sufficient regulatory equivalence to their own"[79], or to harmonize "the applicable rules" in order to "reduce the administrative burden and costs involved for the market participants."[80]

Associated with the problem of regulatory consistency was the concern by the industry about differing expectations of regulators across jurisdictions and a diverging regulatory culture.[81] As an example for differing regulatory approaches one respondent noted the extent to which regulators were willing to provide specific guidance on specific issues.[82] It was observed that regulators working with principle-based regulation might be more reticent to provide specific guidance or direction on issues.

Two commentators were concerned by the confusion and uncertainty generated by differing degrees of focus on the same regulatory issues by different regulators.[83] This

[77] This example was given by a US industry association.
[78] The privacy example was identified by a Canadian market intermediary.
[79] An Australian industry association.
[80] A Netherlands industry association.
[81] Four commentators specifically spoke in terms of regulatory culture and/or expectations.
[82] This comment was provided by a UK industry association.
[83] A Singapore and German industry association.

problem was also seen in the different pace at which different regulators may address a regulatory issue.[84]

One commentator highlighted the possible import of foreign law into the home jurisdiction if a firm establishes a branch in a new jurisdiction (e.g., establishing of a U.S. presence might subject a European "fund of hedge funds" to U.S. SEC regulation of hedge fund advisers).[85]

Commentators addressed these differences through various techniques. One common approach adopted to manage compliance where an entity was operating in more than one jurisdiction was to design single or universal processes and procedures often referred to as "global compliance"[86]. A number of commentators indicated that they would adopt the most stringent of the various standards to which they were subject. Whilst there are good reasons for such an approach, including ease of monitoring, commentators noted the need for local variations to accommodate legislative differences. However, with such variations there was the potential for greater errors. Applying common standards becomes more difficult as the number of jurisdictions and languages used increases. It was also recognised that the one common approach may result in compliance gaps, as particular issues or concerns applicable to one jurisdiction might not have the same emphasis in another.[87]

Cross border activity is also affected by communication barriers. The communication issue applies both to the understanding of the regulatory and legislative requirements in one jurisdiction and the communication between compliance professionals in different jurisdictions. For example, it was suggested that making the relevant compliance information more readily available would assist compliance professionals keeping up to date with relevant regulatory obligations, as local auditors were sometimes unaware of the legal requirements in other relevant jurisdictions.[88] In addition, at least for three commentators the foreign language of a host jurisdiction presented a compliance issue.[89]

Response:

The comments received highlight the need for a globally active intermediary to understand the applicable laws and regulations in each of the jurisdictions in which it operates, to comply with them, and to take steps to help ensure that it has the necessary personnel and expertise to do so.

[84] A Singapore industry association.
[85] A UK market intermediary. A similar comment was made by a US industry association.
[86] The expression "global compliance" was used by a Canadian market intermediary, an Australian, German and US industry association.
[87] A Canadian market intermediary
[88] SROCC and IOSCO affiliate member.
[89] A French IOSCO affiliate member suggested that national requirements be also available in English. A Singapore and US industry associations also cited language as an issue when operating abroad.

The TC notes a key concern of the commentators is the challenge for a globally active intermediary to comply with the myriad and sometimes conflicting laws in the jurisdictions in which it operates. The TC acknowledges the difficulties that arise from differences in requirements from jurisdiction to jurisdiction.

IOSCO works with its members in addressing cross border issues by promoting the following objectives:

- Cooperation to promote high standards of regulation in order to maintain just, efficient and sound markets;
- Exchanging information on their respective experiences in order to promote the development of domestic markets;
- Uniting their efforts to establish standards and an effective surveillance of international securities transactions;
- Providing mutual assistance to promote the integrity of the markets by a rigorous application of the standards and by effective enforcement against offences.

The TC also points out that the IOSCO *Objectives and Principles of Securities Regulation* contain three principles relating to cooperation in regulation that should assist in the efficient supervision of securities firms that operate in more than one country. These three principles are:

- *Principle 11* - The regulator should have authority to share both public and non-public information with domestic and foreign counterparts.
- *Principle 12* - Regulators should establish information sharing mechanisms that set out when and how they will share both public and non-public information with their domestic and foreign counterparts.
- *Principle 13* - The regulatory system should allow for assistance to be provided to foreign regulators who need to make enquiries in the discharge of their functions and exercise of their powers.

Information sharing arrangements between regulators about interactions with international firms may also assist in more efficient and strategic engagement by securities regulators with international securities firms. Information sharing arrangements have also been considered by the Joint Forum on Financial Conglomerates, which adopted *Framework for Supervisory Information Sharing (Supervision of Financial Conglomerates)* (1999) and *Principles for Supervisory Information Sharing* (1999).

Q 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?

Nineteen commentators responded to this question. Generally, their view was that no single approach to compliance has been shown to be superior to another. The commentators indicated that the design of the compliance function for any organization was a combination of many factors.

The compliance function may complement the existing business structure and management functions to be effective. The nature of the enterprise and range of activity undertaken in a particular country may also affect the performance of the compliance function. For example, if an entity is merely engaged with a counterparty in another jurisdiction, this may require a different compliance arrangement to one where the entity establishes a branch office or foreign-based related entity that undertakes ongoing business.

A compliance structure must be suitable for the particular activity that is being undertaken. For example, it was observed that trading desks were generally subject to a centralized compliance, whilst promotional material, which may need to be in different languages, was generally dealt with by the local compliance function.[90]

Some commentators suggested that the best approach to address the regulatory consistency problem was to identify the highest regulatory standard amongst the various jurisdictions in which the intermediary operates and use that as the global benchmark applicable to that activity worldwide.[91]

A centralized compliance function was identified as a common model of compliance arrangements in cross border situations. Commentators suggested that this model resulted in less divergent practices across the firm worldwide. Some commentators stated that, in countries such as Canada, Australia and Singapore where the indigenous securities firms have a significant international presence, some firms have adopted the model of a centralized compliance function. In such cases, there was also a significant local compliance presence, represented by the existence of senior compliance officers. The extent of the local presence was a function of the size of the local operations and the complexity of the relevant regulation.

Furthermore, for global compliance, the use of matrix reporting was suggested as another way in which reporting may be undertaken. For instance, a model proposed by a German industry association would be comprised of three elements: matters relevant to the central compliance function, regional issues and the compliance responsibilities for the different business areas.

[90] A UK industry association.

[91] The following commentators advocated this exact approach: SROCC, an Australian industry association, a Canadian IOSCO affiliate member and industry association.

Response:

The TC agrees with the majority of commentators that the design of the compliance function should be firm specific. It would therefore be unwise for regulators to seek to dictate a particular compliance structure. The TC also notes the comment that most compliance functions appear to be centralized, but are supplemented by personnel resources with expertise in local jurisdictions. This is consistent with the regulatory approaches in most jurisdictions that allow the creation of a centralized compliance function, as revealed in the results of a survey of standing committee members.[92]

The comments received highlight the need for a globally active intermediary to understand the applicable laws and regulations in each of the jurisdictions in which it operates, to comply with them, and to take steps to help ensure that it has the necessary personnel and expertise to do so. In this regard, the TC believes that the principles set forth under topics 1 and 4 are equally applicable to the cross-border context.

***

[92] See Appendix B

Appendix A

Initial survey among SC3 members regarding the compliance function (September 2004)

Topic 1: Establishing a Compliance function

Purpose of the compliance function

A majority of SC3 members indicated that the purpose of a compliance function is to ensure that the market intermediary is complying with securities regulatory requirements. This purpose is either explicitly stated or implicit in the legislation. A small number of SC3 members do not have requirements for market intermediaries to establish a compliance function or to designate compliance officers, instead they place the responsibility for compliance on senior management.

Scope and activities of the compliance function

In jurisdictions where there is a requirement to establish a compliance function or to designate compliance officers, the accountability of the compliance function or designated compliance officers do not vary, regardless of the nature, scale and complexity of the market intermediary's business. However, most jurisdictions recognize that the scope and activities of the compliance function or designated compliance officers, and the structure of a compliance function, will differ based on the nature, scale and complexity of the business. The differences lie in how the compliance function or designated compliance officers carry out their responsibilities. In general, smaller firms with simple business are expected to have simpler compliance functions and less complex policies and operational procedures and controls, provided that the firm is able to demonstrate that its compliance arrangements are effective.

Keeping informed of all relevant laws and amendments thereof

Pakistan has a specific requirement, in their statutes or under a Code of Conduct that intermediaries keep informed of all relevant laws and amendments. In Australia, Germany, Hong Kong, Ontario and Quebec (Canada), Spain, Switzerland, the UK and the US SEC, there is no specific statutory requirement, however the obligation to keep informed could be implicitly understood from the wording of the legislation, for example from continuing education requirements or from requirements to comply with securities regulatory requirements. In Japan, the heads of the compliance departments are obliged to maintain contact with government agencies and SROs to keep up to date. In France, compliance officers, as part of their obligation to prepare a procedures handbook, are required to inform staff and agents of some or all of the provisions mentioned in the handbook.

In Ontario and Quebec (Canada) and the U.S., the SROs impose a continuing education program on registered individuals, which serves as a tool to ensure that these individuals are kept informed of current regulatory requirements.

Designation of a specific organizational structure for compliance

Although most jurisdictions require the establishment of a compliance system or function, they do not specify a particular organizational structure. Germany, Italy, Spain and Switzerland require the establishment of a compliance structure that ensures compliance with relevant laws and regulations, but no specific requirements are imposed. Similarly, Australia, France, Hong Kong, Ontario and Quebec (Canada), the U.K., US CFTC, and US SEC. require market intermediaries to have compliance arrangements, measures and/or procedures in place to ensure compliance with relevant regulatory requirements but do not specifically refer to a structure.

In the U.S., NASD member firms are required to establish and maintain a system to supervise the activities of each registered representative and associated person that is reasonably designed to achieve compliance with applicable securities laws and regulations, and with NASD rules. NYSE member firms are required to establish a compliance structure based on their size, type of business, customer base, and product mix. For example, each office, department, or business activity of a member or member organization (including foreign incorporated branch offices) must be under the supervision and control of the member or member organization establishing it and of the personnel delegated such authority and responsibility. The NYSE has also adopted a rule that requires members and member organizations to develop and maintain adequate internal controls over each of its business activities and include procedures for independent verification and testing of those business activities.

Supervision of registered or licensed individuals
In most cases, the requirement to supervise individuals is part of the general statutory requirement (Ontario and Quebec (Canada), Australia, France, Germany, Japan, Hong Kong, Mexico, Pakistan, Spain, Singapore, US SEC and US CFTC).

In Ontario and Quebec (Canada), and the U.S., SROs also place specific requirements on their members for the supervision of individuals who conduct regulated activities.

In the U.K., firms are required to put in place appropriate supervision arrangements with respect to relevant personnel within the firm.

Internal reporting by the compliance function

The internal reporting requirements for independent compliance personnel differ by jurisdiction. Germany, Italy, Mexico and Spain require compliance personnel to report directly to the board of directors, while Hong Kong requires a report to senior management and France requires the compliance officer to report to senior management on the conditions under which investment services are supervised.

Likewise, in Japan, the head of compliance must report immediately to the president of the company in the case of a serious issue. In the U.S., the NYSE requires its members to submit to its chief executive officer or managing partner an annual report on the member's supervision and compliance effort during the preceding year. In Ontario and Quebec (Canada), the SROs for investment dealers and mutual fund dealers require that the compliance officer report periodically to the board of directors or senior management on the dealer's compliance with securities regulatory requirements.

Notification of breaches of securities regulatory requirements

Many jurisdictions require an intermediary to timely notify the regulator of breaches of specific conduct of business requirements and/or financial regulations. For example, in Australia, a licensee must notify ASIC in writing within five days of a significant breach of its obligations under the Corporations Act taking into account whether the breach impacts the licensee's ability to provide its financial services or results in an actual or potential financial loss to clients or the licensee itself. Similarly, in Singapore, member companies of the Singapore Exchange are required to inform the exchange in writing if any of its employees or agents breaches any relevant law or regulation, the Exchange's rules or directives, the rules of any other exchange, any provision involving fraud or dishonesty, or is the subject of any written complaint or investigation involving fraud or dishonesty.

Other jurisdictions require the intermediary to promptly notify regulators of any breach of financial regulations. For example, the regulator and SROs in Ontario and Quebec (Canada) and US CFTC require registrants to give immediate notice to the regulator if it's adjusted net capital at anytime is less than certain minimums. US SEC rules require intermediaries to send telegraphic or facsimile notice to the Commission upon the occurrence of certain events, including when a broker-dealer's or an OTC derivatives dealer's net capital falls below required levels, if a broker-dealer or OTC derivatives dealer fails to make and keep current the books and records required by exchange rules, if a consolidated supervised entity (CSE) or a supervised investment bank holding company (SIBHC) becomes aware that any financial regulatory agency or SRO has taken significant enforcement or regulatory action against a material affiliate, and if an SIBHC becomes ineligible to be supervised by the Commission as a supervised investment banking holding company. In Singapore, once a license holder becomes aware of its non-compliance with capital requirements, it should immediately notify the MAS, as well as the securities exchange, futures exchange or clearing house of which the licensee is a member, of the non-compliance.

In Japan, intermediaries must notify the regulator of all breaches of all laws and regulations. If a breach of the Securities and Exchange Law is significant, the regulator will take administrative action.

In the U.K., the FSA requires firms to notify it immediately of any significant rule breach by the firm or any of its employees.

Topic 2: Role of Senior Management and the Governing Authority

Accountability

All jurisdictions hold the market intermediary responsible for establishing a proper compliance function and policies and procedures. Some jurisdictions specifically refer to the board of directors, while others refer to senior management. Nine jurisdictions place ultimate accountability to regulators for compliance with securities regulatory requirements on the board of directors of an intermediary.[93] Seven jurisdictions hold senior management accountable for compliance.[94] In Italy, however, while the board of directors is ultimately responsible to regulators, there are a number of minor infringements (such as violations or infringement of a non-systematic nature) where the responsibility would not be directly allocated to the board of the firm but to management. Singapore's securities legislation explicitly holds the chief executive officer and directors of an intermediary liable for any non-compliance. Topic 6 also contains discussion on certification requirements on senior management.

Seven jurisdictions, including France, Japan, Ontario and Quebec (Canada), Singapore, US CFTC and US SEC, place responsibility for compliance on registered/licensed persons as well as senior management. For example, US CFTC's statute states that any CFTC registrant who, directly or indirectly, controls any person who has violated any provision of the *statute or regulations* may be held liable for such violation to the same extent as the controlled person, unless the controlling person acts in good faith.

Establishment of internal policies and procedures

Most jurisdictions have specific statutory obligations that require intermediaries to establish, maintain and comply with effective policies and procedures to prevent violation of securities regulatory requirements (France, Germany, Hong Kong, Japan, Mexico, Ontario and Quebec (Canada), Singapore, Spain, Switzerland and the U.S.).

In Ontario and Quebec (Canada), requirements are also established under rules of the SROs to which the intermediaries belong. In Australia, the requirements are set by a general license condition applied by ASIC and it is a statutory requirement for a licensee to comply with their license conditions.

---

[93] The board of directors is ultimately responsible for compliance in Australia, Germany, Italy Mexico, The Netherlands, Pakistan, Singapore, Spain and Switzerland.

[94] Senior Management is ultimately responsible for compliance in Ontario and Quebec (Canada), Hong Kong, France, US CFTC, US SEC and the U.K. The US SEC may hold a board responsible under appropriate circumstances.

In Pakistan, the requirement is implied, as intermediaries are subject to a statutory requirement for annual audit reviews.

Designation of a compliance officer

France, Germany (for some of the regulated firms), Hong Kong (for fund managers only), Japan (Japan SRO sets such requirements), Mexico, The Netherlands, Ontario and Quebec (Canada), Pakistan, and US SEC and its SROs, require the designation of a "chief compliance officer" or some other designated title such as "internal supervisor". The U.K. requires investment firms to allocate to a director or senior manager the function of (a) having responsibility for oversight of the firm's compliance and (b) reporting to the governing body in respect of that responsibility.

US SEC requires that the board of directors of a registered investment company appoint a chief compliance officer. The rule requires the chief compliance officer to provide a written report to the board, no less frequently than annually, that addresses, among other things, each "material compliance matter" (a defined term) that has occurred since the date of the last report. In addition, persons designated as compliance officers under NASD and NYSE rules must meet certain requirements.

Topic 3: Independence and Ability to Act

Independence

About half of the jurisdictions responding to the survey have requirements pertaining to the independence of the compliance function.[95] Generally, these jurisdictions require compliance personnel to operate separately from any business unit they monitor. For example, Spanish regulations require that individuals in the compliance function must not be involved in the businesses they monitor. Here, the budget and remuneration for the compliance function must ensure objectivity and must not be linked to the financial performance of the firm. Similarly, France and Hong Kong require compliance officers or function to operate independently of all the business units they monitor.

Nearly half of the jurisdictions responding appear not to have independence requirement at all. [96,97] Some regulators recognize the difficulty in ensuring independence for the compliance function in some market intermediaries. In a small organization or branch office, it maybe difficult to have complete independence as the person with primary responsibility for compliance may also

[95] General independence requirements exist in France, Italy, Japan, Hong Kong, Mexico, Singapore, Spain, Switzerland and the U.K.

[96] Germany does not have specific independence requirements on small firms, but requires compliance personnel in larger firms to be independent from all operational and business functions.

[97] Jurisdictions with no independence requirements for the compliance function include Australia, The Netherlands, Ontario and Quebec (Canada), Pakistan, US CFTC and US SEC.

trade and/or provide advice. In this regard, the NYSE has adopted NYSE Rule 342.19, which addresses the independent review of producing branch office managers.[98] The NASD has amended its Rules 3010 and 3012, to align certain supervisory control and inspection requirements with the corresponding supervisory control and inspection requirements in NYSE Rule 342.19 and NYSE Interpretation Handbook provision 342(a)(b)/03.[99]

Prescribed human and/or material resources

No jurisdiction responding to the survey has a specific requirement regarding human and/or material resources that should be devoted or available to the compliance function. Each jurisdiction has a general requirement that the compliance function should be provided with sufficient resources to carry out the activities required by appropriate regulations.

Topic 4: Qualification of Compliance Personnel

Current requirements in all the jurisdictions of SC3 members conform to the above principle. However, jurisdictions vary widely on how they implement this principle. For example, France, Japan, Ontario and Quebec (Canada) and the US SROs have detailed requirements, including registration as a sales representative, successful completion of prescribed courses, successful completion of prescribed examinations, and/or participation in a continuing education program. Other jurisdictions have no specific requirements, but, nonetheless, require that compliance personnel be "competent." It should also be noted that a few jurisdictions have implemented continuing training or education requirements on market intermediaries to ensure that they are kept up-to-date on securities regulatory requirements under a fast changing business and regulatory landscape.

In the U.S., under NASD Rule 1120, governing continuing education requirements, compliance staff that are registered as principals are required to take the appropriate "Regulatory Element" of the continuing education requirement on the second anniversary of the initial securities registration and every three years thereafter. Under NYSE rules, a Branch Office Manager must take the General Securities Sales Supervisor Qualification Examination (Series 9/10) and the General Securities Registered Representative Examination (Series 7). The Chief Compliance Officer must take the Compliance Official Qualification Examination (Series 14). In addition, NYSE Rule 342.13 (a) (Acceptability of Supervisors) requires that the supervisors of any branch office, regional

[98] It is worth noting that the US CFTC and SEC both require financial audits and anti-money laundering audits to be completed by independent personnel. In addition, with respect to advisers to funds, rule 38a-1 under the U.S.'s Investment Company Act of 1940 (the "Investment Company Act") requires each registered fund to appoint a chief compliance officer (CCO) who is responsible for administering the fund's policies and procedures approved by the fund's board under the rule. The rule contains several provisions designed to promote the independence of the CCO from the management of the fund.

[99] See SEC Release No. 34-50477; File No. SR-NASD-2004-116; *69 FR 59972*.

or other group of offices, or any sales department or activity must have a creditable three year record as a registered representative or equivalent experience in addition to passing the Series 9/10, or another examination acceptable to the Exchange that demonstrates competency relevant to assigned responsibilities. NYSE Rule 342.13 (b) requires that the person (or persons) designated to direct day-to-day compliance activity (such as the Compliance Officer, Partner or Director) and each other person at the member organization directly supervising ten or more persons engaged in compliance activity should have overall knowledge of the securities laws and Exchange rules and must pass the Series 14 test. NYSE Rule 345(A) states that no member or member organization shall permit any registered person to continue, and no registered person shall continue, to perform duties as a registered person, unless such person has complied with the continuing education requirements. Each registered person must complete the Regulatory Element of the continuing education program upon their second registration anniversary date and every three years thereafter or as otherwise prescribed by the Exchange.

In Canada, rules of the AMF, the OSC, the IDA and the Mutual Fund Dealers Association of Canada impose specific proficiency requirements on compliance officers at advisers and dealers. Specifically, compliance officers at advisers must complete one of the prescribed courses and certain practical experience and compliance officers at dealers must complete one of the prescribed courses. In addition, the IDA imposes continuing education requirements on the compliance officers of its members and an examination requirement on the Chief Financial Officers (CFO) of its members (the CFO is generally responsible for a member's compliance with the IDA's prudential requirements).

In Japan, compliance personnel, referred to as internal administration supervisors (IAS), must first be qualified as a sales representative. Second, they must pass a special IAS examination administered by the Japan Securities Dealers Association (JSDA). Third, they must be a manager or hold higher position. Finally, they must participate annually in a JSDA administered training program, and also in a training program of his/her own securities company.

Topic 5: Assessment of the Effectiveness of the Compliance Function

Role of external auditors in the effectiveness of a compliance function

External auditor's role differs from jurisdiction to jurisdiction, in terms of the scope of its responsibility regarding a firm's compliance, as well as its obligation to notify the regulators of its findings.

In the majority of the jurisdictions surveyed, external auditors are required to notify the regulators of their findings (e.g. Australia, Germany, Hong Kong, Ontario and Quebec (Canada), Singapore, Spain, Switzerland and the U.K.). However, there are some jurisdictions that only require external auditors to report their findings to the firm's

management (who may, in turn, be required to notify the regulators). In the U.S., broker-dealers and OTC derivatives dealers are required to file with the US SEC an annual audit report conducted by an independent accountant, and where there are material inadequacies with the accounting system, the independent accountant is required, under special circumstances, to report directly to the US SEC on such material inadequacies. [100]

The scope and focus of an external auditor's review differs in different jurisdictions. External auditors may review (i) the intermediary's compliance with securities regulatory requirements, or (ii) the adequacy of the intermediary's compliance function (for instance, external auditor will report on issues such as internal controls). However, it is noted that jurisdictions focusing on (ii) are also concerned with breaches of securities regulatory requirements by the market intermediary, and require external auditors to notify them of such breaches.

Germany, Italy, Mexico, Pakistan, Singapore and Switzerland require external auditors of their intermediaries to report on the adequacy of the intermediaries' compliance function. Germany requires the compliance function to be assessed in relation to the intermediary's size, business structure, and number of accounts and volume of transactions. Italy requires the compliance function to be assessed on its independence from the intermediary's business operations, its authority within the intermediary, its working methods and the skills of its staff.

In Ontario and Quebec (Canada), the SROs require the external auditors of their members to report on the existence of specific internal controls; however, the external auditors are not required to report on the overall effectiveness of a compliance function. The French Banking Commission requires their intermediaries to submit annual report on internal control to external auditors for review. UK FSA requires external auditors to submit an auditor's report but this report is not explicitly required to cover compliance issues. However, auditors are required by accounting standards to assess the extent to which a firm has complied with relevant laws and regulations.

Topic 6 Regulators' Supervision

Examinations by regulators and/or SROs

Most jurisdictions conduct examinations of compliance function as part of their general oversight or surveillance of market intermediaries, whether regularly or on a risk-based approach (Australia, France, Hong Kong, Italy, Japan, Mexico, The Netherlands, Ontario and Quebec (Canada), Singapore, Spain, Switzerland, the U.K. and US SEC). In addition, in four jurisdictions, examinations are conducted via SROs for the firms they regulate (Ontario and Quebec (Canada), Pakistan, and US SEC). In two other jurisdictions, regular examinations are conducted via external auditors (Germany and Switzerland).

[100] Exchange Act Rule 17a-5 (h) (2) and Exchange Act Rule 17a-12 (i) (2).

In addition, Spain explicitly refers to the examination of the compliance function they conduct at the time of license application, and requires the filing of the internal code of conduct of market intermediaries. France and Italy conduct examinations via the review of annual report from compliance officer.

Examination and notification requirements on external auditors

A large majority of jurisdictions (12 out of 16) replied that external auditors had a role to play in ensuring an intermediary's compliance. Australia, Hong Kong, The Netherlands, Ontario and Quebec (Canada) and Spain require the external auditor of a market intermediary to notify the regulators of the intermediary's compliance with (part or all of) securities regulatory requirements. In the U.S., broker-dealers[101] and OTC derivatives dealers[102] must all file with the U.S. SEC an annual audit report conducted by an independent accountant. If, during the course of the audit or interim work, the accountant determines that any material inadequacies exist in the accounting system, internal accounting control, procedures for safeguarding securities, or as otherwise defined, the accountant must call it to the attention of the broker-dealer's chief financial officer, who must inform the U.S. SEC and the broker-dealer's designated examining authority by telegraphic or facsimile notice within 24 hours and furnish the accountant with a copy of the notice. If the accountant fails to receive such notice from the broker-dealer, or if the accountant disagrees with the statements contained in the notice, the accountant must inform the U.S. SEC and the designated examining authority by report of material inadequacy within 24 hours thereafter. Similar requirements apply to commodity brokers regulated by the CFTC. Germany, Italy, Mexico, Pakistan, Singapore, and Switzerland require the external auditors of their market intermediaries to review or report on the adequacy of the intermediary's compliance function.

Some jurisdictions further highlight the requirement that external auditors notify the regulator of an intermediary's non-compliance with relevant rules and regulations. These jurisdictions include Australia, Germany, Hong Kong, Italy, Singapore and The Netherlands. Australia specifically requires an external auditor to notify within seven days any breach of financial requirements. Australia and Singapore specify further that any adverse effects on the licensee's ability to meet its license conditions or any cases of fraud/dishonesty respectively must be reported.

In the U.K., auditors have a role to play to the extent that they are required to assess the extent to which a firm has complied with relevant laws and regulations. Auditors also have a duty to report contraventions by the firm of any relevant requirement, where that contravention would be of material significance to the UK FSA. Meanwhile, firms should consider notifying the FSA if the firm receives a written communication from its auditor commenting on internal controls.

[101] Exchange Act Rule 17a-5.
[102] Exchange Act Rule 17a-12.

Reporting and notification requirements

In addition, nine jurisdictions require a periodic report relating to part or all of the compliance functions to be filed with the regulator.[103] France requires an annual report to the AMF by the supervisor of investment services on the conditions in which investment services and assimilated services are supervised. In addition, a report on internal controls should be established each year and sent to the senior management of the market intermediary, its board, its audit committee, external auditors, and the Banking Commission.

One jurisdiction, Mexico, requires a compliance report to be filed with the regulator "if necessary." In Mexico, regulations empower the Commission to require, at any moment, any information it deems necessary to perform its supervisory functions, including a compliance report.

Certification

Those jurisdictions that require a certification as to the adequacy of part or all of an intermediary's compliance arrangements place at least part of this burden on the external auditor, which must examine the financial controls, and sometimes other aspects of the compliance function and attest to their adequacy. Five jurisdictions require such a certification[104], where the external auditor is required to notify regulators annually of a market intermediary's compliance with internal conduct rules. Of the five jurisdictions requiring certification, three jurisdictions further require senior management to certify the adequacy of the intermediary's compliance function.[105]

In the U.S., NASD Rule 3013 requires that each member's CEO (or equivalent officer) 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 NASD rules, MSRB rules and federal securities laws and regulations.

While Hong Kong and Singapore do not require a formal certification, auditors are required to express an opinion on the adequacy of systems of controls relating to compliance with client asset protection rules and the intermediary's compliance with other specified rules. Upon becoming aware of any non-compliance issues, intermediaries should report to the Commission. While Australia has no specific requirement for certification of the adequacy of the compliance arrangements as a

[103] Compliance reports must be filed with the regulator in the following jurisdictions: France, Germany, Italy, Ontario and Quebec (Canada), Pakistan, Spain, Switzerland, US CFTC and US SEC.
[104] Certification requirements exist in Germany, Pakistan, Spain and Switzerland. US CFTC requires certification relating to financial compliance.
[105] These jurisdictions include Ontario and Quebec (Canada) and Pakistan.

whole, all directors of a managed investment scheme's responsible entity must sign the compliance plan of the scheme.

Examples of jurisdictions requiring no formal certification of the compliance function include The Netherlands. France, which has no procedure of certification, holds senior management responsible for ensuring compliance with the general rules of conduct that the firm and persons acting on its behalf must comply with.

Enforcement actions

All regulators have the authority to bring enforcement actions against market intermediaries relating to their compliance function. This authority is set within the wider context of the regulators' power to bring enforcement action against the intermediaries they have licensed for breaches of the law or of the license obligations or conditions. Regulators have the ability to impose penalties and remedies, including requiring enhancement to the intermediaries' compliance function.

Penalties may include:

- reprimand or warning to the management,
- fines towards a market intermediary or natural persons placed under its authority or acting on its behalf,
- imposing additional license conditions,
- suspension or revocation of the license of a market intermediary and/or its licensed or registered persons,
- suspension or expulsion from membership of SROs,
- actions on the corporate officers involved in breach of the compliance duty in relation to market misconduct (such as requiring dismissal and temporary interdiction of taking new functions as manager or director in another licensed intermediary),
- requiring that the intermediary be compelled to undertake the assistance of an independent consultant, at its own expense, to perform a review of its compliance function and implement any recommendations made by the independent third party,
- a letter to the board of the intermediary raising certain issues and asking for a response to those issues in writing,
- issuing a media release identifying the licensee's offences and the remedy imposed by the regulator,
- liquidation of the intermediary, and
- criminal prosecution by judicial authorities.

Appendix B

Survey of SC3 Members
Centralization of Compliance Function at Market Intermediaries

Further to the comments received on this issue during the public consultation, a survey was conducted among jurisdictions represented in SC3 in order to gain an understanding of the regulatory regime in these jurisdictions. The survey included the following questions:

(1) Cross border consolidation. If a foreign securities firm provides services in your jurisdiction (whether via a subsidiary or branch), would your jurisdiction allow compliance to be centralized within the foreign firm? If so, is this permission subject to any minimum requirements such as requiring:

- Local technical expertise within the foreign firm, and/or
- At least one individual to be present locally who has the ability to deal (at least to an initial degree) with local compliance issues in a timely manner.

(2) Domestic consolidation. If a securities firm is part of a domestic financial institutional group (whether a subsidiary or branch), would your jurisdiction allow compliance to be centralized with the group? If so, is this permission subject to any minimum requirements such as requiring:

- Local expertise within the securities firm, and/or
- At least one individual to be in the securities firm who has the ability to deal (at least to an initial degree) with securities law compliance issues in a timely manner.

The following is a summary of the responses received to this survey.

Responsibility for compliance remains almost always with the regulated entity. As a general rule, the regulated entity is responsible for its compliance and cannot shift that responsibility even where centralization or outsourcing is allowed.

All jurisdictions allow firms to consolidate the compliance function at the domestic level. The majority of jurisdictions also allow consolidation of the compliance function within a foreign based entity. However, in some jurisdictions, the compliance function cannot be centralized outside the domestic jurisdiction with the consequence that each subsidiary and affiliate of a foreign firm must have its own compliance department or compliance officer. For example, NYSE member firms are required to maintain their principal place of business in the United States, which means that the compliance function must be centralized in the U.S. It is also the case in Japan as well as in Mexico, when the

domestic customers' assets account for more than 1.5% of the industry's total. Similarly, an EU Member State firm that has a subsidiary rather than a branch[106] in another Member State must establish local compliance arrangements. EU based subsidiaries of non-EU firms are also required to establish a local compliance function and are not allowed to centralize the compliance function (Germany, Spain, France). In contrast, the NASD does not require its foreign based member firms to have an office or branch in the U.S., which essentially means that the compliance function could and most likely would be centralized abroad, especially since the NASD requires that the compliance function remain under the member's direct control.

Whether the compliance function is consolidated domestically or in a foreign jurisdiction, the majority of jurisdictions require that there be at least one person in charge of compliance at the level of the regulated entity (e.g., a chief or global compliance officer). Thus, a general principle seems to be that a presence at the level of the regulated entity is required in both, domestic and cross-border consolidation.

However, there are exceptions to this general principle:

- where the consolidation in the foreign based firm is permitted, there are some instances where a local compliance presence is not required at all (e.g., NASD, although additional requirements are imposed on the foreign firm in the absence of a local office, and branches of EU firms within the European Union). In other jurisdictions, this may depend on the type of business (e.g., in Australia, whether the foreign firm's underlying business is desk based, such as derivatives dealing) and other issues such as the foreign firm's skills and depth of experience in the compliance function, knowledge of the local compliance regime and proximity of the foreign firm to the local office;
- in the context of domestic consolidation, there is a greater willingness among regulators to allow complete consolidation. In those jurisdictions which allow complete consolidation, the presence of a person in charge of compliance at the level of the regulated entity is not required. In the U.S., however, all such firms must have a chief compliance officer.

[106] As long as the firm uses its 'European passport' to establish a *branch*, compliance is a matter for home member state supervision.

Appendix C

Examples of the main responsibilities and tasks of the compliance function

The following is a list of tasks and responsibilities that may be within the compliance function, created by a combination of tasks indicated by regulators and of tasks indicated by commentators. Firms are not necessarily expected to include all of these in their compliance function.

- Identifying regulatory risks;
- Advice to management, including during the design of internal controls in respect of regulatory risks;
- Ensuring that a business supervisory structure is in place;
- Detection, prevention and management of conflicts of interest;
- Defining and monitoring information barriers;
- Monitoring of areas of potential market manipulation / insider trading monitoring;
- Industry surveillance;
- Anti-money laundering functions including advising on and developing of a firm's money laundering deterrence programme;
- Data privacy, net capital and financial responsibility compliance;
- Monitoring (or ensuring that an internal audit function undertakes such monitoring) of a firm's activities, using a risk-based approach, to confirm, or otherwise, adhere to the policies and procedures designed by the firm to address securities regulatory requirements. As a consequence of this monitoring, the compliance function should present a status report to management;
- Cooperation with the operational risk function and legal service to provide a specific model for management of the intermediary's liability for specific crimes committed by employees on behalf of the intermediary;
- Provide systems, structures and behaviours that engender compliance without undue emphasis on the narrow legal requirements, but rather the broader issues included in codes of conduct, internal policies and procedures etc;
- Dealing with customer complaints;
- Identification and monitoring of data or privacy security and protection;
- Prevention of undue disclosure of confidential information;
- Records and documentation, including safeguards for the privacy protection of client records and information;
- Licensing and registration of the firm and its registered personnel;
- Internal inquiries and investigations, a role that can be played by any or a combination of several control functions within a firm, and may involve the use of third parties;
- Monitoring and surveillance of business units to identify potential issues, including, *inter alia* the handling of customer accounts, including the opening of new client accounts, proprietary trading, and employee-related trading and communications;
- Oversight of risk function and business contingency planning;

- Participating in the rule commenting process, e.g. consultation process, in particular by collating business management comments;
- Participating in industry committees and working groups;
- Measures to identify and document qualifications of individual employees to provide regulated services;
- Compliance with conduct of business rules by the firm and its staff;
- Supervision of advice provided to clients;
- Supervision of the various duties relating to information to clients and marketing information;
- Education and training to keep business personnel and other employees apprised of policies, procedures, regulatory requirements and how to comply with such requirements;
- Staff education programme that should also include explanation of weaknesses or non-compliance noted during any audits or inspection;
- Promotion of ethical behaviour among staff and colleagues;
- Advice to senior management on disciplinary issues, including terminations;
- Escalating compliance issues to management (and if this is to no avail, to an audit/compliance committee or independent directors);
- Periodic reporting to regulatory authorities;
- Acting as the liaison for the regulators with the firm.

Appendix D

The following is an aggregate list of the factors that commentators made individually to the consultative paper that were considered as indicative of a firm's strong compliance culture:

Strong support from top management for the importance of the compliance function:

- Top management and the governing authority's role in encouraging compliance, including:
  - Clear set of published values of the securities firm
  - Management actively seen to be implementing the values
  - A consistency in reward and punishment for similar actions regardless of position - management willingness to take enforcement action on staff,
  - The incorporation of compliance performance in every position description
  - Willingness of management to add compliance personnel when necessary

- Strong culture of social responsibility;
- Principles of compliance evidenced at every level of the structure, permeating the company;
- Management action that occurs independent of compliance;
- Clear communication of compliance priorities to all employees by senior management;
- Alignment of individual objectives to corporate objectives and values;
- Creating incentive structures that reward compliant behaviour and penalize behaviour that sacrifices compliance principles.

Factors related to the organization of the compliance function, such as the existence of sound compliance policies and procedures, sufficient resources being devoted to compliance activities, the quality of reporting lines to senior management, the quality of compliance personnel:

- The existence of technically sound compliance policies and procedures, to enable the compliance function to operate independently and their effective communication throughout the entity, as well as compliance benchmarks against which all relevant staff can be assessed;
- Strong Chinese walls and, for firms that have complex organizations, 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;

- Sufficient resources devoted for compliance activities (including training in regulatory environment and ethics);
- Existence of a clear, well thought-out mandate for the compliance function as well as clear independent role;
- Giving personnel with compliance responsibilities regular and unfettered access to senior management;
- Clear and well-used lines of reporting;
- Periodic compliance reporting to senior management / board of directors;
- Reporting of weaknesses and violations to senior management / board of directors;
- Direct reporting relationship;
- Training and competence requirements for overseers and approved persons requirements for senior management and directors;
- Designated compliance officers and supervisory monitoring by senior management;
- Clear and articulated procedures for self-assessment and other forms of testing of compliance controls;
- Low turn over in personnel.

Factors directly related to the qualities of the compliance function, such as:

- Demonstrated confidence of the organization in the advice given by its compliance function;
- Compliance representation on significant business committees as well as in the discussion, assessment and implementation of proposed business initiatives or in new product development;
- Good working relationship and ongoing communication between the compliance function and the businesses being monitored;
- The quality of the responses to compliance problems;
- Proactive rather than reactive approach to compliance - willingness on the part of compliance personnel to identify problems independently, work on appropriate solutions to problems that are identified;
- Assessing what is the right thing to do instead of looking for rules;
- Proactive in the development and promulgation of new industry standards;
- Avoiding relying on regulators to identify compliance deficiencies;
- Strong role for compliance regarding advising the business;
- Active participation in industry groups that provide an opportunity to share best practices, discuss emerging issues;
- Internal and external reviews of the compliance function result in consistently good ratings.

Factors to be evaluated with regards to staff, such as:

- Understanding of the commercial returns from an effective compliance function;

- Staff commitment to compliance (via awareness of employees of the importance of conforming to the compliance policy and program, and of their role responsibilities within the program);
- Compliance training and awareness;
- Sales force made of salespeople without disciplinary records.

Factors linked to litigation and customer complaints:

- Few litigation matters and small number of client complaints;
- Low number of unresolved complaints;
- Lack of material or substantive regulatory issues that arise or that have arisen in the past;
- Low number of compliance issues;
- Minor infractions;
- Low or no records of fraud;
- Few repeat cases or lack of repeat recommendations in internal audit and compliance monitoring reports;
- Few penalties imposed;
- Effective relationships with regulators and lack of regulatory censure;
- Firm's reputation.