PUBLIC COMMENTS RECEIVED
ON THE IOSCO TECHNICAL COMMITTEE
CONSULTATION REPORT ENTITLED
COMPLIANCE FUNCTION AT MARKET INTERMEDIARIES

INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS

February 2006

List of Organizations that have provided comments:

- French Association of Investment Firms (AFEI)
- Zentraler Kreditausschuss (ZKA)
- Associazione Italiana Intermediari Mobiliari (ASSOSIM)
- Banca Intesa S.p.A
- The Netherlands Bankers' Association (NVB)
- Barclay's
- Bundesverwand Investment und Asset Management e.C (Germany) (BVI)
- National Association of Independent Broker-Dealers (NAIBD)
- The European Federation of Financial Analysts Societies (EFFAS)
- Vereniging van Compliance Officers (VCO)
- Futures and Options Association (FOA)
- Australian Stock Exchange Limited (ASX)
- The International Banks and Securities Association of Australia (IBSA)
- International Financial Data Services Limited ("IFDS")
- The Investment Funds Institute of Canada ("IFIC")
- The Investment Management Association of Singapore (IMAS)
- SRO Consultative Committee
- The Investment Management Association (IMA)
- Japan Securities Dealers Association (JSDA)
- London Investment Banking Association (LIBA)
- Man Financial Singapore
- National Futures Association (NFA)
- FCMBA Capital Market Limited

- Price Waterhouse Coopers
- Bank of North Trustees Limited
- Adejumo Ekisola & Ezeani
- Royal Bank of Canada (RBC)
- The Securities & Derivatives Industry Association
- The Securities Association of Singapore
- The Securities Industry Association (“SIA”)
- TD Bank Financial Group
- The Australian Compliance Institute

Par email : mail@oicv.iosco.org

Une version française de ce document est disponible en page 9.

"Compliance Function at Market Intermediaries"

Consultation Report
- IOSCO -

Response of the French Association of Investment Firms (AFEI)

The Technical Committee of the International Organisation of Securities Commissions (IOSCO) released a consultation report in April 2005 on the compliance function at market intermediaries. With the emergence and development of the compliance function, evidenced in the projects undertaken by IOSCO, the Basel Committee and European institutions, IOSCO's committee deemed it important to set out some high-level principles applicable to compliance.

The French Association of Investment Firms (AFEI), which became an affiliate member of IOSCO in April of this year, has examined the consultation report carefully. AFEI has some 130 members, all of whom are highly active in the equity and derivatives market. Nearly one-third are subsidiaries of foreign institutions.

Broadly, AFEI has noted an increasing tendency for the same issues to be addressed in different forums. And since these bodies pursue different angles of approach, the standards they produce are not always consistent. We therefore support IOSCO's approach, provided it ultimately harmonises the parameters of the compliance function. This function is crucial for market intermediaries since they operate almost entirely on a cross-border basis and thus find it difficult to cope with regulatory discrepancies.

However, the goal of harmonisation cannot be reached unless the principles set out by IOSCO are accepted as a foundation on which all future developments can be built, regardless of which body is responsible for deciding on those developments.

I. Establishing a compliance function *(pp 6 - 7 of the IOSCO report)*

➢ Questions asked by IOSCO

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

Yes, we agree with IOSCO's definition because it is consistent with the definitions framed in other European or international projects such as those of the Basel Committee. Although these projects are aimed squarely at internationally active banks, many countries have also applied them to other categories of market intermediary. As we pointed out in our introductory remarks, it is absolutely essential to harmonise and achieve consistency between the rules produced by different bodies.

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?***

The answer to this question depends on how the intermediaries in question are organised. There is absolutely no need to adopt a prescriptive approach that would prevent intermediaries from linking the two functions if they so choose. Whatever the circumstances, and unless IOSCO can prove otherwise, AFEI cannot see any conflict of interest that would prevent them from doing so.

II. Establishing a compliance function *(pp 8 - 13 ibid)*

AFEI wholeheartedly supports IOSCO's proposal that the compliance function be tailored to the intermediary's size and the nature of its business. We recall that, in view of the increasingly stringent demands placed on financial intermediaries, the possibility for new players to enter the market and enliven competition has been sharply reduced. From this standpoint, acknowledging factors such as size and business scope is an initial and vital response to this problem.

- **Questions asked by IOSCO**

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

No, it should not. Once again, unless we see evidence to the contrary, we believe that financial intermediaries should be given as much leeway as possible in deciding how the compliance function is organised. This will depend on the intermediaries' size and business activities.

The only fundamental principle that should apply is that the head of compliance must be independent and have the human and material resources needed to perform his or her duties.

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

It is important for the regulator to identify and clearly define the core activities of the compliance function. The list of activities proposed by IOSCO *(pp 8 and 9 ibid)* seems to be a sound basis for discussion, provided that any references to laws, regulations and procedures are confined to "securities regulatory requirements", as defined by the Basel Committee, so as to achieve the objective of consistency and uniformity at international level.

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

AFEI finds that the proposals put forward by IOSCO *(pp 8 and 9 ibid)* cover all the basic principles that must be respected. Accordingly, no additional proposals are needed.

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

It is important to respect the boundaries between compliance and operating risk control, or accounting control. Moreover, to forestall conflicts of interest, it is essential to ensure that the control and advisory functions are kept separate at all times.

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?

Naturally, all intermediaries engaged in the same line of business must comply with the same obligations in principle. That said, documenting internal procedures is obviously a more burdensome and costly process for small and midsized firms than for large ones.

Therefore, so as not to put small firms at a disadvantage or in difficulty, the rules for preparing internal documents should be tailored not only to the nature of each firm's business activities but also to the level of risk that these activities entail, both for the financial system as a whole and for the firm's clients. On this last point, unless it is proven that small firms should not exist, the principle that clients should bear no risk whatsoever even though they have been properly informed is not workable.

III. Role and responsibilities of the board of directors or senior management *(pp 14 - 16 ibid*)

- **Questions asked by IOSCO**

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****.*

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

As an association, AFEI cannot provide the requested description. We would point out, however, that issues relating to the responsibility of compliance officers at financial intermediaries are vitally important at a time when these persons are playing an increasingly crucial role and, as a result, have more and more responsibility.

Logically, the general principle should be that the head of compliance does not take on the full burden of answerability, that is to say liability, responsibility and accountability, unless he or she is at the highest echelon of management (board level) and has powers commensurate with that position. A head of compliance at a lower hierarchical level will have a lesser level of answerability, i.e. he or she will be both responsible and accountable.

At present, firms have very different organisational structures – depending on their size, their businesses and also their corporate culture – as regards levels of responsibility, positioning, competence, presence/participation on management bodies, internal delegation of powers, and so on.

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

Yes. At the very least, the head of compliance should have industry-related experience and knowledge that will enable him or her to identify problems on a daily basis.

IV. Independence of the head of compliance *(pp 17 - 19 ibid)*

As we said in our answer to question 3, AFEI supports the IOSCO approach, which stresses the independence of the head of compliance, as is the case with the work of the Basel Committee.

- **Questions asked by IOSCO**

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

In smaller firms, the head of compliance obviously cannot hold only that one position. That a person holds several positions, including head of compliance, does not necessarily infringe the principle of independence on which the compliance function must necessarily be predicated. The main difficulty lies in the way that the function is linked with the firm's business activities.

Whatever the circumstances, a compliance officer will be all the more independent if he or she occupies a senior position in the hierarchy and has the resources needed to perform their duties.

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?***

AFEI does not think that an individual should be responsible for compliance in the business lines for which he or she has managerial responsibilities. In our view, this would create a conflict of interest.

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

Yes, the means proposed by IOSCO for ensuring the independence of the compliance officer seem to be sufficient. The key resources include:

- compensation of the head of compliance and his support team;
- freedom of action and expression;
- having the resources necessary for overseeing compliance procedures and ensuring the observance of laws, rules and professional standards;
- direct access to the board of directors or senior management to discuss material shortcomings in compliance (pp *17 and 18 ibid*).

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

In our response to a previous consultation, on implementing measures for the Markets in Financial Instruments Directive, we pointed out that, in principle, awarding a bonus to the compliance officers is legal and does not pose a problem provided the bonus is discretionary, related to the person rather than the office, and rewards the quality of his or her work. Under these circumstances, the scope of any prohibition should be limited simply to a ban on awarding a wage or bonus related to a specific transaction undertaken by the intermediary.

Moreover, to enable the compliance department to recruit persons from different business lines inside the firm, the compensation rules must to some extent be flexible and consistent with those in force in other departments. For some firms, the key issue will be to create two-way traffic between its functions, making sure the compliance department has people with hands-on experience of the business line they supervise and bringing individuals with a compliance culture into business lines.

V. Qualification of compliance personnel *(pp 20 - 21 ibid)*

- **Questions asked by IOSCO**

15. ***What are the appropriate qualifications for compliance personnel?***

The appropriate qualifications are:

- integrity
- a critical mind
- neutrality
- independent judgment
- educational and communication skills
- knowledge of the industry and prevailing regulations

These personal qualities must be maintained or enhanced through regular training and practical exercises.

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

There is no clear-cut answer to this question. The entire compliance team should be given suitable training in the operations or activities they are required to carry out. However, given the extent to which these activities can vary within a single compliance department, several types of training programme are needed. More broadly, educating compliance personnel consists in organising training programmes for them and regularly updating their knowledge, especially as regards regulatory developments. In any case, it is up the head of compliance to assess the needs of each individual in his or her team to ensure they have the resources needed to acquire knowledge and keep it current.

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

As an association, AFEI is unable to answer this question. It is a fact that the broad range of skills involved in compliance makes it hard to choose appropriate training programmes and that only an individual assessment is truly effective.

VI. Assessment of the effectiveness of the compliance function *(pp 22 - 23 ibid)*

- **Questions asked by IOSCO**

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

Above all, it must be stressed that responsibility for the effectiveness of the compliance function lies with management. It is management that decides, in the light of its assessment, whether to rely on internal and/or external audits.

Be that as it may, there are no grounds for claiming that external audits are intrinsically superior to internal audits. Everything depends on the organisation and business scope of the intermediary.

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

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

The real question is whether the compliance function should actually be outsourced, since many of these external parties do not always have the necessary level of skill. To make sure that an external audit will be effective, it is first necessary to examine the compliance-related aspects of these parties, e.g. their organisation and resources, their expertise in compliance and their grasp of prevailing laws and regulations, and the smooth flow of information.

In any case, it should be remembered that an external audit consists primarily in examining how the compliance function is organised. Assessing the content of the function itself is solely an internal task.

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

The answer to this question depends on several factors, including the size of the intermediary and the nature of its business. It is these factors that determine the level of risk and, hence, the frequency with which controls should be carried out, whether once a year or once every four years.

VII. Regulators' supervision *(pp 24 - 28 ibid)*

- **Questions asked by IOSCO**

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

Effective regulatory supervision hinges on a proper understanding of the objectives of regulation. In many cases, it would help if these objectives were explained in greater detail.

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

Respect for compliance means more than simply observing rules and regulations or preparing appropriate internal codes. It is a mind-set, which must be understood and accepted by intermediaries and regulators alike.

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

The effectiveness of a regulatory framework depends directly on the way in which it deals with certain basic business-related realities and on how it is accepted by the parties to which it applies. In this respect, AFEI believes that a preliminary, interactive dialogue between the regulator, representative associations and the industry is absolutely vital in order to spell out the objectives of regulation and thus identify the most appropriate solutions.

VIII. Cross-border issues *(p 29 ibid)*

- **Questions asked by IOSCO**

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.***

For firms operating in several jurisdictions – an everyday fact of life for financial intermediaries – the main problem is to identify differences arising from national systems built on legal and cultural foundations which, while similar, are always different.

Although this problem seems inevitable, AFEI has noticed that it can be mitigated by improving access – especially via the Internet – to the texts making up a country's statutory framework. Although many countries, including France, have made efforts in this area, major hurdles still exist. For example, some texts are hard to access while others are available in the national language only whereas they should be translated into English at least.

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?***

There is no single answer to this question, because everything depends on the firms in question. That said, it is certain that the presence of a local head of compliance makes country-specific issues easier to understand.

Contact: Aurélie Cauche
Compliance Director
AFEI
13 Rue Auber 75009 Paris, France
Email: acauche@afei.com, tel: +33 1 53 83 00 86

"Compliance Function at Market Intermediaries"

Consultation Report
- IOSCO/OICV -

Commentaires de l'AFEI

Le *Technical Committee* de IOSCO (OICV) a publié en avril 2005 un *consultation report* relatif à la fonction de conformité des intermédiaires de marché. Face à l'émergence et à l'évolution de la fonction de conformité (Cf. les travaux menés par IOSCO, le Comité de Bâle, les institutions européennes), le comité technique de IOSCO a estimé important de définir quelques grands principes que les intermédiaires de marché doivent appliquer en ce qui concerne le secteur de la conformité.

L'AFEI, qui est membre affiliée de IOSCO depuis le mois d'avril dernier, a attentivement examiné le document ainsi produit par IOSCO. L'AFEI regroupe environ 130 adhérents particulièrement actifs sur les marchés actions et dérivés, dont à peu près un tiers sont filiales de groupes étrangers.

De manière générale, l'AFEI constate que, de façon de plus en plus fréquente, les mêmes sujets sont traités au sein de différentes enceintes qui, ayant des angles d'approche différents, produisent des normes dont la cohérence est parfois discutable. Aussi, l'AFEI est favorable à la démarche entreprise par IOSCO si elle doit permettre d'harmoniser les « paramètres » de la fonction *Compliance*, particulièrement décisive chez les intermédiaires de marché dont l'activité presque totalement transfrontières s'accommode mal des divergences de réglementation.

L'harmonisation ainsi souhaitée ne pourra néanmoins être effective que si les grands principes dégagés par IOSCO sont reconnus comme formant le socle à partir duquel doit être envisagée toute évolution ultérieure, et cela quelle que soit l'enceinte au sein de laquelle cette évolution pourra être déterminée.

IX. Définition de la fonction conformité *(page 6 à 7 du document de IOSCO)*

- **Questions posées par IOSCO**

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

Oui, car la définition de la fonction Conformité proposée par IOSCO est cohérente avec celle fournie dans le cadre des autres travaux européens et internationaux tels que ceux du Comité de Bâle. Ces travaux, bien que ne visant expressément que les banques actives à l'international, sont dans de nombreux pays déclinés également sur les autres catégories d'intermédiaire de marché. Comme cela a été souligné à titre liminaire, la cohérence et l'harmonisation entre les différents corps de règles édifiés au sein de différentes enceintes sont tout à fait essentielles.

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?***

La réponse à cette question dépend de l'organisation des intermédiaires financiers en cause. Il n'y aucune raison d'adopter une démarche prescriptive en ne laissant pas la possibilité à ces derniers de pouvoir ou non lier ces deux fonctions. En tout état de cause, et sauf à ce qu'IOSCO fournisse la démonstration contraire, l'AFEI estime qu'il n'existe pas de conflit d'intérêts de principe qui s'y opposerait.

X. La mise en place d'une fonction de conformité *(page 8 à 13 du document de IOSCO*)

L'AFEI soutient totalement la proposition de IOSCO visant à une fonction Conformité adaptée à la taille et aux activités des intermédiaires. Elle rappelle que l'élévation croissante du niveau d'exigences pesant sur les intermédiaires financiers a pour conséquence de réduire fortement les possibilités pour de nouveaux acteurs, « stimulateurs » de concurrence, d'entrer dans les activités de marchés financiers. De ce point de vue, la prise en compte de la taille et des activités menées constitue une première réponse absolument nécessaire par rapport à cette problématique.

- **Questions posées par IOSCO**

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

Non. Sauf encore une fois à ce que la nécessité contraire puisse être établie, l'AFEI considère qu'il convient de laisser un maximum de flexibilité aux intermédiaires financiers dans la détermination de l'organisation matérielle de la fonction Conformité. Cette organisation dépendra de la taille et des métiers de ces structures.

Le seul principe fondamental qui doit s'imposer est que le Responsable de la conformité soit indépendant et dispose des moyens matériels et humains indispensables à la réalisation de sa tâche.

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

Il est important que le cœur d'activité de la fonction de conformité soit identifié et clairement défini par le régulateur. La liste de ses missions telle que proposée par IOSCO *(page 8 et 9 du document)* apparaît une bonne base de réflexion étant entendu que toute référence aux lois, règlements et procédures doit être entendue comme limitée aux *« securities regulatory requirements »*au sens
retenu par le Comité de Bâle pour atteindre l'objectif de cohérence et d'uniformisation de la fonction au niveau international.

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

L'AFEI considère que les propositions faites par IOSCO *(pages 8 et 9 du document IOSCO)* contiennent tous les principes fondamentaux qui doivent être respectés. Elle n'estime donc pas nécessaire de formuler des propositions complémentaires.

6. ***How and when should the compliance function be responsible for managing compliance risk?***
Il est important de respecter les frontières entre les différentes activités que sont la Conformité et le contrôle du risque opérationnel, voire, la comptabilité. Il est par ailleurs essentiel de toujours s'assurer, au risque de voir apparaître un conflit d'intérêts, que les fonctions de contrôle et de conseil sont bien distinctes.

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?***

Il est bien évident que tous les intermédiaires ayant la même activité doivent répondre aux mêmes obligations de principe. Néanmoins, la mise en œuvre de documents de procédures internes dans les petites ou moyennes structures induit nécessairement un niveau de contrainte et un coût proportionnellement plus élevés que dans les grandes structures.

De ce fait, afin de ne pas défavoriser ou mettre en péril les petits établissements, les conditions de documentation interne ne doivent pas seulement être adaptées aux types d'activités menées par chaque établissement, mais également au niveau de risque que ces activités induisent tant vis-à-vis du système financier dans son ensemble que de leurs clients. Sur ce dernier point, et sauf à établir que la présence de petits établissements est indésirable, il ne peut être considéré que par principe le client ne peut supporter aucun risque dès lors qu'il est suffisamment informé de ceux-ci …

XI. Rôle et responsabilité de l'organe exécutif et de l'organe délibérant *(page 14 à 16 du document de IOSCO)*

- **Questions posées par IOSCO**

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****.*

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

De par sa nature, l'AFEI n'est pas en mesure de procéder à la description demandée. Elle souligne toutefois que les questions relatives à la responsabilité du *compliance officer* / responsable conformité au sein des intermédiaires financiers, revêtent une importance toute particulière à une époque où ce dernier acquiert un rôle de plus en plus central dans l'entreprise et, a donc corrélativement, plus de responsabilités.

En toute logique, le principe général devrait être que le Responsable de la conformité ne saurait assumer l'intégralité des responsabilités décrites *(liable + responsible + accountable*) que s'il se situe dans l'organigramme de l'établissement au plus haut niveau hiérarchique (membre du board) et détient les pouvoirs en rapport avec son positionnement. *A contrario*, le Responsable de la conformité aura une responsabilité plus limitée (*responsible + accountable*), s'il se situe plus bas dans l'échelle hiérarchique.

Aujourd'hui, des schémas d'organisation très différents existent dans les établissements en fonction de leur taille, de leurs activités, mais aussi de leur culture d'entreprise, en termes de niveau de responsabilité, de positionnement, de champ de compétence, de présence ou non au sein des organes de direction, de délégations internes de pouvoir …

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

Oui. Le Responsable de la conformité doit avoir un minimum d'expérience et de connaissance « métier » lui permettant de détecter correctement les problèmes du « *day-to-day* ».

XII. Indépendance du responsable de conformité *(page 17 à 19 du document de IOSCO)*

Comme elle l'a déjà exprimé *(voir réponse à question 3)*, l'AFEI est favorable à l'approche de IOSCO qui, comme dans le cadre des travaux du comité de Bâle, insiste sur l'indépendance du Responsable de conformité.

- **Questions posées par IOSCO**

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

Il est évident que la taille de certains intermédiaires ne permet pas que le titulaire de la fonction conformité n'exerce que cette seule fonction. Le fait d'exercer plusieurs fonctions, dont celle de Responsable de la conformité, n'est pas nécessairement en soit une atteinte au principe d'indépendance qui doit animer le titulaire de la fonction. La principale difficulté réside en fait dans les conditions de l'articulation de la fonction Conformité avec les lignes *business*.

En tout état de cause, l'indépendance du Responsable de la Conformité sera d'autant plus effective que ce dernier se situera au plus haut niveau hiérarchique et disposera des moyens nécessaires à la réalisation de sa mission.

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?***

L'AFEI n'est pas favorable à ce qu'une personne puisse être Responsable de la conformité sur les lignes d'activités dont elle par ailleurs le responsable hiérarchique. Elle estime en effet qu'il y a en l'espèce conflit d'intérêts.

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

Oui. Les moyens proposés par IOSCO pour garantir l'indépendance du Responsable de la conformité apparaissent suffisants. Ceux qui paraissent essentiels sont, entre autre :

- la rémunération du responsable de conformité et de l'équipe qui l'assiste ;
- la liberté d'action et d'expression ;
- le fait de disposer des moyens nécessaires au contrôle des procédures de conformité et du respect des lois, règles et normes professionnelles ;
- l'accès direct à l'organe exécutif ou délibérant de l'établissement pour discuter des défaillances significatives de conformité (*page 17 et 18 du document IOSCO*).

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

A l'occasion des observations formulées dans un autre cadre (élaboration des mesures d'exécution de la directive MIF), l'Association a rappelé que le principe d'un bonus octroyé au *compliance* est licite et ne soulève pas de difficulté en soi, pourvu qu'il soit discrétionnaire, lié à la personne du *compliance*, ainsi qu'à la qualité de son travail. Il convient dès lors de limiter la portée d'une éventuelle prohibition en interdisant uniquement qu'un salaire/bonus soit lié à une opération spécifique de l'intermédiaire.

Par ailleurs, il doit être rappelé que pour que le département Conformité puisse recruter des personnes issues des différentes lignes de métiers de l'établissement, il faut que les règles de rémunération puissent être un tant soit peu adaptables et souples et en phase avec ce qui se pratique dans les autres départements. L'enjeu pour un certain nombre d'établissements est de créer une perméabilité entre ses différentes fonctions : adjoindre au département Conformité des personnes qui ont l'expérience effective du métier qu'elles contrôlent ; introduire dans les départements business des personnes ayant une vision Conformité.

XIII. La qualification de l'équipe du responsable de la conformité *(page 20 et 21 du document de IOSCO)*

- **Questions posées par IOSCO**

15. ***What are the appropriate qualifications for compliance personnel?***

Les qualifications nécessaires sont :

- l'intégrité ;
- l'esprit critique ;
- la neutralité ;
- une certaine indépendance de jugement ;
- des capacités pédagogiques et de communication ;
- une connaissance du métier et de la réglementation applicable.

Ces qualifications personnelles doivent en outre être entretenues / accrues au travers de :

- formations et entraînements réguliers ;
- formations aux procédures de contrôle de la conformité adaptées.

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

La réponse ne peut être univoque. Toute l'équipe « conformité » doit bénéficier d'une formation adaptée aux opérations ou activités qu'elle effectue mais, compte tenu de la variété de ces activités au sein même du pôle Conformité, différents types de formation sont nécessaires. Plus largement, la sensibilisation du personnel du pôle doit être organisée aux travers d'actions de formation et d'une actualisation régulière des connaissances des collaborateurs, notamment en termes d'évolutions réglementaires. En tout état de cause, il revient au Responsable de la conformité d'évaluer les besoins de chaque personne au sein de son équipe pour assurer qu'il dispose des moyens nécessaires pour accroître et actualiser les connaissances dont il a besoin.

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

De par sa nature, l'AFEI n'est pas en mesure de répondre directement à la question posée. Elle souligne qu'il est un fait que la diversité des compétences rend complexe le choix des formations à délivrer et que seule une appréciation individuelle peut être totalement efficace.

XIV. Evaluation et efficacité de la fonction de la conformité *(page 22 et 23 du document de IOSCO)*

- **Questions posées par IOSCO**

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

Il doit avant tout être rappelé le fait que l'effectivité de la fonction Conformité est de la responsabilité de l'organe de direction. C'est à lui qu'il appartient de déterminer si dans le cadre de cette évaluation, il convient de s'appuyer sur l'audit interne et/ou externe.

En tout état de cause, il ne peut être affirmé que par essence l'audit externe sera plus efficace que l'audit interne, car tout dépend de l'organisation et du périmètre d'activité de l'intermédiaire.

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

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

Aujourd'hui, c'est la question de l'opportunité même de l'externalisation de la fonction conformité qui se pose, car un certain nombre de ces structures externes n'ont pas forcément la compétence nécessaire. L'effectivité de l'audit externe passe donc en premier lieu par un examen de l'aspect « compétence » de ces structures (organisation, moyens, maîtrise de la fonction Conformité, des textes en vigueur et fluidité de l'information…).

En tout état de cause, dans le cadre d'un audit externe, rappelons qu'il s'agit essentiellement d'un contrôle du mode d'organisation de la fonction conformité, le contrôle du contenu de la fonction étant réservé à une appréciation interne.

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

La réponse à cette question dépend de plusieurs facteurs dont celui de la taille de l'intermédiaire, de la nature de ses activités…. Ces facteurs conditionnent le niveau de risque et donc la fréquence des contrôles à opérer (évalué entre une fois par an et une fois tous les quatre ans).

XV. La supervision des régulateurs *(page 24 à 28 du document de IOSCO)*

- **Questions posées par IOSCO**

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

L'effectivité de la supervision du régulateur passe avant toute chose par une bonne compréhension des objectifs de régulation, qui gagneraient, souvent, à être mieux explicités.

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

Le respect de la conformité va au-delà du respect des textes et de la constitution des codes internes adéquats, il s'agit d'un véritable état d'esprit, qui doit être compris et intégré par les établissements, mais aussi par les régulateurs.

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

L'efficacité d'une réglementation est directement liée tant aux conditions dans lesquelles elle prend en compte certaines réalités incontournables de l'activité qu'à son acceptation sociale par les acteurs auxquels elle s'applique. De ce point de vue, l'AFEI considère que le dialogue préalable et intéractif entre le régulateur, les associations représentatives et les professionnels est tout à fait indispensable pour préciser les objectifs de régulation assignés et, en conséquence, dégager les solutions les plus appropriées.

XVI. Les problèmes de frontières *(page 29 du document de IOSCO)*

- **Questions posées par IOSCO**

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.***

Pour les établissements intervenant de manière transfrontières, ce qui pour les intermédiaires financiers constituent une réalité quotidienne, la principale difficulté consiste à appréhender les différences nées de systèmes nationaux construits sur des bases juridiques et culturelles, parfois proches mais toujours différentes.

Si cette difficulté semble incontournable, l'AFEI constate toutefois qu'elle peut être réduite au travers d'une meilleure accessibilité (notamment par Internet) des différents textes qui forment chaque cadre juridique national. De ce point de vue, si des efforts certains ont été effectués par de nombreux pays, dont la France, il existe néanmoins encore d'importants problèmes : textes non disponibles aisément ou textes disponibles seulement dans la langue nationale alors qu'au moins une version anglaise est nécessaire …

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?***

Il n'y a pas de réponse univoque, car cela dépend des établissements. Il est néanmoins certain que la présence d'un Responsable de la conformité au niveau local facilite l'appréhension des problématiques propre au pays concerné.

ꕥ O ꕥ

Z E N T R A L E R K R E D I T A U S S C H U S S
MITGLIEDER: BUNDESVERBAND DER DEUTSCHEN VOLKSBANKEN UND RAIFFEISENBANKEN E.V. BERLIN · BUNDESVERBAND DEUTSCHER BANKEN E.V. BERLIN BUNDESVERBAND ÖFFENTLICHER BANKEN DEUTSCHLANDS E.V. BERLIN · DEUTSCHER SPARKASSEN- UND GIROVERBAND E.V. BERLIN-BONN VERBAND DEUTSCHER HYPOTHEKENBANKEN E.V. BERLIN

Philippe Richard
IOSCO Secretary General
Oquendo 12
28006 MADRID
SPAIN

via e-mail: mail@oicv.iosco.org

10178 Berlin, den 13 July 2005
Burgstraße 28
AZ ZKA: 413-COMPL
AZ BdB: Hu/Sto – K 26.5.1

Public Comment on *Compliance Function at Market Intermediaries*

Dear Mr. Richard,

The Zentraler Kreditausschuss welcomes the opportunity to comment on IOSCO's discussion paper "*Compliance Function at Market Intermediaries"* and is pleased to enclose a document outlining our joint position.

If you have any queries regarding our comments, please do not hesitate to contact us.

Yours sincerely
on behalf of the Zentraler Kreditausschuss,
Bundesverband deutscher Banken

Herbert Jütten Stefanie Heun

Comments of the Zentraler Kreditausschuss[1] on IOSCO's Discussion Paper *Compliance Function at Market Intermediaries*

April 2005

13 July 2005

[1] The ZKA is the joint committee operated by the central associations of the German banking industry. These associations are the Bundesverband der Deutschen Volksbanken und Raiffeisenbanken (BVR), for the cooperative banks, the Bundesverband deutscher Banken (BdB), for the private commercial banks, the Bundesverband Öffentlicher Banken Deutschlands (VÖB), for the public-sector banks, the Deutscher Sparkassen- und Giroverband (DSGV), for the savings banks financial group, and the Verband deutscher Hypothekenbanken (VdH), for the mortgage banks. Collectively, they represent more than 2,300 banks.

I. General Remarks

The Zentraler Kreditausschuss (ZKA) thanks IOSCO for the opportunity to comment on the Discussion Paper *Compliance Function at Market Intermediaries* and welcomes the basic approach adopted by IOSCO in formulating its principles. Detailed rules on the organisation and structure of the compliance function would not take account of the diverse nature of the companies to which the principles are addressed. Both their size and their business strategies differ considerably from one another. The compliance organisation required by a globally active multinational group will obviously be different to that needed by a small bank with a regional focus. International compliance standards will therefore only do justice to these differences if they remain as abstract as possible. Such an approach would also guard against the risk of possible inconsistencies with other compliance initiatives currently under way and, in particular, with the implementation of the Directive on Markets in Financial Instruments (MiFID). CESR's advice to the European Commission for technical implementing measures of the MiFID, published in January 2005, deals in detail with the role of compliance, compliance policies and procedures. When, at the end of the legislative process, the EU legislation has been implemented in member states, uniform compliance standards will apply throughout Europe. It is essential that any international standards are consistent with these rules.

II. Answers to Specific Questions for Comment

Definition of the Compliance Function and Scope

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

We agree with the wording and scope of the definition, which focuses on securities compliance. It will avoid the compliance function at a market intermediary having to carry out an indeterminably broad range of activities and responsibilities. Definitions aiming at including all kinds of risk tend to result in involving the compliance function in every issue carrying a potential risk. This can lead to "responsibility overload", making it difficult to maintain the oversight needed. It should also be borne in mind that compliance is a specific regulatory requirement for investment firms. The complex legal requirements which they have to fulfil make it necessary to maintain a compliance function. Extending the scope of this function beyond the requirements specific to the regulation of the securities business would not only lack any objective justification, but would also fail to give equal treatment to investment firms and other undertakings. The final sentence of the explanatory remarks on page 6 should therefore be deleted: ~~*A compliance function of a*~~

~~*firm should also have mechanisms in place to protect the firm from any liability arising from abuses committed by its customers*~~.

We strongly recommend incorporating the interpretation of "function" in footnote 10 in the body of the definition itself. This is a key point and needs to be highlighted more clearly. The same goes for the statement – which we warmly welcome and which is reiterated repeatedly in the consultation paper – to the effect that the scope, structure and activities of the compliance function will depend on the nature, scale and complexity of the market intermediary's operations. This should also be included in the definition, or at least be part of the principles.

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?

The responsibilities of compliance and risk management are different. These functions normally operate independently of one another. Nevertheless, there can occasionally be overlaps. The risk management function is often sent a copy of the compliance report for information, for instance. The company's senior management, which is responsible for both functions, is the "linking pin". Only it can decide exactly how to divide responsibilities between the two. It is therefore not possible to generalise about who should be assigned the task of dealing with which specific risk. The important point is that all risks are adequately addressed.

Establishing a Compliance Function

Means for Implementation

Principle (b) (6) on page 9 suggests that the compliance function should notify regulators of any misconduct by the firm even if this is not required by law. We firmly reject any such obligation. First of all, it fails to take account of the differences between member states in the way regulators operate (cf. for details Topic 6, Regulators Supervision, on page 24 f. of the consultation paper, which points out that notification is only one of several measures that regulators can employ to supervise companies). Second, it totally ignores the fact that penalties or fines may be imposed for misconduct in some member states and that, in this case, an obligation to notify regulators would infringe on the right not to have to incriminate oneself. What is more, the entire workforce's trust, which is a sine qua non for performing compliance duties, would be seriously undermined if employees believed any information they gave to the compliance function might be

passed on to the regulators. This is why CESR included no such notification requirement in the advice it issued to the European Commission in January 2005 on technical implementing measures for the MiFID. It is therefore essential to delete the second part of Principle (b) (6): … ~~*where notification is not required by law or regulation, consider notifying the regulators of any misconduct by the firm and the firm's actions with respect to such misconduct, including efforts to prevent future violations*~~.

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

We feel that the organisational structure of a compliance function will depend on various factors. This starts with the regional and operational dimension of the market intermediary and its business. The legal and regulatory environment and the whole culture of conducting business are important factors, too. We are also aware that business is changing at a more rapid pace than ever before. In our view, the needs of both market intermediaries and regulators can only be fulfilled if the aims and tasks of a compliance function are defined in an abstract manner and if the way these aims are fulfilled is left up to each intermediary. The structure of a compliance function will usually reflect the structure of the business. The needs of a small intermediary with a low level of specialisation, for example, can be fulfilled by a corresponding compliance function. A diversified, highly specialised business, on the other hand, will require a more sophisticated compliance function to respond to its needs. A specific organisational structure should therefore not be prescribed. This view, moreover, reflects current, tried-and-tested practice (cf. page 10 f. of the consultation paper).

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

Given the need for the compliance function to be flexible and adaptable, as mentioned above, roles or activities should not be mandated. This is not to say that these roles will not exist, but only that they will evolve from the way of fulfilling regulatory needs. The responsibilities of a compliance function may depend on the way regulation is carried out and on how breaches or infringements are sanctioned in the various jurisdictions.

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

As stated above, we do not recommend the allocation of specific responsibilities to the compliance function.

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

The complex matter of risk management should be carried out by the structure with the optimal fitness for this task at the market intermediary. Only the individual firm can therefore decide who should be entrusted with managing compliance risk in any specific instance (cf. also our reply to question 2).

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?

Only a qualified reply may be given to this question since there is no universally accepted interpretation of the terms “compliance policy” and “compliance procedure”. If “policy” is to be understood in the Anglo-Saxon sense of comprehensive rulebooks, this cannot be applied to member states where requirements are set out in laws and regulatory codes. Additional documentation of these legal and regulatory requirements would be duplication and is therefore to be rejected. As a matter of principle, the extent of documentation must be in reasonable proportion to the importance of the function to be documented.

The decision regarding how staff and other individuals working for the firm are to be kept informed of compliance requirements (cf. page 10 of the consultation document) should also be left to the firm itself. The important point is that it can be verified that compliance requirements have been effectively communicated.

Role and Responsibilities of the Board of Directors

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.

In Germany, the board of managing directors generally has overall accountability for compliance with the applicable laws, rules and regulations. Internal accountability depends on individual responsibility. Managers at all levels, each within their sphere of responsibility, have to know and understand the applicable laws, rules and regulations and establish appropriate policies, procedures and controls to ensure compliance. They

must also have reasonable measures in place to ensure that the employees are informed of, know and understand all applicable laws, rules and regulations and that the employees comply with them.

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

We make a distinction because the different terms relate to different specific aspects. But the meaning of these terms varies widely from one jurisdiction to another, so it should be left to each legislator to establish concrete definitions.

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

Here, too, the answer will depend on the firm's size and the type of business it is engaged in. In an intermediary with complex operations (in the sense of the number and/or variety of transactions and the scale/type of its cross-border business), a senior compliance officer is often responsible for day-to-day compliance. Small and medium-sized intermediaries, on the other hand, normally have extremely flat hierarchies and thus no senior compliance officer or even any specific compliance officer at all. Compliance tasks (such as oversight, organisational issues) are often divided among a number of different employees who have the necessary independence to carry out their compliance responsibilities (cf. next topic). A member of the board will normally be directly responsible for co-ordinating compliance tasks in such cases.

<u>Independence and Ability to Act</u>

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

In principle, all the requirements mentioned in the consultation paper are fulfilled by small firms, too.

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?

These cases must be avoided. If this is not possible, it should be transparent to the regulator (e.g. by asking for prior consent or having a cross-check by the regulator or an independent party).

The situation is different, however, when compliance personnel are assigned from an organisational point of view to the business units they supervise. This type of set-up can be entirely appropriate, both in large, globally active groups and in smaller investment firms. The expertise needed to monitor certain business activities will often be best found in the unit performing those activities. The important point is to ensure that compliance personnel on no account monitor themselves.

13. Are the means for implementation of independence set out above sufficient to achieve independence? Please explain.
Yes. We know of no experience to the contrary.

14. How do you ensure that compensation of compliance personnel is not subject to undue influence? Please explain.
Fixed compensation schemes for compliance personnel make it possible to avoid undue influence on the compliance function via compensation. These fixed schemes should include definitions of the extent to which compliance personnel participate in the firm's success and bonus plans.

Qualification of Compliance Personnel

15. What are the appropriate qualifications for compliance professionals?
There is no one-size-fits-all answer to this question. Qualifications depend first and foremost on the tasks to be performed and the nature, volume and complexity of the firm's business.

The following are minimum qualifications:

- rule expertise;
- expertise in analysing and interpreting rules;
- a strong understanding of the business, its products and processes;
- universal skills such as good presentation and communication skills, strong interpersonal skills and creative problem-solving abilities.

The more complex the business and the greater the risks involved, the more extensive the qualifications will naturally need to be.

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

As mentioned above in our reply to question 15, qualifications will depend on the nature, volume and complexity of the firm's business. The type of position to be filled within the compliance function may also be a determining factor.

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

Given the diversity of compliance tasks, which will vary considerably depending on the individual firm, it would not be appropriate to require compliance personnel to have completed specific courses or passed specific examinations. The firm should deploy personnel who are adequately qualified to carry out the tasks they are expected to perform. There is no one answer to how the necessary qualifications can be acquired. This also applies to the qualifications required in other areas, especially supervisory and monitoring functions (e.g. internal auditing, risk control).

Assessment of the Effectiveness of the Compliance Function

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

The German system is based on double checking by internal and external auditors. Both examine whether shortcomings have been detected and lessons learned. Assessments should always be carried out by qualified professionals with an understanding of different organisational structures and sufficient flexibility to check every intermediary as a unique organisation, without giving preference to certain solutions or structures.

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

See our reply to question 18.

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

Among the practical concerns are possible conflicts of interests, e.g. an auditor should not be remunerated for other services. To enable an external assessment to go into depth without tying up inappropriate resources at the intermediary, the period and the topics to be assessed should be clearly defined in advance by the auditor and/or regulator.

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

The scope and frequency should vary depending on the type of business of the intermediary. In general, assessments should not be carried out more often than once a year unless there is a special reason for doing so. The frequency of the assessments should give the firm sufficient time to implement any changes in processes or activities identified as necessary in prior assessments.

The possibility cannot be excluded that the wide-ranging harmonisation of the securities business in Europe (including the area of compliance) will also have an impact on the type and scope of external auditing. IOSCO should refrain from prescribing excessively strict rules ahead of these possible future developments.

With this in mind, principle (b) should be amended to include the following qualification: *In addition to any internal evaluations, and where required by law and regulation, the compliance function should be subject to periodic review by independent third parties, …*".

Regulators' Supervision

Reporting and notification requirements

We should like to point out in connection with footnote 30 on page 26 that, in Germany, only intermediaries that deal with compliance-relevant information on a regular basis have to prepare a compliance report at least once a year. Only the firm's senior management receive a copy of the compliance report direct. It is possible, however, that the report may also be mentioned in the external auditor's report.

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

This also depends on the intermediary's business and the type of risk it has to face. Where standardised transactions are concerned, monitoring can be done by random sample. If transactions are not standardised, monitoring should be carried out on the basis of an adequate database of comparable transactions or should be checked manually if the volume of transactions justifies this.

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

A strong compliance culture is characterised by the fact that compliance is accepted and practised throughout the firm. The prerequisites for this are that compliance is seen as one of the firm's core tasks and is accepted as such by the entire staff. The term "compliance culture" thus indicates a firm's sensitivity to compliance tasks. No concrete organisational criteria can be inferred, however.

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

No. The consultation paper covers all major aspects (see in particular our reply to question 3).

Cross Border Issues

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.

- Determining the hierarchy of cross-border regulations.
- Determining the applicability of the various rules in the various regulatory jurisdictions in respect to a cross-border transaction.
- Different regulatory requirements in different jurisdictions for the same issue, e.g. equity threshold reporting.

- Differing degrees of focus on the same regulatory issue by different regulators can lead to uncertainty and confusion, e.g. “hot topics”.

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?

- For a global compliance organisation, a matrix reporting/communication structure could be followed based on a three-column approach, with one central function column, a second column reflecting regional responsibilities and a third column reflecting the responsibilities for the different business areas of an intermediary.
- Information relating to the various cross-border regulatory requirements could be disseminated via regular news letters/bulletins both to the various compliance officers and business lines, e.g. *Compliance Informs* or *Compliance Alert*.
- The compliance function could develop and conduct training programmes on specific cross-border issues.

PIAZZA BORROMEO 1 - 20123 MILANO
TEL. 02/86454996 R.A.
TELEFAX 02/867898
e.mail assosim@assosim.it
www.assosim.it

ASSOSIM®

ASSOCIAZIONE
ITALIANA
INTERMEDIARI
MOBILIARI

Milano, 15th July 2005
Sped96-07-05
MCO/mco

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

RE: Consultation Report – Compliance Function at Market Intermediaries.

ASSOSIM is the Italian Association of Financial Intermediaries, which represents the majority of Italian investment firms, banks and branches of foreign institutions, active in the Investment Services Industry (see the Members' list enclosed).

ASSOSIM is keen to participate in the open and transparent consultation process carried out by the IOSCO. We deeply believe in the importance of the dialogue between the Institutions and the Industry for shaping a balanced legislative framework of investment services.

The premise of the Consultation Report is the increased focus on compliance by regulators in different jurisdictions in the world. We appreciate indeed the will of the Organisation to raise a discussion at international level which will contribute to get as much "harmonisation" of different legislations as possible in the perspective of a global financial market. We are very sensitive to this problem since in Europe we are witnessing the experience of the integration of financial markets, but we are all aware that this is only the first step in the right direction and that the dialogue with other countries in the world is also a key issue.

Given the increasing attention to this issue we would suggest the Authorities to look for as much consistency as possible among the documents they issue (i.e. Basilea).

Definition of the Compliance Function and Scope

Before addressing to the specific questions below, we would like to make some considerations on the sentence in the paragraph C) on the definition of the Compliance Function which requires such function "to have mechanisms in place to protect the firm from any liability arising from abuses committed by its customers".
We have some difficulties in understanding what these mechanisms should be like and more importantly the type of liability arising from abuses committed by customers the IOSCO is describing.
This expression is far too generic in consideration of the fact that we are dealing with situations which might be considered as crimes (i.e. money laundering, market manipulations).
Therefore we believe that it is very important to determine the sentence given the possible implications of such an obligation on the activity of intermediaries.
As Europeans we can bring the experience we are having and the difficulties we are facing with the implementation of the procedures to identify the operations of customers suspect of market manipulation.
An administrative liability is provided for by the legislation in case the intermediary does not notify the suspicious transaction to the Authority.

1. Do you agree with the definition and description of the scope of a compliance function?
We have noticed that the definition does not consider among the activities of the function the establishment of policies and procedures which is nonetheless considered in the Means for Implementation of Topic 1.
We are satisfied with that choice as long as it recognises the recent changes in the activities and the new challenges of the compliance function which will increasingly be focused on the setting of the procedures.

We obviously have the European point of view and we believe that the profound changes brought about by the MIFID will - among other things – have a big impact on the compliance function in its activity of setting the procedures (i.e. the best execution policy and the systematic internaliser's activity).

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?
This question has been a reason for concern for our intermediaries worried about the fact that the regulation could not provide for enough clarity regarding the necessary distinctions to be done among the activities which should be carried out by various departments of a firm.
Our view is that the risk management function should not be part of a compliance function, since the activities they carry out are very different. Some evidence of the difference of those activities is the diversity of qualifications and skills of human resources involved.

3. Should a specific organizational structure for compliance be prescribed? Please explain.
In our view the legislation should not prescribe a specific organizational structure of the function. As long as each intermediary has got an independent compliance function, we believe that a certain degree of flexibility should be granted when dealing with the organisational issues. This approach will let each intermediary arrange its structure in the most appropriate way according to the business activities it carries out.

4. Are there any essential roles, responsibilities or activities for the compliance function that should be mandated or otherwise identified by regulators?
See answer number 3.

5. Please identify responsibilities other than those described above that are carried out by the compliance function at market intermediaries.
We do not have any specific comment.

6. How and when should the compliance function be responsible for managing compliance risk?
See answer number 2 above.

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?
Costs could be the only concern rising from requiring documentation of policies and procedures for smaller, less complex, market intermediaries. On the other hand, we do not believe that a firm though small can carry out any business without documented policies and procedures.
Certainly such policies and procedures should be highly consistent with the size and structure of the firm.
We do believe that it is more appropriate to speak of complexity of procedures which should mirror the complexity of the business more than by degree of detail, which should be enough to implement the activity effectively.

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.
We are not giving an answer to the above question which describes the structure of a specific firm, since we are an Association and we bring the experience of all our members.
However, we believe that it is important to address the issue of accountability for compliance.
In Italy the function is accountable and so is the board of directors in that it is the organ to which the function reports to.
Anyway, as highlighted in the Report at pag. 15, in Italy, 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 the management. We believe that such a choice is right because given that the procedures are set there is room for discretion on single business units that cannot be effectively handled by the function and the board of directors (i.e. According to the procedures and the law

the OTC transactions should be reported to the market within 15 minutes, even though the head of equity may end up notifying the transaction within a longer period of time).

9. Do you distinguish among responsibility, accountability and liability? Please explain.
We do not have specific comments.

10. Should a senior officer be designated for the day-to-day compliance responsibilities? Please explain.
Yes there should be a designated senior officer given the significance of the role this subject should carry out.

11. What requirements relating to independence and ability to act are relevant to a small firm?
We firmly believe that any firm even though small should in our view have an independent compliance function.
We do not believe, in fact, that the characteristic of independence can be sacrificed, with respect to the type and size of the investment firm, though we recognize, as a rule, the need for the law-maker to take into due account the specificity of the different entities addressed by the regulation.
Nevertheless in our view, there are some obligations which are necessary to comply with in order to carry out the activities in a professional and efficient manner and they cannot be considered in the light of the "principle of proportionality".

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?
We do not believe that the legislation should allow such a possibility.
See the previous and the following answer.

13. Are the means of implementation of independence set out above sufficient to achieve independence? Please explain.
Yes they are. In the light of the answers 11 and 12 we believe that the use of specific human resources performing the compliance function only should be stressed and it should be the rule.
We do not agree with provision set forth by lett. d) which provides for the case where individuals perform both business and compliance activities.

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

15. What are the appropriate qualifications for compliance professional?
If "qualification" is meant to be a specific certification got after taking a prescribed examinations as in lett. b) in order to carry out that specific function, we believe that the idea is good and useful in the light of circulation of professionals. However, it is probably too early to put it into practice. In Italy, at the moment, we are witnessing the difficulties of introducing something like this for the sales', traders' and analysts' professions.
We do not exclude that in the future this is what to aim at.

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

17. How do you evaluate the adequacy of courses and training for compliance personnel?
We reckon it opportune to train the staff in general on a regular basis, in particular the compliance personnel which has always to be up to date with recent reforms of legislation.

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

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

The external auditors should asses and control the set procedures and the systems in place in order to comply with the legislation.

20. What are the practical concerns of requiring an external party to conduct periodic assessment of a compliance function?
We do not have specific comments.

21. What should be the scope and frequency of the assessment by an internal party and/or an external party?
The assessment should be carried out on an annual basis.

22. Please identify the methods of monitoring that are the most effective from your perspective and explain why.
We do not have any specific comments.

23. What factors are indicative of a strong compliance culture and a weak compliance culture? Please explain.
We do not have any specific comments.

24. Are there other means for implementation that we should consider?
No there are not.

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.
The problems raised by global firms concern the differences in legislations they have to face in different countries where they are based.

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?
We do not have any specific comments.

We would like to conclude with a few considerations regarding the Appendix A.
It gives a list of specific issues that should be considered for internal compliance policies and procedures. Among these issues there are some which, in our view, are closer to the activity that an internal control function should carry out (i.e. controlling compliance with prudential rules;
records and documentation, including safeguarding for the privacy protection of client records and information business continuity plans). Therefore we suggest that the listed issues be considered as topics which an intermediary have to deal with, but letting him arrange the structure of the firm in the way most suitable to the activity carried out.
Which in turn means to let the intermediary decide whether or not to set a specific and separate internal control function. In such a case many of the listed issues will be dealt with by such a function.
The above considerations lead to the need of addressing the issue of clear and incontrovertible definitions of compliance and internal control functions.

We are available to clarify any further possible question.

Yours sincerely

The Secretary General
Franco Gherra

TO: International Organization of Securities

BY: Banca Intesa S.p.A.

Milan, July 14, 2005

Object: Comments to the IOSCO discussion paper called "Consultation Report Compliance Function at Market Intermediaries".

The purpose of this note is to provide some proposals in order to the issues raised by the International Organization of Securities in the discussion paper called "Consultation Report Compliance Function at Market Intermediaries" published in April 2005:

1) **[IOSCO: *"Do you agree with the definition and description of the scope of a compliance function? Please explain."*]**
   In relation to the definition and description of the scope of the compliance function, we propose that such function protect the firm exclusively from the liabilities arising from the abuses committed by its customers through transactions that are assigned to the competence of the compliance function;

2) **[IOSCO: *"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?"*]**
   In relation to the relationship between the compliance function and the risk management function, we believe the two activities have a very different scope; the compliance function should be an independent structure and its responsibilities may appear similar in nature to the monitoring of market and operating risk but focused on legal, compliance and reputational risk. In particular the compliance function should identify, estimate, advise, control and report in relation to the legal and administrative sanctions, the financial losses, the **[**losses of reputation/image**]** of the market intermediary arising from breach of laws, regulations, procedures, codes of conduct and best practices.

3) **[IOSCO: *"Should a specific organizational structure for compliance be prescribed? Please explain*"]**
   In relation to the organizational structure of the compliance function, it would be advisable to have a dedicated unit which shall be independent from the business functions;

4) **[IOSCO: *"Are there any essential roles, responsibilities or activities for the compliance function that should be mandated or otherwise identified by regulators?*]**
   In relation to further responsibilities or activities for the compliance function that should be mandated or otherwise identified by regulators, we propose that the compliance function cooperates with the operational risk function and legal service to provide a specific model for management of the administrative liability of the market intermediary when its employees commit specific crimes on behalf of the same market intermediary and there are specific rules in order to such liability on the Country on which the compliance function operates. In Italy the compliance function would have to provide a model for management of such kind of liability under the Legislative Decree N° 231/2001;

5) [IOSCO: *"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?"*]

In relation to the effective means to ensure that a market intermediary or its related entities are complying with securities regulatory requirements in all jurisdictions it or its related entities operate, we propose that:

(i) any market intermediary have a central compliance office and a number of local compliance offices in each of its foreign head offices,

(ii) each local compliance office reports to the central compliance office in relation to the applicable laws and their interpretation in the Country of the relevant foreign head offices, and

(iii) the local compliance offices and the central compliance office agree and provide in a uniform way internal policies in relation to: (a) the management of the relationship between the central compliance office and the local compliance offices and (b) the reception of the external rules into their Group.

Consultation IOSCO Report – Compliance Function at Market Intermediaries

The Netherlands Bankers' Association Compliance Working Group appreciates the IOSCO Technical Committee's consultation process regarding the Consultation Report Compliance Function at Market Intermediaries (hereafter: Consultation Report). We share the Technical Committee's believe that publication of this paper, after proper consultation with market participants, will bring greater clarity and focus on the compliance function.

We trust the following comments to the Technical Committee's questions will assist IOSCO's Technical Committee Standing Committee on the Regulation of Market Intermediaries (SC3) in finalising its views and recommendations and present a final report on the compliance function at market intermediaries to the IOSCO Technical Committee for approval. We also want to refer to our comments on the Basel paper Compliance and the compliance function in banks (enclosed).

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

Compliance function in the Consultation Report is defined as a function that, on an on-going basis, identifies, assesses, advises on, monitors and reports on a market intermediary's compliance with securities regulatory requirements, including whether there are appropriate supervisory procedures in place. Contrary to footnote 13, this definition is different from the definition of Compliance Risk in the final version of the Basel paper Compliance and the compliance function in banks. It's imperative that regulators, whether securities regulators or banking regulators, harmonize the definition of the compliance function or the definition of compliance risk, or preferably use the same definition. Securities institutions often form part of a larger financial (banking) group. Harmonisation of regulatory requirements, also with respect to compliance function, is very important.

Both the definition of Compliance function in the Consultation Report and the definition of compliance risk in the Basel document are too broadly defined. Whereas in the Basel document, banks are expected to comply with <u>all</u> applicable laws and regulations applicable to its business activities, the IOSCO definition of compliance function mentions 'compliance with securities regulatory requirements'. An example of this is the solvency rules (Basel 2) applicable to both banks and certain securities institutions. It is the securities institutions and banks' finance officers and not their compliance officers who typically deal with these solvency rules. The scope of Compliance rules in this respect is usually limited to the subset of Conduct of Business rules as part of the total set of securities rules.

We suggest the following definition of the Compliance function that mentions an explicit relation to the integrity of the institution:
'An independent function within the organisation, aimed at the furthering and supervision of the observation of such laws, rules and standards that are relevant to the integrity, and in connection with this, the reputation of the institution'.
This definition could be used for both banks and securities institutions. Although it is possible to mention certain matters that would typically be part of the scope of compliance within most securities institutions (and banks), like standards of market conduct, conflicts of interest, personal account dealing, anti-money laundering and the prevention of terrorist financing, we suggest to leave it up to each individual securities institution/bank to further defining the scope of what is considered compliance within their securities institution/bank. This way, each securities institution (and bank) will have the necessary flexibility in defining the scope of compliance within their firm. Although the securities institution (and bank) is required to comply with all rules applicable to their business, the securities institution (or bank) could decide for itself what part of the applicable rules is considered compliance.

It is unclear what is meant by 'monitoring for compliance with securities regulatory requirements' as mentioned in paragraph C Definition of the Compliance function and scope. A compliance officer typically

doesn't have the resources for, and doesn't perform elaborate tests or audits on adherence to compliance rules. This is usually performed by an Internal Control and/or Internal Audit department. Compliance monitoring consists of limited testing of compliance rules in order to evaluate existence and proper function of internal compliance procedures, procedures and guidelines.

Paragraph C on the Definition of the Compliance Function and Scope also mentions that 'A compliance function of a firm should also have mechanisms in place to protect the firm from any liability arising from abuses committed to its customers. Although the Compliance Department will usually be informed and possibly involved (e.g. if there are regulatory issues involved), in practice, these issues are handled by Corporate Security Departments in firms/banks.

The Netherlands Bankers' Association Compliance Working Group agrees with the statement that the principles set forth in the Consultation Report must be sufficiently flexible to adapt to the nature, scale and complexity of the markets intermediary's business and operations.

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?

In practice, the Compliance function could be separate from Risk Management, or could be part of the Risk Management function. Obviously, both functions work close together, irrespective of how these functions are structured within a firm. As long as all compliance risks applicable to securities institutions are sufficiently mitigated by the securities institution, it is not important whether compliance is considered part of risk management or a separate function. Again, it should be up to the securities institution to decide upon this.

Topic 1 Establishing a Compliance function

The paragraph on 'Establishing a Compliance function' (Topic 1) mentions what a compliance function should generally perform. The activities as mentioned under (3), 'providing information to the board of directors and/or senior management on applicable laws and regulations to assist them with their compliance responsibilities', applies to all staff, not just the board of directors and/or senior management. Although the management of the firm is ultimately responsible for compliance, compliance to applicable laws and regulations is everybody's business in the firm. It is the compliance officers' responsibility to assist in informing all relevant staff on applicable rules.

The activities described under (6) mention the notification of material breaches to the regulator. The role of Compliance with respect to the regulator(s) is broader than this. In general, the compliance officer is the liaison for the financial regulators within the firm. This activity of the compliance function is under-exposed in the description of the compliance function activities.

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

A specific organizational structure for compliance should <u>not</u> be prescribed. As long as the compliance activities are adequately performed and the proper reporting lines are in place, it should be left to the firm to structure compliance as appropriate.

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

See also the comments mentioned above. An activity that may be identified by regulators is the fact that the compliance officer also usually acts as the liaison for the financial regulators within the firm. Requests for information from regulators are usually handled by the compliance department and communication from and to financial regulators also go through the compliance department, via senior management.

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

Compliance Officers may also play an active role in the rule commenting process, e.g. this consultation process. This may provide valuable feedback for regulators in finalizing draft rules on the one hand and may contribute to practicable rules for the firm on the other hand.

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

Senior management is ultimately responsible for compliance to all applicable rules. It is the responsibility of the compliance officer to help (senior) management with this by performing the activities described, i.e. the compliance officer is responsible for performing these activities in an adequate manner in order for senior management to assume its responsibility regarding compliance to all applicable rules.

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?

Within smaller firms, the independence of compliance may be difficult or even impossible to achieve. For example, in smaller firms, a director may perform the role of compliance officer. There are both advantages and disadvantages to this situation. Smaller firms usually have less resources available for compliance. Because the number and size of the business lines in smaller firms is also smaller, there is no need to require the same documentation of policies and procedures as larger firms. Although it is important that compliance policies and procedures are not only documented in larger firms, but also in smaller firms, these policies and procedures should be tailored to the specific risks, lines of businesses and size of the operations.

Topic 2 Role and responsibilities of the Board of Directors or Senior management

The paragraph regarding 'Role and responsibilities of the Board of Directors or senior management' (Topic 2) refers to Appendix A, which lists of topics that may be covered in the compliance policies and procedures. Some of the topics described are not considered to be the main responsibility of the compliance function. Therefore, they may not be called compliance policies and procedures within a firm.

With respect to the Supervision of opening of new client accounts, Supervision of trading practices, including proprietary trading of the firm, Supervision of portfolio management processes, Supervision of advice provided to clients, Supervision of the various duties relating to information to clients and marketing information and Controlling compliance with prudential rules, Compliance may play a certain role regarding the applicable compliance rules regarding these topics, but the supervision of these processes is usually not a task for the compliance function. The same applies to Dealing with customer complaints and business continuity plans. Again, the compliance officer will play a role regarding the regulatory issues in this respect, but the actual dealing with client complaints and business continuity would be performed by other officers.

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.

Depending on the specific situation, board of directors, senior management, the compliance officer and business personnel could be responsible and accountable for compliance to applicable rules related to their particular jobs. Senior management is ultimately responsible for compliance of the firm to all applicable (compliance) rules.

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

A distinction can be made among responsibility, accountability and liability, but associate's liability may be different for different jurisdictions as a result of different labour laws.
As said above, all associates are responsible and accountable for compliance to applicable rules related to their particular jobs. Senior management is ultimately responsible for compliance of the firm to all applicable (compliance) rules. Senior management could be held liable for certain non-compliance issues.

Depending on the jurisdiction, individual associates could also be held liable. In some jurisdictions, this is limited to very serious breaches.

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

Yes. In principle, all firms should have a designated compliance officer. Depending on the size of the firm, this role could either be performed by an independent compliance officer for larger firms or someone with other responsibilities (e.g. a director, risk officer) for smaller firms. See also comments on question 11.

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

In practice, the compliance function within smaller firms is usually performed by someone performing other duties as well. The requirement for an independent compliance function in such cases would be disproportionate. Therefore, independence of the compliance function should only be required where this is appropriate and proportionate in view of the complexity of its business and other relevant factors, including the nature and scale of the business. In said cases, other measures could be taken to ensure independence, given the special nature and/or scale of the firm. For example, an employee with non-commercial responsibilities or one of the directors (the 'financial director'; not the 'commercial' director) could perform the compliance duties.

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?

See also the answer to question 11. Furthermore, in order to ascertain if the (smaller) firm has adequate compliance procedures and policies and is in compliance with the applicable rules, regulators could review the audit reports of internal or external auditors of perform their own regulatory audits.

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

Yes, although the means for implementation mentioned under (d) 'cases where individuals perform both business and compliance activities, they should not be supervising their own business activities', may be prohibitive for smaller firms. The role of compliance officer is sometimes performed by a director, risk manager or other function.

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

The compensation of compliance personnel should not be directly dependent on the performance of a business line, product or transaction. In practice, the compensation of compliance officers could also consist of a bonus that is partly dependent of the financial performance of the bank as a whole. A bonus would mainly be based on the performance of the compliance officer. This is evaluated by the compliance officer's manager. In practice, no problems or undue influence are experienced with regard to this.

15. What are the appropriate qualifications for compliance personnel?

A compliance officer must be qualified to advise the business in an adequate manner about compliance issues. For example, if the business associates operate at university level, the compliance officer must also be required to operate at the same level. In practice, a compliance officer could have a degree in law, economics or have an accounting/auditing background (e.g. chartered accountant or certified public accountant). Although it may be helpful for a compliance officer to have an education with some applicable legal topics, it would not be considered a conditio sine qua non. A compliance officer should also have the necessary social skills and have a basic understanding of the business processes of the firm in order to advise the various lines of business in an adequate manner.

A compliance officer must not only have affinity with (financial) rules, but must also keep up to speed with new (draft) compliance related rules. Therefore, continued education is very important to the adequate functioning of a compliance officer.

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

Yes. The more senior the compliance officer, the higher the required qualifications should be. Senior compliance officers must have relevant working experience. Given the increasing complexity of financial institutions, compliance officer functions within the larger financial institutions are getting more and more specialized. As a result of this, the (continued) education should, where needed, be tailored to the specific compliance officer's tasks.

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

There are not many compliance courses available at the moment. The main reason for this is that the profession doesn't have a long history in most countries. Most training is done 'on the job'.

Training for compliance personnel could be evaluated by the number of internal compliance courses followed, external courses, positive compliance examination results and possible registrations.

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

The chief compliance officer or group compliance officer should be in the best position to ascertain the effectiveness of the compliance function, because he/she gets informed about all major compliance issues within the firm. Internal audit could form an opinion about certain parts of the compliance function when auditing certain processes within the firm. Given the vast variety of compliance related topics, it would be impossible to audit all compliance related aspects. In practice, only certain compliance topics are audited each year (e.g. AML audit), based on a risk analysis, or compliance related topics are audited as part of a financial or operational audit.

Although external auditors can, and sometimes must, report on compliance related topics, the purpose of their audit is usually related to the financial audit of the financial figures, with materiality thresholds built into the audit. As a result, the external auditor's assessment of the effectiveness of the compliance function has its limitations.

In general, external compliance audits lead to an increased administrative burden for the firms involved, with limited assurance (see above). The current mix of compliance self-assessments, compliance monitoring, internal audits, possible external auditor's compliance audits and regulatory examinations by the supervisory authorities itself, are sufficient to mitigate the firm's compliance risks.

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

The role of an external party, i.e. an external auditor, should be limited to report on any compliance issues encountered when performing the financial audits as required by (local) law. Taking into account the external auditor's materiality concept and the limited knowledge of certain specific compliance related topics, their assessment of the compliance function should be limited to those subjects that are already part of the financial audit.

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

See answer to question 19.

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

The assessment of the compliance function by an internal audit department is usually based on a risk analysis. This means that not all compliance related topics would be audited within a year, but certain topics with a higher perceived risk would be audited more than topics with a lower risk.

If the scope of the external audit by external auditors is limited to those subjects that are already part of the financial audit, the frequency would be once/year.

General comments to Topic 6 Regulators' Supervision

Topic 6 on 'Regulator's Supervision' mentions that some regulators believe that, requiring market intermediaries to notify them of significant breaches of securities requirements and/or customer complaints, that this approach allows them to assess the overall compliance of an intermediary, and thus, the effectiveness of its compliance function. In practice, there is no causal relationship between the number of breaches of securities rules and the effectiveness of the compliance function. Although the reported breaches may say something about the overall compliance of an intermediary, the compliance function may function properly, irrespective of the reported breaches.

As said in our comments to question 8, all associates are responsible for compliance to applicable rules related to their particular jobs. It is the responsibility of the compliance officer to help (senior) management with the compliance activities described earlier in the Consultation Report in an adequate manner in order for senior management to assume its responsibility regarding compliance to all applicable rules.

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

The methods of monitoring that are most effective from a firms' perspective are monitoring performed by Compliance itself and internal audit reports. See also our earlier comments regarding external audits.

Please be advised that the compliance officers' role regarding monitoring is limited. As said in our comments to question 1, a compliance officer typically doesn't have the resources for, and doesn't perform elaborate tests or audits on adherence to compliance rules. This is usually performed by an Internal Control and/or Internal Audit department. Compliance monitoring consists of limited testing of compliance rules in order to evaluate existence and proper function of internal compliance procedures, procedures and guidelines.

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

Factors that may indicate a strong compliance culture:
- management commitment
- adequately sourced compliance function
- existence of adequate compliance policies and procedures
- proper functioning of corporate compliance policies
- strong role for compliance regarding advising the business
- compliance training and awareness
- periodic compliance reporting to senior management
- co-operative relationship with the regulator

Absence of the above mentioned factors may indicate a weak compliance culture.

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

The means for implementation of the regulators' supervision as described in the Consultative document are pretty complete. Regarding the examination by external auditors (d), we refer to our comments to question 19.

The means for implementation as mentioned under (f), the periodic self-assessment and/or certification by the board of directors or senior management of market intermediaries, which would be filed with the regulators, are far reaching and, in our opinion, unnecessary. Regulators are able to review compliance reports when they are auditing the firm. Moreover, in many jurisdictions, firms are required to report material breaches to the regulator anyway. Hence, given the current measures already in place, there is no need for a (certified) periodic self-assessment.

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.

Market intermediaries that operate in multiple jurisdictions must comply with all applicable local rules. Despite the harmonisation of some rules applicable to securities firms (e.g. ISD/ MIFID) across Europe, there are still many differences in securities rules across the globe. Regulators can play an important role in further harmonization of the applicable rules and reduce the administrative burden and costs involved for the market participants.

A specific issue for smaller branches is the issue of independence of the compliance function. It may be unavoidable to combine the compliance function with another function within the branch. See our earlier comments with respect to the independence of the compliance function.

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?

The compliance organization should be tailored to the specific size and activities of the firm.
The centralized compliance function could deal with the compliance rules applicable to all offices of the firm, whereas the local offices should primarily deal with compliance to local issues and act as a liaison with local regulators. Local branch compliance officers should have a reporting line to local branch management and the compliance function at the firm's head office.

Netherlands Bankers' Association
Working Group Compliance Amsterdam, July 14th 2005

Barclays Compliance
29th Floor
One Churchill Place
Canary Wharf
London
E14 5HP

Tel 0207 116 1000
www.barclays.co.uk

15 July 2005

Mr Philippe Richard
Secretary General
IOSCO
Oquendo 12
28006 Madrid
Spain

Consultation Report – Compliance Function at Market Intermediaries – April 2005

Dear Mr. Richard,

Barclays PLC welcomes the opportunity to respond to the various issues raised within this consultation paper.

In general, we are content with the important role played by compliance functions in the management of regulation across the financial services industry. We welcome any proposals that may create industry-wide harmonisations, hence, providing an opportunity for potential improvement to the status quo.

By way of background, Barclays PLC is a UK-based financial services group engaged primarily in banking, credit cards, investment banking and investment management. In terms of assets employed, Barclays is one of the largest financial services groups in the United Kingdom. The Group also operates in many other countries around the world and is a leading provider of co-ordinated global services to multinational corporations and financial institutions in the world's main financial centres. Barclays has been involved in banking for over 300 years and operates in over 60 countries.

More specifically in a UK context, Barclays Bank PLC, and its various FSA authorised and regulated subsidiaries, are major providers and distributors of retail and wholesale financial services products. As such, we have a great interest in the issues raised in this Consultation Paper and how those issues may impact industry standards as a whole. It is in the collective interest of consumers and the industry that there is confidence in the harmonisation across the industry of regulatory requirements.

I. Introduction

Definition of the Compliance Function and Scope:

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

Yes, we broadly agree that a compliance function's responsibility is to identify, assess, advise, monitor and report on financial services regulatory requirements. Additionally, it is of key importance that the compliance function maintains strong relationships with industry regulators. The definition of the Compliance function and its scope should also represent a financial services industry wide definition as opposed to a 'market intermediary's' definition.

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?

The role of Compliance should involve the management and oversight of regulatory risk. The Risk department may or may not be a separate function to Compliance, depending on the structure of individual firms. However, it is important that the Risk department supports the Compliance function when required and communication is on-going via monthly reports, risk committees and steering committees that identify key risk areas. The Compliance function's role monitors regulatory risk by assessing, analysing and prioritising the risks of non-compliance.

As an example, within Barclays PLC, the role of Compliance involves the management and oversight of regulatory risk, whilst, the Risk department is a separate function based at the group centre. Additionally, there are teams of Risk Type Experts dedicated to manage all aspects of risk management across the Barclay's group.

II. Principles and Topics for Discussion and Consultation
Topic 1: Establishing a Compliance Function:

Q.3 Should a specific organisational structure for compliance be subscribed?

It is important for a Compliance function to develop and maintain adequate systems and controls and ensure that are satisfactory compliance arrangements, measures and/or procedures in place to ensure effective compliance. Specific organisational structural requirements should not be mandated across the industry; however, the compliance function should have a formal status within the bank, thus giving compliance appropriate standing, authority and independence.

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

Existing local regulatory guidance by the UK regulator (FSA) should be an adequate measure to ensure appropriate systems and controls are embedded within a compliance function. For instance, current UK regulator (FSA) requirements involve details on the responsibility of the bank's board of directors and their responsibility for oversight of regulatory risk; senior management responsibilities for effective management and communication of relevant policies and effective reporting; and compliance function responsibilities including; advice, regulatory risk management, guidance and training.

Q.5 Please identify responsibilities other than those described above that are carried out by the compliance function at market intermediaries. However, depending on the size and nature of the firm there will be others as well.

We consider the responsibilities listed are the principle ones carried out by a compliance function at market intermediaries.

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

The compliance function should be responsible for overseeing the management of compliance risk at all times. Philosophically, we would argue that the first line of defence is the business itself, which is responsible for understanding and managing the risk. It is not compliance's responsibility to manage the risk, but to oversee and independently monitor the management of the risk as part of the second line of defence. The third line of defence is the internal and external audit function, complemented by the regulators. In practice, Compliance takes on some of the day to day cross-business compliance tasks such as the licensing of employees for efficiency reasons, or personal security trade monitoring, for confidentiality reasons.

Q.7 Are there any practical concerns for requiring documentation of policies and procedures for smaller, less complex, market intermediaries? Please explain it policies.

There are no practical concerns to be raised. In principle, the requirements here should be independent of the size of a firm.

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? Explain

The Board of Directors and other members of senior management are responsible for Compliance globally with all applicable laws and regulations, reporting requirements and controls imposed by the relevant central banks and financial services regulatory authorities.

They are supported in the discharge of these responsibilities by the Group Head of Compliance and by Compliance Directors in each Business Cluster. They are responsible for oversight of Compliance with the FSA's Handbook, the similar requirements of the financial services regulators in other territories where Barclays operates and other applicable legal and regulatory requirements.

Under the UK FSA's Principles for Business, senior management is responsible for the overall effectiveness of the control functions. The board of directors is responsible for obtaining adequate assurance that management is carrying out its responsibilities effectively. Businesses are responsible for monitoring their compliance with applicable controls, policies and procedures are fit for purpose, with support from the Legal and Compliance.

In the example given, the primary responsibility for failure to establish proper procedures would rest with the business unit. However, the compliance function might have to accept certain accountabilities for either failing to ensure that procedures were in place or for failure to identify, monitor and escalate the problem. It would not be expected that senior management or the board of directors assume responsibility unless there was a pattern of non-compliance or the board of directors felt that senior management had failed in its duty to adequately and appropriately set provisions of resources from a high level.

Q.9 Do you distinguish amongst responsibility, accountability and liability? Explain

Without comment to the position at Barclays, we would distinguish amongst responsibility, accountability and liability as follows:

- Liability is the financial, legal or regulatory consequence of a compliance failure, whether personal or for the firm.
- Responsibility is the clear articulation of what is expect from the participants in a process.
- Accountability is the attribution of blame for failure to carry out the articulated responsibilities.

Therefore, senior management has the authority to decide the accountability between the people and functions within the firm. The board has the authority to decide the accountability of senior management and the shareholders have the authority to decide the accountability of the directors, often aided by regulators, litigators and the press.

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

The person responsible for the day-to-day management of compliance should be of sufficient stature and standing within the firm to be able to operate effectively and with credibility. This suggests that he/she should be a senior officer within a financial services institution. In a UK context this is a required control function.

Topic 3: Independence and Ability to Act

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

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.

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?

It would be sensible for individuals not to supervise their own business activities as this may create 'conflict of interest'. The validity of the individual's roles may be undermined if they are placed in a position where there is a potential clash between their compliance responsibilities and their other responsibilities. However, this may not be practice for smaller institutions and should be escalated to the compliance/risk committee for a decision to be determined accordingly, and in fitting with the business.

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

Yes. There is a clear expectation that the budget for the compliance function should not be directly dependant on the financial performance of the business, but, remuneration for compliance personnel may be dependant on the firm's annual performance and that the compliance budget should be large enough to manage sufficient resources when required. Compliance staff should also and be able to communicate with all employees and senior management (and the board of directors) with unhindered access in appropriate circumstances.

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

To ensure that compensation of compliance personnel is not subject to undue influence the compensation scheme should be driven by performance against objectives. Internal processes should be developed in order to ensure that business influence is at a minimum.

Topic 4: Qualification of Compliance Personnel

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

Compliance personnel must be 'competent' to retain their respective roles. There are no specific qualifications required, although, there are many desirable qualifications one may obtain, for example a Master of Arts (Compliance), post graduate courses or industry specific courses. In general, however, we would expect a senior compliance officer to be a graduate, either with a professional qualification (i.e. Accountant, Lawyer…) or someone who has well development knowledge of the regulatory environment gained through working within the financial services industry or for a regulator.

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

In addition to financial services and industry experience it is often appropriate to achieve further qualifications in order to operate successfully in a business environment. The desired qualifications would differ depending on the function, responsibility and seniority achieved within the business.

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

National regulators / SROs' generally evaluate training and/or courses available throughout the industry. In general, if a firm is able to complement individual development with other internal and/or external training programmes it is commendable.

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? Explain.

The main responsibility should be with the intermediary itself. It would be anticipated that a firm develop (in one form or another) a self-evaluation procedure supplemented by involvement from internal audit.

External assessments would be based around a periodic assessment (for 'bank' regulators). Where data exists which questions the effectiveness of the compliance function an assessment would be required, e.g. the number of violations increases, creating the trigger mechanism for a more formal external regulatory assessment.

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

The role of an external auditor would be prescribed by current regulation or prompted by failures to comply.

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

The main concern any firm should have with regard to the conduct of third party assessments would principally be to establish which party would add most value to the completion of periodic assessments. Other considerations include; what benefits the third party can offer and what are the potential costs are involved. When selecting a third party assessor it is important to measure the calibre of resource available, ensuring that there is a high quality skill set available.

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

We would consider that bi-annual (or more frequent) assessments would provide an appropriate level of risk mitigation and measurement. Bi-annual assessments would be appropriate for demonstrably low risk firms and therefore, assessments that are more frequent would be required for demonstrably higher risk firms.

Topic 6: Regulators' Supervision

Q.22 Please identify the methods of monitoring that are the most effective from your perspective. Explain why?

Periodic regulatory examinations are more effective in respect to evaluating risks from a holistic and systematic approach. However, self-assessments that are more frequent would be recommended in order to monitor and mitigate potential compliance risks. All assessments should be reported up through the compliance function reporting line in accordance with the banks risk management requirements. Monthly regulatory risk reports would be the most frequent form of reporting, highlighting any changes in the compliance risk profile based on key performance indicators. All breaches and/or deficiencies should be raised within these reports.

Q.23 What factors are indicative of a strong compliance culture and a weak compliance culture? Explain

Compliance should be part of culture of the entire organisation. It would be sensible to adopt a top down and bottom up approach when implementing a compliance strategy including governance and regulatory requirements. It is essential that communication with key stakeholders is consistent, clear and adequate. If key accountabilities (including Risk management) are transparent and agreed by senior management (and the business) a strong compliance culture is more likely to be embedded and maintained within the institution.

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

The development of a compliance cultures should be addressed in all policies and procedures that are governed by the organisation. The Compliance programme should ensure that the culture is embedded across all levels of the business.

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 on jurisdiction.

The introduction of specific regulations to a different geography via the establishment of a branch of a vehicle in a new jurisdiction. For example, establishing a branch of a US vehicle might introduce ERISA regulation to Europe. Establishing a physical presence in the US might introduce SEC regulation of hedge funds to a European fund of head funds. Also, branches require decisions to be made in areas where requirements differ across geographies; e.g. which set of personal securities trading policies or which set of gift and entertainment policies apply to a new local branch or an offshore entity.

The central compliance function endorses clear and transparent communication across all jurisdictions. Periodic meetings provide a forum to discuss global issues and concerns. The national agenda in each location takes precedence with consideration to global requirements. Global solutions are the desired way forward where appropriate (e.g. Anti-money laundering).

We would naturally be pleased to discuss this response or to provide any clarification. Please contact either me (details above) or my colleagues, Andrew Podd 0207 116 2657 or Sharon Martin on 0207 116 3421.

Yours sincerely

Mike Walters
Director, Group Head of Compliance and Regulatory Affairs

Barclays Compliance
29th Floor
One Churchill Place
Canary Wharf
London
E14 5HP

Tel 0207 116 1000
www.barclays.com

brian.harte@barclays.co.uk

13 April 2005

D Strachan Esq
Director
Financial Services Authority
25 The North Colonnade
Canary Wharf
London
E14 5HS

Enforcement Process Review – Issues Paper
Barclays welcomes the announcement of this review by the FSA and the opportunity to comment on the Issues Paper published on 11 March 2005. We set out our principal observations and themes below under four broad headings. In addition, Barclays has provided detailed input to both the BBA and LIBA trade association responses, and we have therefore not sought to repeat those comments here. Needless to say, both these responses carry our strong support.

Current Enforcement Model

We consider that the current enforcement model (ie. FSA Decision Process and RDC hearing) together with the right of appeal to the FSMT (Tribunal), is an appropriate model for the majority of enforcement cases that occur. However, in order to ensure that the process is (and is perceived to be) fair, objective, efficient and proportionate, there are certain areas where improvements could be effected which would benefit the industry as a whole and raise the standing of FSA Enforcement going forward.

We also consider the FSA needs to decide once and for all whether it is an enforcement or a supervision led regulator. Whilst the FSA has publicly stated on a number of occasions that it is not enforcement led, the FSA should ensure that its words and actions do not give the opposite impression.

Regulatory decisions - transparency

A greater level of detail and transparency around how the current process works would be welcomed and, in particular, further detail regarding referral of matters from Supervision to Enforcement and others parts of the investigations in which those subject to Enforcement action/investigation may not be included. FSA staff are also uniquely placed in terms of the provision of information to RDC, which the firm under investigation will not see. The lack of transparency on such issues creates suspicion around the whole process and does nothing to enhance the perception of fairness. We are of the view that both the FSA and the firm should be on an equal footing in terms on ongoing dialogue and access to information while an investigation is taking place. We are also concerned that the outcome of enforcement decisions may create precedent and/or future policy which should not be the case.

Although the present model appears to be appropriate, the fact that the RDC remains accountable to the FSA Board may shed doubt on the independence and may contribute to the perception that the process in unfair, especially so considering the tribunal process has been relatively infrequently used to date (although this may now be increasing). We do however recognise that there would be no merit in imposing a full tribunal process before the FSA can make an enforcement decision.

Perceived fairness in the process

We welcome the risk based approach to enforcement and consider that the normal dialogue should appropriately remain through the Supervision channel, with the enforcement process only being used when absolutely necessary. We also consider that FSA resource should not be a determining factor in the decision as to whether an investigation will take place within Enforcement or Supervision as the two roles should be entirely separate and staffed appropriately with skilled people.

We recognise that certain decisions may be appropriately taken by means of "Executive Procedures" taken by FSA staff but would emphasis the importance of those taking such decisions to remain unconnected with the matter in question in the interest of perceived fairness and transparency in the overall process. We are also of the view that the decisions carrying potentially serious consequences for firms, such as reputational or financial should be referred to the RDC in order to demonstrate impartiality and fairness.

With regards to the RDC members, we agree that an appropriate split of practitioners/non practitioners and past and present practitioners remains the most appropriate structure, thereby providing both current and past industry knowledge to reflect the current and past issues investigated by the FSA as well as an element of objectivity. However training should be considered for RDC members to ensure that they provide fair and objective input to a consistent standard. Additionally for more complex cases the RDC should either meet on two/three occasions or in extended sessions to ensure that appropriate consideration of the issues can occur before the decision notice is issued.

Credibility of outcome

Finally, we are also of the view that both increased transparency and the perception of fairness by all parties will in turn add further credibility to the outcome of FSA enforcement investigation and decisions. It is in the interests of the FSA and firms alike that the process is perceived to be a credible one and helps to ensure that the integrity of the supervisory process is maintained if such an approach is seen by all parties to be the case.

In closing, we trust these comments will be of assistance to the review, and would be pleased to discuss them further if that would be helpful.

Brian A Harte
Director, Group Head of Compliance and Regulatory Affairs
Mr. Philippe Richard
IOSCO Secretary General
Oquendo 12
28006 Madrid
SPAIN

Public Comment on Compliance Function at Market Intermediaries

BUNDESVERWAND INVESTMENT UND ASSET MANAGEMENT e.V.

Dear Mr. Richard,

BVI[2] gladly takes the opportunity to contribute on the Technical Committee's Consultation Paper concerning the Compliance Function at Market Intermediaries, dd. April 2005.

General Remarks:

Initially, we would like to point out that in Germany – like in many other countries featuring developed financial markets – the existing national compliance regulation already ensures effective compliance units and procedures for fund and asset management companies. It is a core interest of national market intermediaries to keep these efficient national compliance mechanisms functional.

In this respect, the findings and proposals laid down in the consultation document appear appropriate and well balanced. We do, however, urge IOSCO to keep this issue in mind with respect to future regulatory initiatives, which should be flexible and liberal enough to leave room for established and efficient national compliance systems.

Specific Questions:

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

   BVI agrees with the proposed definition and scope of a compliance function. The described definition is already the scope of compliance in Germany.

2. *What is the relationship between the compliance function and risk management function?*

   Especially within large groups, the compliance function of a fund management company is organized as a "divisional function" which means that primarily reporting lines are established to the group compliance officer and not to the business or to the management board of the different entities (e.g. fund management company). The risk management function, on the other hand, reports primarily to management board of a fund management company. Such a structure can ensure an independent compliance function.

   Compliance as such, on the other hand, is part of the whole risk function. Therefore a smooth cooperation between risk functions like risk management, audit and compliance is mandatory.

   The borderline between compliance and risk management is that in general compliance takes care of reputational and regulatory risk, whereas risk management accounts for market, operational and counterparty risk.

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

---

[2] BVI Bundesverband Investment und Asset Management e.V. represents the interest of the German investment fund and asset management industry. Its 77 members currently manage more than 7,600 investment funds with assets under management in excess of € one trillion. The units of these funds are held by some 15 million unit holders. For more information, please visit www.bvi.de.

The most important quality of a compliance function is its efficiency. A high level of efficiency, however, can most likely be obtained under very different organizational structures. Defining a mandatory organizational structure for compliance could outlaw existing functional compliance systems without any good reason. We therefore think that the organizational structure of compliance should be left to national discretion.

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

No. A proper definition of the compliance function and scope is sufficient.

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

This question depends on the size and the complexity of the business. Appendix A gives a good description of the tasks, but it lacks flexibility. For instance, qualification of individual staff needs to be covered by human resources, supervision of portfolio management processes and advice provided to clients needs to be performed by the responsible management, other tasks need to be covered, but not necessarily by compliance.

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?*

We think that some basic documentation of policies and procedures is required also for smaller, less complex market intermediaries. Such documentation allows these entities to demonstrate that a compliance function is in place. The documentation of policies as such, however, needs not necessarily to be done by compliance itself.

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

In Germany, the management board has to announce one (ore more) designated Compliance Officer(s) with a direct reporting line (among others) to the Management Board. The requirement that a senior officer is in charge should be restricted to larger companies.

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?*

Business activities which are relevant to compliance, if performed by the person in charge of compliance, could give cause for major conflicts of interest. In smaller firms, however, a full functional separation in person may prove illusive. Therefore, it should not be mandatory.

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

Yes, since they leave sufficient room for the broad variety of business set-ups and sizes. Proper escalation rules, in addition, may prove to be helpful.

15. *What are the appropriate qualifications for compliance professional?*

Legal and/or compliance background, banking expertise. The level of qualification required should reflect the size of the company.

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

At least this should be possible, particularly in consideration of size and business of the company and of the tasks to be carried out by the staff.

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

In big organisations, the assessment can be performed by compliance itself. Auditors are also capable of evaluating the quality of compliance.

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

The assessment should clearly show any weaknesses detected, thus enabling compliance to improve its efficiency.

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

In some cases, the evaluation of compliance issues is not the core competency of auditors.

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

An annual assessment should bring forward any deficiencies detected in the compliance function of a market intermediary.

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

Apart from enforcement actions from the regulator, the handling of respective issues and the acceptance among staff members of an undertaking as well as its reputation might be indicative for the quality of its compliance culture.

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.*

Compliance and/or legal expertise must be established for all jurisdictions concerned. A strong cooperation between these offices ensures an efficient function. There must be a standard of internal compliance requirements with respect to the local regulatory environment.

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?*

Cf. question No. 25.

We hope these comments are helpful for IOSCO's future work on compliance issues. In case you need any further information, please feel free to contact us any time.

Yours sincerely

BVI Bundesverband Investment und Asset Management e.V.

signed, Stefan Seip

signed, Magdalena Kuper

July 15, 2005

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

Re: International Organization of Securities Commissions
Public Comment on Compliance Function at Market Intermediaries

Dear Mr. Richard;

We are writing to comment on the Consultation Report (the Report) noted above as it relates to small firms.

The National Association of Independent Broker-Dealers is a 20-year old association whose membership is comprised of more than 150 broker-dealer members of the NASD. Our mission is to provide a collective voice in advocacy of regulatory and legislative issues that affect our members. While each of our members is of a unique size and type, many are small or mid-sized firms – firms that face significant challenges in the face of increasing regulation. Your proposal raises several points of great interest and import to our membership.

We recognize the extent to which the Organization has sought to consider the interests of small firms throughout the Report, and trust that in our effort to address specific issues, we succeed in providing additional insight that will be of value in formulating final recommendations.

Questions 1 and 2, Page 8:
We note that the definition of Compliance Function as presented in the Report is meant to describe the staff or groups of staff responsible for carrying out certain specific activities and responsibilities. For small firms, the effort to separate functions such as risk management from compliance, and compliance from supervision is often simply a question of available personnel.

We understand and support the position of our US regulators that responsibility for compliance may not be delegated, but rather that senior management must take responsibility and accountability for the overall culture of compliance within the firm. Notwithstanding this, provided adequate records are maintained as evidence of efficacy, we ask that the definitions allow for an independent third party, such as an auditor or compliance professional, to be assigned duties of monitoring and reporting. Further, we feel that it is important for the definition to contemplate the reality that one individual may carry out multiple functions, and therefore request that “size” or “numbers of available personnel”, in addition to nature, scale and complexity, be added throughout the Report wherever applicable, and in particular, in the definitions.

Question 3, Page 13:
We do not feel that a specific prescription for the organization of a compliance structure is practical, nor do we feel that it is necessary. We urge you to consider the fact that many small firms are quite successful in their

compliance efforts. Although we do not have a statistic to report, we encourage you to consider that many of the significant failures in compliance that have shaken investor confidence over the past several years, such as breaches of fiduciary duties in promulgating research and recommendations, price manipulation and late trading issues, and numerous other 'headline' crises, were not the result of compliance failures at small firms. Many small firms are founded on the reputation of the founder within his/her small community, or on the particular culture or mission of the principals. To small firms, reputation and integrity are often the core ingredient to success and longevity, and it is our observation that the majority of small firms are sensitive and attentive to undue risk. These hard-working and conscientious business persons must be granted the ability to design and implement systems that suit their unique practices and should not be forced into specific organizational structures.

Question 7, Page 14:
Irrespective of their size, broker-dealers and federally covered investment advisers in the US are required to maintain written procedures. Our members recognize and adhere to this responsibility. Provided the requirement for written procedures remains mostly limited to those procedures in which the firm engages and those particular requirements which are applicable to all firms, such as selling away, anti-money laundering and ethical considerations, we feel the requirement for procedures is generally.

Question 11, Page 20:
It is our observation that small firms have experienced success in their efforts to address objectivity and independence through effective means of internal checks and balances, and in some cases through outsourcing. In any event, we feel strongly that specific granular requirements that would impose certain cycles, percentages or document requirements are just as likely to fail as to succeed in enhancing compliance. We use as our example NASD Rules 3010 as amended and Rule 3012. As noted in the Report, NASD Rules 3010 and 3012 impose specific requirements for supervision of producing managers, among other requirements. Although the rules have been in effect since January 2005, many of our members continue to struggle with implementation of these procedures. We feel strongly that the struggle to successfully implement these rules are a result of the complexity and specificity of the rules themselves, and not the underlying challenge of effectively supervising producing managers.

If the goal is in fact to accomplish effective compliance and supervision, then we urge the Technical Committee to avoid the degree of specificity found in rules such as 3010 and 3012 in its own recommendations and rulemaking. We invite the Technical Committee to reach out to us for more information regarding the difficulties of implementation of Rules 3010 as amended and Rule 3012 among small firms in the US.

Question 12, Page 20 and Question 18-21, Page 24:
We have observed the increasing use of external parties to support the compliance function within small firms. We support this practice based on the fact that many such third parties are competent professionals whose objective input is pertinent and valuable, but whom small firms could not otherwise afford to employ.

We understand that the NASD is in the process of preparing a Notice to Members to address the use of compliance consultants and other service bureaus in assigning certain required functions such as branch inspections. While we do not have access to the Notice as of the date of this response, we expect that it will reinforce the regulator's expectation that while duties and functions may be delegated, the responsibility for oversight must remain with one or more senior principles within the firm. We feel that the Technical Committee should adopt a similar position.

We feel that the scope and frequency of internal inspection requirements is clearly and adequately defined in US regulations for broker-dealers and investment advisers, and should be considered as a model for the Organization.

Thank you for the opportunity to comment on this important release. Should you require further input from the NAIBD, I invite you to contact me directly.

Best regards,

Lisa Roth, President

EFFAS THE EUROPEAN FEDERATION OF FINANCIAL ANALYSTS SOCIETIES

Einsteinstrasse 5
DE - 63303 Dreieich

Contact: Claudia Stinnes
Direct number: +49 6103 5833-48
Fax number: +49 6103 / 5833-35
e-Mail: claudia.stinnes@effas.com
Internet: www.effas.com

Public Comment on *Compliance Function at Market Intermediaries*

Response by EFFAS European Federation of Financial Analysts Societies

Dear Mr. Richard,

The European Federation of Financial Analysts Societies, EFFAS, is the European umbrella organisation of national analysts societies. It comprises 23 member societies representing more than 17,000 investment professionals in the areas of Equity and Bond Research, Asset and Portfolio Management, Investment Advice.

In the following please find our discussion of the technical consultation and our answers to the specific questions.

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

The present question is based on a definition of the following compliance function:

"A function that, on an on-going basis, identifies, assesses, advises on, monitors and reports on a market intermediary's compliance with securities regulatory requirements, including whether there are appropriate supervisory procedures in
place."

The compliance function has been already defined in slightly more detail as follows:

"To assist in managing the risk of legal or regulatory sanctions, financial loss, or loss of reputation a firm may suffer as a result of its failure to comply with all applicable laws, regulations, codes of conduct and standards

of good practice. Compliance risk is sometimes also referred to as integrity risk, because the firm's reputation is closely connected with its adherence to principles of integrity and fair dealing."

The compliance function is one of the three elements of the broader concept of internal control[3].

Internal control is defined as a process, effected by an entity's board of directors/trustees, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

Effectiveness and efficiency of operations.
Reliability of financial reporting.
Compliance with laws and regulations.

Compliance with laws and regulations issued by legislators and competent authorities is a concept which ought to be accepted by everybody without any further reasons required. It is the basis of any modern society. In the context of capital market participants, the concept of compliance function is one of control and supervision. Therefore, we prefer the earlier concept as published by IOSCO, that the compliance function is one element of "internal control".

In practice, the emphasis of the compliance function has been on the prevention and monitoring of conflicts of interests in the handling of insider information and the closely related thereto, of employees' dealings. In addition, the compliance function is essential in preventing market abuse.

For smaller intermediaries offering non-complex services and products, the compliance function overlaps to a large extent with the general function of internal control, because inside information, employee's dealings and market abuse may not be relevant.

Internal control means the timely supervision by management or a special function of the activities of an intermediary, whereas internal and external audits are an additional regular supervision which, however, does not take place on an ongoing basis and is not necessarily close in time to the activity or transactions supervised.

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?

If risk management and compliance are understood and defined in a general manner encompassing all areas of a firm's activities, the compliance function is one part of the risk management function. This discussion of definitions, however, does not lead anywhere from a practical point of view. It would be much better to rather identify specific problems and issues in the operation and organisation of capital market intermediaries and address the functions which should be established to deal with these problems and issues. In this context, risk management is the analysis and monitoring of solvency risks inherent in proprietary activities of an intermediary (e.g. dealing in financial instruments on own account and counterpart risks) or in the financial exposures created by customer business (brokerage). The compliance function primarily addresses questions of operational risks resulting from conflicts of interests and treatment of customers. Whether these functions are called risk management or compliance functions it is basically irrelevant.

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

There should be no mandatory provisions for a specific organisation for the compliance functions. The legislator and regulators should set the general – high level - principles which should be observed in the organisation of the compliance function. The transformation of these principles into a specific organisational structure should be left to the firms.

[3] FRAMEWORK FOR INTERNAL CONTROL SYSTEMS IN BANKING ORGANISATIONS Basle Committee on Banking Supervision, Basle September 1998

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

As already indicated above, there are certain areas which are of primary concern to the compliance function. Those are:

- identification and monitoring of conflicts of interest
- defining and monitoring Chinese walls and inside information
- monitoring of areas of potential market manipulation
- handling of customer complaints.

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

Additional tasks which may be, and are in many cases, attached to the compliance function are the identification and monitoring of money laundering cases and the identification and monitoring of data or privacy security and protection.

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

In this question, we understand "managing compliance risks" as deciding how to proceed in cases in which a decision becomes necessary (e.g. reaction to a complaint, solving conflicts of interests etc.). It should be left to the firms to organise the risk managing function. The risk management in this context may, depending on the size of the firm, be attached to the compliance function or be reserved for the firm's senior management or may be distributed among both functions, according to the nature and the potential financial impact of such risk.

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?

Small firms must also have a policy and procedures of internal control, including the compliance function. Depending on the circumstances these might be very simple, describing who is reviewing at which frequency which transaction or business activity. The general description which ought to be documented and submitted when applying for a license must be supplemented by documentation of the reviews performed. This may be a simple dating and initialling of the transaction or activity documentation reviewed. Regulators should expect only the minimum documentation necessary to prove that an internal control policy has been established and that it is carried out. Regulators should direct their attention to the policy and implementation of the handling of complaints and of conflicts of interests, if any. Customer complaints are an early indicator of operational risks and of a lack of compliance culture.

Questions 8, 9, 10.

Small intermediaries with non-complex business (investment advice, introducing brokerage, portfolio management without handling of customer funds) have flat hierarchies and rarely distinguish between senior and other management.

It might be that these firms do not distinguish between responsibility, accountability and liability.

As a rule larger firms should have a senior officer designated for the day to day compliance responsibility.

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

We subscribe to the following statement in the consultation report also for small firms, wherever and whenever this is physically possible.

"(d) In cases where individuals perform both business and compliance activities, they should not be supervising their own business activities."

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?

The consultation report assumes that there are no individual practitioners acting as market intermediaries. This may be the case in many jurisdictions which do not license one-person firms as market intermediaries. This is, however, not true for all jurisdictions. The European Directive on Markets in Financial Instruments (MiFiD – 2004/39/EC) provides expressly in Art. 9 Nr. 4 that one-man firms are admissible when and if the sound and prudent management of such firms is ensured.

In cases where there is more than one person in the firm, the principle should apply that the activities of one person should be reviewed by another person, except in such cases where the geographical distance between the members makes it impossible or impractical or too costly to apply this principle. These exceptional cases should be treated as a combination of one-person-firms and should be treated accordingly.

In one-person-firms, internal control, including compliance, can only be practised in two ways – outsourcing or self-control of the intermediary. The former method should not be made mandatory. First, it is cost intensive and may be out of proportion for the purpose to be achieved. Second, if it were made financially feasible, it is probably not a timely review of transactions and of practices, but rather a time-deferred periodic exercise resembling an internal or external audit. We think that it is not necessary to duplicate these functions.

In a one-person firm, the proprietor is responsible for the business and for the control function. It is necessarily self-control. A review of the activity performed can only be a relative time-deferred (evening, weekend) self-control based on check-lists. The purpose of this self control is the detection and prevention of negligent or inadvertent activity in the hectic of the business, resulting in mistakes or errors or the non observance of regulatory requirements. This form of control is not independent because the review is made by the person responsible for the activity. Such control does not prevent wilful or malicious action on the part of a one-person firm. Administrative regulation should, however, not be based on the assumption that intermediaries are wilfully or intentionally braking the rules, until proven otherwise, but rather that the aim of internal control and compliance is to avoid lax and careless operations. It seems to us that this type of self-control should be accepted for small firms with non complex products or services, in particular for those firms not having customer funds and assets in their custody.

Question 13 and 14: Reference is made to the above answers.

15. What are the appropriate qualifications for compliance personnel?

Compliance officers should have practical experience in the operative business controlled by them. In addition, they need additional theoretical training on the regulatory provisions applicable to their firm's activities. They also need training in the techniques and procedures of internal control. To a lesser degree, the requirements in theoretical knowledge are also applicable to the persons performing compliance functions in small firms. They should be trained in those areas which are applicable to the firm's business.

Such training, preferably not only in-house, should be made mandatory. Training by outside firms will broaden the horizon of the students and will avoid tunnel vision restricted to the firms own, possibly deficient, culture and methods.

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

Yes. The compliance function is a mirror of the distribution of operational functions. The required qualifications should depend on the responsibilities of the compliance personnel. The head of a compliance department in a large firm will be a senior person with overall experience and thorough training in all major aspects of the firm's business. Junior staff will have or acquire experience and the theoretical background in one or several areas. It is also advisable that in larger firms non-senior compliance personnel rotate regularly into operations in order to maintain the understanding of the operations whose compliance they are to monitor.

In small firms this connection is usually guaranteed by the combination of managing their own business and monitoring the business of other persons (cross-checking).

The organisation of the training should be basically left to the firms and their trade organisations. Regulators should restrict themselves to establishing high level principles.

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

The evaluation is based on the content of the training programme in relation to the functions and needs of the firms whose personnel is participating. Such programmes will differ for the compliance functionaries in small non-complex firms and larger firms or firms handling customer funds and securities.

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

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

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

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

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

In large firms, the compliance function should be assessed and monitored by the internal as well as the external auditors. They are trained to evaluate the basic set up of compliance functions and the actual performance of compliance tasks. They are also equipped to evaluate the adequacy of procedures in relation to the intermediary‘s size and complexity. Time and frequency of audit activities depend on the size and the complexity of the firm. They depend also on the firms compliance history. A firm with a proven record of strong compliance needs less frequent audits than firms with a history of weak compliance. The methods to be employed are the review of the documented compliance policy and procedure and their adequacy. This base review must be accompanied by the activity audit on whether the policies and procedures are carried out within the firm.

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

No, or few customer complaints vs. many customer complaints or frequent litigation.
Strong chinese walls vs. many cross-over activities and responsibilities not clearly delineated.

Expenses for training in regulatory environment and ethics.
Proper documentation.

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

If other means were considered, they should not cause expenses which are unreasonable in relation to the size and complexity of business. The expenses for compliance functions must be earned by the intermediaries and must eventually be paid by the investors. Over-regulation will stifle markets.

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.

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 centralised compliance function?

Cross-border activities of intermediaries may be simple cross-border transactions between an intermediary located in one jurisdiction and the customer or counterpart located in another jurisdiction. A closer connection to another jurisdiction is the establishment of a branch office in the foreign jurisdiction.These two modi-operandi require a different approach in compliance functions. In the case of simple cross border transactions, the compliance function should be located in the intermediary's home jurisdiction. Any other solution would create extremely complicated and expensive structures.

Another issue is the application of laws and regulations in such transactions. In those jurisdictions which belong to a harmonised system of legislation and regulation (e.g. EU/EC), it should suffice that the compliance function monitor compliance of cross-border transactions under the harmonised home state rules.

In those cases in which the intermediary has established a branch in the foreign jurisdiction, the branch must comply with local requirements. The compliance function will have to monitor this compliance. The decision to organise the compliance function, either locally or centrally at the location of the home office or elsewhere should be left to the intermediary. A high level principle should be introduced which requires that revisable documentation of the compliance policies and procedures and their application in the branch be submitted locally at the request of the auditor or local regulator in charge of the branch.

Yours sincerely,

Fritz H Rau
Chairman of EFFAS

VERENIGING VAN COMPLIANCE OFFICERS

De waterkamer 114
7325 HX Apeldoorn
Telefoon 06 – 22648974
Fax 055 – 3550001
Email secretariaat@vco.nl
Website www.VCO.nl

by mail: mail@oicv.iosco.org
Mr. Philippe Richard
IOSCO Secretary General
Oquendo 12
28006 Madrid
SPAIN

Amsterdam, August 15, 2005

Re: Public Comment on *Compliance Function at Market Intermediaries*

Dear Mr. Richard,

I'm writing on behalf of the Association of Compliance officers in The Netherlands (Vereniging van Compliance Officers, VCO) in reply to the IOSCO's request for comments on the IOSCO consultation report, compliance function at Market Intermediaries dated April 2005.

We welcome the opportunity to present our views on the report since it is evident that the role of compliance officers is central in a number of regulatory initiatives, which seek to respond to events that have taken place in the recent past in the securities markets.

Without hesitation one may state that compliance professionals are a key constituency in consultations of this nature as they are regarded by some as important if not pivotal to achieving regulatory objectives.

Before responding to the questions raised in the report we would like to make a number of preliminary comments.

Preliminary comments

The report correctly recognises a number of national and international initiatives concerning the nature and function of Compliance at Banks and Market Intermediaries. If we analyse the approaches one can see that there is a wide-ranging difference in these approaches.

This in itself raises the concern that we (markets participants, compliance professionals and regulators) may not as yet have a clear understanding of the role of the compliance function and its future development in the financial industry in general.

This would in our view indicate that the matter requires a more fundamental discussion and the development of a vision of the compliance function which will lead us forward in the coming years.
Our second and related observation concerns the fact that generally speaking, expectations with regard to market behaviour are changing rapidly. These expectations are presently being formed by many different types of stakeholders or interested parties and touch on a wide range of issues such as consumer protection, proper governance, behavioural integrity, reputation, the protection of a company's name or brand.

We ask ourselves whether an approach to compliance based on what one may call regulatory compliance i.e. adhering to rules and regulations is adequate in view of these developments. Is this not too narrow and if so what should be our approach for the future and where does compliance fit into this dynamism?

Our third observation is that a Compliance function will generally differ depending on the risk profile of the activities. For example when dealing with the investments of private customers, duties of care and the suitability of investment advice will generally be high on the agenda because of the specific risks and business drivers involved in providing investment services to customers. By contrast this specific topic will be of lesser interest in a wholesale environment where one will find a different risk profile. In consequence while it may be possible to formulate a harmonised conceptual approach to the role of compliance as a whole, we concur that one should not underestimate the necessity to differentiate in day to day practice depending on the risk profile and business drivers of the activity.

Fourthly, we feel that in assessing the effectiveness of a compliance function substance over form should prevail. Some regulatory approaches tend to emphasise the existence of written policies and procedures to evidence the proper functioning of compliance. We agree that written procedures and policies tend to indicate organised thinking regarding compliance issues, however this need not necessarily lead to highly detailed paperwork nor does it provide conclusive evidence of a properly functioning compliance function.

We will now address the questions in part C, definition of the Compliance Function and Scope, of your paper.

Question 1:

Do you agree with the definition and description of the scope of a compliance function?

As stated above the definition of compliance based solely on adherence to regulatory rules, approaches the subject matter from a rules and regulations viewpoint. Is this an appropriate approach to compliance in our "post nineties" environment?

Secondly, not all rules and regulations should fall within the scope of Compliance for instance capital adequacy rules may not necessarily be dealt with by Compliance. The Basel paper on Compliance functions in Banks for instance specifies certain generic topics which will typically be dealt with by Compliance and places these topics within concepts as "compliance risk" and "compliance laws, rules and standards".

The IOSCO report lists in appendix A a number of issues that should be considered.
The list reflects the rules and regulations approach and is task oriented.

Thirdly, one should realise that not all Compliance functions are sufficiently resourced to conduct for instance ongoing monitoring activities and, in larger institutions, the audit department and other departments may be involved in monitoring activities.

Furthermore monitoring activities will reflect prioritisation and assessment of risks. High-risk areas require more monitoring than low risk areas.

The description of the Compliance function refers to abuses committed by its customers. It is unclear what is meant by abuses. Serious matters such as fraudulent activities usually fall within the scope of dedicated functions such as security functions in larger institutions or may be referred to judicial authorities. Less serious matters may be referred to legal departments to determine whether there is the risk of incurring criminal or civil law liability.

In The Netherlands and in other jurisdictions there has been debate whether a regulatory obligation to report a customer to the authorities is acceptable. The discussion took place within the context of the Market Abuse Directive and proved to be a sensitive subject. We would therefore encourage a prudent approach to matters of reporting customers and denunciation to authorities, bearing in mind strong cultural differences to this subject.

In anti money laundering practice there is a growing trend to appoint dedicated anti money laundering compliance officers. See for instance present practice and regulation in the UK.

Question 2:

What is the relationship between the compliance function and risk management function?

Compliance and risk management must be seen as complementary functions, each with its own area of competence in the total risk management and governance framework of an institution.

These functions are certainly not identical, for instance:

- Subject matter: regulatory risk versus financial risk
- The methodological approaches. Reputational risk is not easily captured in present day statistical modelling approaches employed by credit risk, market risk and operational risk

There is however strong potential for interaction, a few examples:

- Credit risk management is in a position to alert compliance to customer activities that may put the reputation of the institution at risk
- Market risk management may alert Compliance to customer activity which may constitute insider trading or market abuse
- Operational risk management may alert compliance to the rise in out of court settlements with investment customers indicating insufficient controls over the investment advice processes and the application of duty of care
- Market risk management may alert Compliance to pricing anomalies in trade execution indicating a violation of the “best execution” rule

Topic 1 Establishing a Compliance function

Question 3:

Should a specific organisational structure be prescribed?

No, only certain specific characteristics should be prescribed such as independence, direct access and reporting lines to the CEO of the institution, access to company supervisory bodies such as audit committees or supervisory boards.

A cautionary remark should be made here regarding the notion of independence. Nobody is absolutely independent since one cannot act in an organisation with all its commercial and other interests as if these did not exist. Quite the contrary compliance should be mindful of these interests when for instance providing advice and guidance.

Independence does mean independence of thinking and the absence of undue influence in the opinions of compliance and their practical outcome.

Question 4:

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

Yes, there are a number of essential roles that should be identified:

General function:- proactive reputational and integrity risk management
- assessing the reputational, integrity and regulatory risks

Specific:
- advice, training and education, monitoring of policies, reporting
- liaison to regulators
- initiating remedial measures and
- intervention in acute situations

Notifying regulators of breaches is generally seen as the responsibility of senior management.

Question 5:

Please identify responsibilities other than those described above that are carried out by the Compliance function at market intermediaries?

In some jurisdictions certain highly operational tasks are carried out by Compliance.

Examples:

- checking customer acceptance files
- checking transaction flows
- computation and reporting of capital adequacy

In addition specific other areas may fall within the scope of compliance depending on the institution, for instance:

- certain tax issues
- privacy and data protection
- outsourcing arrangements
- integrity issues relating to employees
- competition law

We submit that every institute should decide for itself whether these types of activity should be carried out by Compliance. However our view is that in discriminating what should and what should not be done by compliance, one should consider where the compliance function can provide the greatest added value.

We should on the one hand avoid the Compliance function being burdened with tasks that could equally be performed by other functions but on the other one should also allow specialisation within the compliance function leading to specialists in market abuse, AML, CDD, data protection etc.

Question 6:

How and when should the Compliance function be responsible for managing Compliance risk?

The responsibility of the Compliance function is to alert and assist management (the CEO) to address reputational and integrity risk issues. Ideally the principle of prevention should be foremost in the culture and mindset. This requires that the Compliance is involved from the beginning in business processes and developments.

Question 7:

Are there any practical concerns for requiring documentation of policies and procedures for smaller, less complex, market intermediaries?

Yes, in assessing the effectiveness of a Compliance function substance should prevail over form. Formal written policies and procedures are important, but we should not encourage a bureaucratic approach. The absence of written policies may indicate an underperforming compliance function but this is not necessarily the case. Furthermore one should not prescribe a certain level of detail in the procedures. They should be adequate to manage an identified compliance risk depending on the severity of the risk.

Topic 2 Role and Responsibilities of the Board of Directors or Senior Management

Question 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.

In practice you will see different models regarding responsibility and accountability, depending on the jurisdiction and institution. The key still remains however that senior management bears the responsibility for the institution's compliance. However compliance is generally accountable for the proper performance of its own role in advising, educating and monitoring. The same applies if compliance were to refrain from taking remedial action in the event that a weakness has been identified. In such cases compliance must "speak up".

Increasingly employees such as accountmanagers and HR personnel are accountable for instance for adhering to policies and codes of conduct.

Question 9:

Do you distinguish among responsibility, accountability and liability?

Yes, one should distinguish between the three:

- responsibility relates to management responsibilities to maintain an adequate culture and framework of reputational and integrity risk management.
- compliance is accountable if it has failed to analyse weaknesses or has failed to bring this to the attention of management.
- Liability relates to external regulatory, criminal law or civil law liability. In some jurisdictions Compliance officers are increasingly concerned, that they are personally liable in cases where the organisation has failed to address compliance issues. In the present atmosphere of enhanced enforcement this fear is fully justified.

Question 10:

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

Yes, all institutions should ideally have a chief of Compliance for the following reasons:

- Compliance is a separate and increasingly important function which requires dedicated attention.
- Seniority is required as the function is often complex and requires very specific skills
- The very existence of a chief compliance officer evidences that the institution takes matters seriously and that the institution is prepared to allot resources to Compliance.

We submit that in smaller institutions there will be budgetary constraints and that certain combinations of functions should be allowed.

Topic 3 Independence and Ability to Act

Question 11:

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

In smaller firms compliance functions are some times combined with other functions. One should however follow certain principles: the compliance functions should not be combined with evidently incompatible functions or roles e.g. commercial responsibility.

In smaller firms the Compliance function should be better protected from inappropriate managerial pressure. In larger institutions inappropriate pressure can be discussed in a larger group and addressed properly. Smaller institutions do not have that luxury. One approach would be an enhanced role for internal or external audit.

Question 12:

In cases where individuals perform both business and Compliance activities, should they be allowed to supervise their own business activities?

Ideally no, an institution where this combination occurs represents a potentially higher risk to regulatory objectives and therefor requires more intense oversight by regulators.

Question 13:

Are the means of implementation of independence set out above sufficient to achieve indepence?

Generally yes, one should however consider additional protective measures. Compliance officers regularly receive confidential information and are required to communicate opinions, views and incidents confidentially. Compliance officers do not have something comparable to attorney – client privilege which allows an open exchange of views. This is not conducive to open communication and may inhibit the internal discourse required to create a culture of compliance.

Compliance officers should furthermore be protected against labour law penalties, sanctions or dismissal for the role they play. We by no means imply that there is abuse in this area but it would certainly strengthen our position if requirements would be introduced in this field.

Question 14:

How do you ensure that compensation of Compliance personnel is not subject to undue influence?

There are a number of ways to do this:

- Transparent setting of objectives to enable transparent performance appraisal
- The appraisal is done by a superior who is either a Compliance officer or for instance a board member who is not responsible for commercial activity
- Written remuneration and bonus policies to enhance transparency
- Remuneration and bonus policies should not depend on the commercial performance of the institution
- Remuneration and bonus payments should reflect the relatively high risk Compliance officers run

Topic 4 Qualification of Compliance Personnel

Question 15:

What are the appropriate qualifications for Compliance professional?

Presently Compliance officers are recruited from a number of backgrounds. Law, economics accounting and controlling, and even business backgrounds generally provide good intellectual skills and understanding of business on business processes to be able meeting high levels of professionalism.

Depending on the required level of seniority academic backgrounds may be appropriate but certainly not always required.

Equally important are "human skills" and personality traits. A Compliance officer must:

- Be a good communicator
- Have the ability to convince and to influence behaviour
- Have the ability to operate in stressful situations or in conflictual circumstances
- Have the ability to resolve issues creatively
- Depending on the level of seniority, have the ability to think in terms of compliance strategy and think ahead
- Demonstrate characteristics as honesty, transparency, resolve despite pressure

Question 16:

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

Yes, generally speaking the more senior the position the higher the requirements should be. Equally in riskier or more complex types of business qualification requirements should be higher.

Question 17:

How do you evaluate the adequacy of courses and training for Compliance personnel?

This is a difficult question to answer. In The Netherlands there are a growing number of courses that can be followed which are provided by both commercial and non-commercial institutions. The depth of the courses, the approaches and the practical application differ widely. Only recently one of our universities introduced a post academic course.

Our association has been approached a number of times to endorse certain courses, something we have no done to this date.

We have however formulated a **professional competence profile** to describe what we think a Compliance officer should ideally have in the way of qualification and training. We hope that in the future the profile will carry some authoritative influence.

Topic 5 Assessment of the Effectiveness of the Compliance Function

Question 18:

Who, within or external to a market intermediary, is best placed to assess the effectiveness of the Compliance function?

First of all the Chief Compliance officer should have the managerial skills to assess whether the Compliance function is operating properly and whether management is responding to compliance's input.

Further objective assessment can added by allowing internal audit to periodically assess the performance of the Compliance function. External audit can play a role in institutions where there is no internal audit function. There is however an issue of cost effectiveness and knowledge when involving an external auditor.

There is a trend towards regulators making assessments of the compliance function within an institution to ascertain that it is functioning adequately.

Question 19:

What should be the role of an external party in assessing the effectiveness of a Compliance function?

The main point of assessment should be the adequacy of the compliance function in terms of staffing, structure, independence and reporting. Generally speaking external auditors will lack the knowledge and expertise to assess the Compliance issues themselves.

Question 20:

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

The main drawbacks are:

- Knowledge and understanding of the issues
- Too much distance to the business and the Compliance function
- The risk that the auditor will form the compliance function and its priorities instead of management undertaking that role
- Cost.

Question 21:

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

The depends on the risks involved in the business, but generally speaking an annual assessment on how the Compliance function is performing adequate.

Topic 6 Regulators' Supervision

Question 22:

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

We understand monitoring to mean monitoring by the regulator.

One of the best approaches is regular open dialogue with the regulator on issues and incidents that have occurred. This requires regular meetings both with management and Compliance.

Most jurisdictions require the reporting of material incidents to regulators. Although important one should not overemphasize this requirement as a monitoring tool. Incidents can happen even with the best of Compliance functions, it is only when incidents reflect a pattern that more regulatory interest is justified.

Finally, formal assessments of a compliance function by regulators should equally be one of the monitoring tools.

Question 23:

What factors are indicative of a strong compliance culture and a weak Compliance culture?

The following are indicative of a strong Compliance culture:

- Senior management not only says it wishes a strong Compliance culture but actually makes it possible and accepts responsibility at the highest level
- Management does not create a business environment nor sets business targets in word or deed, which may lead to non-compliance. It is noted that the very structure or commercial ambition of an institution might contribute to non compliance
- A well resourced Compliance function with sufficient seniority
- A well positioned and visible Compliance function
- Open and structured dialogue within the institution on reputational and integrity issues
- A Compliance organisation that meets regularly and documents its activities
- Effective training
- Evidence of an energetic, proactive function as opposed to a passive and reactive function.

Question 24:

Are there other means for implementation that we should consider?

The listed means for implementation are complete but they are solely aimed at assessment and “checking”.

The consultative document leans towards enforcement and supervision. An aspect that requires more thought is the development within the industry of proper approaches to prevent non compliance and reputational damage.

Topic 7 Cross-border issues

Question 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?

Having to operate and manage a compliance function in more than one jurisdiction is very difficult a can be very frustrating. A few examples:

- The definitions of Compliance and the role of Compliance are far from uniform
- There are significant cross border differences in regulation, culture and approaches. For instance rule based approaches versus principles based approaches versus risk based apporaches. Substance over form or form over substance?
- Cross border business structures can hinder uniform Compliance approaches and policies. Some institutions are very complex.
- Regulatory (securities, banking, insurance) co-operation for instance in the EU is urgently required and should be accelerated to arrive at harmonised approaches for instance between the banking and securities regulators.

Question 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?

Generally speaking the Compliance organisation will reflect the business organisation. These are a number of points that are relevant in cross border organisations:

- The Compliance function should form an organisation which is coherently managed, Compliance management is extremely important
- A cross border Compliance organisation will have both decentralised and centralised characteristics which must remain in balance, for instance it might not be a good idea to perform the customer due diligence of Netherlands customers by a compliance function abroad. Decentralised customer due diligence on the basis of an international CDD policy or framework will work very well provided however the policy fits well within local regulation **meets local requirements as a minimum** but also fits well within the local compliance culture.

  Therefor one should distinguish between policy, setting and local execution of policy.

We hope that our responses to your questions will contribute to the ongoing discussion on the future role of compliance and we would be very pleased to assist in any way we can.

Yours faithfully,

Nico Zwikker
Chairman VCO
nico.zwikker@nl.fortisbank.com

COMPLIANCE FUNCTION OF MARKET INTERMEDIARIES: AN IOSCO CONSULTATION PAPER

A response from the Futures and Options Association

July 2005

COMPLIANCE FUNCTION OF MARKET INTERMEDIARIES:
AN IOSCO CONSULTATION PAPER

1. Introduction

1.1 The Futures and Options Association (FOA) is the industry association for some 160 firms and institutions which engage in the carrying on of derivatives business, particularly in relation to exchange-traded transactions, and whose membership includes banks, brokerage houses and other financial institutions, commodity trade houses, power and energy companies, exchanges and clearing houses, as well as a number of firms and organisations supplying services into the futures and options sector. Further details are available on our website, www.foa.co.uk.

1.2 The FOA very much support IOSCO's general approach to defining the compliance function and, in particular, its recognition of the need for flexibility in para C, (page 6), but believes this should be emphasised at the outset of the paper.

1.3 The IOSCO Discussion Paper refers to the term "securities", but does not cross-refer to any definition of that term. The FOA accepts that this may be addressed in other IOSCO papers, but as IOSCO will know, this definition varies from jurisdiction to jurisdiction and it would be helpful to know whether IOSCO's approach to the term "securities" is intended to align itself with those definitions as they apply in each jurisdiction or whether there is a common definition by which IOSCO would determine the scope of its recommendations.

1.4 Reference is made to the compliance function having "systems or processes in place to ensure that …" (para 2, page 3). Such an obligation i.e. "ensure" places on intermediaries not only an unreasonable and unobtainable standard, but one that is higher than the regulatory authorities can themselves achieve in relation to their own statutory objectives. Surely, this obligation should be cast in terms of market intermediaries having in place systems or processes that are "designed to ensure" or "can reasonably be expected to ensure that …".

The FOA would urge IOSCO to look carefully through its Discussion Paper to ensure that all the standards it seeks to set for market intermediaries are practical, deliverable and cost-efficient and do not seek to impose standards of unattainable excellence or are the product of regulatory idealism.

1.5 Since varying degrees of protection will apply to different classes of clients, the word "appropriate" should be used on a consistent basis when referring to investor protection (e.g. in para A, page 4). It would be wrong to suggest that market intermediaries must always protect the interests of their clients when those clients are market counterparties dealing in wholesale markets. The duty owed to such counterparties is not "protection" but an obligation to act fairly, honestly and professionally and in accordance with applicable rules of the intermediary's regulatory authority.

1.6 By way of a general observation, the UK's Financial Services Skills Council is producing a set of specifications and standards for compliance officers and Money Laundering Reporting Officers. While the consultation period is now closed, the proposals can be downloaded from the website of the Council (www.fssc.org.uk).

2. Responses to CP questions

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

1.1 In our view, because of the spread of jurisdictional coverage by IOSCO, the fourth paragraph in the Introduction should really be the first paragraph and it should encapsulate in more detail the "common belief" regarding the compliance function which is held by different jurisdictions e.g:

> "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 and market intermediaries play an essential role in:
>
> - preventing possible misconduct, including particularly breaches in securities laws, regulations and rules (referred to in this paper as "securities regulatory requirements");
> - promoting ethical behaviour and acceptable market practice;
> - through contributing to ensuring the operation of fair and orderly markets, underpinning market integrity and investor confidence in those markets;
> - in sustaining applicable standards of investor protection."

This approach obviates the need for the first paragraph in the Introduction by emphasising that the starting point for reviewing and agreeing on the compliance function and in setting associated standards is to establish the objectives that can be held in common by the regulatory authorities of different jurisdictions.

1.2 In para A, page 4, the FOA notes the obligation of establishing "a separate compliance function". There has been a considerable debate within the EU arising in connection with the requirement for "independence" of the compliance function in terms of agreeing an appropriate approach in the Markets in Financial Instruments Directive (MIFID). This debate has centred on:

(a) the economic problems faced by small firms in establishing an independent compliance function; and

(b) for all firms, the problems of the requirement that compliance officers should not be involved in the delivery of the services of the firm ? founded on the argument that, if the compliance function is to operate efficiently, it has to have some engagement regarding the delivery of those services, particularly where they involve retail clients and/or high risk activities.

1.3 Surely, the common position for all firms is the need to be satisfied and to have key processes in place to satisfy themselves that the compliance function is being carried out efficiently and that any conflicts of interest are being appropriately managed (which may necessitate segregation). This issue arises again in relation to some of the comments in the first para of para B (page 4) of the Discussion Paper.

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?*

2.1 Since the nature of this relationship will vary significantly from firm to firm, depending upon the level of risk that attaches to its activities, the extent to which it is covered by regulatory obligations and the size and resources of the organisation, this question is most appropriately answered in its detail by individual firms.

2.2 On a more general basis, the management of a firm's risks will usually cover a wider spectrum of risk than is covered by regulatory requirements and therefore, while there will be some degree of overlap

(particularly with individuals/divisions responsible for business conduct compliance or compliance with prudential or capital rules or even exchange rules, e.g. market, credit and some aspects of operational risk), the risk function will not be subsumed within compliance. Moreover, the reporting function line of the risk management function will usually be internal, whereas the reporting line of the compliance function will, in addition to being internal, carry certain information obligations owed to regulatory authorities.

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

3.1 No. Reflecting IOSCO's own recognition of the importance of flexibility as set out in para C of its paper, the focus should be on the setting of the standards and delineating the scope of the function of compliance. The process of delivery and the organisational structure which stands behind the delivery of that function is a matter for the firm itself (on the basis that it is much better placed than the regulatory authority to make that determination).

3.2 Such a non-prescriptive approach will not only reflect the need for flexibility, but will also give proper and practical recognition of the fact that:

(a) regulatory authorities are increasingly recognising that they must avoid becoming overly interventionist in firms' structures and internal organisation or in the right of "managers to manage"; and

(b) it will accord with IOSCO's statement in Topic 1 (b) (on page 8) in which it states "The scope, structuring activities of the compliance function should be proportionate to the nature, scale and complexity of a market intermediary's business." (If IOSCO believes this to be true, then, logically, it cannot be prescriptive about an organisation's structure of a compliance function.)

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

4.1 In the view of the FOA, these are set out comprehensively in para (b) to Topic 1 (on page 8). The FOA believes, however, that, the test of proportionality set out in the beginning of that para should include, alongside "the nature, scale and complexity of the market intermediaries business", such additional factors as the "risk" of that business and the nature of an intermediary's client base.

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

5.1 In general terms, none, aside from those already referred to in response to Question 4. However, there will be variables in the range of responsibilities as directed by individual firms.

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

6.1 The FOA does not entirely understand the nature of this question. For example, "when" suggests that there will be times when the compliance function will not be responsible for managing compliance risk?! Surely, it is a continuous obligation and responsibility?!

6.2 In terms of "how", the compliance function must be responsible through the usual management structure but the head of compliance should always have some means of direct access to the chief

executive officer (who should retain overall responsibility for the efficiency of the compliance function, but allowing for appropriate and informed delegation of that function to competent staff). In addition, compliance officers will usually be placed under general disclosure obligations to the intermediary's regulatory authorities, sometimes supported by specific mandated "whistleblowing" obligations (which also provide protection to the "whistleblower") and, sometimes – usually where compliance officers are the subject of separate individual licensing requirements – by mandated behavioural obligations.

6.3 In general, the FOA believes that there should be at least an annual reporting function on the performance of all compliance functions to the CEO which should also be distributed to the Board of Directors.

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?*

7.1 Arguably, if the issue of "separation"/"independence" of the compliance function is relaxed for smaller market intermediaries and replaced by a burden of oversight of the competence of key staff to manage conflicts of interest and of the performance of the compliance function, there will be a need for supporting documentation to cover this differentiated treatment. Ideally, this would be developed by industry associations as an industry standard. That documentation would, of course, itself, be subject to inspection by the regulatory authority (as well as the standards of compliance with that documentation). As with all other institutions, the degree of documentation needs to be flexible because it obviously focuses on the nature and risk of the business being undertaken by the intermediary i.e. if the risk of conflicts of interest were significantly lower, then the documentation need not be so detailed. Once again, in the interests of flexibility in reflecting the diversity of the function of market intermediaries, it is important not to be overly prescriptive in this area.

8, 9 and 10. *Accountability.*

8/10.1 The specificity of the nature of these questions means that, in general terms, they may only be answered by individual firms, but the FOA would support the principles of IOSCO in determining the role and responsibilities of the Board of Directors and senior management.

8/10.2 The FOA, in general, supports the concept that a senior officer should be designated for handling responsibility for a firm's compliance function, but:

- In the case of large global houses, it is unreasonable to expect one individual to be responsible for overseeing day-to-day compliance. This is a role that could be disbursed across a number of senior compliance officers based either on a jurisdictional responsibility across a range of markets/products (e.g. in the case of a small branch) or, in the case of a much larger operation on a product/market sector basis. That said, there is usually a person appointed to the position of Head of Global Compliance who has general overall responsibility, but who would not be involved in day-to-day compliance.

- It should also be noted that senior officers may well be required to perform other functions for an intermediary, particularly if the intermediary is small-sized. This is an added reason why the FOA continues to be concerned about the cost burden of requiring "independence"/"separation".

11/14 *What requirements relating to independence and ability to act are relevant to a small firm? Etc.*

11/14.1 The FOA in general supports the principles that the compliance function should be "able to operate on its own initiative" and "without improper influence from other parts of the business". However, the FOA does not accept that it is necessary to mandate "separation" or "independence" to ensure observation of these principles. In line with the need for flexibility (emphasised in IOSCO's report) and allowing the firms themselves to develop appropriate processes and procedures for meeting the standards set by IOSCO, the issue of how the compliance function manages conflicts of interest should be left to the firm – as is the case generally with regard to the management of other conflicts of interest faced by firms.

11/14.2The FOA particularly welcomes the recognition that "regulators need to recognise, however, the difficulty of achieving complete independence from the compliance function of the smallest firms". The FOA would also emphasise the importance of the compliance function being able to engage itself in the delivery of services for the purposes only of oversight and compliance. For this reason, the concept of "independence" needs to be given careful consideration.

11/14.3In relation to Question 14, the FOA very much supports IOSCO's view that the remuneration of the compliance function should not be dependent on the performance of a particular service in a direct or exclusive sense, but that such remuneration may (and should) reflect the overall performance of a company on the basis that an efficient compliance function will add immeasurably to the reputation and performance of the firm and will underpin the trust placed in the firm by its client base.

In real practical terms, there is no way of "ensuring" that the compensation of compliance personnel does not exceed undue influence to the extent that the question of influence will vary from individual to individual. In many cases, it is only that individual who will be aware of how and the extent to which he or she is or is capable of being influenced. What can be reasonably expected of the firms is that they have procedures in place to comply with IOSCO's approach and that they monitor those areas where a particular compliance officer may be viewed as being at risk of undue influence. In other respects, it is a question of individual reputation, competence, experience and ethical values. In this context, the FOA has held its own Compliance Course over a period of many years and has, since its inception, incorporated a section on ethical values and good business practice.

15. *What are the appropriate qualifications for compliance professionals?*

15.1 The FOA agrees with IOSCO's means for implementation (page 20) and that there should be qualifications for compliance professionals. In the UK, these are now being set by the Financial Services Skills Council, which will be responsible for setting standards and accrediting courses. In terms of content, this is addressed in the response to Question 16, but in terms of the level of qualification, most jurisdictions should mandate a minimum level entry qualification to be satisfied that those who are responsible for the compliance function have a minimum acceptable understanding of the relevant rules that need to be observed.

The question of higher level qualifications should, in the view of the FOA, be a matter for the individuals themselves and their employers.

There should be a proper framework of mutual recognition in compliance qualifications, although it is recognised that this may not be appropriate where there are significant differences between the rules of different jurisdictions.

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

16.1 Yes, although as indicated in the FOA's response to Question 15, there should be a minimum entry qualification requirement of a general nature. The question of which qualifications would be appropriate for individuals will depend upon the nature of the investment services provided by the firm with the result that any form of sectoral training should be a matter for the firm and the individual concerned.

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

17.1 The FOA would refer IOSCO to the standards being set by the Financial Services Skills Council in the UK. In terms of the FOA's own course, the trainer is held in very high regard by the industry and, indeed, by the regulatory authority; the content is reviewed on a reasonably regular basis to ensure that it is up-to-date with regulatory changes; and "students" are examined and only qualify if they pass all three parts of the examining process.

The examination process comprises a multiple-choice question paper, the completion of an essay and an interview by senior compliance officers who are independent of the course, but who will probe the knowledge and understanding of "students" on pre-set problems (under the chairmanship of an independent moderator).

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

18.1 Since the responsibility of compliance is disbursed across senior managers as well as falling within the direct responsibility of the compliance section within an intermediary, the measurement of the effectiveness of the compliance function is driven by this process of internal inter-dependence. There is also the overall responsibility of the heads of compliance to the global head of compliance and the various strands of accountability to the highest levels of directoral responsibility within an organisation (depending upon its structure). At the same time, the intermediary's regulatory authority will assess compliance as part of its supervisory visits and of its review of the information provided to it by the intermediary. Finally, in most jurisdictions there is some responsibility placed on external auditors in this regard, although the extent of the oversight and intrusiveness will vary from jurisdiction to jurisdiction.

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

19.1 In most cases this will fall to the regulatory authority whose role should be to monitor and supervise the processes and procedures and efficiency of the compliance function (often through themed visits or regular or "spot" supervisory visits), by identifying compliance weaknesses, prompting solutions and identifying any enforcing breaches. It should be noted that in the UK, there is a risk-based approach to supervision which means that firms that are, in general terms, classified as higher risk for a variety of reasons, will be visited more frequently than lower risk firms. Inevitably, visits generated by the carrying on of higher risk activities or retail investor protection considerations will result in more intrusive as well as more frequent visits.

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

20.1 The main concerns of the industry are unnecessary duplication of assessments and visits made by regulatory authorities and/or exchange operators (and between regulatory authorities and exchange operators), risks to the need to preserve commercial confidentiality and the imposition of an unnecessary or excessive cost burden. It should be noted that, in the view of the FOA, the issue of whether or not to appoint an external party to conduct such a review should be a matter for the firm itself. The regulatory authorities should exercise any powers they have in this regard sparingly and only for good and justifiable cause. There is a risk that, because the cost will be borne directly by the firm, regulatory authorities could use this kind of power of appointment in order to fulfil, say, their general inspection obligations at no cost to themselves.

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

21.1 This will be wholly dependent upon the nature of the business of the intermediary, its client base (e.g. wholesale or retail), the level of risk that attaches to that business, its track record in terms of compliance and its financial strength. In the circumstances, there can be no clear minimum mandated requirement in this area, particularly where the regulatory approach is founded on risk-based principles.

22/24 *Questions relating to supervision by regulatory authorities.*

22/24.1 The regulatory function is multi-disciplined, requiring a variety of different approaches depending upon each situation. In some cases, the regulator will look to "nurse" a firm into compliance where it believes there is minimum risk to investors, etc. In other cases, especially with high risk firms, it may feel it appropriate to operate more of a "policing" role. In cases of tangible misconduct of a serious nature, it will almost certainly adopt a "prosecuting" role. It is important, however, that it is able to balance various conflicts of interest efficiently in determining how it should approach the issue of compliance breaches. For example, consideration must be given to the reputational risk of the firm, the soundness of its resources and finances, the regulatory objective to protect the interests of customers, the fulfilment of its own statutory objectives and, of course, the public interest. Balancing each of these factors will vary according to the nature of the firm and the nature of any identified weaknesses or breaches.

22/24.2 The FOA agrees with the various identified "means for implementation", subject to the following observations:

- The use of external auditors by the regulatory authority must be handled carefully and cost-sensitively for the reasons set out in para 21.1 of this paper. The FOA believes that the general supervisory function should be carried out by a regulatory authority as part of its overall responsibility and paid for out of its own cost-base.

- Regulatory authorities should rely much more significantly on each other's inspections and examinations to avoid unnecessary duplication in visits or the incurring of unnecessary cost.

- Regulatory authorities should avoid unnecessary duplication with the regulatory role of exchange operators responsible for supervising their markets.

- The FOA does not agree that self-assessment reports, certified by the Board of Directors or as may be appropriate, should be sent to regulatory authorities unless it is within a scaled back regulatory framework whose compliance is founded on the principle of self regulation. Intermediaries should be entitled to correct and manage inefficiencies in their internal compliance processes and procedures without having to disclose every identified weakness in the context of a report. Equally, the Board should feel free to encourage the production to it of full and frank reports. To require disclosure of documents of this nature would be to force

firms to address these matters “underground”. The regulatory authorities should rely on the general information disclosure obligations that are placed on their regulated intermediaries without mandated disclosures of this nature which can only impair the efficiency of internal compliance and its management.

19 July 2005

Mr Philippe Richard
Secretary General
International Organisation of Securities Commissions
Oquendo 12
28006 Madrid
Spain

By email: mail@oicv.iosco.org

Dear Mr Richard,
Compliance Function at Market Intermediaries

ASX welcomes the opportunity to contribute to the IOSCO consultation on the role of the compliance function at market intermediaries.

ASX operates Australia's primary national stock exchange and clearing house for equities, derivatives and fixed interest securities. It also provides comprehensive market data and information to a range of users. All these operations are underpinned by comprehensive high-quality information technology systems.

Ensuring the integrity of the market – a market that is fair, orderly and transparent – is central to ASX's business. This is important as both a matter of principle and commerciality. Indeed, as a licensed market operator, ASX is obliged by law to provide it.

A market of high integrity creates a level-playing field for all market users, inspiring confidence among investors, brokers, companies, regulators and the broader community. A market that operates with the confidence of its users attracts capital, transfers risk and has the potential to generate wealth across the economy fairly, efficiently and at the lowest cost.

ASX's commitment to maintaining the integrity of the market is absolute. In pursuing the highest level of market integrity, ASX undertakes comprehensive supervision of companies, stockbrokers and broking firms, and general trading activity in the market.

The reputation of ASX's markets for fairness and integrity is very important to ASX. Maintaining this reputation involves constant and vigilant supervision. Through effective supervision, ASX strives to enhance its reputation as a market of integrity, providing an investing environment of internationally high repute.

ASX's supervisory activities are focused upon:

- supervising companies compliance with the ASX Listing Rules;

- supervising trading activity in the market and compliance with the ASX Market Rules;
- supervising compliance with the ACH Clearing Rules;
- supervising compliance with the ASTC Settlement Rules; and
- helping meet the regulatory obligations of ASX under the Corporations Act

To give effect to this, ASX's Supervision Division comprises Issuer Supervision; Participant Compliance; Market Surveillance; Prudential Risk Management; and Investigations and Enforcement departments.

ASX considers a robust compliance function within financial intermediaries operating in our markets, clearing and settlement facilities to be an integral element of maintaining the integrity of our markets.

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

The consultation paper defines and describes the compliance function as follows:

> "A function that, on an on-going basis, identifies, assesses, advises on, monitors and reports on a market intermediary's compliance with securities regulatory requirements, including whether there are appropriate supervisory procedures in place."

We believe this definition and description is too narrow. The modern compliance function is more than that set out above. The modern compliance practice should be a strategic enabler of value to an organisation. In that regard, the language of the definition above focuses upon the defensive nature of the compliance function.

The definition and description of the compliance function is considered in the *Australian Standard on Compliance Programs AS3806.* However, we believe the definition and description of the compliance function is best established by those in the compliance profession, rather than by regulatory prescription. Hence we believe the function is best defined as set out by the Australian Compliance Institute (http://www.compliance.org.au):

"Compliance is defined as the provision of services that facilitate an organisation *identifying and meeting its obligations* whether they arise from:

- laws
- regulations
- contract
- industry standards, or
- internal policy
-

Achieving effective and efficient compliance requires:

- commitment and leadership from the Board and the CEO;
- analysis of requirements and identification of risks, requirements and exposures;
- development of systems and procedures; and
- the creation of an organisation wide compliance culture.

Cost effective compliance is achieved when the organisational culture integrates compliance into the fabric of how business is conducted.

The primary responsibilities of a compliance professional are founded in the *social and business expectation* that organisations will be managed in a way that meets the legal requirements. Compliance management systems form one of the primary platforms for strong corporate governance.

The compliance professional's responsibilities can therefore be stated as follows:

- primary responsibility to the **Board** to ensure that the organisation has a compliance management framework that is effective and efficient and deals with key compliance risks to the organisation. This is a responsibility that is **independent** of the business requirements and goes to good corporate governance practices. There is an emerging trend for Boards to create Compliance Committees separate from the audit function.
- a responsibility to the **Senior Management** to assist them in understanding the regulatory and legal obligations from a practical perspective, identify risks and develop appropriate management systems and operational procedures to deal with those risks.

If there is a conflict between compliance requirements and business objectives, it is the compliance professional's responsibility to assess the commercial and legal risks of non-compliance objectively and ensure that the Board and Senior Management are advised of these risks. It is the responsibility of the Board and Senior Management to determine how the compliance risk is to be managed. There should be an independent reporting line between the Board and the Compliance Professional to assist in escalation of these types of issues.

The key objectives of a compliance professional in relation to their organisation are as follows:

- To assist the Board and the Senior Management in the *development of an organisational culture* that proactively supports compliance activity and to provide current information to the organisation about the "philosophy" of compliance practices and how it is being implemented within an organisation.
- To design and assist in the establishment of a *compliance management framework* that:
    - identifies relevant compliance requirements and understands the risks involved;
    - codifies the compliance requirements into policies, procedures and controls;
    - ensures appropriate levels of staff knowledge about compliance requirements;
    - monitors the effectiveness and efficiencies of compliance procedures and controls; and
    - provides relevant and appropriate reporting procedures for compliance issues.
- To provide commercial / practical insight into regulatory and legal compliance requirements that align with business objectives and to generate flexible and innovative solutions to the achievement of compliance requirements within the operational context."

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*?*

Compliance is about meeting particular acknowledged obligations that may have a mandatory component to them. Risk management does not have a mandatory component to it, as the organisation may determine how it wishes to deal with risky situations.

The compliance function may use risk management techniques and may primarily address a key risk – regulatory risk – but it will generally involve a different and distinct methodology to that of risk management. The relationship between the risk management and compliance functions within any particular financial intermediary will largely be a function of the size of the intermediary.

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

ASX believes that there are some structural aspects of the role of a compliance function which could be prescribed, but that it is not appropriate to prescribe a specific organisational structure for all organisations.
The basic elements of structural requirements have been set out in the *Australian Standard on Compliance Programs AS3806*. However, ASX submits that the key structural element is the need for independent lines of communication between the compliance function and the governing body of the organisation. In many cases, direct reporting relationships between the compliance function and senior management may be the most appropriate. However, even in these cases, there is a need for avenues of independent communication to the governing body as a mechanism for addressing situations where the compliance interests of the entity and management may diverge.
Prescription will generally not serve to take account of the divergent needs and business models of various intermediaries, such as size, geographic dispersion, internal culture or regulatory environment. Effective and efficient market development requires guidance and flexibility in the internal structures of intermediaries.
ASX believes it is appropriate for indicative standards to be established, as is the case with the *Australian Standard on Compliance Programs AS3806*, but not to be prescribed.

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

Our response is generally encompassed in the responses to questions 1, 2 and 3 above. Specifically:

- The modern compliance practice should be a strategic enabler of value to an organisation. In that regard, prescription of roles, responsibilities or activities would detract from that objective.

- Cost effective compliance is achieved when the organisational culture integrates compliance into the fabric of how business is conducted. Prescription of roles, responsibilities or activities may detract from that objective.

- the *Australian Standard on Compliance Programs AS3806* sets out a framework for the compliance function;

- Prescription will generally not serve to take account of the divergent needs and business models of various intermediaries, such as size, geographic dispersion, internal culture or regulatory environment. Effective and efficient market development requires guidance and flexibility in the internal structures of intermediaries.

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

Our response is generally encompassed in the responses to questions 1, 2 and 3 above. Specifically:

- The compliance professional's responsibilities can therefore be stated as follows:

    - primary responsibility to the **Board** to ensure that the organisation has a compliance management framework that is effective and efficient and deals with key compliance risks to the organisation. This is a responsibility that is **independent** of the business requirements and goes to good corporate governance practices. There is an emerging trend for Boards to create Compliance Committees separate from the audit function.

- a responsibility to the **Senior Management** to assist them in understanding the regulatory and legal obligations from a practical perspective, identify risks and develop appropriate management systems and operational procedures to deal with those risks.

- The key objectives of a compliance professional in relation to their organisation are as follows:
    - To assist the Board and the Senior Management in the *development of an organisational culture* that proactively supports compliance activity and to provide current information to the organisation about the "philosophy" of compliance practices and how it is being implemented within an organisation.
    - To design and assist in the establishment of a *compliance management framework* that:
        - identifies relevant compliance requirements and understands the risks involved;
        - codifies the compliance requirements into policies, procedures and controls;
        - ensures appropriate levels of staff knowledge about compliance requirements;
        - monitors the effectiveness and efficiencies of compliance procedures and controls; and
        - provides relevant and appropriate reporting procedures for compliance issues.
    - To provide commercial / practical insight into regulatory and legal compliance requirements that align with business objectives and to generate flexible and innovative solutions to the achievement of compliance requirements within the operational context.

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

In responding to this question, we first draw a distinction between responsibility, accountability and liability.
The compliance function should be responsible for identification, prevention and remediation of the planning and response to compliance risk.
Line management should be accountable for the implementation of actions to manage or avoid compliance risks.
The governing body should be accountable and liable for the implementation of actions to manage or avoid compliance risks.
ASX's view is set out in its Guidance Note "Ongoing compliance and supervision – responsibilities of Responsible Executives". ASX is of the view that compliance executives should not be line managers. Such a mixing of functions undermines the compliance executive's independent support and monitoring functions. Line management is directly accountable for day to day compliance by those people under their management.
ASX takes the view that line management is accountable for supervising the design and implementation activities and the functioning and review of the operations and processes under their management. Line management must have sufficient seniority and authority within the financial intermediary to exert control, leadership, influence and supervision over those operations and processes under their management.
Accountable line management will generally be a line manager accountable for the supervisory controls, processes, systems and culture within an intermediary and will have the power to hire, fire, punish or reward a subordinate employee. Compliance executives generally are not line managers for business units, although they may be line managers with respect to employees in the compliance department. Compliance executives may advise accountable line management about the hiring, firing and discipline of employees, but they generally do not make actual decisions in these areas.

In performing their duties accountable line management may rely upon the advice and services of a compliance executive to, for example, provide advice, inform them of compliance related issues and to monitor the satisfaction of compliance related obligations.
However, ASX acknowledges that for various reasons an intermediary may wish to appoint a compliance executive in an accountable line management role for some purposes.
A compliance executive will generally not be held accountable by ASX for failure to supervise another person unless they have the responsibility, ability and authority to affect the other person's conduct in a line management capacity.

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?

ASX expects all its market participants to adopt written policies and procedures, irrespective of size. However, of more importance than the existence of the documentation, are the outcomes of the policies and procedures which have been documented.
ASX experience has been that some very large organisations have had very high standards of documentation and poor compliance outcomes, whilst some small organisations 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.

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.

ASX's view is set out in its Guidance Note "Ongoing compliance and supervision – responsibilities of Responsible Executives", a copy of which is attached.

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

Our response is generally encompassed in the responses to question 6 above. Specifically, we draw a distinction between responsibility, accountability and liability.
The compliance function should be responsible for identification, prevention and remediation of the planning and response to compliance risk.
Line management should be accountable for the implementation of actions to manage or avoid compliance risks.
The governing body should be accountable and liable for the implementation of actions to manage or avoid compliance risks.

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

Our response is generally encompassed in the responses to questions 6 and 8 above.
Line management is directly accountable for day to day compliance by those people under their management.
ASX takes the view that line management is accountable for supervising the design and implementation activities and the functioning and review of the operations and processes under their management. Line management must have sufficient seniority and authority within the financial intermediary to exert control, leadership, influence and supervision over those operations and processes under their management.
In performing their duties line management may rely upon the advice and services of a compliance executive to, for example, provide advice, inform them of compliance related issues and to monitor the satisfaction of compliance related obligations.
A compliance executive will generally not be held accountable by ASX for failure to supervise another person unless they have the responsibility, ability and authority to affect the other person's conduct in a line management capacity.

In addition, we would submit that the "positioning" of the senior compliance executive within the intermediary is critical. It sends a clear message about seniority, access to power (for example, direct access to the Board or CEO), authority and the relative importance which the organisation places on the function.

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

ASX submits that there should not be any "requirements". We submit that there needs to be recognition of the issues faced by small firms in any regulatory framework. The special circumstances of small firms and factors which may be taken into account are specifically recognised in the *Australian Standard on Compliance Programs AS3806.*

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?

Our response is generally encompassed in the responses to questions 6, 8 and 11 above.

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

The means of implementation should not be prescribed. For the reasons set out above, expectations can be established, but should not be set out in prescriptive form as to do so deprives what is an inherently fast moving and dynamic industry of the flexibility it requires to adapt.

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

The measurement of compliance performance is inherently difficult. The remuneration of compliance personnel should not be directly related to the financial drivers of the organisation or particular business unit.
Appropriate recognition may be derived from external indicators (for example, client perception of the compliance culture of the organisation, internal perception, Board perception); external review findings; reviews by central regulators, exchanges or SROs; industry benchmarking studies or other indirect indicators.

What are the appropriate qualifications for compliance personnel?

Compliance professionals derive from a wide range of backgrounds, whether regulatory or commercial. The Australian Compliance Institute has established a skills and accreditation framework of the 27 essential competencies of a compliance professional, independent of profession or industry sector. These include competencies such as assertiveness, negotiation skills, training skills, investigations skills, etc. The level of competence for each of these varies according to the seniority and experience of the individual. Overlaid on those competencies are specific technical knowledge applicable to the relevant profession or industry sector of the individual.
ASX submits that it is the role of professional bodies to determine the standards and competence considered appropriate within a profession, rather than the role of the regulator. It is the role of the regulator to engage with those professional bodies during the development of those competency standards and on an ongoing basis to promote the relevance and maintenance of those standards, not to prescribe them.

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

Yes. Our response is generally encompassed in the responses to question 15 above. Specifically ASX submits that it is the role of professional bodies to determine the standards and competence considered appropriate within a profession, rather than the role of the regulator. It is the role of the regulator to engage with those professional bodies during the development of those competency standards and on an ongoing basis to promote the relevance and maintenance of those standards, not to prescribe them.

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

Our response is generally encompassed in the responses to question 15 above. Specifically, it is the role of a professional body to undertake the assessment and for the regulator to engage with those professional bodies

during the development of those courses and on an ongoing basis to promote the relevance and maintenance of those course standards, not to prescribe them

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

ASX submits that there is no single answer to this issue as there are inherent conflicts in any such activity, whether the reviewer is internal or external.
ASX submits that the issue is not who is best placed, but what are the objectives, parameters, constraints and scope of the brief of the reviewer. In that regard, ASX has recently had input into the development by the Australian Compliance Institute of *Protocols for Reviewing and Assessing the Adequacy, Effectiveness and Efficiency of Compliance Protocols*. Those protocols have been specifically developed to enable organisations to:

More effectively plan and undertake internal reviews;

Obtain more value from compliance reviews by being able to negotiate more effectively with external reviewers; and

Better understand what is required of them when they are subject to a mandated compliance review as part of a regulator's enforcement program.

They have also been developed to enable the compliance industry to have a minimum standard for compliance programme reviews and reporting that will enable more realistic comparison and benchmarking across organisations as to the effectiveness of compliance measures.
ASX submits that the establishment of industry standard processes and benchmarks will be the key determinant of assessing roles and effectiveness, not the relationship of the person conducting the review.

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

ASX submits that there is no single answer to this issue as the role of the external reviewer will be dependant upon the objectives and the desired outcomes of the review.
Our response is generally encompassed in the response to question 18 above. Specifically, ASX has recently had input into the development by the Australian Compliance Institute of *Protocols for Reviewing and Assessing the Adequacy, Effectiveness and Efficiency of Compliance Protocols*. Those protocols have been specifically developed to enable organisations to, amongst other things, obtain more value from compliance reviews by ensuring the role of the reviewer is defined and better understanding the roles of all parties when they are subject to a mandated compliance review as part of a regulator's enforcement program.

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

Our response is generally encompassed in the response to question 18 above. Specifically, ASX has recently had input into the development by the Australian Compliance Institute of *Protocols for Reviewing and Assessing the Adequacy, Effectiveness and Efficiency of Compliance Protocols*. Those protocols have been specifically developed to enable organisations to:

More effectively plan and undertake internal reviews;

Obtain more value from compliance reviews by being able to negotiate more effectively with external reviewers; and

Better understand what is required of them when they are subject to a mandated compliance review as part of a regulator's enforcement program.

Further, the twelve protocols, developed in consultation with both compliance professionals and regulators, specifically address many of the practical concerns which would ordinarily be experienced by the intermediary and/or the reviewer. For example, these include:

- defining who will be relying upon the review;
- defining the scope and limitations of the review;
- defining the methodology; and
- disclosing conflicts of interest.

A key practical concern in the conduct of an external review is ensuring there is a clear understanding of the role of the reviewer in the event the reviewer identifies a significant breach. Issues which arise include:

- the obligation (if any) of the reviewer to report to the intermediary;
- the obligation (if any) of the reviewer in the event the intermediary declines to take action in response to the breach;
- the obligation (if any) of the reviewer to report to the regulator;
- the impact (if any) on the reviewer (including any professional indemnity insurance issues) in the event that reporting to the regulator by the reviewer is outside the scope of the review; and
- the liability (if any) – moral or legal - upon the reviewer for not reporting to the regulator in the event the intermediary declines to take action in response to the breach.

Factors such as these will have a critical impact upon the scope, methodology and outcome of the review.

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

There is no single frequency. The scope and frequency is dependent upon the regulatory risk appetite and past compliance (or non-compliance) performance of the intermediary.

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

The most effective methodology is dependent upon the nature of the business being undertaken, the design of the methodology and the value of the outcome of that methodology.

ASX submits that a key element of "effectiveness" is attaining an appropriate balance between internal monitoring by the financial intermediary and external monitoring by the regulator. Excessive external monitoring can diminish the effectiveness of internal monitoring by diverting essential (and effective) internal resources to tasks associated with servicing external monitors. Excessive external monitoring can arise from a range of factors including inefficient practices by a regulator; multiple regulators or untimely regulation.

In general, participants in the ASX markets are supervised by, at least, ASX and ASIC. In order to minimise overlapping and/or clashing supervision and hence reduce inefficient regulation, ASX advises ASIC of upcoming key programs and fieldwork in order to avoid excessive negative compliance resource impact upon our participants.

ASX adopts a model of supervision based upon the "regulatory pyramid" encompassing the full spectrum of supervisory activity ranging from education of investors and participants to termination of participation in the market.

The most effective internal methodology observed within a financial intermediary to date has been peer monitoring. However, this can only ever occur where the organisational culture integrates compliance into the fabric of how business is conducted. That is, compliance monitoring is integral to the operational processes of

the business. This has been observed as a very effective method in at least one stockbroking organisation participating in ASX's markets.
Measurement of the effectiveness of supervisory action can be problematic. There is an inherent tendency to measure effectiveness solely by statistical measures of "activities" undertaken (for example, the number of prosecutions, number of surveillances or examinations, etc). Such measures tend to provide indicators of activity which may or may not be linked with outcomes or effectiveness. The converse is also true in many regards, that supervisory activity can be driven by what can be measured, not by addressing the key issues underlying the supervisory objectives.
The most effective methodologies are those which clearly identify the key regulatory issues to be addressed, then identify the causes, the solutions, the outcomes and the appropriate measurement of those outcomes to the contribution to the desired objectives.

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

As stated in question 22, the best indicator of a strong compliance culture is where the organisational culture integrates compliance into the fabric of how business is conducted. That is, the culture of the organisation is "the way we do things around here – when no one is watching".
Indicators of a strong compliance culture are leadership from senior management; accountability; clear organisational values; clear and strong implementation of those values (even when, at times, detrimental to the revenues or profits of the organisation); consistency of reward and punishment; alignment of individual objectives to corporate objectives and values; and strong culture of social responsibility.

Are there other means for implementation that we should consider?

A key issue for financial intermediaries is the response of regulators to self reporting of breaches and the existence, or otherwise, of any sort of self-examination (or professional privilege) defence for compliance professionals.
ASX submits that further development of thinking, policy and dialogue on these issues will have a significant positive impact upon the corporate response to compliance practices and standards.

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

No comment

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?

No comment

Should you wish to seek further clarification of any matters within this submission, please do not hesitate to contact David Lawrence at david.lawrence@asx.com.au. or Eric Mayne at eric.mayne@asx.com.au

Yours sincerely,

Eric Mayne
Group Executive, Market Supervision
Direct Tel; (612) 9227 0405
Direct Fax; (612) 9227 0428
Email; eric.mayne@asx.com.au

INTERNATIONAL
BANKS AND SECURITIES
ASSOCIATION OF AUSTRALIA

IOSCO Consultation Report
– Compliance Function at Market Intermediaries

22 July 2005

Introduction

The International Banks and Securities Association of Australia (IBSA) represents investment banks and securities companies operating in Australia. All members have a significant international dimension to their business, either as domestic banks with overseas operations, or as a branch or subsidiary of a foreign financial institution. Many form part of a conglomerate group. Thus, their compliance function must typically manage regulation emanating from a number of jurisdictions and regulators.

In recent years, IBSA has observed both an increase in the complexity and scope of regulation and the enhancement of member firms' compliance functions. The significant commitment of resources to the compliance function is a consequence of changes to regulation, as banks and securities companies manage their regulatory obligations. However, it also reflects a strong commercial impetus for regulated entities to be compliant and seen as conducting their business in an ethical manner. A range of stakeholders expect a regulated entity to operate in a competent and ethical manner and penalise those who do not do so. Apart from the risk of regulatory action against an entity and its officers, an entity's business may suffer if its reputation or 'brand name' is harmed by a compliance failure.

The importance of a diligent and effective compliance function in a financial institution is understood and international institutions typically have well-established, experienced and competent compliance functions. We believe it is important that the principles adopted by IOSCO provide clarity about the levels of responsibility within an entity for accepting compliance risk, implementing measures to manage this risk and monitoring the effectiveness of those measures. This must adequately capture the different role and responsibilities of the board, senior management and the compliance function in dealing effectively with compliance risk.

For instance, the compliance function cannot "enforce" compliance policies and procedures but, rather, must work in conjunction with senior management (and with the cooperation of business units) to ensure they are effective. Ultimately, the senior management of an entity, with oversight by its board, is responsible for ensuring the effective management of the compliance risk and must make decisions accordingly. Compliance should form part of an embedded operating culture within a firm that reflects the ideals that underpin regulation, rather than merely following prescriptive regulatory rules.

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

The Consultation Report defines the compliance function as a function that, on an on-going basis, identifies, assesses, advises on, monitors and reports on a market intermediary's compliance with securities regulatory requirements, including whether there are appropriate supervisory procedures in place.

Our principal comment on this definition is that the scope of the compliance function is generally broader than that envisaged in the Consultation Report.

- The compliance function in a financial institution typically covers a range of regulation, beyond 'securities regulation' in the narrow sense. This reflects the growing integration of financial services business and conglomeration. For example, the compliance function within a bank would have responsibility for the bank's participation in securities and capital markets as well as banking regulation. While we appreciate that the focus of the Report is securities regulation, both the regulator's administration of regulation and the compliance measures adopted by financial institutions should reflect the broader scope of many institutions' business to avoid inconsistencies, or double-ups and to promote the maximum efficiency of regulation.

  The Basel Committee on Banking Supervision recently issued principles to govern the compliance function in banks.[4] The IOSCO principles should recognise the adequacy of the Basel Committee principles for banks that are involved in the securities markets and subject to securities regulation and deem them to have adequate compliance controls.[5] To the greatest extent possible, the IOSCO approach should be consistent with that adopted by the Basel Committee; for example, IOSCO's scope of the compliance function is narrow and would benefit from a broadening to reflect matters like reputation risks, which are better recognised by the Basel Committee.[6]

- The compliance function is a support function that works in partnership with business units within the entity to assist them to conduct their business in a manner that complies with the law and the entity's internal polices. For instance, it can play an important role by advising business units on how to deal with market innovation and change, especially in new developments not covered by existing regulatory instruments. In this manner, the compliance function must be seen to add value to the business, which helps to nurture a good compliance culture within the entity. In contrast, if compliance were presented simply as an internal regulator or policeman due to its monitoring role, this would unsettle the cooperative relationship with business lines that is a prerequisite for effective compliance.

- The compliance function in a financial institution is not limited to external regulation and it may have responsibility for the monitoring and reporting of internal policies and industry codes. Thus, it may extend beyond strict legal obligations and cover other matters of ethics and good behaviour. Many financial institutions adopt a range of internal policies and procedures, some of which are to ensure compliance with external regulations. In other instances measures are undertaken to enhance their stakeholder relationships and contain reputation risk. For example, some investment banks have adopted global controls to manage research related conflict of interest that are more restrictive than the requirements in some jurisdictions that they operate in.

  The compliance function plays an important role in preserving the value of these client-relationship and reputation assets. The maintenance of a sound compliance function is a matter of commercial sense, having regard to the expectations of clients, the importance of confidence in financial markets and the potential harm to business from damage to an entity's reputation.

- The compliance function within an entity undertakes a range of other tasks. It contributes to the Government's development of legislation and regulatory instruments and the efficient administration of the law by the regulator. This involves participation in government or regulator sponsored consultations to bring industry experience and know-how into the design of regulatory policy and related instruments. This role is particularly important in jurisdictions where SRO's have a role in

---

[4] Compliance and the Compliance Function in Banks, Basel Committee on Banking Supervision, April 2005.

[5] The Basel Committee principles apply to entities that are banks and to bank groups (which may include securities company subsidiaries0.

[6] The Basle Committee defines "compliance risk" as - the risk of legal or regulatory sanctions, material financial loss, or loss to reputation a bank may suffer as a result of its failure to comply with laws, regulations, rules, related self-regulatory organisation standards, and codes of conduct applicable to its banking activities. The expression "compliance function" is used to describe staff carrying out compliance responsibilities.

regulation, as it helps to inject a pragmatic business focus to the regulatory development and implementation process.

The compliance function is important to the entity's relationship with the regulator and serves as a link between a regulator and an entity's business units. This needs to be recognised in the way that the entity deals with the regulator and in the way that the regulator manages individual licensee arrangements. Both the entity, through its compliance function, and the regulator should have a planned capability in this area. Our experience with regulators outside of the securities sphere is that dedicated relationship managers for large and complex financial institutions help the compliance process. Apart from streamlining administration, this helps the regulator to develop a rapport with the industry, better understand the nature of the business and promote regulatory objectives.

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?

The compliance and risk management functions are interrelated and have overlapping objectives. For example, a failure to correctly assess a client's reputable standing and creditworthiness may create the risk of financial loss and reputation harm to the entity. In practice, compliance is one aspect of a multi-dimensional risk management objective. The manner in which different entities manage this relationship need not be prescribed, for the reasons discussed below.

Topic 1: Establishing a Compliance Function

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

No.

Once the sought-after regulatory outcomes are clear, each entity should be given discretion on how it can structure its compliance function to best meet its associated obligations. An entity that applies its expertise and resources to meet its regulatory responsibilities in the most efficient manner may gain an advantage over its competitors and mandating a rigid structure may unduly impede this aspect of market discipline. Providing an acceptable degree of flexibility would not preclude the setting of minimum standards (like independence, adequate resources and suitable access to information and senior management), but it would enhance the likelihood of them being met comprehensively.

Financial entities conduct a range of businesses, of differing scales in a variety of operating structures. For example:

- Some may operate as locally incorporated entities, while other may operate internationally through a branch network;
- Some entities have a wide range of business units (product line and/or geographically), others may have a narrow business focus;
- Some entities may conduct wholesale business only, while others may have a significant retail component to their business.

Since the weight and scope of regulation may vary depending on an individual entity's circumstances, it would be inappropriate to prescribe a specific structure for its compliance function. A prescriptive approach would risk being overly restrictive and insensitive to the commercial aspects of a business, or unduly complex if it were to try and accommodate each possible structure within declared rules. An entity should be permitted to adopt whichever compliance structures and practices it decides is optimal from its business perspective, once it can demonstrate that these are effective by reference to the underlying policy objectives.

Further, the Consultation Report correctly identifies the significance of corporate culture and ethics in determining the approach to compliance within a financial intermediary. No particular organisational structure will overcome deficiencies in this area.

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

No.

For the reasons outlined above, a better regulatory outcome would be achieved through the implementation flexibility within a framework of sound and transparent policy principles.

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

See the answer to Question 1.

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

The compliance function should be responsible for the implementation of compliance policies and procedures within the governance framework established by the board and senior management of the entity. This implies the delegation of appropriate implementation authority and appropriate support (financial and otherwise) from the board and senior management, who have ultimate responsibility for ensuring that compliance risks are managed. The following paragraphs consider relative responsibilities in broad terms.

The board is responsible for ensuring that an appropriate policy is in place to manage compliance risk and has oversight of its implementation. It sets the tone for the standards and values to be promoted within the entity.

The senior management is responsible for the implementation of the board's compliance policy. For instance, it should settle the specifications of the policy approved by the board and provide adequate resources to ensure the compliance function can operate effectively. It should actively promote and endorse the implementation of policies and allocate time to understand and keep abreast of compliance matters. This may involve action to mitigate potential problems, including disciplinary measures where necessary. It should set the performance benchmarks for both the compliance function and its personnel.

The compliance function assists the senior management to manage the entity's compliance risks and implements the associated compliance policies. Usually, it will monitor regulatory and internal policy developments, provide advice to senior management on compliance matters, identify and evaluate compliance risks in the business, undertake surveillance and testing of compliance, report to senior management on compliance matters, assist in education and training, and provide guidance to staff on compliance matters.

As outlined above, the compliance function should not be seen as a unit divorced from the business units within the entity. In practice, there is a broad-based responsibility within a regulated entity for managing its compliance risk.

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?

No comment.

Topic 2: Role and Responsibilities of the Board of Directors or Senior Management

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.

The Consultation Report proposes that the board of directors or senior management is responsible for the entity's compliance with securities regulatory requirements. This principle is ambiguous about the relative roles of the board and the senior management of an entity and the reason for this is not clear.

There must be a much clearer line of responsibility running from the board (which should approve the compliance policy) to senior management (eg it should establish a compliance policy and function), to the compliance function responsibilities (eg implementation of the compliance program). In this regard, it is relevant to note that the Basel Committee approach offers greater clarity on the allocation of compliance responsibilities.

The board and senior management have an important responsibility to foster a culture of compliance, by creating and embedding a sound compliance culture within the entity.

Foreign branch operations present slightly different issues, as they would not have a local board to report to (unlike locally incorporated entities). In this situation, the senior management of the branch would have 'board' type responsibilities for local compliance function, though this authority would sit within the board approved compliance framework for the global entity that is overseen by its global senior management and compliance function.

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

See answer to Question 8.

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

Yes.

A senior officer should generally be made responsible for the day-to-day management of the compliance function, including the identification and management of compliance risks. With the support of senior management and the board, this person would have the necessary authority to ensure that the compliance function operates effectively.

Large and complex financial entities, especially those with significant international operations, would have a sizeable compliance staff dispersed within the entity (by location and/or business unit). It would be necessary to have a focal point to coordinate compliance activities, including compliance reporting, to maintain control of the compliance risks across the entity.

Topic 3: Independence and Ability to Act

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

No comment.

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?

Several factors come into play in determining the approach to be taken to manage compliance risk. These will include personal attributes (like experience, character and qualifications) of the individual concerned, the particulars of the compliance role and potential conflicts of interest and the nature of senior management and board oversight. Thus, a prescriptive regulatory approach is not appropriate – this emphasises the need for a principles-based approach to compliance that is focused on the underlying regulatory objectives.

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

The compliance function forms part of the total business of a financial institution and is not wholly independent from the remainder of the firm. A compliance function could not function effectively if it were separate from the business units that fall within its area of responsibility. To achieve its objectives, a compliance function must maintain an open dialogue with business units about the ongoing conduct of business, changing business practices and methods and new areas of business in order to assess its relevance to regulation and compliance practices. The compliance function's contribution to this dialogue is one factor that should be considered as part of an assessment of its effectiveness, though it must be balanced against other important compliance objectives.

To facilitate this level of engagement and at the same time assuredly facilitate the firm's compliance with securities (and other) regulations, it is important that clear lines of responsibility are set, policies and procedures are approved and actively supported by the board and senior management (including an adequate budget) and communicated within the firm. In particular, it is important that the compliance function is not answerable to the business unit, but rather to senior management of the whole entity. This would address the risk of undue or improper influence on the compliance function by other parts of the business.

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

It would be reasonable for the compensation of the compliance function personnel to reflect the performance of the entity as a whole, but it would be inappropriate for remuneration (or promotion or tenure) to be linked to an individual business unit or transaction, given potential conflicts of interest this would create.

Topic 4: Qualification of Compliance Personnel

15. What are the appropriate qualifications for compliance professionals?

The requisite competency for compliance personnel depends on the range of regulation and business activities that are their responsibility. In general, compliance personnel should have a sound technical knowledge of relevant law, regulatory instruments, standards and codes. Moreover, compliance personnel should understand the nature of the business they operate within, so they are well-placed to advise business units and to identify emerging compliance issues at an early stage. The financial services industry and the manner of its regulation are continually evolving, so that it is necessary to provide ongoing education and training within the compliance program.

In addition, there is a range of personal qualities (eg interpersonal and problem solving skills) that are desirable including:

- A high ethical standard;
- Preparedness to speak up (to challenge management to strive for a high ethical standard);
- Ability to deal with general principles and apply them in specific situations (especially new factual situations);
- Problem solving and project management skills;
- Willingness to say no, when it is required.

While these general comments can be made about the attributes of compliance personnel, the actual requirements may depend on business circumstance and the individual's role, as well as the professional skills and specialist expertise of other members of the compliance team who they must complement. Thus, there will an element of judgement involved.

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

Yes – Decisions about this should be a matter for the management of the entity rather than in detailed regulation.

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

No comment.

Topic 5: Assessment of the Effectiveness of the Compliance Function

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

Internally, senior management are best placed to judge the effectiveness of the compliance function, as they have the requisite range of information and insights to make an informed assessment.

Externally, regulators will inevitably make an assessment on the effectiveness of a regulated entity's compliance function, as part of its administration of the licensing system. This is likely to occur both at the time of licensing and an on-going basis. Post-licensing, it should fit within the within the framework of a risk-based approach to supervision (as discussed below).

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

The industry regulator should provide adequate policy guidance on the benchmarks against which it will assess regulated entities and be open to engagement on matters of ambiguity to enable the compliance function to perform effectively. This requires the regulator to be well attuned to the evolving nature of the industry. A sound, ongoing dialogue between the regulator and industry can assist in this respect, by facilitating a flow of information about market developments and identifying potential issues before they emerge to become a real problem.

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

The cost of an external review needs to be managed to keep both the dollar costs and the distraction of compliance and management personnel from their core functions at an acceptable level. To assist this process, reviews should be scheduled to minimise the degree of disruption to the normal operations of the compliance function.

Any party conducting an assessment of an entity's compliance function should have a demonstrated competency to undertake this task, to minimise the potential for irritation and ensure a smooth review process. Thus, regulators must acquire, develop and maintain the relevant expertise to confidently undertake this task.

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

This should be a matter determined by the licensed entity

Topic 6: Regulators' Supervision

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

Subsequent to the initial licensing process, a risk-based approach to prioritising regulatory supervision offers the best prospect to allocating a regulator's limited resources, as it would push resources to the area of greatest need. This would be superior to a rigid code (eg mandated periodic reviews) for regulator's supervision on

compliance functions and should be supported by an on-going dialogue with industry of the type outlined above.

Often a financial intermediary would be subject to supervision by more than one regulator. From a practical perspective, regulators should actively seek to minimise the disruptive effect of an external review; for example, they should avoid a review coinciding with that of another regulator, or another review it is conducting, to the greatest extent possible

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

By their very nature, matters of organisation culture are difficult to measure or assess, as they are ingrained in the way an entity reacts to issues. Indeed, were it possible to prescribe in a regulatory instrument the features of a good culture, this would have been done by now.

With this significant qualification in mind, the following are factors suggested to us that may indicate the effectiveness of a compliance function:

- Board and senior management commitment to the compliance function (including adequate resources, suitable access to personnel and information, active participation in compliance initiatives etc.) and ongoing communication of the importance of compliance;
- Understanding of the commercial returns from an effective compliance function (i.e. a holistic appreciation of compliance risks);
- The existence of technically sound compliance policies and procedures and their effective communication throughout the entity, as well as compliance benchmarks against which all relevant staff can be assessed;
- The response to compliance problems – the fact that problems may occur should not of itself be seen as a compliance failure; rather their identification may reflect a compliance strength and the nature of the entity's response to it may be a good indicator of the importance attached to compliance;
- The ability of bad news to escalate to the senior management at the same speed as good news.

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

As mentioned in the answer to Question 1 above, the compliance function in a regulated entity usually manages the relationship with the entity's regulator. It is important for the regulator to manage this line of communication effectively. In this context, the appointment by the regulator of client relationship managers for large, complex entities would streamline day-to-day dealings between it and the financial entities it regulates. It would also provide the regulator with an opportunity to develop a greater understanding of the industry and provide additional insights into emerging business and regulatory issues.

Topic 7: Cross-border Issues

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.

While the substance of regulation across jurisdictions with advanced financial markets is sufficiently similar to deliver broad regulatory equivalence, there are both obvious and subtle differences in approach. Thus, entities that operate across several jurisdictions must adhere to laws, regulations and rules that vary across those jurisdictions, which heightens compliance risk (in the broad sense as discussed above). In addition, the type of business conducted in each location may vary; for example, many foreign banks in Australia limit their business to the wholesale markets, though they have a strong retail presence in their home jurisdiction.

This requires flexibility within the broad mantle of the entity's global compliance function to accommodate local conditions. This is generally achieved by maintaining a local compliance presence, within the overarching global compliance framework.

National regulators should recognise overseas regulatory regimes that have sufficient regulatory equivalence to their own and promote the alignment of international regulatory standards to enhance the degree of comparability in regulation across jurisdictions. This would provide a framework within which cross-border compliance risk could be reduced. In this context, IOSCO's regulatory guidance through its international principles and standards has a significant influence on the approach taken by regulators. Together with the Basle Committee and the Joint Forum, this has the potential to improve the consistency of international securities regulation over time. Moreover, IOSCO's recent commitment to a regular consultation process is welcome.

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?

Some entities that operate a global business have adopted a compliance model with a centralised compliance function (within a region and/or globally) that administers the entity's global compliance procedures and policies. The local operation in a jurisdiction will satisfy the local law, but it may also satisfy additional compliance controls that apply to the global operations.

In our experience, the operations of foreign-owned banks in Australia have a significant local compliance presence. This includes senior compliance officers, responsible for advice, interpretation and administration of, and reporting on, Australian law and regulations, amongst other things. In practice, this is necessary to provide the necessary support to sizeable local operations and to keep abreast with the pace of regulatory change. Practical complications can arise for local compliance functions within a global organisation. For instance, the local compliance function may have limited influence over global resource allocations and related matters (eg salaries) for compliance. This requires consideration of the responsibility given to the function and the authority accorded it, so the right balance is achieved.

Domestic banks with overseas operations have similarly committed significant resources to meeting regulatory obligations in the overseas jurisdiction that they operate in.

In financial markets that are becoming increasingly globally integrated, compliance officers with an international exposure play a valuable role in identifying best practise in approaches to compliance and regulation and through our dialogue with regulators, help to improve the quality of the regulatory system.

****

Response to the IOSCO Consultation:
Compliance Function at Market Intermediaries

International Financial Data Services Limited ("IFDS") performs outsourced administration (dealing and registration functions) for approximately 30% of the UK collective investment funds market. While various tasks are therefore performed in the name of our various Management Company clients IFDS is itself an authorised firm regulated by the UK Financial Services Authority.

In the UK IFDS has over 1,400 staff and has recently commenced offshore operations based in India.

We read with interest the IOSCO consultation paper considering the role and independence of the Compliance function and wish to offer the following comments, based on our experience of operating within the FSA's regulatory environment.

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

In our view the Compliance function of a financial services firm is the area with direct responsibility to that firm to provide information to the firm as a whole in order to maintain compliant processes and procedures within that firm. It is therefore more accurately to be described as a Compliance oversight function (and throughout our response any references to the Compliance function should be understood to relate to the function of Compliance oversight). In different jurisdictions the exact nature of such compliance oversight will therefore differ, as it will according to the scale and diversification of a firm's activities, as the core requirements considered by the Compliance function must be the local regulations.

The Compliance function should ensure that necessary tasks, activities, and controls are not simply done, but *seen* to be done. To this end the Compliance function itself might perform only a small number of actual tasks, each focussed on oversight tasks to ensure that Business Operations are being run in a demonstrably compliance manner.

Where the accurate processing of transaction data is a core risk for a firm in evidencing that it complies with local regulations there is a clear need for the quality of work to be objectively assessed and the processes monitored. However, it is not necessarily the case that such monitoring must entirely be performed by the Compliance function. Quality assessment teams within the operational business areas concerned are in some cases better equipped to perform the high-volume sample-tests required by key exposures. As a firm's operations expand, so does the need for detailed knowledge in a variety of fields. By localising the detailed operational knowledge in quality control teams the Compliance function's role becomes more focussed, and the central theme of oversight becomes more visible:

- To ensure that the quality teams are each performing adequate review; and
- Assisting the business areas in procedural changes to ensure that all processes remain in line with evolving regulatory requirements.

The need for independence is key to any compliance function – whether itself monitoring the core processes or reviewing and analysing the peer reviews performed within operational areas. Such independence should cover management accountability (with its subsequent application to promotion and remuneration) and reporting lines, as compliance staff must be assured that a conscientious and diligent performance of their duties will not be detrimental to their career development.

For this reason (and others) the seniority of the Compliance Officer is vital. The Compliance Officer should have budgetary control (in order to ensure control over resources and remuneration), and also be a member of the Board (and accountable only to the Board rather than to operational colleagues).

We therefore generally consider the principles set out in the consultation paper to reflect this need for flexibility, but consider the consultation paper's definition and description of the compliance function should

be enhanced to better reflect the focus on overseeing the operational business units to ensure their operations are compliant.

2 What is the relationship between the compliance function and risk management function?

Risk as a discipline continues to evolve and we consider that the implementation of risk management processes within a firm can be considered as unique to the nature, experience, and extent of that firm. While there is an overlap between the spheres of interest for the risk and compliance – both seeking to provide oversight, consultancy, and advice functionality to support the business areas – it seems impossible to rule which function would more correctly be viewed as a sub-set of the other. Both duties live outside the Operational arena, serving the firm by ensuring the ongoing permission to carry out regulated business. As such a number of firms will choose to combine the two functions. However, we do not consider there is any benefit to the industry by requiring the duties be combined or by recommending that such a position be taken across a full jurisdiction.

The question continued to ask how the two areas would interact when dealing with compliance issues. Our thinking is that the risk management area is focussed on mitigation of risks: considering the impact on a firm where a particular action is not performed, and what mitigants are available to ensure that any issues that do arise do not grow in significance or impact. The Compliance area by comparison (and as noted above) is concerned with whether the firm's procedures are compliant with the regulations, and in ensuring that those procedures are then followed. In essence, Compliance oversight ensures that a firm's standard business procedures will comply with regulations when they are performed, and also monitors that performance to ensure the procedures are being followed; Risk provides the "What if…?" analysis to ensure that the firm can manage the impact where a standard procedure cannot be performed for any reason.

While Compliance oversight is largely perceived as 'reflective', with Risk primarily viewed as 'projective', we would suggest that in the way in which oversight duties are performed both functions provide a blend of reflective and projective measures. Compliance will reflect on monitoring results, while the Technical Compliance area will project the likely impact of regulatory changes. Risk will project the potential impacts arising from various events or exposures taken, but can only truly do so having reflected on historic data and changes in the surrounding environment.

Both functions exist to support the business areas in meeting the applicable requirements, and provide reassurance to stakeholders (both internal to the company and those outside). On occasion each function will have input to offer the other, but we do not consider that any specific approach can be proposed to apply to all firms in all circumstances.

3 Should a specific organisational structure for compliance be prescribed?

We do not consider such a step should be taken. The industry continues to move from prescriptive regulation towards principle-based regulation, where a firm is required to assess its own position and implement requirements based on that assessment in order to demonstrate compliance.

It is not possible to prescribe a single model to exist in all firms – particularly due to the great differences in the sizes of firms. Any prescribed solution would require a step-approach (one model intended for small firms, changing the structure as a firm grows) – but such an approach would present a barrier to growth for a successful firm, where the firm's development would require a restructuring of its Compliance function. We would also be concerned that such a restructuring of the firm's independent Compliance function would occur at a time of increased need for monitoring and oversight. The Compliance reorganisation required by the business expansion would itself reduce the Compliance function's ability to monitor the very increase of activity for which it was restructured.

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

We consider the key roles to be Compliance Officer and Money Laundering Reporting Officer. These are the roles that we consider should retain accountability to the regulator. As noted above the Compliance Officer should have Board responsibility for the Compliance oversight function. In order that the firm's Compliance function is itself accountable it is appropriate for the head of that function to be directly accountable to the regulator as well as to the firm's board.

The firm should appoint a person with overall responsibility for protecting its interests in relation to money laundering regulations. Such a person, known within the UK industry as the "Money Laundering Reporting Officer", is the firm's central point of contact for law enforcement and regulatory issues relating to financial crime. As such we consider it appropriate for this person to be directly accountable to the regulator.

We consider that the underlying activities of a Compliance function are all focussed on bringing the firm to the position where the Compliance Officer and MLRO respectively can demonstrate to the regulator that the firm as a whole (and its business areas in particular) is compliant with the applicable regulations.

We recognise that the role of 'Risk Director' should be considered. We have acknowledged above the potential overlaps in this area and so would caution against a prescriptive proposal. The firm's Board should ensure that Risk can been identified, assessed, and mitigated – even if no director has been appointed with such a specific sole focus. We note that within the UK environment each member of the Board is accountable to the regulator, and that the regulatory principles applying to a firm include the responsibilities of all persons who control the key functions of the firm (such as directors in general and those with specific areas of responsibility, such as Finance or the Chief Executive).

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

The chief additional duty carried out within the Compliance oversight function of IFDS is responsibility for the prevention of money laundering and other financial crime. The Compliance Officer is also appointed as Money Laundering Reporting Officer ("MLRO"), with a senior compliance manager acting as Deputy MLRO and certain members of the compliance team specifically working on the investigation and resolution of suspicious activity reports ("SARs") raised by the operational areas.

The MLRO function within Compliance takes a key role in assessing changes to the Guidance Notes issued by the UK's Joint Money Laundering Steering Group ("JMLSG") and holding meetings with business areas to assess the procedural changes that may be required. It also works with the business areas to assess any changes to processes arising from SAR work – both changes to operational processes and to the communication requirements and channels to be used for investigations.

Within IFDS the risk function is contained within the Compliance area, as is responsibility for business contingency planning.

In both respects the Compliance function again serves an oversight purpose, with the operational business areas having the responsibility for ensuring that business processes are in line with regulatory requirements.

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

This matter will be subject to the structure of a given firm – specifically how closely the firm has aligned the compliance and risk functions. The compliance function would need to liaise with the risk function 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 – particularly where the local regulator has based regulatory requirements around the work of risk management.

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

We consider the regulatory requirements must be both appropriate and proportionate. The extent of business activity (along the axes of both size and diversification) must be considered when a firm documents its policies and procedures. By establishing principle-based regulations the regulator can ensure that smaller, less complex, intermediaries are not subject to an onerous regulatory burden but are subject to appropriate requirements to ensure the necessary protection for that firm's clients and other market intermediaries.

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.

Our Compliance Officer is a member of the Board, and is subject to the FSA's regulations for "Approved Persons" and "Controlled Functions" (including those with "significant influence"). All Board members are subject to these regulations, though the role of 'Compliance Oversight' is individually specified (in the same way that the roles of Chief Executive Officer and Non-Executive Director are specified in the regulations) to reflect primary responsibility for maintaining the compliance function.

The Board is responsible for ensuring that the firm operates in an appropriate manner and so oversees the work of the Compliance function (each board meeting receives a report from the Compliance function detailing the current key work areas and issues arising from regulatory changes).

Senior management has responsibility for ensuring that procedures used in their area are current and complete. The Compliance function is available as a resource to review any changes or to comment upon changes to the regulations applicable to a given task. Senior management is also responsible for ensuring that actions identified during monitoring reviews are taken, as a means of restoring ongoing compliance.

Business unit personnel are responsible for carrying out their duties in line with these procedures, but are also encouraged to consider the wider implications of their roles – particularly in respect of financial crime prevention.

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

We consider this distinction to be necessary – though each aspect must be recognisable for each level within the firm.

All jobs have a job description, specifying the nature of the role (the responsibilities of the role). Each appointee is responsible for carrying out his duties in line with this job description. At each level within the company these responsibilities are overseen by the person (or group) to whom the person is accountable. This might be their direct superior; administrator to supervisor; supervisor to manager; manager to director; director to Board.

Where a member of the company does not meet their responsibilities they must expect a consequence. This liability might come in various manners, and its extent will be dependent upon the nature of responsibility concerned. A lower-level member of the company might receive an unfavourable regular assessment (with impact upon their next salary increase) or, for a more serious matter, a disciplinary warning. More senior staff may find that the failure to satisfy a responsibility removes their ability to be appointed to a particular role – i.e. the liability of demotion where they do not satisfy a "training & competence" or "approved person" requirement.

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

We consider this to be necessary. We further maintain that the need for the Compliance oversight function to be independent requires that this senior officer be a Director and thus a member of the firm's board. While all members of staff have job description detailing their responsibility to perform allotted tasks, the need to ensure that all those activities build together to form a compliant whole (and the need to independently verify that fact) necessitates in our opinion that a director be appointed as Compliance Officer. The Compliance Officer is accountable to the Board for the activities of the Compliance function and ensuring that day-to-day responsibilities are satisfied.

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

We consider it important that the focus must be **independence** and not *isolation*. In a small firm it is understandable that staff performing the compliance function are not set aside wholly to that activity. There is clearly a risk to the scope of monitoring activities where the monitors perform the business tasks being monitored – but that should not automatically preclude a member of staff serving in one operational area for part of their contracted hours from performing compliance oversight of some other operational area during the remainder of their contractual hours. This comment should not be read as undermining the value of a high-percentage 'quality checking' task within an operational area in order to ensure that transactions are processed correctly; only that the broader aspect required from a compliance monitoring function requires separation from the actual activity being assessed.

We consider that a principle-based framework (rather than a prescriptive requirement) should enable the small firm to implement the necessary controls and separation of duties to create an independent compliance function. We consider the main requirements of such a framework to be:

- Resource / budget: the budget for compliance tasks should be determined and specified at a senior level of the company, and not reduced due to operational shortage;
- Staffing: the staff used to fulfil compliance roles should be identifiable within the firm (responsibility), with job descriptions clarifying the nature and extent of their compliance responsibilities. This enables the firm to ensure that the resource budgeted for compliance is being provided;
- Independence of monitoring: the staff performing compliance activities should have sufficient knowledge of an area to properly understand the tasks being performed and the issues faced – but should not themselves be active within the firm in performing either the task being monitored or any

task adjacent in the process chain (either directly contributing to the process or receiving the output form the process). While the detailed perspective that comes from close connection with a given task has value for a process review / best practice project, the need for compliance tasks to be objective and independent requires that the monitoring programme not become a political arena enabling staff to criticise or punish those who affect other aspects of their own work. While a firm would presumably have procedures to prevent such actions we consider it appropriate for the potential issue not to occur.

We recognise however that in a very small and focussed firm all staff might be excluded from monitoring certain tasks if this approach were implemented. This might require the firm to use external resource or indeed to establish a compliance resource outwith the business operations of the firm.

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?

As noted above, we consider that such direct and detailed knowledge of a process is advantageous for quality control checks, best process reviews, etc. but not necessary for compliance monitoring activity. Compliance activities require objectivity and impartiality to assess actions and consider the findings that arise from those assessments, which can be undermined by a politically charged environment. While we acknowledge that a firm would be able to implement behavioural expectations and parameters over the use and application of monitoring findings, we consider that the firm is best served where not only is a member of staff prohibited from monitoring the business activities that they perform themselves, but also prohibited from any directly adjacent task in the process chain.

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

Before directly addressing this question we consider it necessary to comment on statement (c) from page 18 of the consultation. We consider that the means as currently drafted risks excessive inconvenience to the board. We suggest that this item be redrafted to clarify that *certain* senior compliance personnel should have access to the board of directors and senior management to discuss significant compliance matters. We consider this change is necessary to ensure that the firm's senior management is not subject to premature issues.

That said, we generally consider the means stated in the consultation to be sufficient – though as noted in our earlier answers we consider that means (d) could be enhanced by prohibiting staff from performing monitoring on any task adjacent to their own in the process chain of the firm.

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

Salaries for compliance staff are established with reference to market information and are not tied to any sort of 'commission'. Performance is used to guide annual pay increases, but the "Performance and Development Review" process used to make that assessment is broad and applied in all areas of the firm.

Bonus payments are made along the same basis as in operational areas: the head of the business unit is provided with a budget, reflecting the relative seniority of staff in that area, and the money is allocated according to overall performance assessments. The position for staff in general is that where the company as a whole does well staff are rewarded. Where an individual within a department performs at a higher level against others in the same role, he would receive a greater reward.

15 What are the appropriate qualifications for compliance personnel?

Any mandatory application of qualifications to compliance staff should reflect the distinction between senior compliance staff (such as those individually registered with the regulator) and other members of the compliance function.

The underlying requirement for qualifications should be the ability to demonstrate competence to act – a driver's licence is intended to show that a person has received the necessary training and been deemed competent to drive a vehicle. Competence is a function of knowledge and experience and so no qualification can ever, by itself, demonstrate competence.

Further, the need to demonstrate knowledge need not require a prescribed examination. Many professions – even those with examination requirements – use a structure of Continual Professional Development ("CPD") to enable their members to demonstrate an ongoing commitment to their personal competence in a changing working environment.

The need to ensure consistency within a market (while also aiding the fluidity of the labour market) suggests that a standard qualification structure can be beneficial. Within the UK industry the FSA's training and competence requirements ("T&C") have for many years required staff with day-to-day decision-making responsibilities to demonstrate competence. The Investment Administration Qualification of the Securities and Investments Institute was specified as the approved examination, though this qualification is modular and so grants scope to individuals to select certain modules to both gain the qualification and satisfy the regulator. More recently the FSA has amended the requirement so that other qualifications can be accepted as evidence towards the wider issue of competence.

It does seem appropriate that any member of compliance charged with monitoring the decisions taken in an operational area should have the level of overall knowledge that would be required to work in that area (though not necessarily the detailed system knowledge of performing the task in a given firm). This should ensure a mutual respect around monitoring work, as well as an appreciation of the issues concerned with a given task.

However, other compliance functions go beyond monitoring tasks. In larger firms some posts more closely resemble legal operations (assessing the impact of consultation, drafting a response, acting as a reference point to advise on the regulatory implications of decisions being taken within the business). Traditional legal qualifications would not seem to be a necessity – especially given the implication on remuneration budgets arising from such qualifications – though it must be noted that various senior compliance staff within the industry do currently have a legal background.

It must be recognised that Compliance itself is still a relatively young specialism in the industry. Compliance has emerged from a history linked to the legal office of various firms (arising, as it does, from the legal and regulatory obligations imposed on a firm) and so there is no widespread senior-level qualification similar to a law degree. However, certain universities have now formed Masters degree courses in Regulatory Compliance or Financial Regulation. While such courses could be useful in gaining a breadth of experience beyond a person's own firm the number of places available for such courses would make it unsuitable as a prerequisite for holding a compliance post.

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

As noted in our answer above, we consider "competence" rather than "qualification" to be the issue. A qualification can be applied or not (consider a qualified lawyer now working in a compliance role – much of the knowledge used to gain the qualification is rarely, if ever, called upon), but competence must be assessed directly against the current job specification. As such the measurement of competence must remain relevant to the current role, requiring a different form of evidence as seniority increases. It seems appropriate that the more senior a person is (the greater their responsibilities within a firm) the higher their qualification should be – in order to enable them to fully grasp the liabilities that arise from their increased responsibility.

However, in the lack of any specific documented market failure it would seem excessive to impose a mandatory qualification on the industry. Firms, however, should remain free to define the required or preferred items on the job specifications of their senior managers.

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

Evaluation of training necessitates some form of measurement or assessment. Gaining a qualification such as the IAQ demonstrates that the person has acquired the necessary knowledge to pass the given examination. Firms would be able to define similar tests for other courses or training provided to its compliance staff.

However, we recognise the value of the FSA's two-fold approach to competence. In addition to qualifications (knowledge) a member of staff must be deemed to have the necessary experience before being recorded as "competent". Progress towards this experience requirement is recorded in appraisals and is useful in staff development. This supports our overall view that we are not focussed on evaluating the adequacy of courses so much evaluating whether staff are and remain competent to fulfil their duties.

We note also that the UK Financial Services Skills Council has recently published material seeking to establish standards for staff in Compliance and Anti Money Laundering positions. Again we consider a focus on standards rather than simply examinations (demonstrating knowledge at a given point in time) as being key.

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

The vast majority of financial firms are at some stage during a year subject to review by an external body. Fund managers are subject to audits and testing by trustee/depositary firms; third party administrators are also audited by their clients; and in many firms the required financial audit is accompanied by a SAS70 or FRAG21 review of processes and controls. Add to this the visits and testing performed by the regulator and it can be seen that any financial firm is subject to regular independent monitoring.

The question becomes whether such external review is necessary to assess the effectiveness of the compliance function, and indeed whether it does assess that effectiveness. There has to come a point where a firm stops monitoring its own activities, and having any internal party monitor compliance would lead to the monitoring being monitored. We would argue that the Compliance Officer's accountability to the board is the final stage of being monitored. The Compliance Officer's reports to the board enables the board to consider whether it considers the compliance function is operating effectively. The UK Approved Persons regulations ensure that each board member is accountable to the regulator for meeting the requirements of their role, preventing their being any interest in suppressing deficiencies identified within such monitoring reports.

From the external perspective – and particularly from IFDS's position as TPA for multiple outsourcing management companies – there may be an increasing need for compliance to be assessed by an external expert party. In the years following an outsourcing decision a fund management firm's collective skill and experience of the tasks now outsourced will decrease. In order that monitoring remains comprehensive there is an argument to clearly permit firms that have outsourced activities to use the services of a professional firm to perform compliance monitoring of the TPA on its behalf.

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

Again, different firms will seek different degrees of examination from external parties. Some firms will seek detailed assessments of all controls within the business, such as an SAS70 or FRAG21 that would feature all controls in all areas. Other firms would take sufficient comfort from reviews performed by the fund manager / trustee/depositary / delegating firm / etc. – reviews performed to enable those firms to evidence appropriate diligence in relation to tasks being undertaken.

As noted above, for fund managers that have delegated activities there may be an increasing requirement over time to retain the services of a professional firm or "Skilled Person" to provide knowledgeable assessment of compliance in relation to delegated tasks.

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

The most significant concern of requiring review by an external party is cost. It is expensive to retain the services of an external body to perform assessment of the compliance function, and the benefit received where no regulatory requirement exists is unclear – particularly where there is use of internal compliance monitoring.

In the absence of any clear market failure in this regard it would seem unreasonable for regulators to impose such a cost burden on firms, given the existing monitoring regime that affects so many firms in a variety of ways.

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

We support the use of a risk-based approach to monitoring – both in terms of internal review and external monitoring. The frequency with which any given activity is assessed should be determined in relation to the associated risk of error, itself reflecting the nature of findings previously identified and investigated.

We would note that sample sizes should be determined along sound statistical lines. Reduced frequency does not correlate with reduced sample sizes where to do so would undermine the statistical significance or reliability of the findings.

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

In the first instance we support the use of statistical sampling checks against a defined test matrix. This ensures that a consistent monitoring approach is applied to all items within a single test area – both during a given review but also between one review and the next.

Where the statistical sample test suggests that a problem exists it might be appropriate simply to record the finding and require the business area concerned to respond to the perceived deficiency (providing the steps to be taken to improve the situation, etc.). However, in a more serious case we adopt the use of focussed process reviews to increase the sample size and focus on those parts of the wider process that seem more susceptible to failure. These reviews, while more costly in terms of resource consumption, can be very useful to the business area in providing additional understanding of a problem. The provision of additional support from Compliance in amending the processes to resolve the issue is also generally appreciated.

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

We suggest that the extent of compliance culture can be considered in relation to three categories: people, procedures, and systems. These apply in different ways throughout the organisational structure of administrator / supervisor / management / board. For the organisation to have a strong compliance culture the principles of compliance should be evidenced at every level of the structure – permeating the company and reinforcing the understanding that the role of the Compliance function is oversight of the compliance of respective operational business units.

To consider people first: Within the UK framework the FSA regulations set useful parameters on the knowledge of staff at various levels of the corporate hierarchy. Training and Competence requirements apply

to “overseers” (supervisory grades), while Senior Management and Directors are subject to the Approved Persons and Controlled Functions requirements. These provide a benchmark for knowledge at various levels, and a company would demonstrate a strong compliance culture where these regulatory minimums are exceeded (i.e. administration staff encouraged to study for qualifications above their current grade; board members exceeding any regulatory minimums for being an approved person).

In terms of procedures, the evidence of well-maintained, comprehensive procedure manuals is strong. Such documents represent an investment of time in establishing the manual, and an active reflection on working practices over time. At a higher level of the organisation the Corporate Governance Manual and Corporate Business Contingency Plan indicate that such documents are recognised valuable.

System issues tend to concern “the way things are done” rather than simply the use of information technology. Does the operational area set up a new process without considering the compliance perspective of the new product/service? Are members of staff from the Operational and Compliance functions able to hold positive discussions, recognising each other’s value to the organisation, or has resentment grown up between the departments?

The findings of monitoring work, and the response of the relevant areas to those findings, are also indicators of the strength of compliance culture within a firm.

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

The consultation is focussed on direct examination, and so fails to consider the ability of regulators to use indirect means to inform their monitoring activities (bringing an overall reduction in the costs of monitoring by better focussing its efforts on key areas affecting a given firm). Within the UK the FSA has reassessed its information reporting requirements in order to obtain information and data that it will use to build up an understanding of the business being transacted.

Within the UK this includes data from fund management firms being used to inform the monitoring of brokers and advisors. While such an approach is clearly beneficial to the regulator it is unfortunate that it did not seem to compensate the firms bearing the costs of data manipulation and reporting in order to bring economies and improvements to a different market sector.

We would again comment that, in the absence of any specific market failure we do not consider it appropriate to add further to the existing costs on firms from monitoring activities (either by internal or external means – including regulatory supervision which is paid for by the industry via fee tariffs).

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.

The key issues are knowledge of the detailed rules of each jurisdiction, together with clear documentation relating the distinct regulatory requirements to the tasks being undertaken for the respective jurisdictions.

This impact is, of course, reduced by ensuring that a local compliance presence exists within each jurisdiction. The impact is increased where a single office / location is made responsible for the compliance of an operation based in or under the rules of a different jurisdiction.

Within the EU itself all jurisdictions are subject to the same Directives – but implementation differs between Member States. When a firm operates in jurisdictions other than the EU the scale of divergence increases. Unique requirements (such as the US Patriot Act or Sarbanes-Oxley) must be assessed as a firm plans to enter a particular jurisdiction.

Some might argue that this is a reason for moving towards an internationally agreed set of standards – or even a centralised, detailed EU Financial Regulation Rulebook – though we view that approach with caution. The

investment industry is one that thrives on distinctiveness and we consider the role of regulation to be enabling such distinctiveness, within broad principles, rather than forcing uniformity. To attempt to require all regulators to apply a single model would cause significant issues without necessarily adding value. The FSA recently took on regulatory responsibility for the UK insurance market, with the inevitable impact upon its resources and focus, but was not required to fit its approach to an inflexible internationally-agreed model.

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 centralised compliance function.

Our firm operates in a small number of jurisdictions, but does so using a localised resource to ensure compliance. This localised resource is, in each case, appropriate to the requirements of the local jurisdiction: in the UK an FSA-registered Compliance Officer; in Luxembourg an Internal Auditor has local responsibility for Compliance. However, as IFDS offices are not 'branches' there is very little overlap in the Compliance oversight duties across sites.

The UK operation does provide occasional additional resource to Luxembourg to assist with monitoring activities, but essentially each jurisdiction is resourced to fulfil its own obligations.

THE INVESTMENT FUNDS INSTITUTE OF CANADA
L'INSTITUT DES FONDS D'INVESTISSEMENT DU CANADA
151 YONGE ST., 5TH FLOOR, TORONTO, ONTARIO, M5C 2W7 TEL 416 363-2158 FAX 416 861-9937

By Mail & E-mail: mail@oicv.iosco.org

July 14, 2005

IOSCO Secretary General
Oquendo 12
28006 Madrid
Spain
Attn: Mr. Philippe Richard

Dear Sirs/Mesdames:

Re: IFIC Comment on *Compliance Function at Market Intermediaries*

We are pleased to provide the comments of The Investment Funds Institute of Canada ("IFIC") and its Members with respect to the *Compliance Function at Market Intermediaries* Consultation Report published for comment in April 2005 by the Technical Committee of the International Organization of Securities Commissions ("IOSCO").

Founded in 1962, IFIC is the industry association of the Canadian investment funds industry. IFIC membership includes investment fund managers and dealers managing over $520 billion in assets on behalf of Canadian investors, and service providers to such firms.

We endorse IOSCO's initiative to identify and discuss principles that should be considered by financial market intermediaries when establishing compliance regimes. A compliance regime that enables appropriate compliance with securities laws is part of the essential foundation of a fair and orderly capital market that promotes investor protection.

We commend IOSCO for reviewing the compliance initiatives of different regulators who share a common belief that the compliance function at financial market intermediaries plays a crucial role in preventing misconduct, promoting ethical behavior and protecting investors. Financial intermediaries and the markets that they serve will no doubt benefit from an understanding of international practices and experiences in compliance matters.

***

We thank you for this opportunity to comment on IOSCO's *Compliance Function at Market Intermediaries* Consultation Report, and look forward to IOSCO's Final Report in this matter. Please contact the undersigned at (416) 363-2150 x 225 / jmurray@ific.ca or Stacey Shein, Legal Counsel, Regulation at (416) 363-2150 x 238 / sshein@ific.ca should you have any questions.

Yours truly,

THE INVESTMENT FUNDS INSTITUTE OF CANADA

"Original signed by John W. Murray"

John W. Murray
Vice President, Regulation & Corporate Affairs

INVESTMENT MANAGEMENT ASSOCIATION OF SINGAPORE

10 Collyer Quay
#19-08 Ocean Building
Singapore 049315
Telephone: 65 6230-9513
Facsimile: 65 6536-1360

Investment Management Association of Singapore

Singapore industry comments on

IOSCO Consultation Paper on "Compliance Function at Market Intermediaries"

13th July 2005

Andrew Kwek
Executive Director
Investment Management Association of Singapore
Tel: 65 6230 9717
Email: andrew_kwek@imas.org.sg
www.imas.org.sg

Dear Sirs

IMAS thanks IOSCO for the opportunity to respond to the IOSCO Consultation Paper on Compliance. Our comments are as follows (the number order follows the order of questions in the consultation paper) :

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

The scope should include understanding 'best practices" in terms of Compliance policies and hence, compliance with 'best practices'. It should not be restricted to regulatory compliance, instead, include investment compliance and compliance with internal procedures. A compliance function should also engage in the identification and prevention of violations of these securities regulatory requirements and that this could involve compliance input when the new business lines are considered so that any potential requirements or compliance concerns posed by the new business lines are highlighted early on.

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?**

Both functions are closely related and are co-related. Risk management is indeed the more generic term and Compliance risk is but one of several risks (e.g market, investment, legal, operations, reputational etc) faced by a market intermediary. Compliance related issues are more specific and should be handled by a Compliance professional. Inevitably, because of the monitoring role performed by Compliance in order to provide management with the comfort that the system of internal controls implemented is operating effectively, it therefore means that there is an overlap between the Compliance and the Risk function.

There should be communication lines between the two functions to identify potential risks, report breaches, detail rectification action taken etc.

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

No, as each company is different in terms of size, staffing, structure etc. It is perhaps better to follow NYSE's rules i.e ensure that management implements proper company wide structure and internal controls ; and have Compliance acting as an independent and on-going check on the status of controls. The Compliance function should be given the full support of management. The function itself should be determined by senior management having regard to the nature of the business, its size and scope.

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

The regulators should mandate that the Compliance function be given full support, expressly, and perhaps on an annual basis, by the Board of Directors or senior management. Suggest that the regulators mandate the set up of ' Compliance & Risk ' or ' Compliance Committees ' and the participants of such committees. Re-emphasize that the management should actively promote and inculcate a good compliance culture within the market intermediary.

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

This would depend on the business, but examples could include investment compliance and compliance with internal procedures.

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

Compliance should be responsible for setting policies, communicating policies to staff and monitoring compliance with the same on an ongoing basis.

Managing Compliance risk is the responsibility of management and the respective heads of department. The Compliance function should be involved as advisors as early as practicable. The Compliance function should be seen as 'business partners' and not as 'show stoppers'.

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?**

Resources constraint in writing up the manuals and keeping them updated. The content should depend on the size and scope of the business, suitable to the market intermediary.

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.**

Each of the board of directors, senior management, designated compliance office and business unit personnel are each held accountable -

Board of Directors/Senior management - (a) to give the Compliance function the full support, (b) ensure that the function is appropriately staffed and (c) appropriately trained,

Business unit personnel - (a) to understand what compliance risks are and (b) to manage compliance risk within their respective units and to ensure that in doubt, the correct personnel are consulted.

Designated Compliance officer - (a) to ensure that there is a proper compliance monitoring process in place; (b) monitoring and advisory activities are reported to senior management and (c) ensure that the company is aware of applicable regulations / best practices.

The ultimate responsibility for ensuring compliance procedures are in place and for any breaches rests with the senior management/board.

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

Yes - responsibility & accountability go together. To be accountable, the person must be responsible and if the person is responsible, he must bear the liability if anything goes wrong.

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

Yes - so as to emphasize the importance of the role and to ensure that there is undivided attention on review and management of this risk by the company. This will depend on the size and scope of the business.

11. **What requirements relating to independence and ability to act are relevant to a small firm?**
Budget, and given that it is a small firm, the actual ability to implement the structure. The person must be given the authority to perform his duties, e.g. to make reasonable inquiry into any processes or procedures within the company without fear of negative consequences.

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?**

No, as there is a lack of objectivity. The regulators can require more frequent reviews by internal/external audit; regulatory inspections or more frequent contact between the company and the regulator.

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

Yes. A compliance officer should be allowed to operate in the knowledge that any action he/she takes in good faith which may have a negative effect on the firm's business or a particular individual will not be held against him/her. More generally firms should consider implementing a 'whistle blower' policy to protect anyone who speaks out in good faith against perceived failings of the firm or any of its individuals.

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

Independent review for consistency with market/industry rates. Compensation to be reviewed by independent directors.

15. **What are the appropriate qualifications for compliance professional?**

Minimum of tertiary education or professional qualification. Further requirements depends on seniority of position. Appropriate qualifications for compliance personnel may include individuals who are legally qualified or who have an accounting or financial background.

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

Yes. Qualifications may vary depending on the function performed. For compliance staff performing monitoring activities, an audit background may be appropriate, however for compliance staff performing a consultative role or those who conduct training for staff, a legal background may be more appropriate.

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

Difficult to evaluate but it should not be based on number of hours. The adequacy of courses and training for compliance personnel will be crucial in ensuring that compliance personnel receive continuing education and are kept up to date with changes in applicable rules and regulations. Courses and/or training seminar should be made available every time there are material changes in applicable rules and regulations and these should be conducted appropriately qualified individuals such as compliance professionals from the industry, legal practitioners or consultants who specialize in securities and regulatory compliance issues. It may be useful for an industry body to organize such courses or training for compliance professionals in the investment industry. Singapore is implementing a certification program - perhaps that may assist in determining this issue.

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

Regulators and internal auditors. Independence is key here and internal auditors should have excellent knowledge of the companies business to make such as assessment. Regulators are also suitable as they can compare and contrast with other industry players.

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

Consultants in highlighting best practices.

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

Cost, knowledge and expertise of the third parties; trade secrets shown to such third parties, potential disruption to the day-to-day business.

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

Dependent on the compliance culture and control environment of the company, under normal circumstances, an annual assessment should be sufficient.

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

If a risk based approach is adopted by the regulator, then a mix of methods would be appropriate - (a) periodic direct examination for a hands on feel of the company; (b) requiring the board of directors to provide periodic self assessment to the regulators - they can appoint internal and external auditors to include an audit of the compliance function and report accordingly (c) on going dialogue with management and (d) notification to the regulators on significant changes to the Compliance personnel in the companies.

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

Strong compliance culture - (a) strong management commitment; (b) staff awareness of the function and the rules in general (c) evidence of active involvement of Compliance within the company (d) sufficient resources (e) evidence of clear policies and procedures to identify, correct, and where necessary, impose punishment for breaches.

Weak compliance culture - (a) no evidence of Compliance involvement (b) management dismissive of compliance risks (c) lack of or low quality compliance resources

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

Embedment of regulatory compliance in the day-to-day operations and getting compliance's involvement in new initiatives.

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.**

Problems with understanding the local regulations in other jurisdictions. Some specific issues are : language; culture of the local jurisdiction and culture of the regulator on dealing with the market intermediaries; different paces and stages of development; different regulatory models and requirements of the compliance function; and staffing issues.

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?**

By appointing local compliance officers with a centralised compliance head to oversee and co-ordinate common issues across jurisdictions. In addition, by having regular contacts with local management, local legal counsel and local regulators (where acceptable to the local regulator).

July 15, 2005

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

Re: SRO Consultative Committee's Comments on IOSCOs Consultation Report: Compliance Function at Market Intermediaries

Dear Mr. Richard,

The SRO Consultative Committee (SROCC)[7] would like to thank you and your colleagues at IOSCO for the work that has gone into the Consultation Report *Compliance Function at Market Intermediaries* (Report). The Report highlights many of the critical issues that currently exist today and it raises some important issues that are worthy of further discussion. It is our hope that the discussion generated from the Report will bring greater clarity and focus on compliance issues. To assist you in your work we will provide some general comments and then provide you with responses to the specific questions you pose in the Report.[8]

General Comments and Concerns

The Report highlights many important industry issues however, clarification on a number of issues is required. First, a distinction needs to be made in the Report between the compliance department and the compliance function as a whole. The Report does not distinguish between the two concepts and it is important to make sure these concepts remain separate. The entire market intermediary has a compliance responsibility and the compliance department has responsibilities within that framework and must bring the issue of compliance to everyone's attention. The compliance department should not be seen as the custodian of all compliance issues but instead as having an advisory, monitoring and reporting role.

Second, clarification is required under topic one "Establishing a Compliance Function" which looks at the means for implementing compliance. Is the intention of section b(6) that market intermediaries are required to go beyond what is already required under their current rules or is the section aimed at those jurisdictions where no requirements exist?

Third, clarification is required on page 11 of the Report with respect to the discussion on reporting. It is unclear whether this is referring to the monitoring and reporting lines of communication or whether it is referring to the actual report that compliance departments produce and give to the Board of Directors or senior management.

It would also be advisable to have some additional discussion with respect to lines of reporting and communication within the market intermediary. Making sure that adequate reporting structures are in place is the cornerstone of an effective compliance system for all market intermediaries. Communication channels between compliance and the Board of Directors and senior management is important and such requirements need to be reviewed and assessed on a regular basis to ensure their effectiveness and adequacy.[9]

---

[7] The SROCC is comprised of 52 IOSCO affiliate members, representing securities and derivatives markets as well as other self-regulatory organizations in developed and emerging markets.

[8] The views expressed in this letter represent five members of the SROCC who provided feedback on the Report (Amman Stock Exchange, Investment Dealers Association of Canada, Mutual Fund Dealers Association of Canada, Stock Exchange of Thailand and Taiwan Futures Exchange). The Taiwan Futures Exchange did not have any specific responses to the questions posed in the Report but stated that the Report would assist market intermediaries in increasing effectiveness of their compliance function.

[9] For instance, IDA By-law 38 requires firms to appoint a Chief Compliance Officer (CCO) who is responsible to report to the Board on the status of compliance. The mandate of the CCO is to provide the Board with reasonable assurance that standards of the applicable self–regulatory organization are met. Such reporting is required at least annually, but more if necessary.

Questions Posed in Report

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

The SROCC generally agrees with the proposed definition and description of the "compliance function" as outlined in the Report which states:

> "A function that, on an on-going basis, identifies, assesses, advises on, monitors and reports on a market intermediary's compliance with securities regulatory requirements, including whether there are appropriate supervisory procedures in place."

However, clarification with respect to the following would be appreciated.

1. The last line of the definition states "whether there are appropriate supervisory procedures in place," and it is not clear if this refers to the compliance department ensuring there are adequate supervisors in place or overall supervision within the market intermediary?

2. Clarification is needed in terms of how the proposed description of the compliance function fits with the discussion of the purpose of the compliance function on page 9 of the Report. The Report states that the purpose of the function is to ensure market intermediaries comply with requirements. Ensuring these things is different then what is required under the proposed definition, which is to identify, assess, advise on, monitor on and report on compliance.

It should also be noted that reference is made to the fact that the compliance function should engage in the identification and prevention of violations of regulatory requirements. However, prevention is difficult in every case and as such it might be more appropriate to state that the compliance function should be directed at making sure that preventative controls are in place and that such controls are monitored and assessed on a regular basis. As such, it is suggested that an additional phrase could be included at the end of the definition which recommends that revisions to procedures be discussed as a way to help prevent future violations.[10]

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?

The SROCC agrees that the compliance function and risk management function are closely integrated. In the absence of compliance, risk increases for both the client and the market intermediary. It is important to make sure that there is a dialogue between the two functions as a total separation of the two could create a conflict and a weakness in the risk management function.[11]

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

The SROCC is not in favor of mandating a specific compliance structure, as market intermediaries are extremely diverse. However, each market intermediary should be required to clearly set out their organizational structure and that structure should be adequate for the nature of the business operation. For instance, market intermediaries can range from having thousands of employees to those with only a few employees. It would be difficult to mandate a one-size fits all approach to compliance and it is more appropriate to tailor each compliance structure to the specific business operation. As outlined in the Report,

[10] Suggested by the Stock Exchange of Thailand.
[11] The Stock Exchange of Thailand suggests that some independence is required.

there are numerous factors that must be considered in designing a compliance function including the nature, scale and complexity of the business and the risks undertaken.[12]

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

Members should be required to establish, maintain and enforce a supervisory system, but the way the system is structured should not be mandated. Terms and conditions of the compliance function should be outlined as well as who is responsible for what. There needs to be some guidance as to who can fill specific roles as well as a requirement that there should be periodic reporting especially when a deficiency is discovered.

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

In addition to the responsibilities described in the Report, the view has been expressed that the scope of the compliance function responsibilities should go beyond the supervisory role and have the authority to carry out its duties as well as have the power to take actions against any illegal practices or employees.[13]

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

The compliance function is to assist the market intermediary in identifying and managing compliance risk and reporting issues to the Board of Directors and senior management. Those responsible for compliance act as "gatekeepers" and this is key to investor protection and efficient capital markets. Both the Investment Dealers Association of Canada (IDA) and Mutual Fund Dealers Association of Canada (MFDA) are of the opinion that the overall responsibility for compliance rests with the market intermediary as a whole and the Board of Directors and senior management, who have the authority to make decisions, allocate resources and enforce compliance.

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?

Market intermediaries should provide as much detail as possible in their policies and procedures as required for their type of business regardless of size. It is possible that a smaller, less complex market intermediary might indeed have a less detailed policy, based on the nature of their business, but they should still provide as much detail as possible when putting together their policies and procedures. However, operational implementation of policies may need to be more flexible for smaller, less complex market intermediaries.

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.

Amman Stock Exchange (ASE) – The ASE is subject to the monitoring and supervision of the Jordan Securities Commission. The ASE Board of Directors is accountable to the General Assembly, the CEO is accountable to the Board of Directors, the senior management is accountable to the CEO and the Board, and the heads of departments and employees are accountable to the Deputy CEO.

[12] The Stock Exchange of Thailand states that whether or not a compliance structure should be prescribed depends on each country's culture and regulatory structure. Currently, most jurisdictions require the establishment of a compliance system but they do not mandate a specific approach.

[13] Amman Stock Exchange and Stock Exchange of Thailand.

Investment Dealers Association of Canada (IDA) - The IDA is subject to monitoring by the Canadian Securities Administrators. IDA By-law 38 sets out the accountability for compliance at Member firms. Under By-law 38.1 senior management is ultimately responsible to the self-regulatory organizations (SROs) for the conduct of the market intermediary and the supervision of its employees. The By-law specifically states that an Ultimate Designated Person (UDP) must be appointed and those that can hold the designation include: the Chief Executive Officer, the President, the Chief Operating Officer or the Chief Financial Officer. Depending on the structure of the firm there can be more then one UDP. The Chief Financial Officer and the Chief Executive Officer are responsible for financial compliance. An Alternate Designated Person (ADP) must also be appointed and they report to the UDP and are responsible for compliance. The ADP must ensure that the business is carried out in compliance with applicable by-laws, regulations, policies and forms. The ADP will also act as the Chief Compliance Officer (CCO). In this role the CCO shall monitor adherence to the policies and procedures to ensure that the compliance function is effective and shall report to the Board of Directors as necessary but at least annually on the status of compliance. The Board of Directors is responsible for reviewing the reports of the CCO and determining what actions need to be taken and to ensure that such actions are carried out in order to address any compliance deficiencies.

Mutual Fund Dealers Association of Canada (MFDA) – The MFDA is subject to monitoring by the Canadian Securities Administrators. The Board of Directors has the ultimate responsibility for establishing the compliance function and ensuring that any issues identified by the compliance officer are resolved. Senior management is responsible for managing the compliance function and is responsible for notifying the Board of compliance issues. The compliance officer has the day-to-day responsibilities for carrying out the compliance function, monitoring effectiveness and identifying issues to report. Business unit personnel is responsible for notifying or communicating with compliance where new business is proposed.

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

The Amman Stock Exchange and the Stock Exchange of Thailand indicated that they distinguish among the concepts while the IDA and MFDA agree that responsibility, accountability and liability are essentially the same idea. According to the Amman Stock Exchange responsibility is the task that the compliance function should perform, accountability refers to the compliance function being held accountable for tasks it assumed to do and liability is the obligation of the compliance function.

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

Most of those who responded agreed that a senior officer should be responsible for the day-to-day compliance responsibility, depending on the structure of the market intermediary.[14]

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

The responses received were mixed relating to independence for small firms. Some responded that in order to be effective compliance cannot be totally independent from the rest of the firm. In fact, small firms may have to be even less independent then large firms simply due to the size of the firm and therefore having an overlapping of roles and responsibilities. Other responses indicated that all requirements relating to independence are relevant to small firms because such requirements are independent of firm size. The views expressed indicated that there should be sufficient independence between the departments including independence between the business, senior management and sales department in order to ensure the compliance department can effectively perform its advisory role.

[14] The Stock Exchange of Thailand disagrees.

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?

Some Members of the SROCC agree that individuals who perform both business and compliance activities should not be able to supervise their own activities as this could create a conflict of interest.[15] Where possible a segregation of duties is preferable. However, in a small firm there may not be enough personnel to separate the functions, so guidelines should exist to separate functions to help eliminate potential conflicts.

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

Yes, the means appear to be sufficient (especially for large intermediaries).

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

Members of the SROCC all agree that compensation should not provide any incentives to reduce the effectiveness of compliance or be influenced by inappropriate considerations. The ASE requires that internal rules include terms and conditions of compliance personnel. The IDA does not regulate compensation but agrees that compensation should not be subject to undue influence.

15. What are the appropriate qualifications for compliance personnel?

Qualifications include: industry experience, educational requirements (including continuing education), a sound understanding of applicable laws and rules, analytical skills, integrity, a good questioning mind, good communication skills, discretion and tact as well as the capability to robustly challenge others in the organization on compliance issues.

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

A Majority of those who responded agreed that qualifications should vary depending on the functions, responsibility and seniority of the compliance personnel.[16]

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

There is a variety of ways that members of the SROCC evaluate the adequacy and training for compliance personnel. For instance, the Stock Exchange of Thailand requires the regulator or the auditors to evaluate the work results of compliance personnel. The Amman Stock Exchange requires continuous training each time a modification has been made to their rules. The IDA has an accreditation process whereby all types of educational programs including seminars and written and electronic courses may apply for accreditation to an accreditation provider. All courses are evaluated and a recommendation made as to whether the course should be accredited as qualifying towards compliance study or professional development study, and the hours of credit assigned to the course will also be determined.

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

Some members of the SROCC feel that external parties (regulator or auditor) are in the best position to assess the effectiveness of the compliance function as they are in a better position to assess any weaknesses and may be more objective and independent. However, some members feel that individuals within the market

[15] The Amman Stock Exchange does agree that individuals should be allowed to perform both business and compliance activities regardless of who performs the supervision.
[16] Amman Stock Exchange requires all compliance personnel to fulfill the stated qualifications.

intermediary are in the best position to assess the status of compliance if they are properly staffed, organized and work effectively as they are in the best position to know how their structure works.

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

Please see response to question 18 above.

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

The practical concerns could include: costs of having an external party conduct the review, expertise of the external party (should have adequate knowledge of rules being enforced as the risk exists that they may have regulatory knowledge but no operational knowledge of how the particular firm works) and conflicts of interests.[17]

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

Different requirements exist with respect to the scope and frequency of assessments. For instance, for external assessment of market intermediaries, the IDA uses a Joint Compliance Risk Trend Report (JCRTR) which is a risk based approached to compliance which starts with an analysis of major risk factors affecting the business operations of the Member. The model takes into account both the risk factors affecting the business operations and its ability to identify and mitigate these risks by establishing appropriate internal control procedures. A risk ranking of high, medium and low is then assigned to each Member based on an overall risk score. The risk ranking then determines the extent and frequency of compliance field reviews. The IDA recently endorsed a report of HM Treasury which states: *"The fundamental principle of risk assessment is that scarce resources should not be used to inspect or require data from businesses that are low-risk, either because the work they do is inherently safe, or because their systems for managing the regulatory risk are good."*[18] A firm could also be selected if numerous complaints have been received against the firm. Members can also be audited by the Securities Commissions who will review all major functional areas of the business. Likewise, the MFDA requires external assessments of the market intermediaries every two to three years. The ASE requires a yearly assessment.

With respect to internal assessment of the market intermediary, the ASE requires the internal party to make an assessment every three months whereas the Stock Exchange of Thailand does not have a set time requirement but bases the frequency of audits on the intermediaries past record, size, complexity and trading volume. The IDA and MFDA require a yearly assessment and more frequently if necessary.

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

Periodic audits and self-reporting are methods that can be used to monitor the effectiveness of the compliance system. With self-reporting it must be looked at in the context of how material something is.

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

<u>Strong Compliance Culture</u>
-small number of client complaints
-resources (to be able to implement new rules and regulations)
-direct reporting relationship (strong connection with senior management)
-management action that occurs independent of compliance

[17] Amman Stock Exchange states that the external party could be more reliable and more efficient than an internal party.
[18] <u>Reducing Administrative Burdens: Effective Inspection and Enforcement</u>, Philip Hampton, HM Treasury March 2005, p.27.

-proactive rather than reactive approach to compliance
-low number of compliance issues
-minor infractions
-few repeat cases

Weak Compliance Culture
-litigation and large number of client complaints
-high turn over in personnel
-high number of unresolved complaints
-penalties imposed
-relying on regulators to identify compliance deficiencies
-responding slowly to correct externally identified compliance deficiencies
-looking for rules rather than assessing what is the right thing to do

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

Having more control over service providers would be helpful and reporting all client complaints, civil claims, regulatory and criminal actions to regulators (not all jurisdictions currently require this).

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.

Issues that arise include: slight variation in securities rules in different jurisdictions, different expectations from the various regulators, different rules in various jurisdictions (not just with respect to securities laws ie: patriot act, privacy acts), auditors of the market intermediary not knowing the rules of other jurisdictions in sufficient detail or having means to investigate outside their jurisdiction and jurisdictional issues in the case of a conflict between an international investor and a global marker intermediary.

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?

Market intermediaries should adopt the highest standards in all jurisdictions to ensure compliance with regulatory requirements in all jurisdictions.

Once again, thank you for providing us with this opportunity to comment on the Report.

Sincerely,

SRO Consultative Committee

14 July 2005

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

Dear Mr. Richard

Compliance Function at Market Intermediaries

The IMA represents the UK-based investment management industry. Our Members include independent fund managers, the investment arms of retail banks, life insurers and investment banks, and the managers of occupational pension schemes. They are responsible for the management of about £2 trillion of funds (US$ 3.7 trillion, Euro 2.9 trillion) based in the UK, Europe and elsewhere, including authorised investment funds, institutional funds (e.g. pensions and life funds), private client accounts and a wide range of pooled investment vehicles. In particular, our Members represent 99% of funds under management in UK-authorised collective investment schemes, i.e. the UK equivalent to US mutual funds.

The IMA is pleased to comment on your Consultation Document on Compliance Function at Market Intermediaries and a number of detailed comments are laid out in the attached paper.

We would be very happy to discuss the points raised in our response if you would find this helpful.

Yours sincerely

James Irving, Senior Adviser - Regulation

cc: Dan Waters, Asset Management Sector Leader, UK Financial Services Authority.

IMA response to IOSCO Consultation Report on Compliance Function at Market Intermediaries

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

IMA response

IMA does not agree with IOSCO's definition and description, which fails to emphasise that prime responsibility for compliance with securities regulatory requirements rests with line management of the business areas concerned.

IMA supports the position taken by the EU Commission's Working Paper prepared by the European Securities Committee ("ESC") in its recently issued Draft Commission Document on "Organisational requirements and identification, management and disclosure of conflicts of interest by investment firms", which places responsibility for complying with European Directives with the overall investment firm rather than the compliance function. The Document further states that the firm should establish and maintain policies and arrangements aimed at ensuring effective compliance by the firm and its personnel. These policies and arrangements should identify and assess the risk of, and risks associated with, a failure by the firm to comply with its regulatory obligations and put in place adequate measures and procedures to minimise any such risk.

IMA believes that it is essential that business management remains accountable for the conduct of the firm for the sake of good governance, and supports IOSCO Principle 12.5 which states that "The management of a market intermediary should bear primary responsibility for ensuring the maintenance of appropriate standards of conduct and adherence to proper procedures by the whole firm". IMA is concerned that if senior line management believes that it can in some way hand responsibility for Compliance over to someone else, then this will not drive the delivery of a compliance culture, which IOSCO acknowledges as important, and which can only effectively be driven from the top.

The ESC paper goes on to state that an investment firm should maintain a permanent and effective compliance function, and, in contrast with the IOSCO paper, more narrowly defines that function's responsibilities to:

1) monitoring on an ongoing basis, the adequacy and effectiveness of:
- the measures and procedures put in place by the firm for ensuring compliance with relevant regulations and client mandates; and
- actions taken by the firm to address any deficiencies in its compliance with those regulations

2) advising and assisting persons responsible for carrying out investment services and activities on behalf of the firm, to promote compliance with the regulations

In line with the stance in the ESC paper, IMA suggests that the compliance function should have a responsibility for identifying relevant securities regulations, advising business management of the impact on their particular operations, identifying regulatory risks, and supporting and advising business management during the design of internal controls in respect of such regulatory risks. The compliance function will also undertake monitoring (or ensure that an internal audit function undertakes such monitoring) of a firm's activities, using a risk-based approach, to confirm, or otherwise, adherence to those policies and procedures designed by the firm to address securities regulatory requirements. As a consequence of this monitoring the compliance function will present a status report to business management, which may include details of regulatory breaches identified during the limited sampling of the particular monitoring review. In addition, the compliance function will have a central role in promoting a compliance and ethical culture.

Responsibility for prevention of breaches of regulations, and day-to-day identification of those instances when controls have been ineffective, lies with line management of the particular business area concerned.

IMA also disagrees with the suggestion that the compliance function will have a responsibility for managing legal risk or for having mechanisms to protect the firm from any liability arising from abuses committed by the firm's customers. These responsibilities are more appropriate for a legal department or business function. A firm may choose to site these two functions within the same department, but that should be a matter for the firm to decide and not a matter to be dictated by regulation.

Q2. 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?

IMA response

As compliance/regulatory risk is a specialist segment within overall business risk, focusing more on risk to clients than risk to the business, the compliance function usually forms a discrete unit, either within, or external to the risk management function. Whether or not the compliance function is located within the risk management function, there will be close liaison between the two units, with the compliance function providing expert/specialist input.

Q3. Should a specific organizational structure for compliance be prescribed? Please explain.

IMA response

A specific organisational structure for compliance should not be prescribed, as structures will necessarily vary depending upon the type, culture and size of the firms concerned. Some firms may find that a central compliance function is most effective whilst others find that smaller specialist units, embedded within different business areas, is more effective. Clearly it will be important that compliance functions within the disparate model liaise closely in order to ensure that common standards are maintained.

The test should be one of effectiveness of the function, not what specific organisational structure is adopted. However there are characteristics of the organisational structure that should be considered, including appropriate reporting lines, properly documented roles and accountability, rights of access to staff and records and so forth. We believe developing a list of such characteristics based on the ESC Document (mentioned above) and other extant standards (including IOSCO Standards) would be beneficial.

Q4. Are there any essential roles, responsibilities or activities for the compliance function that should be mandated or otherwise identified by regulators?

IMA response

In line with IMA's response to Q1 above, the prime responsibility for compliance with securities regulatory requirements rests with line management. The compliance function should, however, have a mandatory responsibility for identifying relevant securities regulations, advising business management of the impact on their particular operations, identifying regulatory risks, escalating compliance issues to management (and if this is to no avail, to an audit/compliance committee or independent directors) and supporting and advising business management during the design of internal controls in respect of such regulatory risks. In the event that law, or regulation, oblige the compliance function, or individuals within that function, to report, then those obligations should be followed.

Compliance input may be most effective if compliance personnel are included in strategic/business discussions and in teams carrying out projects with regulatory implications. It should, however, be recognised that the compliance function should have the ability to outsource aspects of the work, while retaining overall responsibility. An example would be using the assistance of an audit firm to help design control functions for client money, or the use of IT experts to assist in the design of computer systems to monitor personal trading.

The compliance function should also undertake monitoring (or ensure that an internal audit function undertakes such monitoring) of a firm's activities, using a risk-based approach, to confirm, or otherwise, adherence to those 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.

Q5. Please identify responsibilities other those described above that are carried out by the compliance function at market intermediaries.

IMA response

IMA believes that there is perhaps too much issue being made of the compliance function as it relates to intermediaries. Indeed, the core elements of compliance remain true across the financial services spectrum, although the nature of the activity and the specific regulatory environment will differ.

Compliance functions may have responsibility for periodic reporting to regulatory authorities, for collating business management comments in response to consultations by regulatory authorities, for dealing with customer complaints, and for providing regulatory training to business units. These duties are, however, provided by way of added value and do not constitute the prime responsibility of the compliance functions. For example, many firms will use a central training function to deliver compliance education or the finance department to file reports.

We note that compliance will often have responsibility for advising on and developing a firm's money laundering deterrence programme, and this may include responsibility for reporting suspicious transactions to the authorities. However, this should not be mandatory and should only be undertaken if sufficient expertise and resources are available within the Compliance department. Again, how firms choose to organise their money laundering deterrence vis-à-vis the Compliance function should be a matter for firms to decide and should not be dictated by regulation.

It is, therefore, terribly important that the exact scope of the role of the compliance function is agreed and documented. It should be the responsibility of senior management to ensure that all regulatory risks are addressed and the compliance function should not acquire responsibilities "by default" simply because no one else is carrying them out.

It is important, however, that where possible (and it may not always be so in smaller firms) Compliance is independent of the activities and functions which it has to advise and monitor.

Q6. How and when should the compliance function be responsible for managing compliance risk?

IMA response

Whilst the compliance function has a major contribution to make, it should not be responsible for managing compliance risk. As stated in responses to Q1 and Q4 above, this is the prime responsibility of business management. The compliance function with its roles of regulatory risk assessment, advice in respect of those identified risks, and independent monitoring is an important part of line management's toolkit for ensuring a compliant firm. Other parts of the toolkit might include a risk function, internal audit, external audit, in-house or external legal counsel, and the use of other specialists such as actuaries, computer programmers or credit analysts.

Q7. 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?

IMA response

Any firm, regardless of its size or the complexity of its business, needs to have documented policies and procedures, as an *aide memoire* for personnel carrying out their day-to-day duties and as a training guide for new staff to provide continuity of standards. The variation in the scale and complexity of firms' business will naturally translate into more or less detailed and voluminous procedural documentation. However, documentation for both complex and more straightforward businesses, should be sufficiently comprehensive as to provide process maps for all critical activities. It is also increasingly common to find that compliance and other external obligations are incorporated within a single set of operating or procedural manuals that are themselves calibrated in terms of detail to the complexity and size of the firm concerned.

The level of documentation at smaller, less complex firms should be assessed in terms of the risk that it represents to the investor and or the financial system.

Q8. 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.

IMA response

The ESC paper referred to in Q1 above, and which IMA supports, proposes that the compliance function should report directly to senior management and that compliance personnel should not be involved in performance of services or activities over which they have a compliance monitoring responsibility.

In the example described, business unit personnel would be primarily accountable for such a failure, with line responsibility passing up through senior management to the board of directors. The designated compliance officer would be accountable to the extent that he had failed to appropriately advise/support line management, or to monitor the compliance risk.

This supports the contention that responsibility for compliance should form part of the general management responsibility that managers have. The ability to deliver compliance for a specific area should be seen as a core competence of the manager of that area.

Q9. Do you distinguish among responsibility, accountability and liability? Please explain.

IMA response

One analysis would be as follows. Liability will often be based upon a strict legal test; responsibility is usually the function of an allocated role; and accountability a matter of fact based upon specific circumstances. Therefore, if a firm were to breach its client money rules, for example, the firm is liable to the client to make good any loss or damage, the board of the firm, and specifically the director responsible for the back office, is responsible for the failure. The individual who failed to carry out the necessary procedure, and his or her supervisor, are accountable (in that their failure explains the lack of compliance). However, it is also possible to describe each of these aspects as "responsibility", so IMA is unclear as to the merit of retaining such fine distinctions. What remains important is that senior line management, the governing body of the firm, is where the responsibility resides and where the authority to discharge that responsibility also resides.

Q10. Should a senior officer be designated for the day-to-day compliance responsibility? Please explain.

IMA response

Whilst a senior officer will be appointed to have overall responsibility for the effectiveness of the compliance function, as this is a support function this individual will not have overall responsibility for compliance of the investment firm itself. This overall compliance responsibility will rest with the chief executive/board of directors of the firm.

The senior officer responsible for the compliance function will, however, be in a position to give a voice to, and promote, good compliance.

Q11. What requirements relating to independence and ability to act are relevant to a small firm?

IMA response

True independence of the compliance function in a smaller firm will almost certainly involve higher costs. It may not be possible in small firms to have a compliance function which does not carry out some other roles – there is simply insufficient numbers to create proper segregation of duties. In such cases the extra roles taken on should, where possible, not create conflicts of interest that cannot be managed. In the circumstances where the compliance function is not a full-time role, there is a risk that the function will not internally be considered as having sufficient standing and authority and that its reporting line will be to a main board director who has operational responsibilities with consequent possible conflicts.

Where genuine independence is not possible due to the small size of the firm, then one option would be to use an independent external body to provide the necessary level of independence, although it is recognised that this would add to regulatory costs and could be argued to be a barrier to entry for small/medium sized investment firms.

Q12. 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?

IMA response

The ESC paper described in Q1 above, and which IMA supports, states that compliance personnel should not be involved in the performance of services or activities they monitor in the course of carrying out duties related to the compliance function. It may be possible to address such issues in smaller firms through the use of external auditors carrying out checks.

Q13. Are the means for implementation of independence set out above sufficient to achieve independence? Please explain.

IMA response

IMA would not promote the NASC model as suited to all types of firm and all types of environment. Firms which are members of the NASD or NYSE are already of a relatively sophisticated and complex character. Such a model would not transfer to the world of the niche investment manager or small personal financial adviser, for example.

Q14. How do you ensure that compensation of compliance personnel is not subject to undue influence? Please explain.

IMA response

The ESC paper described in Q1 above, and which IMA supports, states that investment firms should ensure that the method of determining the remuneration of compliance personnel does not and is not likely to compromise their objectivity.

This does not mean that compliance personnel should not share in the success of the firm. If IOSCO subscribes to the notion that good compliance is good business, then the compliance function will play a role in the commercial success of an organisation over the long term, and should be rewarded. It is also important that compliance personnel are remunerated on a comparable basis to staff in other areas so that good quality recruits and entrants are attracted to the role. In many organisations, the compliance function is within a discrete cost centre, with its own budget, which can be helpful in achieving independence.

As with many things, it becomes a matter of degree. We would not support, for example, compliance personnel being remunerated on a commission basis for sales volume. However, we see no reason why there could not be a bonus scheme or participation that was based on profitability, which is in part driven by sales volume.

There is no foolproof means by which any remuneration package can be ensured not to have a particular effect, as this involves a response by the individual to a particular system and individuals will have individual circumstances and individual responses. We would suggest that, in the first instance, senior management with its responsibility for compliance, is best placed to judge.

We would also caution against any assumption that the other “direction” to worry about is an undue influence for a compliance officer to say “Yes” to the business, when he should say “No”. We believe that there are dangers also in unduly influencing compliance officers to always say “No”.

Q15. What are the appropriate qualifications for compliance personnel?

IMA response

In the UK there are currently no widely accepted professional qualifications specifically for compliance personnel. Typically, however, compliance personnel are either, qualified accountants/internal auditors, or lawyers, or have established a proven track record working within the investment industry. We are aware however that the UK Financial Skills Council (FSC) has recently consulted on the skills and expertise required of compliance officers, perhaps as the basis for a qualification, although this is very much work in progress and we would not support the basis of a number of the suggestions made by the FSC.

Where there are qualifications elsewhere in the world, these naturally focus on technical knowledge of the regulations, and this is clearly the bedrock of compliance. However, particularly at senior levels, the quality of judgment is what marks a good from a bad compliance officer.

We would support the recognition of technical qualifications (which would need to have a degree of internal mutual recognition), but with the caveat that this has to be employed alongside, and as part of, other qualities to be effective.

Q16. Should the qualifications vary depending on functions, responsibility or seniority?

IMA response

Whilst, as noted in Q15 above, there are currently no widely accepted professional qualifications specifically for compliance personnel, certain qualifications clearly are particularly appropriate for specialised compliance functions, e.g. accounting/auditing in relation to compliance monitoring, or an understanding of the functioning of capital markets for those dealing in such markets.

Q17. How do you evaluate the adequacy of courses and training for compliance personnel?

IMA response

Managers of compliance functions generally get to know the training providers and the quality/content of their courses, matching this to the individual requirements of their compliance staff. Whilst much compliance training quite correctly focuses on team management and interpersonal skills, none of the available compliance specific courses or qualifications has attained any universal level of acceptance which would tend us to think that they do not serve all needs, even if they may be regarded as adequate for some purposes. While exams are one way of demonstrating competency there is still a lot to be said for experience when it comes to compliance.

Q18. Who, within or external to a market intermediary, is best placed to assess the effectiveness of the compliance function? Please explain.

IMA response

In the first instance that judgement has to be made by the senior management of the firm that is relying upon the compliance function to assist it in fulfilling a key responsibility. We also see that external auditors have a

role to play. Indeed, the level and type of auditor reporting in a number of countries, including the UK, obliges the external auditor to comment on aspects of compliance that will reflect in one way or another on the compliance of the firm, and indirectly on the compliance function. Clients of a market intermediary will also have valuable input on the effectiveness of a compliance function.

Q19. What should be the role of an external party in assessing the effectiveness of a compliance function?

IMA response

There are several ways in which an external party might be used to assess a compliance function, but the IMA does not believe any of these should be mandated. They would include:

- the use of external auditors to test compliance critical functions such as the compliance risk assessment process on which the monitoring programme is based, compliance reporting to senior management, and the effectiveness of client money reconciliations;
- the use of external lawyers/accountants to review client documentation and promotional material;
- the use of external specialists in the areas of review of best advice, CIS pricing etc;
- the use of consultants and research firms to benchmark against other compliance functions.

Q20. What are the practical concerns of requiring an external party to conduct periodic assessment of a compliance function?

IMA response

Many of the services on offer are relatively expensive and offer limited recourse should they miss a significant problem. It is also a continuing challenge to tailor what are essentially off-the-peg assessment models to the circumstances and culture of a particular firm, bearing in mind that any external party will understand the business less than the compliance function. Obtaining an unbiased/objective view of the efficiency of the compliance function is therefore very difficult. It is also notoriously difficult to measure the success of the compliance function as there are no obvious metrics.

Accordingly, the usefulness of such services is constrained and management need to understand the inherent limitations of such an approach. Such external services should never be used as a proxy for the governing body to have an informed opinion on the adequacy and effectiveness of its own compliance function.

Q21. What should be the scope and frequency of the assessment by an internal party and/or external party?

IMA response

Senior management should have discretion as to the scope of such assessments. It would seem impractical and unnecessary for this to be stipulated in regulation as necessarily needing to be more frequent than annual for internal reviews and bi-annual for external reviews. If firms believe it appropriate in certain circumstances and in certain areas to conduct more frequent assessment, that is a matter for them and is fully commensurate with a risk-based approach.

Q22. Please identify the methods of monitoring that are the most effective from your perspective and explain why.

IMA response

These will differ according to the nature of the activity and the nature of the compliance control. Some aspects of compliance will have a measurable financial outcome (e.g. client money reconciliations that balance) that can be periodically measured through traditional auditing techniques. Other aspects, such as whether staff have reported all personal security transactions, must rely upon different methods of enquiry and assessment. Computer based reviews provide the most scope for monitoring allied to exception based reports, which allow the compliance function to focus on areas of concern.

Q23. What factors are indicative of a strong compliance culture and a weak compliance culture? Please explain.

IMA response

The overall level of breaches will give indications about the compliance culture of the firm, but cannot be used as a strong indicator without further analysis. For example, problems with NAV pricing of a collective investment scheme could be due to disruption at securities price vendors. Persistent breaches will however tend to be an indicator of problems.

The quality of the response to breaches is also important. There is no way in which a firm can have no breaches – human and technical error cannot be entirely eradicated in any organisation functioning in the complex environment of financial services, so it is impossible to eliminate the chance of breach entirely.

The elements that will tend to be present in strong compliance cultures are:

- Leadership from the top – commitment from senior management, in word and deed, to the principles of compliance
- Clear and well-used lines of reporting
- Well defined and documented roles and responsibilities
- Transparency of the organisation to compliance and other control processes
- Lack of repeat recommendations in internal audit and compliance monitoring reports
- Demonstrated confidence of the organisation in the advice given by its compliance function
- Compliance representation on significant business committees
- Effective relationships with regulators and lack of regulatory censure
- Clear and articulated procedures for self-assessment and other forms of testing of compliance controls

Q24. Are there other means for implementation that we should consider?

IMA response

In line with the FSA's emphasis on senior management, systems and controls, regulators should spend time with senior management to gain comfort as to the compliance culture and how they are managing the business in a controlled and compliance manner.

Q25. Please identify the specific issues that arise for the compliance function of a market intermediary if it is operating in more than one jurisdiction.

IMA response

The obvious issues of different rules and cultures are the most difficult issues to address. This may mean, for example, that promotional material that is legitimate in one jurisdiction may not pass muster in another. Many firms will try and tend towards single designs for processes and procedures and there are sound reasons for this in terms of technology platforms and ease of monitoring, but there will need to be local variations and these introduce a higher than usual risk of error.

Regulatory cultures also diverge. For example, the level of interpretation a regulator is willing to offer, the ability to do something that is not specifically proscribed by the rules, and the use of principles versus a rules-based regime will all have a significant impact. To be effective the compliance function must factor in all these elements. Often, this involves producing a set of procedures that are universally acceptable, but this is never simple and not always possible. Clearly, the more jurisdictions in which the market intermediary operates and the number of different languages used, the more challenging it will be to apply common standards.

Q26. 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?

IMA response

As stated above, the compliance function is part of the management toolkit enabling it to achieve compliance by the firm. Accordingly, the compliance organisation designed to address a multi-jurisdictional environment must be sympathetic to the general management structure. If for example, there is a head of country for general management, then the compliance function must have a means of reporting to that person on matters relating to that country.

There will be no one structure that works for all types of activity, even within a single firm. For example, it is quite common for trading desks to be subject to relatively centralised compliance as there is usually a single technological platform, the area is relatively specialist and most firms have global policies on matters such as best execution and trade allocation. However, promotional material will be in different languages by jurisdiction, and is less likely to be subject to a single set of criteria, so it often makes sense for a local compliance function to support that activity.

Japan Securities Dealers Association
Tokyo Shoken Kaikan Bldg.
1-5-8, Kayaba-cho, Nihonbashi, Chuo-ku
TOKYO 103-0025, JAPAN
Phone: (813) 3667-8451 Fax: (813) 3666-8009

July 13, 2005

Mr. Philippe Richard
Secretary General
IOSCO
Oquendo 12
E-28006 Madrid
Spain

Re: JSDA's Comment on the Compliance Function at Market Intermediaries

Dear Mr. Richard:

Japan Securities Dealers Association (JSDA) would like to thank you and your colleagues for giving us the opportunity to comment on this issue. JSDA is a self-regulatory organization and a trade association for more than 270 securities broker houses and investment banks in Japan. We are pleased to submit our comments as given below on behalf of our member companies.

Our comments fall under following three points.

Introduction
C. "Definition of the Compliance Function and Scope"

Topic "Establishing a Compliance function"

As with any other risk managements such as market risk, credit risk or internal audit functions, compliance function should be established upon risk-based approach.
We request that you should state the definition of compliance function in the principle that, it should be "proportionate to the level of compliance risk"
It is considered that the definition (explanation) about a "compliance risk" is not clear. We request that you should add the definition (explanation) about a "compliance risk".

2. Topic 2 "Role and Responsibilities of the Board of Directors or Senior Management"

We cannot emphasize too much about the importance of the responsibility of the board of directors or senior management for establishing effective compliance function and setting the high standard of ethics. However, given the practical limitation on day-to-day supervision of each and every employee in the organization, manager's supervisory responsibilities over individual employee at lower level as well as each employee's responsibility to abide by such rules and regulations should be equally emphasized in the principle.

Example,
The responsibilities of the staff carrying out the compliance should be assist senior management in managing effectively the compliance risk faced by the securities.
If some of these responsibilities are carried out by staff in other departments, the allocation of the responsibilities to each department should be clear.

3. Topic 5 "Assessment of the Effectiveness of the Compliance Functions"

We have general reservations about the effectiveness of review by an external auditor and the idea of adopting such review as a principle for the following reasons.

Such review inherently requires an in-depth knowledge and proper understanding of applicable rules and regulations, the nature and the complexity of business or organizational structure specific to a securities and only a few external auditors expected to possess such expertise. Regulators or SROs are in a better position to perform such review.

Any meaningful review is expected to take enormous resources off a market intermediary and there is concern that it may deprive a market intermediary of its resources necessary for discharging day-to-day compliance responsibilities if such review becomes mandatory on top of regulator's or SRO's review.

Please do not hesitate to contact me or Mr. Yoshinori Iso, General Manager of the General Administration Department, in regards to the comments in this letter.

Sincerely yours,

Tatsuo Watanabe
Vice-Chairman
Japan Securities Dealers Association

LIBA

LONDON INVESTMENT BANKING ASSOCIATION
6 Frederick's Place, London, EC2R 8BT
Tel: 020 7796 3606 Fax: 020 7796 4345
e-mail: liba@liba.org.uk website: www.liba.org.uk

IOSCO Consultation Report on the "Compliance Function at Market Intermediaries"

A submission by the London Investment Banking Association

A. Introduction

1. Our Members – a list of whom is attached• – have asked us to respond to the Consultation Report.

2. The purpose of the consultation is to identify possible supplementary principles to Principle 23 of the IOSCO Objectives and Principles of Securities Regulation; in addition, a number of issues are raised for discussion.

3. Our Members believe that in developing supplementary principles IOSCO should focus on developing statements of intended *outcomes*. In this light, and as we explain below, there are concerns about a number of the proposals in the Report.

B. Definition of compliance function

4. For the purposes of the exercise, "compliance function" is defined as follows:

> "A function that, on an on-going basis, identifies, assesses, advises on, monitors and reports on a market intermediary's compliance with securities regulatory requirements, including whether there are appropriate supervisory procedures in place …"[19]

and it is made clear that the expression 'function' refers to staff responsible for carrying out specific compliance activities: "the expression does not intend to denote any particular organisational structure". The latter is important because it is essential that any articulation of principles for compliance should take into account that firms will organise their activities and internal procedures in different ways to reflect the different kinds of business that they undertake and the associated risk profile. In a similar vein, the Report acknowledges that small and large firms are in a very different position although, nonetheless, it should be possible to establish *general* principles that apply to the great majority of firms.

---

[19] Page 6 of the Consultation Report

5. These aspects of IOSCO's approach to the definition of the compliance function are welcome, therefore, because they confirm the need for a flexible approach. However, we are concerned that as drafted the definition does not cover explicitly the important proactive risk mitigation role fulfilled by compliance in establishing procedures to minimise the risk of a firm failing to comply with its obligations, advising members of a firm in order to promote compliance, and in ensuring that arrangements for appropriate training are in place. Furthermore, it should be made clear that the various functions described in the paper can be shared with other functions such as legal, internal audit and financial control.

6. On a drafting issue, it is not clear *whom* the compliance function advices: should the current Principle 2 – on the responsibilities of the Board/senior management – precede the Principle on establishing a compliance function, therefore? Also, given that compliance generally advises on issues additional to *securities regulatory* requirements – for example on exchanges' rules and on banking supervisors' requirements (where a firm is a bank) – perhaps the definition should reflect this.

C. LIBA Members' concerns

7. More generally, there are concerns that what is driving this consultation exercise may be a wish – at least amongst some members of IOSCO – to move towards a more prescriptive approach.

8. Thus, although we have few comments on the six suggested Principles or on the cross-border issues and outsourcing Topics as currently drafted[20] – but see Section D below – we are concerned that a number of the matters covered in the Discussion parts of the Report may point to the wish to introduce an additional layer of regulation which would be inappropriate at the global level at which IOSCO works. This impression is heightened by the majority of questions that are raised, not least a number of the questions that are addressed to *firms*. (Examples of the latter include questions 2, 8, 14, 17 and 22.)

9. We must stress that the responsibility for establishing the precise organisation and controls/reporting arrangements that need to be maintained in order to achieve compliance with relevant requirements and rules should rest with *firms themselves*, so that IOSCO should not do more than indicate the *principles* that need to be met: the *methods* firms use in order to satisfy requirements should be left to a firm's management to determine (with *national regulators* introducing guidelines/particular standards for the firms they supervise if they consider that to be necessary).

10. The account in the consultation Report of the rules that different regulators have made to achieve regulatory objectives is also a source of unease. This is because differences in requirements and approach are raised *topic by topic* without an overview of the overall regime in the various jurisdictions. The account fails, therefore, to give weight to the extent that regulators have a range of tools for achieving their objectives so that a given *level of regulation* can be established in *different* ways. It is only by considering the full range of powers available to a regulator, and the way in which these powers are used, that it will be possible to determine whether an apparent "shortfall" in one area is offset by measures with an equivalent effect elsewhere. (We would also note that there are concerns in some areas that the account provided of the requirements in particular jurisdictions may not capture the complete picture[21].)

---

[20] Copy attached for convenience.

[21] An example is the section of the Report dealing with the role of external auditors (in Topic 5). Here it is stated that in the UK "auditors are required by accounting standards to assess the extent to which a firm has complied with relevant laws and regulations" whereas, in fact, there are *legislative* provisions dealing with the circumstances in which auditors are obliged to disclose information to the FSA; in addition, auditors have a specific duty to report on firms' compliance with the FSA rules dealing with client assets.

11. Finally, we should stress that there are also concerns about the timing of this consultation and about the relationship it may have with other initiatives that are in train. Thus, although the Report makes reference to the work undertaken by the Basel Committee's Task Force on Accounting Issues, it was published *before* the "Compliance and the compliance function in banks" paper had been published. In addition, within the EU, firms are considering the implications of the wide-ranging proposals for legislation that have been developed by the Committee of European Securities Regulators and the European Commission in their work on implementing the Markets in Financial Instruments Directive. Once finalised, this material will be binding on the Member States, and will necessitate many changes in regulatory requirements relating to the compliance function. It would have been helpful, therefore, if IOSCO had deferred its consultation until the shape of the new regime in Europe was clearer and, given the current position, it will be particularly important to ensure that the conclusions of this consultative exercise are co-ordinated with those of the European bodies and the Basel Committee.

D. Comments on particular Principles/Topics

12. A key point for our Members is that the Principles should recognise clearly that compliance assists the firm and its senior management in managing compliance risk: compliance should not be seen as being responsible for managing that risk itself. A second important theme is the need to recognise that firms vary – in size, types of products they deal in and types of clients they deal with – so that it must be acknowledged that one size cannot fit all and that specific organisational structures should not be prescribed. (For example, the relationship between the compliance function and risk management will differ firm by firm.) We believe that IOSCO endorses this approach but the implication is that the Principles will need to be very generic or will need to be carefully caveated to make clear that they need to be interpreted in the light of a firm's circumstances.

- *Topic 1*

13. See our comments on the "compliance function" definition in Section B above.

- *Topic 2*

14. Although the Means for Implementation/Discussion sections in the Report cover some of the ground, the Independence Principle itself should make clear that firms need to take reasonable steps to ensure:

a) the compliance function reports directly to the senior management;
b) the personnel designated to carry out the compliance function have the necessary authority, resources and access to all relevant information;
c) those personnel are not involved in the performance of services or activities they monitor in the course of carrying out duties related to the compliance function;
d) the method of determining the remuneration of those personnel does not and is not likely to compromise their objectivity.

15. There would be practical concerns if excessive documentation of policies was required, and the costs involved in producing the material and keeping it up to date may well be unduly burdensome for smaller, less complex firms. The central question is – as for new regulations – does the cost of producing and keeping a document up to date outweigh the benefits which the documentation delivers.

- *Topic 4*

16. What matters is that compliance staff have the skills, knowledge and expertise necessary for the discharge of the responsibilities allocated to them. However, as drafted, the Principle appears to imply that compliance personnel need formal qualifications. In our Members' experience it is clear that a compliance-specific qualification is not necessarily needed. The emphasis in this Principle should be on the ability of compliance staff to perform their role, therefore, and it should be amended to recognise that they may have that ability by reason of experience rather than through study.

- *Topic 5*

17. Principles dealing with the assessment of the effectiveness of the compliance function should not be overly prescriptive as regards frequency of review of compliance by internal audit or other external parties.

- *Topic 7*

18. Our Members have made some general comments on cross-border issues: the position varies depending on whether business is undertaken through a branch or on a cross-border basis, and there can be issues as regards different languages, different legal principles/interpretations of requirements and differing views on good market practice. It is impossible to generalise, however, because the issues that arise are very specific to the jurisdictions in which a firm operates.

E. Conclusion

19. We would be pleased, of course, to discuss the issues covered in this submission with IOSCO or to provide further information about any of the matters which our Members have raised if that would be helpful.

London Investment Banking Association
July 2005

IOSCO Consultation Report on the "Compliance Function at Market Intermediaries"

IOSCO Principles

Principle 23 of the *IOSCO Objectives and Principles of Securities Regulation* for market intermediaries states the following:

> 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".

Principles and Topics for Discussion and Consultation

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 to identify, assess, advise on, monitor and report on a market intermediary's compliance with securities regulatory requirements and the appropriateness of its s supervisory procedures.

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.

Topic: 2: Role and Responsibilities of the Board of Directors or Senior Management

Principles:

(a) The board of directors or senior management is responsible for the firm's compliance with securities regulatory requirements.

(b) The board of directors or senior management should establish and maintain a compliance function, and compliance policies and procedures designed to ensure compliance with securities regulatory requirements. The board of directors or senior management should assess whether the compliance policies and procedures are being observed and are appropriate on an on-going basis.

Due to differences in their size and internal organization, market intermediaries will employ different structures to ensure compliance with securities regulatory requirements. Placing ultimate responsibility on the highest 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.

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 and should report to the board of directors or senior management.

Topic 4: Qualification of Compliance Personnel

Principle:

Staff exercising compliance responsibilities should have the necessary qualifications, experience and professional and personal qualities to enable them to carry out their duties effectively.

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 review by independent third parties, such as the intermediary's external auditors, SROs or regulators.*

In order to 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.

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.*

Topic 7 Cross-border issues

… Market intermediaries that have cross-border activities should carefully consider the applicable regulatory requirements. Regulators, too, should be cognizant of the implication of cross-border issues for the performance of the compliance function. Regulators should consider whether market intermediaries have arrangements for compliance with all applicable regulatory requirements.

<u>Specific questions for comment</u>

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

2. 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?

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. The IOSCO Technical Committee 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[22].

[22] Note: the Joint Forum has also developed principles for Outsourcing – these are not referred to in the Consultation Report.

Man-Financial
Singapore

Public Comment on Compliance Function at Market Intermediaries

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

   Yes. Compliance function should not be reactive in checking whether a breach has occurred. It should be an ongoing process to identify and prevent violations. In this regard, Compliance should be involved in all new businesses, including products, to provide advice on regulatory requirements and measures to be taken to ensure compliance.

2. What is the relationship between the compliance function and risk management function?

This depends on the size and complexity of business. In a large organization, the compliance function can be separated into two sub-functions – enforcement compliance - reviewing and monitoring of regulatory compliance and advisory compliance that forms part of the risk management team in advising on new business lines or products. However, in smaller and less complex firms, the compliance function may fall within the general risk management framework.

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

   No.

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

Generally no.

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

Compliance officers should have a proper program to educate staff on changes in regulatory requirements and explain weaknesses or non-compliance noted during any audits or inspection.

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

See (2) above.

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

Yes. Due to the small setup, if too much time is spent on documentation of policies and other paper work, the intermediaries may lose focus on the actual work that needs to be done thereby compromising compliance and risk management standards. However, this does not mean that there should not be any

documentation. Documentation should at least cover in point form the key policy or procedure, the rationale or principle for having such policy or procedure, reference to any regulatory requirements and the process for implementation (can be in a simple flow chart).

Regulators should avoid micro managing the documentation process by requiring every single detail of a process flow to be documented. Instead the focus should be on whether the documentation is sufficient to explain the process flow for the regulators to identify any possible risk areas that requires a thorough review.

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.

Accountability is at all levels, depending on the level that fails.

Business managers should be accountable for failing to comply with set procedures or policies that results in a violation. This is because they are the primary executors of the procedures and policies.

Compliance Head should be accountable for

a. Failing to update the relevant parties of changes in existing regulations or new regulations,
b. Amending or drawing up new sets of procedures or policies for the company to comply with the changes in or new regulations.
c. Failing to do compliance checks to ensure business managers comply with the requirements and recommending action against those who fail to comply

Senior management should be accountable if they do not require Compliance to escalate any violations to them or refuse to act on any serious non-compliance highlighted by Compliance. Senior management should also be accountable if it is shown that they have unreasonably withheld procedures and policies meant to comply with regulations or they override existing procedures or policies without any valid grounds resulting in a violation.

Board of directors should be accountable only if they fail to ensure that the company has a proper structure to ensure compliance or it can be shown that the board of directors generally tolerates non-compliance to achieve business goals.

9. Should a senior officer be designated for day to day compliance responsibilities ?

Yes. Compliance needs someone with authority especially opposite business managers.

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

Compliance should not review their activities. This should be done by an external party, either by external auditors or by someone from the head office.

11. See (11).

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

Yes.

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

Compensation should be decided either by the board of directors or head office's Compliance head. The board can rely on comments from external auditors or head office on the performance and effectiveness of Compliance to decide appropriate compensation.

14. What are the appropriate qualifications for compliance qualifications?

In addition to academic qualifications, there should be structured compliance qualifications at entry levels and subsequent bi-annual continuing education programs.

Entry level examination should cover the following :-

a. General understanding of the industry
b. Role and responsibility of a compliance officer
c. Detailed coverage of relevant rules and regulations to be enforced
d. How should rules and regulations be interpreted
e. Basic understanding of trading terms and practices
f. Application of such rules and regulations in the office environment
g. How to develop compliance programs
h. Case studies on problems of firms such as Barings, Daiwa and Sumitomo etc
i. Handling of business vs compliance problems
j. How to handle rules that are unclear and ambiguous
k. How to deal with unreasonable business managers or directors

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

Not the basic qualification.

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

Whether the courses are generally theoretical and do not equip the compliance person to perform the function effectively.

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

SRO. The experience of auditing different intermediaries and knowledge of the industry should help the SRO in assessing the effectiveness of the compliance function.

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

The external party should review the compliance steps taken, reports and recommendations made. The management response should be reviewed to assess whether there are management overrides.

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

Requiring the intermediary to follow the practice of another intermediary without considering the suitability of such practice.

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

Once in every 3 years.

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

A combination of SRO review and notification of significant breaches and/or customer complaints are the most effective.

SROs are generally more “in touch” with the market practices than a regulator.

Regulators and SROs should encourage reporting of breaches without fear of facing any repercussions, especially when the intermediaries took internal disciplinary actions against the parties involved or already has in place procedures (which were not followed). Generally intermediaries are reluctant to report for fear of being penalized with fines or undue bad publicity. There is also the perception that those who does less “get away” because there is nothing to report.

A combination of the carrot and stick approach should help develop a strong compliance culture. This means that heavy penalties will be meted out if a SRO found violations that should be detected in the normal course of compliance work while only the persons involved and not the firm is penalized when its compliance detected and report such violations.

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

Factors that shows a strong compliance culture include :-

a. involvement of compliance in new product development
b. periodic compliance review of processes
c. reporting of weaknesses and violations to senior management and board of directors
d. staff familiarity with rules and regulations

NATIONAL FUTURES ASSOCIATION

Via E-Mail (mail@oicv.iosco.org)

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

Re: Public Comment on Compliance Function at Market Intermediaries

Dear Mr. Richard:

National Futures Association (NFA) greatly appreciates the opportunity to comment on the Consultation Report entitled Compliance Function at Market Intermediaries. NFA is a registered futures association under the U.S. Commodity Exchange Act and an affiliate member of IOSCO. NFA is the industry-wide self-regulatory body for the U.S. futures industry and regulates the activities of over 4,000 Member firms and approximately 55,000 registered account executives who work for those Members. Our mission is to work as a partner with the CFTC to provide the industry with regulation that is both effective and efficient.

NFA has reviewed the consultation report which sets out a number of supplementary principles with measures for implementation to assist market intermediaries increase the effectiveness of their compliance function. We share the report's common belief that the compliance function at market intermediaries plays an essential role in preventing possible misconduct and in promoting ethical behavior. We also believe very strongly that market intermediaries should have the flexibility to design and implement their compliance function based on their size, nature of business and the types of clients served. The consultation report correctly recognizes that innovation may result in various acceptable compliance function structures and regulators should not attempt to design a "one size fits all" compliance function requirement.

The consultation report contains a section describing recent initiatives by international regulators regarding the compliance function. We would like to take the opportunity to describe an initiative implemented by NFA that does not fall into the category of recent because it was put in place over 10 years ago, but it does address the adequacy of supervisory and compliance procedures in place at our Member firms. NFA Members must complete a comprehensive self-audit questionnaire that requires Members to review the adequacy of their supervisory procedures on an annual basis. NFA's self-audit questionnaire can be located on NFA's web-site at http://www.nfa.futures.org/compliance/selfexam.asp. The questionnaire aids Members in recognizing potential problem areas and alerts them to procedures that need to be revised or strengthened. The questionnaire must be reviewed by the firm's appropriate supervisory personnel. After this review, the appropriate supervisory person must sign the questionnaire stating that the Member's operations have been evaluated based upon the questionnaire and attesting that the Member's procedures comply with all applicable NFA requirements. Members are required to retain the signed questionnaires in their files for a period of five years and provide the signed questionnaires for inspection upon request by NFA.

NFA is not a market intermediary, although most of its Members are market intermediaries. Therefore, we will only make comments on the narrative and supplementary principles and answer those

questions that we feel can be adequately addressed based on our experience as a self-regulatory organization responsible for ensuring that our Members comply with our rules and CFTC regulations. It is difficult to respond to questions that attempt to obtain specific details about a particular firm's operations due to the diversity of our membership as to size, type of clients and organizational structures.

Definition of the Compliance Function and Scope

Answers to Specific Questions for Comment:
Question 1: Yes

Topic 1: Establishing a Compliance Function

The sub-section entitled "Designation of a specific organizational structure for compliance" describes some of the supervisory requirements of specific securities SROs in the U.S. It is also important to identify that NFA, a U.S. SRO for the futures industry, places a broad and continuing requirement on its Members to diligently supervise its employees and agents in every aspect of their futures activities. NFA's supervisory rule is intended to provide supervisory guidelines rather than dictate a "one size fits all" form of supervision. NFA's supervisory rule, NFA Compliance Rule 2-9, and related interpretive notices can be located on NFA's web-site at http://www.nfa.futures.org/nfaManual/manualCompliance.asp#2-9. NFA's supervisory rule also contains criteria that dictate when a firm is required to implement enhanced supervisory procedures over its telemarketing activities.

The sub-section entitled "Notification of breaches of securities regulatory requirements" fails to describe that U.S futures SROs also requires members/registrants to give immediate notice to the regulator if its adjusted net capital at anytime is less than certain minimums, if it fails to keep current books and records, if its certified public accountant notifies it of a material inadequacy, or if it has a shortfall in the funds held for customers.

Answers to Specific Questions for Comment:
Question 3: No

Question 4: No, however, someone at the firm must be responsible for ensuring that the company complies with its regulatory requirements.

Question 7: There do not appear to be any real practical concerns related to requiring documentation of policies and procedures for smaller, less complex market intermediaries. However, as stated throughout this response any documentation requirements should be flexible and the level of detail should be driven by the size and complexity of the market intermediary.

Topic 3: Independence and Ability to Act

Answers to Specific Questions for Comment:

Question 11: For a small firm, any specific requirements relating to independence and ability to act may be difficult to achieve. Therefore, a broader requirement for market intermediaries to diligently supervise every aspect of their futures activities may be more relevant and practical for small firms.

Question 12: As stated throughout this response, it is difficult to dictate a "one size fits all" form of supervision. In certain situations, it may be acceptable for individuals who perform business and compliance activities to supervise their own business activities.

Question 13: It is very difficult to state generally that the means of independence set out in this report are sufficient to achieve independence because of the diversity of market intermediaries, from one-man operations to large conglomerates. When supervisory deficiencies are noted, a regulator may

want to evaluate whether a lack of independence or an inability to act resulted in supervisory deficiencies and instruct the market intermediary to address and correct these particular concerns.

Topic 4:Qualifications of Compliance Personnel

Answers to Specific Questions for Comment:

Question 15: Compliance personnel should have a thorough understanding of the relevant regulatory requirements and how the market operates.

Question 16: Yes

Topic 5: Assessment of the Effectiveness of the Compliance Function

Answers to Specific Questions for Comment:

Question 19: CFTC Regulation 1.16 requires that a registrant file with its annual report a supplemental report by the external accountant describing any material inadequacies.

Question 20: The practical concerns of requiring an external party to conduct periodic assessments of a compliance function involve costs associated with any business interruption and costs associated with compensating the external party. Another practical concern involves finding an affordable external party with the experience and knowledge to complete a satisfactory assessment.

Question 21: As stated earlier in this response, NFA Members have a continuing responsibility to supervise every aspect of their futures activities. Furthermore, NFA Members must complete a comprehensive self-audit questionnaire that requires Members to review the adequacy of their supervisory procedures on an annual basis.

Topic 6: Regulators' Supervision

As a self-regulatory organization responsible for overseeing the activities of numerous market intermediaries, we carefully reviewed the supplementary principles and means for implementation and discussion in this section. NFA agrees with the two supplementary principles. In the comments directly below the supplementary principles, the consultation report correctly states that some regulators rely on SROs to directly regulate and monitor the compliance function at market intermediaries. However, the means for implementation listed as (a), (b), and (c) only address direct examinations by the regulator and do not add the option that these direct examinations may be done by SROs. Means for implementation Item (d) should also allow for examinations by SROs of market intermediaries using a risk-based approach.

Under the discussion section, the consultation report fails to mention that examinations are also conducted via SROs for a number of firms regulated by the US (CFTC). In the sub-section entitled certification, the consultation report may want to consider adding information regarding NFA's self-audit questionnaire that was described earlier in this response. In the sub-section entitled "Enforcement Actions," it may be worth mentioning that SROs also have the authority to bring enforcement actions against market intermediaries and impose penalties and remedies.

Answers to Specific Questions for Comments:

Question 22: The consultation report mentions a number of effective methods for monitoring market intermediaries including risk-based examinations and material inadequacy letters from external accountants. Another method that we find very effective in monitoring market intermediaries is the use of the self-audit questionnaire that we mentioned several times throughout this report. Other means of monitoring market intermediaries include reviewing customer complaints and its sales practices.

Question 23: Clearly this is not an exhaustive list, but some factors that may be indicative of a weak compliance culture include sloppy books and records, late filings, significant volume of customer complaints, failure to take action to correct instances of non-compliance, insufficient capital, and a sales force made up of salespeople that have disciplinary records or salespeople that have worked for firms with disciplinary records. NFA evaluates the employment histories and disciplinary backgrounds of a firm's principals and senior management in assessing whether the firm has a weak or strong compliance culture. Employment histories and disciplinary backgrounds for US futures registrants can be obtained by using NFA's BASIC system at www.nfa.futures.org.

NFA would like to thank IOSCO for the opportunity to respond to this consultation report. If you have any questions concerning this letter or need any additional detail, please contact me at kwuertz@nfa.futures.org.

Respectfully submitted,

Karen K. Wuertz
Senior Vice President
Strategic Planning and Communications

1. **FCMB capital market Limited- response**

COMPLIANCE FUNCTION AT MARKET INTERMEDIARIES

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

Answer.
We are in agreement with the definition and description of the scope of a compliance function. Compliance involves ensuring that market intermediaries comply with existing securities regulations, laws and rules, in order to protect the parties in order to promote fair and orderly markets as well as investor protection.

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; if they are separate, how do they interact when dealing with compliance issues?

Answer.
The compliance function and risk management function are separate. The compliance function ensures that activities of market operators are in compliance with the rules and regulations, whilst the risk management function deals with managing the operators risk exposure.

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

Answer
Yes, there should be a clearly defined scope of responsibility as well as duties of compliance officers which should be established by the securities regulatory organization.

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

Answer
None

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

Answer
None, the responsibilities listed in the consultation report are quite exhaustive.

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

Answer
The compliance officers in conjunction with senior management should be responsible for managing compliance risk at all times. Whenever the compliance officer comes across a situation that may result in a compliance risk, the officer should bring this to the notice of senior management, who would assist in managing the compliance risk.

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

Answer
There should be documentation of policies and procedures for market intermediaries to ensure standardization of compliance procedures and functions.

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 who would be accountable and what would be the extent of their accountability? Please explain your answer?

Answer
At our firm, a compliance officer is designated to handle all compliance related issues. The compliance officer reports directly to the business unit head, who is a senior member of staff. Ultimate accountability is borne by members of executive management.

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

Answer
No, the compliance officer is responsible and accountable with regards to his or her compliance functions. The firm is liable for any sanctions or penalties effected although this rarely occurs.

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

Answer
No, the senior officer should supervise the activities of the designated Compliance Officer, whilst the Compliance officer performs the day-to-day compliance functions.

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

Answer
The compliance officer should be given the requisite latitude(i.e training, authority and etc) to carry out his/her compliance function by senior management.

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

Answer
No, they should not, the business unit head should supervise both the business and compliance activities.

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

Answer
Yes

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

Answer
The compensation of compliance personnel should be primarily tied to ensuring minimal violation of regulatory rules and stipulations. The way to ensure that compensation of compliance personnel is not subject to undue influence, is to compensate them on a parallel level as other members of staff at his or her grade. Only very severe penalties will apply, where gross negligence can be attributed to the compliance officer.

15. What are the appropriate qualifications for compliance professional?

Answer
A compliance professional should have a legal background at the minimum, and should also have a sound knowledge of the businesses, so as to have the ability to understand where any loopholes exist, and therefore pre-empt any violations.

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

Answer
Yes, qualifications should vary depending on responsibility.

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

Answer
The adequacy of the courses and training of compliance personnel will be evaluated by the improvement in the performance of their compliance functions following attendance of courses and training.

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

Answer
The business unit head would be best placed to assess the effectiveness of the compliance function due to his or her supervisory obligations. A member of the regulatory body/organization would also be suitable for assessing the effectiveness of the compliance function.

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

Answer
The assessment would involve checking whether the scope and responsibilities of compliance, allows the compliance officer sufficient flexibility to prevent violation, and also ensures that there are avenues to empower compliance officers and senior members of staff to apply sanctions where violations or breaches occur.

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

Answer
There are no concerns as long as the regulatory bodies have pre-screened such external parties.

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

Answer
At least annually for an external party, and semi-annually for an internal party.

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

Answer
On-site visitation, the inspection of the books, as well as the direct examination of the internal policies and operational procedures and controls of the market intermediaries by regulatory authorities are effective methods of monitoring. This is what obtains in Nigeria and has proven to be very effective in monitoring violation of the regulatory rules and procedures.

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

Answer
Factors that are indicative of a strong compliance culture are the availability of set rules, guidelines and procedures for regulatory compliance; designated compliance officer(s); supervisory monitoring by senior management, as well as low incidences of violations of regulatory requirements and vice-versa.

24. Are there other means for implementation that we should consider.
Answer
None

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

Answer
The issues that would arise would be subjectivity to multiple compliance laws. The compliance officer will have to be adept in all the various compliance requirements in each jurisdiction.

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

Answer
There should be Compliance Officer locally situated in all jurisdictions to ensure that they have an in-depth knowledge of the regulatory requirements of the specific jurisdiction where his/her business intermediary operates.

Pricewaterhousecoopers'- response

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

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? ***The compliance function is part of the firm's overall and integrated risk management system. As a firm, there are standards, rules, regulations and practices that have been designed by management to ensure that all potential risk areas of the business, including compliance with regulatory provisions, are adequately mitigated. There are global procedures and code of conduct which we all subscribe to.***

3. Should a specific organizational structure for compliance be prescribed? Please explain. ***A blanket approach will not only be inapplicable but also unreasonable because different intermediaries have different organizational structures, sizes, natures of business and local peculiarities. It***

4. Are there any essential roles, responsibilities or activities for the compliance function that should be mandated or otherwise identified by regulators? ***The roles defined in the definition of a compliance officer of identifying, assessing, advising on, monitoring and reporting on a market intermediary's compliance with securities regulatory requirements and the appropriateness of its supervisory procedures are adequate and all embracing. Enforcement of these roles by the regulators is however necessary.***

5. Please identify responsibilities other those described above that are carried out by the compliance function at market intermediaries. ***As already noted in this document, different intermediaries have different functions for compliance officers. These may include reporting to management/board on financial and operational misconduct as well as breach of laid down regulations and procedures. In Nigeria, the additional role of reporting breach of SEC's regulation to SEC is not seen as an integral part of the compliance officer's function. Compliance departments, where they exist, are more internal audit department, ensuring compliance with operational procedures for management as opposed to being the watchdog of compliance with SEC rules and regulatory. This has to be communicated and emphasized to operators.***

6. How and when should the compliance function be responsible for managing compliance risk?
SEC in collaboration with intermediaries should develop a procedural manual and performance standards for compliance officers. These should, among other things, specify the areas to report on and the appropriate format to use, the timeline for reporting, the corrective measures and/or sanctions that they re authorized to provide in intermediaries' offices and penalties for failing to perform at set standards.

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?
The main issue is that very small operators are unlikely to have defined ways of doing most things as most of their actions will depend on prevailing circumstances. Nonetheless, they can still document the procedures they will employ under normal conditions.

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. ***This is a professional services firm with well established procedures for accountability and responsibility. Each person is supervised by a superior officer in the hierarchy right to the top. At the very top, where the buck stops, a committee is set up to ensure that decisions taken are in tandem with procedures and regulations. This is because, for most of the activities performed, the partnership is jointly and severally liable for any legal action. In essence, each person is a compliance officer and has a duty to ensure compliance at all times although in each region, there is a designated risk management officer who ensures compliance at all times.***

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

10. Should a senior officer be designated for the day-to-day compliance responsibility? Please explain. ***Indeed, the best system would have been to have an external compliance officer/firm. Where this is not possible, the internal compliance officer must be a senior officer who cannot be intimidated by management.***

11. What requirements relating to independence and ability to act are relevant to a small firm? ***The compliance officer should be under the protection of SEC but also report to the board. His appointment and dismissal should be subject to SEC's or some other legal entity's approval***

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?
Compliance officers should not take active part in business activities

13. Are the means for implementation of independence set out above sufficient to achieve independence? Please explain. ***See 11 above***

14. How do you ensure that compensation of compliance personnel is not subject to undue influence? Please explain. ***This can be regulated by SEC. Salaries should be fixed based on the compliance officer's level and industry/company structure.***

15. What are the appropriate qualifications for compliance personnel? ***In addition to a university degree or its equivalent, compliance officers must take a qualifying examination to be administered by SEC or its authorized agency certifying them to perform the job .***

16. Should the qualifications vary depending on functions, responsibility or seniority?
Yes, especially on level of experience.

17. How do you evaluate the adequacy of courses and training for compliance personnel? ***It is currently insufficient. See 15***

18. Who, within or external to a market intermediary, is best placed to assess the effectiveness of the compliance function? Please explain. ***It should be carried out by an enforcement/compliance/monitoring team from SEC, which should not have direct dealings with the intermediaries unless they suspect complicity or foul play.***

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

20. What are the practical concerns of requiring an external party to conduct periodic

assessment of a compliance function? ***Who foots the bills?***

21. What should be the scope and frequency of the assessment by an internal party and/or external party? ***The scope, which must be contained in the compliance procedure manual to be prepared by SEC in conjunction with operators, must cover all the activities of the company as corporate governance transcends all areas of business.***

22. Please identify the methods of monitoring that are the most effective from your perspective and explain why. ***Scheduled and unscheduled visits by SEC's team***

23. What factors are indicative of a strong compliance culture and a weak compliance culture? Please explain. ***Sanctity of procedures, timely reporting, and the availability of a verile internal control/compliance department are indicative of a strong compliance culture.***

24. Are there other means for implementation that we should consider? ***See 10***

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. ***There is obvious difficulty in standardizing reporting format, uniform procedures and employment of one compliance officer due different legal and regulatory environments.***

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? ***See 10 and 18***

RESPONSES FROM BANK OF THE NORTH TRUSTEES LIMITED

1. Yes. It aptly presents an ideal scope of the compliance function. The definition can be applied to all jurisdictions covered by IOSCO

2. The two functions complement each other in maintaining the much needed sanity and vibrancy of the Capital Market. The compliance function is part of the risk management function.

3. It is important that every capital Market intermediary should make provision for a department or section that would specifically handle the compliance function. The department should report directly to the Chief Executive Officer.

4. Most of these roles are already included in the ISA and its Rules.

5. The compliance function should liaise with the Corporate Affairs/Public Relations department in promoting transparency and thereby enhancing public confidence in the market.

6. It should be responsible for managing compliance risk right from the beginning of a transaction and cover the lower, middle and management levels in the organization.

7. All market intermediaries should have a comprehensive operational manual which should cover its mission statement, policies and procedures including operational limits of officials. This should be irrespective of the size of the intermediary.

8. The Board of Directors formulates policy for the company while Management implements it. As for accountability, the Board and Management jointly ensure proper conduct and compliance because they are accountable to the regulatory authorities in case of non-compliance with statutory rules.

9. There is no clear distinction in the use and application of these words. They can be used interchangeably.

10. As stated in 3. above, a senior officer should be assigned the day to day compliance responsibility and he should report directly to the CEO. This would provide the compliance function some measure of autonomy.

11. Adequate share capital requirement should be prescribed for them.

12. Conflict of interest situation may arise. Their compliance function should be handled by another intermediary.

13. Yes. They are sufficient to achieve independence.

14. 'Whistle blowing' should be encouraged by the regulators whenever such situations arise or are suspected.

15. A minimum of university degree.

16. Yes.

17. Compliance personnel, more than any other staff require constant education in order to keep abreast of the rules and their application.

18. The Capital Market Regulator is better placed to make such a assessment.

19. The role of the external party should be to guide the intermediary and in some cases impose sanctions.

20. Such periodic assessment would amount to an oversight function and would keep the compliance personnel on their toes always.

21. The scope should be the entirety of the business activity of the intermediary and frequency should be at least half-yearly.

22. The regulation should prescribe some form of quarterly or semi-annual returns to be rendered by the intermediaries.

23. An intermediary that records nil or less incidence of fraud indicates that it has a strong compliance culture while the opposite is the case for a fraud-prone intermediary.

24. Aggressive public enlightenment programmers should be carried out by the authorities.

25. When it is operating in more than one jurisdiction, conflict of laws issues are bound to arise.

26. The regulator should be given enough powers and funds to enable it carry out its functions effectively.

Response from Adejumo Ekisola & Ezeani

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

Answer: I do not agree with the definition for these reasons:

First, it seems to exclude the discharge of the compliance function in small firms. Some small firms acting as market intermediaries may be so small and their businesses simple and ad hoc that it does not make sense to keep or carryout any compliance function on an 'on-going basis'. I interprete 'on-going basis' to include rendering of regular reports to management and the establishment of structures which support this.

Secondly, I believe that the definition focuses solely on compliance with existing regulations leaving out adherence to accepted new custom, practice and standards. This is important when we remember that law/rules typically play 'catch-up' with human behaviour and new practices; especially in a developing country like ours where the legislative and rule making functions are still being developed and strengthened. The compliance function should also take the lead to drive a business or firm to new standards.

Thirdly, the definition focuses on things done i.e it casts the compliance function as one which is reactive but it should also be proactive. Indeed, it should be more proactive than reactive; otherwise there will not be anything different between the in-house compliance function and the police or law enforcement agents. I believe this role is important because it will affect, fundamentally, how colleagues and other staff in the company view and react to the compliance officer. If they see compliance officers only as whistle-blowers and snoops then they are likely, not only to avoid them, but to exclude them. Casting the compliance function in a proactive light shows the compliance officer as a partner, one concerned with the success of the project or enterprise.

Question 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 functions and if they are separate, how do they interact when dealing with compliance issues?

Answer: In my view the compliance and risk management functions are the same thing. Risk abounds in life and can be managed either pro-actively or reactively. Risk Management (I will rather call it risk planning) as defined in this paper is the main stay of the compliance function.

Question 3: Should a specific organisational structure for compliance be prescribed? Please explain.

Answer: No. This allows for flexibility and 'fit' on this matter. Each organisation, according to its size and the complexity of its business should be allowed to determine its organisational structure. The only requirement is that the preferred structure must lead to compliance with minimum acceptable standards.

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

I believe that certain key roles and responsibilities should be identified for the compliance function in general or broad terms. Failure to identify these minimum roles will make the compliance function largely ineffective and incoherent. Some of these key roles are

- Monitoring of compliance with applicable regulations;
- [Future] Risk Management;
- Training and sensitization of staff and customers on applicable rules and regulations;
- Notification of breaches of securities regulatory requirements (Internal & External Notification).

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

Answer: An example is Promotion of ethical behaviour among staff and colleagues.

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

Answer: Risk should be managed proactively. The compliance function should very early on be conscious of and work to eliminate or reduce probable risk as much as possible. This implies that it must be let in on any innovation in interpretation, design, process or product offering and on any significant modification of existing ways of doing business.

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

Answer: I believe that small firms with simple operation should be made to document policies and procedures. What will differ in their documentation vis-à-vis those of bigger organizations is the degree of detail specified. It will suffice to require that small companies with simple operations stipulate as their policy the twin goals of

(1) Protecting the interest of their client
(2) Preserving the integrity of the market.

Question 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.

Answer: Ours is a partnership. To that end, ultimate accountability for compliance with regulations rests on the partners. However, the primary responsibility for compliance in respect of issues arising from any instruction rests on the partner in charge of the brief.

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

Answer: No. The Nigerian Investment and Securities Act Cap 124 Laws of the Federation of Nigeria 2004 does not make the distinction. By S.253 of the Act, Responsibility Accountability and Liability are the same. This is as it should be. Recognizing any distinction will lead to evasion and laxity in compliance function.

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

Answer: Yes, this will ensure top management commitment to the compliance function. It will also give enough authority to the compliance officer in the discharge of his functions.

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

Answer: The following will be relevant

(1) A requirement of full and rank disclosure to all the partners of any securities transaction, potential and actual breaches and remedies planned or applied.

(2) Empowerment of employees in small and big firms. This will be by way of mandatory training and establishment of whistle-blower protection programme.

Question 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 regulators ensure that they supervise their own business activities in an objective manner?

Answer: On a day to day basis, it is better for individuals to supervise their own business activities than to ask them to be concerned with their neighbour's**.** The reason is obvious. There will be less interference and more work done. The individual's objectivity can be ensured by

(1) Tying some part of his compensation to achieving certain milestones on the compliance function.

(2) Prescribing sanctions for neglect or disregard of compliance issues

(3) Establishing an independent audit process.

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

Answer: No, they are not sufficient. Additional matters necessary to ensure independence include:

(1) A clear prescription

- a) For a separate budget for the compliance function
- b) That the budget must be such as to ensure reasonable effectiveness of the compliance function.
- c) To report to the Securities Commission the amount budgeted on compliance and its relationship to
  - i) The total firm budget
  - ii) The operations to be undertaken
  - iii) Previous years budgets
- d) Sanction for inadequate budgetary provision and awards for effective budgeting and compliance. These awards could come in the form of discounts and waivers on fees payable to the Securities Commission on transactions.

(2) Establishing whistle-blower programmes.

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

Answer: Undue influence can be avoided by

(a) Ensuring the remuneration of compliance officers are agreed to in writing.

(b) Establishing clear objective and achievable milestones and targets to which compensation and promotion are tied.

(c) Requiring consent of a second officer of at least the same rank as the compliance officer before his compensation is reduced

(d) Prescribing and enforcing sanctions for undue influence on compliance personnel.

Question 15: What are the appropriate qualifications for compliance personnel?

Answer: This will include

(1) A university degree or other professional qualification in a Post-graduate degree in law, Sociology or Business Administration

(2) Demonstration of good knowledge of securities regulations
(3) Good Character
(4) Leadership qualities

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

Answer: Yes

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

Answer: I will base my evaluation on the following parameters

(a) Relevance:- is the course relevant to specific compliance function?
(b) Emphasis (focus) what does the course aim to impact?
(c) Breadth of issues covered (Scope)
(d) Depth (Detail)
(e) Communication
(f) Duration

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

Answer: The external auditor has the best chance of an objective assessment of the compliance function, especially when he knows that his report will be sent to the regulator. An internal examiner will find it more difficult, I believe, to extricate himself from pressures prejudices and expectations, albeit subtle, that exist in the firm.

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

Answer: The role of an external party should be to

a) Gather all relevant facts relating to the compliance function as regards
   i) Qualification of compliance personnel
   ii) Their remuneration
   iii) Training attended during the year in review.
   iv) Independence of compliance function
   v) Processes and procedure in place to ensure compliance
   vi) Reporting channels
   vii) Measures available for preventive and remedial action
b) Assess the independence of the compliance function
c) Assess the effectiveness of the compliance function in terms of
   i) Awareness of rules and regulation by employees
   ii) Employees' awareness of the processes and procedures for ensuring compliance, prevention and report of breaches and obtaining remedial action.
d) Assess the accessibility of the Board and top management to compliance staff by evaluating the policy and structure in place.
e) Assess the independence of the compliance function.
f) Assess feedback/report mechanism for communication with top management, Board and regulators.

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

Answer: One of the matters of concern I envisage will be fees. The time and resources of the external auditors has to be paid for and in a country like Nigeria, it may be difficult getting a good audit on little or no fee.

The second matter flows also from it and from our experience of auditing generally. It is widely known that a significant number of the audits done in Nigeria are not thorough nor are the reports to be relied on by any serious minded appraiser. We believe that this is an issue that could also occur in the audit of the compliance function. Can we trust the auditor for a good appraisal? His integrity and judgement are key.

Another concern will be the accessibility/availability of Board member and top management to external audit staff. Will the external auditor be able to insist on meeting Board members and getting answers to his question?

Protection of confidential information is another area of concern.

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

Answer: An internal audit should be conducted at least twice yearly while an external audit should be conducted once in a year.

The scope of the two audits should basically be the same. The audit should cover all key issues and matters of concern to the compliance function.

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

Answer: The methods of monitoring that will be most effective in Nigeria are

1) Examinations by regulators backed by enforcement actions. People or companies in Nigeria are wont to take compliance as another of those requirements: in their view compliance will only be necessary if the (short term) personnel benefit outweighs the long term good to society. Most of the time this will not be so. Therefore enforcement actions are important particularly imposition of hefty fines.

2) External audits. See answer to question 18 for reasons.

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

Answer: The presence or absence of the following factors will show a strong or weak compliance culture:

- Frequent compliance training for staff
- Management willingness to take enforcement action on staff
- Establishment of clear and objective policies and
- Staff awareness of the compliance policy.

Culture is the way a people behave. And one of the ways of ascertaining that culture or way of life is to look at how they are trained, and the things that shape their world view. In the same way the factors listed above indicate the strength of a culture of compliance in an organisation.

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

Answer: I believe the means of implementation is adequate.

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

Answer: These issues include

a) Ascertaining applicable law
b) Identifying the supervising regulator in multiple jurisdiction transactions.
c) Harmonisation of the law of the home country of the intermediary and that of the place where the transaction is conducted
d) Co-ordination of the compliance function in more than one jurisdiction and
e) Harmonizing policies and processes – standardizing them while catering to differences in local circumstances.
f) Challenge of maintaining a strong compliance culture especially when there is significant business coming from countries were the culture is weak and suspension not robust. In this case the tendency to adopt a weak compliance culture particularly in the face of limiting bureaucracy is high.

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

Answer: Local compliance function is essential but it should report to a central chief compliance officer.

July 22, 2005

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

Dear Mr. Richard:

RE: Public Comment on *Consultation Report: Compliance Function at Market Intermediaries* ("Report")

On behalf of RBC Financial Group ("RBC"), we would like to express our appreciation to IOSCO for undertaking the global review of the compliance function at market intermediaries. We hope that this review will result in a harmonized, principle-based approach to the regulation of the compliance function.

In the body of this letter, we have responded thematically to the principles, means for implementation and some of IOSCO's questions set out in the Report. We have also answered some of the other questions in **Appendix A** to this letter.

General Comments

We support the principles and means for implementation outlined in the Report and their underlying intentions. The principles are consistent with what we see as the overall approach to the compliance function taken by other regulators of financial institutions. However, we believe the principles in their current form do not distinguish clearly enough between a market intermediary's overall responsibility for compliance management oversight and the duties of the compliance function itself. Although the principles appropriately outline the responsibility of the board of directors (the "Board") and senior management, there are several statements in the Report that could be read to imply that compliance is the responsibility solely of compliance personnel, rather than a matter for which the organization and all its employees in some measure have responsibility. The compliance function serves both as an independent oversight function and as a resource to assist the businesses in achieving compliance with applicable laws and regulations.

We believe market intermediaries should create a culture of compliance, an environment that puts high standards of behaviour first, top to bottom. Such a compliance culture empowers the compliance function so that it is viewed as a trusted partner to the business and not solely as a "watchdog." The role of the compliance function in that culture is to provide direction, advice, monitoring and reporting with respect to compliance matters. However, responsibility for day-to-day compliance should form a part of each employee's mandate.

RBC supports a principles-based approach to the regulation of the compliance function given the varying degrees of size and complexity of market intermediaries. This will provide market intermediaries the flexibility to determine how they will comply with the principles based on their respective sizes, business structures, complexity and requirements. In our view, through a principles-based approach, the Board and the senior management of market intermediaries will be able to focus on complying with the spirit or intention of the principles rather than focusing simply on meeting specific procedural requirements.

Definition of the Compliance function and its relationship to Risk Management:

We agree with and support the proposed definition and description of the compliance function, so long as it is read jointly with the means for implementation under the first principle of the Report. We encourage IOSCO to broaden the definition so that it incorporates the critical role played by the compliance function as outlined in the means for implementation and more accurately reflects the tasks normally undertaken by the compliance function**.**

Topic 1: Establishing a Compliance Function

We certainly agree it is necessary for market intermediaries to have a compliance function. In our view, the role of the regulator is to develop a framework that outlines in broad terms the roles, responsibilities and activities expected of the compliance function. The framework should foster compliance's independence and allow for the escalation of significant compliance matters without prescribing the frequency, scope or means of reporting. We believe that regulators should permit market intermediaries to determine their own compliance organizational structures within that framework, having regard to each market intermediary's size, structure, complexity, geographical locations, and the nature of its business. One concern we have with the Report is that, by its emphasis on organizational structures, it may imply that the Board and senior management can fulfill their responsibility for compliance simply by setting up a good compliance function and that the

compliance function is then solely responsible for attaining compliance. In reality, the business has a key responsibility for ensuring compliance with applicable regulatory requirements, which needs to be clarified in this part of the Report.

The following are our comments relating to the means for implementation that accompany this principle. First, in our view, what is meant by the requirement for the compliance function to "measure" key securities requirements is unclear. If the term "measure" is intended to mean "assess the regulatory risk associated with" key securities requirements, we agree with this means for implementation, and believe IOSCO should consider rephrasing this particular requirement accordingly.

Second, a number of the requirements set out in the means for implementation are activities in which we agree that the compliance function plays a key role, but we would like to see greater acknowledgement that compliance works in concert with the business in achieving them. For example, with respect to policies and procedures, compliance determines which regulations apply to which market intermediaries, works with the business' legal advisors to decide on the proper interpretation of those regulations and how to apply them to the business, develops and communicates appropriate policies and then works with the business to create the appropriate controls to implement them. Compliance also has a key role in measuring the effects of any compliance problems, in the escalation of compliance issues and in their resolution. While this includes notifying regulators of any material breaches identified and facilitating communications with the regulators, we believe it would be helpful also to note the responsibility the business in this regard.

Further, we support 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.

Topic 2: Role and Responsibilities of the Board of Directors or Senior Management

We agree with the principle as stated in the Report. To the extent that specific roles and responsibilities are assigned to the Board and/or senior management, we agree with the means for implementation as outlined in the Report. Where regulators have imposed a certification requirement relating to compliance of a market intermediary, this certification should not be provided by the compliance function but rather by the business (i.e. senior management). It is our view that regulators should not prescribe the means a market intermediary utilizes to assess its compliance for the purposes of certification. It is our view that market intermediaries should be permitted to choose the method of compliance review best suited for their particular businesses.

Topic 3: Independence and Ability to Act

RBC supports a compliance framework that facilitates the independence of the compliance function, allows for the designation of specific designated senior compliance officers for the business, and provides compliance (and specifically these designated officers) access and the ability to report directly on significant matters of compliance to the Board or senior management. We agree with the intention of the means for implementation to ensure that the compliance function has unrestricted access to the Board and senior management to discuss significant compliance matters. We would like to suggest that the reference to compliance "personnel" be replaced with the term "function" in order to be consistent with the principle relating to the responsibility of senior management and to allow for access through a designated senior officer.

With respect to compensation of the compliance personnel, we believe it would be incumbent on the market intermediary to achieve the right balance in its compensation plans to ensure a level of objectivity is maintained when proposed business initiatives add regulatory risk to the firm, and to minimize the potential for conflicts of interest.. Recognizing the importance of compliance's relationship with and knowledge of the business, however, we suggest that the term "improper" used in the principle be replaced with the term "undue", to avoid an unnecessary negative connotation regarding the interaction between compliance and the business.

Topic 4: Qualification of Compliance Personnel

We agree with the principle and most of the means for implementation as stated in the Report, but we do not believe that ***all*** compliance personnel must necessarily complete prescribed examinations. Qualifications of compliance personnel should vary according to function and seniority. While it may be appropriate for regulators to require the completion of prescribed examinations for the chief compliance officer and certain other roles within market intermediaries, we believe the framework for proficiency requirements should allow the market intermediary to take into account an officer's industry experience in lieu of examinations, when appropriate. Any minimum proficiency requirements established by regulators should emphasize industry experience.

Topic 5: Assessment of the Effectiveness of the Compliance Function

We agree with the Report that the compliance function should be assessed for effectiveness. In this regard, please see our responses in **Appendix A** to specific questions relating to this principle.

Topic 6: Regulator Supervision

We agree with the principle relating to the supervision of the compliance function by the regulators as outlined in the Report. We have given some responses in **Appendix A** to specific questions relating to this principle.

Topic 7: Cross-border Issues

RBC has numerous entities that operate globally and are subject to various regulatory regimes. The costs associated with reconciling conflicting regulatory requirements across jurisdictions are high. Furthermore, implementing a range of different processes to satisfy requirements that are essentially the same or largely similar in substance, but carry different procedural requirements, adds unnecessary duplication of processes and costs. In our view, the resources dedicated to these activities would be better spent strengthening the businesses' compliance function and undertaking proactive measures to prevent potential future compliance breaches. Some of the particular cross border issues faced by RBC and its subsidiaries are discussed below.

RBC and its subsidiaries face duplicative costs associated with meeting the registration and reporting requirements due to a lack of a unified global system of financial regulation. In addition, a global movement by regulators towards more regulation and additional enforcement has resulted in international firms facing ever-increasing challenges and allocation of resources just to keep up with technical compliance, rather than focusing on proactive management of regulatory risk.

Market intermediaries are also required to incorporate in each jurisdiction in order to ensure that each regulator retains jurisdiction over that market intermediary. This further increases the costs of doing business and the inefficient use of capital. In many jurisdictions, market intermediaries must set up back office operations to meet the local regulatory requirements, thus further increasing the cost of doing business.

To balance the goals of investor protection and the maintenance of efficient and effective capital markets, we would suggest that regulators place greater reliance on bilateral memoranda of understanding among the regulators and/or other joint guidance or requirements, such as those proposed in the Report. In our view, this approach will assist in alleviating the burden on market intermediaries to meet the various regulatory requirements without compromising investor protection.

Thank you for providing us with the opportunity to comment on IOSCO's proposal. We look forward to continuing the dialogue with IOSCO to formulate a consistent global view of the role of the compliance function at market intermediaries. We fully support principles which result in the establishment of the appropriate roles and responsibilities of the Board, senior management, compliance function and business, while at the same time allowing each market intermediary the flexibility to design a function that is unique to the nature, scale and complexity of its businesses.

Very truly yours,

cc: Peggy Dowdall-Logie, Head, Global Retail Securities Compliance & Personal Trust (Canada)
RBC Financial Group

Dave Lang, Head, Global Institutional Securities and Capital markets Compliance
RBC Financial Group

Toni Ferrari, Head, Policy Development & Implementation, Enterprise Compliance Management
RBC Financial Group

Randee Pavalow, Director, Capital Markets, Ontario Securities Commission

Appendix A:

Introduction

Q2: 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?

The relationship between risk management and compliance depends on the firm, its size and complexity. In our view, risk management and compliance are intricately linked. At RBC, where compliance is part of the risk management function, risk management focuses on identifying, assessing and managing many different business risks (e.g. credit, market, liquidity), including, through the compliance function, regulatory and compliance risk and the associated reputational and operational risks.

Topic 2

Q9: Do you distinguish among responsibility, accountability and liability? Please explain.

It is our opinion that the distinction between responsibility, accountability and liability is as follows:

Every employee is responsible for compliance;

The Board is ultimately accountable for a firm's compliance through senior management by setting the tone and compliance culture, and establishing policies, procedures and controls designed to ensure compliance with regulatory requirements; this accountability is usually delegated appropriately throughout the organization to appropriate members of the management team (including the compliance function); and

Liability is imposed by the applicable law and applies to all involved in executing business: Board, senior management, compliance and business personnel, as it pertains to each of their roles.

Topic 5:

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

The response to this question will depend on the size and complexity of the business. In multi-national firms with well-established and independent Internal Audit functions, we believe that Internal Audit is in the best position to evaluate the effectiveness of the compliance function. In addition, larger firms may also have established Risk Control Self Assessment programs or Internal Control Review processes to identify gaps internally. Some of the challenges to having external parties making such assessments include:

Increased costs for market intermediaries, which may be particularly prohibitive to smaller entities;

Lack of consistency in standards applied by external parties in the evaluation of the compliance function at various market intermediaries;

An increase in the examination burden on the market intermediary, in addition to internal and regulatory audits;

Availability of external parties with right knowledge of the business and regulatory compliance requirements and qualified people to effectively conduct a proper assessment of the effectiveness of compliance.

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

We believe that a risk-based approach taking into consideration the size and complexity of the business is appropriate to determining the scope and frequency of review. Given the multitude of regulations, review of the various components of regulatory requirements and of the compliance function's role in oversight or day-to-day monitoring of requirements should be staggered.

Topic 6

Q23: What factors are indicative of a weak compliance culture? Please explain.

Indicators of a weak compliance culture within the firm culture may include:

a high number of compliance breaches and repeat occurrences of such breaches;

numerous law-suits;

a large number of client complaints;

lack of clearly stated policies and/or procedures;

lack of willingness of senior management to add compliance personnel when necessary;

lack of resources for compliance training;

failure to include compliance in the discussion, assessment and implementation of proposed business initiatives;

lack of direct reporting between compliance and the Board; and

high employee turnover in the compliance group.

SECURITIES & DERIVATIVES INDUSTRY ASSOCIATION

Level 3
95 Pitt Street Sydney
GPO Box 3655 Sydney NSW 2000
Telephone: (61 2) 9776 7911
Facsimile: (61 2) 9776 4488
Email: info@sdia.org.au
Web: www.sdia.org.au
ABN 91 089 767 706

14 July 2005

Mr Philippe Richard
Secretary General
International Organization of Securities Commissions
Oquendo 12
28006 Madrid
Spain

By email: mail@oicv.iosco.org

Dear Mr Richard,

Compliance Function at Market Intermediaries
Public Comment on the Consultation Report by the Technical Committee of the International Organization Of Securities Commissions
April 2005

The Securities & Derivatives Industry Association is the peak body representing the interests of market participants in Australia. SDIA was formed in 1999 at the time of the demutualisation of the Australian Stock Exchange. Currently we have 65 Principal Member organisations that account for some $2.5b worth of trading daily on the ASX that accounts for approximately 98% of the market. Our member firms range from small domestic stockbroking businesses, to subsidiaries of major international banks and brokerages. In addition we have over 1300 individual members and are working to build the profession of stockbroking. Our member firms employ in excess of 8,000 people.

SDIA is pleased to participate in this review by the Technical Committee. After consultation with our Members, we would like to set out comments on the questions in the Consultation Report. In doing so we adopt the numbering scheme of the Report.

Part I. Introduction

Specific Questions for Comment

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

The definition and description of a *compliance function* that is proposed in the Consultation Report is:

> *A function that, on an on-going basis, identifies, assesses, advises on, monitors and reports on a market intermediary's compliance with securities regulatory requirements, including whether there are appropriate supervisory procedures in place.* (Report p.6)

While the above definition is useful and reasonable, we note that there are already a number of definitions and guidance that apply to our Members' businesses.

In Australia, our Principal Members, as market intermediaries, must be licensed by the Australian Securities and Investments Commission (ASIC, a member of IOSCO), under the requirements of the *Corporations Act (Cth) 2001*. Under the *Act*, each licensee must, among other things,

- comply with the conditions on the licence;
- comply with the financial services laws; and
- have adequate risk management systems… [23]

Our Principal Members are also recognised by the Australian Stock Exchange (ASX) as Market Participants. As such, they are subject to the *ASX Market Rules*, which include the following management and supervision requirement:

> *[A Market Participant] must have appropriate supervisory policies and procedures, and meet any standards or requirements set out or referred to in the Procedures, to ensure compliance by [the Market Participant] and each person involved in its business…with these Rules and the Corporations Act.*[24]

ASIC has published guidance on its view and expectations of the compliance measures licensees should have in place[25]. Some of the salient points of that guidance are:

- structurally, the compliance function may be separate, even outsourced to a third party, but this separation may not always be appropriate, especially for smaller licensees[26]
- whether or not the compliance function is separate, a director or senior manager should have responsibility for overseeing the compliance function and reporting to the governing body (to which that person should have ready access)[27], and
- the compliance function must be independent, adequately resourced and have adequate access to records[28].

While accepting that departures may be appropriate, ASIC makes particular reference to the *Australian Standard on Compliance Programs* (AS-3806-1998). It is a '…useful benchmark…' that ASIC expects licensees to use as a guide to implementing compliance measures.[29]

The *Australian Standard on Compliance Programs* contains **structural**, **operational** and **maintenance** elements.

Key **Structural Elements** in the Standard are management responsibility and resourcing of the compliance function:

M a n a g e m e n t R e s p o n s i b i l i t y

Compliance is the responsibility of line management. Compliance issues should be formalised as part of the position descriptions of Key personnel and included in their performance evaluations.

Resources

Adequate resources are necessary, at the appropriate levels of management, to implement the compliance policy. The Compliance Manager must have ready access to the CEO and compliance

---

[23] *Corporations Act* s.912A(1)(b), (c) & (h)
[24] *ASX Market Rule* 3.6.3
[25] ASIC *Policy Statement 164*, Part C
[26] ASIC PS164.51
[27] ASIC PS164.52
[28] ASIC PS164.53
[29] ASIC PS164.54

and audit committees.[30]

Operational Elements of the Australian Standard stress the need for adequate internal monitoring and reporting of compliance issues, and appropriate remedial measures where breaches are detected, including documentation, training, and disciplinary measures[31]. Management's responsibility in this area is also stressed.

Maintenance Elements include education and training, communication, and monitoring and assessment.[32]

At the industry level in Australia, there is also guidance as to the definition and role of the compliance function and those who work in it. **The Australian Compliance Institute** is '…the peak body for the development and practice of compliance and the integration of compliance, ethics, governance and risk into the fabric of organisations to help develop a dynamic, robust and compliant culture.'[33] The Australian Compliance Institute describes Compliance, and the role of Compliance Professionals, as follows[34]:

> ***Compliance***
> *The discipline of organisational compliance can be defined as the provision of services that facilitate an organisation identifying and meeting it primary obligations whether they arise in a legal, regulatory, contractual, industry standard or internal policy context and building an organisational culture capable of sustaining compliance with these obligations. The primary responsibility is to the Board of Directors.*
>
> ***What do Compliance Professionals do?***
> *The primary responsibilities of a compliance professional are founded in the* social and business expectation *that organisations will be managed in a way that meets the legal requirements. Compliance management systems form one of the primary platforms for strong corporate governance. The compliance professional's responsibilities can therefore be stated as follows:*
>
> - *primary responsibility to the **Board** to ensure that the organisation has a compliance management framework that is effective and efficient and deals with key compliance risks to the organisation. This is a responsibility that is **independent** of the business requirements and goes to good corporate governance practices. There is an emerging trend for Boards to create Compliance Committees separate from the audit function.*
> - *a responsibility to the **Senior Management** to assist them in understanding the regulatory and legal obligations from a practical perspective, identify risks and develop appropriate management systems and operational procedures to deal with those risks.*
>
> *If there is a conflict between compliance requirements and business objectives, it is the compliance professional's responsibility to assess the commercial and legal risks of non-compliance objectively and ensure that the Board and Senior Management are advised of these risks. It is the responsibility of the Board and Senior Management to determine how the compliance risk is to be managed. There should be an independent reporting line between the Board and the Compliance Professional to assist in escalation of these types of issues.*
>
> *The key objectives of a compliance professional in relation to their organisation are as follows:*
>
> - *To assist the Board and the Senior Management in the* development of an organisational culture *that proactively supports compliance activity and to provide current information to the organisation about the "philosophy" of compliance practices and how it is being implemented within an organisation.*
> - *To design and assist in the establishment of a* compliance management framework *that:*
>   - *identifies relevant compliance requirements and understands the risks involved;*

---

[30] AS3806 Pt. 1.3&1.4
[31] AS3806 Pt. 2
[32] AS3806 Pt. 3
[33] ACI Website, as of 27 June 2005
[34] *ibid*

- *codifies the compliance requirements into policies, procedures and controls;*
- *ensures appropriate levels of staff knowledge about compliance requirements;*
- *monitors the effectiveness and efficiencies of compliance procedures and controls; and*
- *provides relevant and appropriate reporting procedures for compliance issues.*

- *To provide commercial / practical insight into regulatory and legal compliance requirements that align with business objectives and to generate flexible and innovative solutions to the achievement of compliance requirements within the operational context.*

Accordingly, there has already been much thought here and no doubt overseas devoted to the role of the compliance function.

Our Members see that a pivotal role of the compliance function is interpretation and interpolation, in particular:

- to interpret legislation, regulation, policy directives, industry rules and standards in the context of the market intermediary's business, and
- to translate the requirements into language that all staff within the business will comprehend.

In addition, the compliance function acts as a 'regulatory radar' detecting new or changing requirements on the regulatory landscape, and keeping management abreast of regulatory developments, assessing their relevance and significance.

There is no lack of existing guidance on the definition and description of *the compliance function*. Accordingly, the need for a definitive definition of the compliance function may be over-stressed. Our Members prefer a flexible, high-level, principles-based definition that acknowledges the differing size and nature of market intermediaries' businesses, stresses the advisory role of the compliance function and the overall management responsibility for compliance. This approach has proved to be effective in Australia, both in adapting to the complex and ever-changing world of the financial markets, and in protecting the interests of investors.

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?

As noted above, Australian market intermediaries have a positive obligation under their licences and the Law to have proper compliance and risk management measures in place.[35]

Across the Australian stockbroking industry, there are different structures for the structure of the compliance and risk management functions, and the relationships between the two. Regulatory and legal risk tends to be the main focus of the compliance function. Risk management involves the assessment of risks to the business, which may include regulatory, legal and a variety of other risks as well.

Some firms have a separate compliance and risk management function. This is especially the case with the larger firms. Some firms have compliance and risk management in the same department, or the same personnel responsible for both.

In principle, the compliance function should be integral with the risk management function. In practice, this may be effected, for example, by having compliance representatives on risk committees. However, once again we would prefer to see a flexible approach continued here, rather than any mandatory requirements, for example as to structuring of the two functions.

Part II. Principles and Topics for Discussion and Consultation

[35] *Corporations Act* s.912A(1)(b),(c)&(h)

Topic 1: Establishing a Compliance function

Specific Questions for Comment

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

Consistent with our earlier comments, our Members are against a prescriptive approach to the structuring of the compliance function. This is the approach that underpins the current legal and regulatory framework in Australia, which we trust will continue.

Practitioners will always be more imaginative, practical and efficient than regulators in the structures they establish to achieve compliance outcomes. Manifestly, business operators understand their businesses and can take account matters regulators cannot possibly be cognisant of (for example, personality matters). Regulatory measures should be confined to establishing policies and outcomes utilising a 'principles-based' approach rather than being prescriptive on implementation matters.

Overly prescriptive regulation is as much a threat to the efficient and fair operation of markets as other deleterious factors. This is particularly so where compliance is costly or cumbersome for market intermediaries to implement, since those consumers who should be most protected are often ignored once the cost of doing business with them is assessed. By introducing prescriptive measures, regulators run the risk of disenfranchising the investors who most rely on the expertise of the market intermediary.

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

Our Members believe not. With a principles-based approach, businesses can decide what best suits the scope and size of their organisational structures. Businesses are so disparate in structure that any prescription will be inappropriate, inefficient or ineffectual in many instances. If regulators clearly define *what* is required, businesses will inexorably deal with *how* it will be achieved. In this respect, the more flexible – but no less effective - Australian approach is preferred.

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

The Compliance function in our Members' businesses carry out a range of the responsibilities discussed in answer to Question 1. above. The nature and extent of the responsibilities varies with the nature, size and extent of the relevant firm.

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

The compliance function should not be responsible for managing compliance risk if 'responsible' is intended to mean 'ultimately accountable for'. Consistent with the Australian requirements discussed at Question 1. above, it is the management of the business that should be 'ultimately accountable for' the management of compliance risk. However, the compliance function should have the expertise and opportunity to identify potential or actual requirements and compliance breaches – and make recommendations to business management for the mitigation of the risks.

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?

ASIC encourages licensees to document compliance measures, processes and procedures[36], and it is generally the case that policies and procedures are documented and published by way of compliance or procedures manuals in hard copy or accessible on an internal intranet site. ASX requires proper documentation policies and procedures to be in place to ensure proper management and supervision.[37]

Again, it is the outcome or attainment of policy objectives upon which regulators should focus. Businesses must be at liberty to determine *how* the objectives are met. Prescriptive edicts by regulators will only serve to stifle innovative methods businesses will devise to meet their obligations.

Part II Topic 2: Role and Responsibilities of the Board of Directors or Senior Management

Specific Questions for Comment

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.

There are a number of different models in our industry. Generally, across our 65 Member firms the Compliance function reports to senior management. There is no regulatory requirement to appoint a registered Compliance Officer, but as discussed earlier the regulators expect a sufficiently senior person to be responsible for the area.[38]

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

We once against stress, as per the *Australian Standard on Compliance Programs* discussed above, that compliance is a management responsibility. In terms of the question, we would distinguish as follows:

- The Compliance function is responsible for compliance.
- Management is responsible and accountable for compliance.
- The Governing board and/or owners are responsible, accountable and liable for compliance.

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

We would reiterate the flexible approach noted at 8. above.

Topic 3: Independence and Ability to Act

Specific Questions for Comment

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

The requirements need to be flexible and able to take into account the varying nature and extent of the securities business being operated. While a pristine structure would have the compliance function completely separate from the business, the realities of a small firm are that this may not be able to be achieved. This is acknowledged by the requirements which apply in Australia[39].

---

[36] ASIC PS164.138A
[37] see discussion of *ASX Market Rule* 3.6.3 at Note 2 above
[38] see discussion at Question 1 above
[39] see, *Addendum* to AS3806-98 on compliance programs for small business

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?

In relation to 'dual supervision', please see 11. above.

The regulatory response to 'dual supervision' should acknowledge that the means by which regulators can ensure businesses appropriately supervise their activities should be the same for small and large businesses. Any prescriptive differences will only create definitional problems on determining, for instance, what is a small or large business, or what is a simple or complex business. The key is a flexible, principles-based approach.

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

The means of implementing should not be prescribed. The principles approach is far more effective.

The important thing is that the compliance function possesses unfettered opportunity to monitor business activities and report on its observations with complete impartiality and independence.

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

While to some extent the level of remuneration of *all* employees, including compliance personnel, depends on the profitability of the business, compliance remuneration should not solely be dependent on the profitability of the business. Undue influence may be avoided by proper recognition and seniority of the compliance function.

Topic 4: Qualification of Compliance Personnel

Specific Questions for Comment

15. What are the appropriate qualifications for compliance professional?

Once again, consistent with our flexible approach, no such qualifications are mandated in Australia. Our Members prefer a flexible approach. Compliance personnel should possess both business and compliance training. Some of the most effective compliance personnel emerge from the business, due to their wider understanding of the business. Recently the Australian Compliance Institute has launched an accreditation program for compliance professionals, but our Members do not see prescription as necessary. .

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

While it is reasonable to expect that people are appropriately trained, our Members do not believe in a prescriptive approach. If they were prescribed at all, it should be left to industry bodies to define and recommend them in collaboration with the regulator.

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

Industry bodies such as SDIA and the ACI should evaluate the adequacy of courses and training in conjunction with regulators and providers of educational services (for instance, in the way that ASIC recognises overseas accreditation and training of retail advisers under ASIC *Policy Statement 146*).

Topic 5: Assessment of the Effectiveness of the Compliance Function

Specific Questions for Comments:

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

This would vary across our membership. Some are audited by internal or external auditors or assessors. For some, the assessment is properly carried out at Board or Senior Management level.

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

To determine, through sampling or other measures, if the business has measures in place to effect compliance with the relevant regulatory requirements.

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

External assessments (if required) would be extremely time consuming and expensive and can be a strain on busy compliance staff (and business practitioners). Due consideration should be given to ensure that the timing of audits are not overly disruptive (for example, they should not coincide with financial year end or festive seasons), and that requests for information are "clear, concise and effective". Auditors should have an unambiguously articulated charter for the conduct of each audit. Draft audit results should be presented to businesses for clarification and comment prior to settling final reports.

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

Internal or external assessments if required should be entirely at the discretion of the compliance function. These should be mapped out in some sort of annual plan but should also accommodate the need for particular reviews where specific weaknesses or actual breaches are discovered.

Topic 6 Regulators' Supervision

Specific Questions for Comments:

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

At the outset, it should be made clear that the number of bodies conducting audits should be held to a minimum. The paper suggests that self-regulatory organisations should be involved in assessing the compliance measures at market intermediaries. This, on top of internal audits, independent third-party assessments and regulatory assessments is excessive.

The methods of monitoring should be a matter for the regulators. However, like external third-party auditors, regulators should be subject to the same kinds of principles and considerations.

Regulators must remember that external audits are extremely time consuming and expensive and can be a strain on busy compliance staff (and business practitioners). Due consideration should be given to ensure that the timing of audits are not overly disruptive (for example, they should not coincide with financial year end or festive seasons or indeed – as our Members have recently experienced in Australia – at the same time as reviews by other regulators), and that requests for information are clear, concise and effective. Regulators should not simply trawl for data – especially where it is incumbent on the business to prepare expensive forms or to assemble information that is not readily available.

Where industries are regulated by multiple authorities (for example, in Australia, where our Members are regulated by the Government agency, ASIC, as well as ASX), due consideration should be given to ensure concurrent reviews do not overwhelm businesses.

While a non-compliant business is a threat to some investors and some market activity, a poorly performing regulator is either irrelevant, expensive or dangerous to an entire industry. As such, regulators should have clearly articulated objectives by which they can be measured. Their performance against results should be examined by either an independent third party, a statutory body or the legislative body itself.

One particular type of practice that should be subject to critical examination – both in terms of its ethical basis and efficacy – is that of 'shadow shopping' (where 'real' consumers are deputised to seek investment services to assess the intermediary's responses). In ethical terms, these types of campaigns by regulators tend to merely reinforce weary stereotypes. Moreover, the extrapolation of the results of a handful of such reviews across the whole industry is potentially misleading or incorrect. It is *not* the role of regulators to help undermine investor confidence. It is their role to help ensure the integrity and efficiency of markets. Furthermore, the use of inexpert 'consumers' used as inexpert auditors may provide inexpert feedback. The lack of rigor associated with such practices may produce results which lack fairness and accuracy.

Rather than exclusively focusing on unconstructive methods and outcomes, regulators might do well to find out what *does* work, what *does* help investors and what *does* promote safe and effective investment environments. Among many things, this might include:

- **education** of investors (e.g. how markets work; how products work; what strategies work; what the risks are; what to expect from service providers; what are the rights and obligations of investors); and

- **surveys** of investors (e.g. what forms of disclosure work?; what rules and laws are helping?; what do investors really want from their market intermediaries?; what concerns or fears do investors have?; how well do investors understand the risks associated with their choices?)

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

Indicators of a strong compliance culture include:
- compliance assessments built-in to all new business proposals
- priority to compliance issues, resourcing and function
- lines of communication open to the compliance function
- clear and concise compliance procedures
- compliance function seen as an adviser not a policeman.

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

See above.

Topic 7 Cross-border issues.

Specific questions for comment

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.

Several of our Members are subsidiaries of international groups, or themselves operate in foreign jurisdictions. In these cases there can be dual regulation without mutual recognition of requirements by the regulators. This leads to different requirements of the 'parent' jurisdiction being applied in another jurisdiction where the parent and the home have different requirements. If additional requirements are imposed on the international firms, this may lead to domestic firms having a business advantage over international firms in terms of compliance burdens.

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?

A number of Members have overlapping requirements which are addressed by local and centralised (firm-wide) compliance functions.

SDIA is pleased to have had this opportunity to provide information to assist the work of the Technical Committee, which we appreciate may influence our local regulatory requirements.

Should you require any further assistance, please contact me by email: dhorsfield@sdia.org.au , or Doug Clark, Policy Executive, dclark@sdia.org.au .

Yours sincerely,

David Horsfield
Managing Director / CEO

SECURITIES ASSOCIATION OF SINGAPORE

IOSCO Questions

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

Yes. Definition is comprehensive, covering the key areas of monitoring, identification and prevention of breaches.

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?

The compliance function focuses on compliance with regulatory requirements while risk management is more of an internal monitoring system of business risks. In the Singapore context, most broking houses keep these two functions separate although in some cases, they may ultimately report to one divisional head. The compliance function usually reports to the MD and the Board of Directors while the risk management function reports to Credit Control and the Risk Committee. Ultimately, the CEO presides over both compliance and risk management responsibilities.

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

No. This is to provide flexibility for different types of organizational structures and ownership structure. For example, broking firms which are owned by bank holding companies will have a different compliance structure from those which are autonomously owned.

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

No.

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

None. The responsibilities outlined in the Consultation Paper are already sufficient.

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

The compliance function should be both proactive and preemptive. It should identify potential risk areas and anticipate the likelihood of various types of violations rather than wait for violations to occur before safeguards are put in place. The management of the compliance risk function should be

risk-based, i.e. each institution should have to assess the relative importance of each type of risks and determine the necessary frequency of review for each type of risks.

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 broking firms are expected to meet the same standards of compliance regardless of size. As such, the major practical concern for the smaller broking firms is that the cost of compliance is relatively higher for them.

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.

If a failure to comply is spotted, the MD/CEO is the first to be informed. The next level of accountability is the audit committee and then the Board of Directors. Appropriate actions/decisions are taken at each level.

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

Although the compliance function is a shared responsibility between the staff in the compliance department and the management of the firm, the ultimate responsibility, accountability and liability rest with the CEO

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

Yes. This is for ease of operations and practical convenience.

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

The consolidation of the broking industry from 32 firms in 2000 to 21 firms currently has seen the disappearance of many small firms from the broking scene in Singapore. The problem of independence and ability to act in small firms is therefore no longer a significant issue in the Singapore context.

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?

More appropriate for regulatory body to respond.

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

More appropriate for regulatory body to respond.

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

The budget and compensation of compliance departments are not linked to business performance, unlike the compensations of staff employed in dealing and sales.

15. What are the appropriate qualifications for compliance personnel?

Compliance staff should enrol for Modules 1-5 of the CMFAS (Capital Markets and Financial Advisory Services) conducted by the Institute of Banking and Finance. In addition, they should have some knowledge of the business of stockbroking; some legal background would be an advantage.

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

Yes. Senior staff should have both experience in Compliance Supervision and detailed knowledge and understanding of the rules and regulations governing stockbroking activities. Qualifications for entry level positions are less demanding.

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

Courses are evaluated based on such criteria as objectives, relevance and suitability. General courses on compliance are not available, hence most training is provided in-house. Various agencies offer training on specific topics like corporate governance and money laundering. They are assessed based on their own merits and relevance and the credentials of the person conducting the course.

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

The regulatory authority is best placed to assess the effectiveness of the compliance function as it has the industry overview and can therefore make inter-company comparisons. It can undertake this function as part of its normal inspection/supervision.

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

One of the key roles would be to identify the weaknesses in the existing systems and to recommend improvements and further safeguards.

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

The external party (such as an external auditor) may not be familiar with the operations and systems of the firm and a great deal of time is spent familiarizing the external party with these operations and systems. Moreover, lack of continuity of the staff undertaking the periodic assessment often requires the firm to familiarize the new staff all over again each time when the next assessment takes place.

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

The Compliance function should be subject to periodic review. The scope and frequency will depend on the relative importance of each area of compliance as determined by the significance of the risks involved and the frequency of assessment will depend on the cycle of inspection for each area.

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

More appropriate for the MAS to respond.

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

More appropriate for the MAS to respond.

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

More appropriate for the MAS to respond.

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.

First and foremost, the operating unit in each country has to ensure that it meets the compliance rules and standards of its own jurisdiction. If there are compliance requirements from the HO regulator to be met, the overseas unit may have to undertake additional compliance supervision. Such instances are rare.

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?

Only significant breaches need to be reported to the Head Office. Some firms have a system of weekly reporting of breaches.

SECURITIES ASSOCIATION OF SINGAPORE

3 June 2005

Securities Industry Association
120 Broadway - 35 Fl. • New York, NY 10271-0080 • (212) 608-1500, Fax (212) 968-0703
1425 K Street, NW • Washington, DC 20005-3500 • (202) 216-2000, Fax (202) 216-2119
www.sia.com, info@sia.com

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

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

Dear Mr. Richard:

Thank you for giving the Federal Regulation Committee of the Securities Industry Association ("SIA")[40] the opportunity to comment on the above-captioned consultation report (the "Consultation Report" or "Report"). Broker-dealers in the United States have devoted significant resources over many years in developing robust compliance programs, both to fulfill regulatory requirements and as a good business practice. We applaud the International Organization of Securities Commissions ("IOSCO") for undertaking this initiative to assist market intermediaries to increase the effectiveness of their compliance programs.

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

Overview and Summary.

The role and purpose of the compliance function in the United States is rapidly changing and expanding, as it is in other nations. For example, the National Association of Securities Dealers ("NASD") recently issued a set of new rules detailing a host of new process requirements and standards for broker-dealers' compliance efforts.[41] Other initiatives by the SEC and state regulators have also recently changed the

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

[41] The new NASD initiatives include, *inter alia* (1) a new rule requiring member firms to designate one or more principals to establish, maintain, and enforce a system of supervisory control policies and procedures that

compliance landscape.[42] These changes prompted SIA's Compliance and Legal Division to recently issue an extensive White Paper on the Role of Compliance ("White Paper"). The White Paper, a copy of which is attached to this letter, focuses on many of the issues raised in the Consultation Report. In particular, the White Paper discusses the scope and responsibilities of compliance departments in U.S. broker-dealers, and the distinctions between (a) general efforts by firms designed to achieve compliance with securities regulatory obligations, and the specific functions of compliance departments in support of those goals, as well as (b) management's responsibility to supervise, and the monitoring and surveillance role of compliance departments. Because of the diversity of the broker-dealer community in the United States, in terms of size, resources, and lines of business, both the White Paper and United States regulators recognize that regulatory requirements for broker-dealer compliance programs have to be flexible.

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

1. We urge IOSCO to adopt a principles-based approach to the requirements for a compliance function. This approach should focus on the characteristics of a sound compliance organization as opposed to cataloguing prescriptively specific requirements or steps that firms must take. We believe that in many respects this will address the need for flexibility described above, as well as the following issues.[43]

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

A related issue is the Consultation Report's view of the independence of the "compliance function." While we fully agree with the principle stated in Topic 3, the suggestion that the "compliance function . . . should

---

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

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

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

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

2. Compliance and supervision are distinct and separate concepts in the regulatory scheme in the United States, which provide that the supervisors in the business are responsible for implementing and enforcing all firm policies and procedures.[44] Except in rare instances, having compliance responsibility should not imply having supervisory responsibility. The Consultation Report recognizes this in principle (a) under Topic 2, yet it conflates the two in some places, especially Appendix A.

3. The Consultation Report appropriately defines the role of the "compliance function" under principle (b) of Topic 1, yet in several other places it describes the role of compliance as being "to ensure" compliance with all applicable legal requirements. It would be more consistent with Topic 1 principle (b), and more consistent with U.S. law, to describe the role of the compliance function as being to develop and implement systems and procedures reasonably designed to achieve compliance. This clarification is critical to make the Consultation Report both internally consistent, and consistent with well-established supervisory principles and regulatory standards in the United States.[45] Moreover, as a practical matter, firms need to deploy surveillance resources in a risk-based and cost-effective manner, and any implication to the contrary could create unrealistic expectations by regulators or investors.

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

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

Responses to Questions.

---

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

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

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

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

First, except for the risk management function, the Consultation Report does not explicitly recognize that these compliance functions can, and usually do, reside in several locations within a firm in addition to the compliance department. It is important to note that the "compliance function" must be fulfilled by more than one arm of a firm. Depending on a firm's size, organizational structure and type of business, both Compliance Department reporting lines and the allocation of compliance-type functions can vary. Consequently, it is not uncommon for professionals outside a Compliance Department to have responsibility for many of the "Compliance Functions" to which the Consultation Report refers. For example, as a matter of practice, oversight of a firm's activities relating to the firm's financial controls and compliance with regulatory financial reporting requirements usually reside with the broker-dealer's Controller, Chief Financial Officer or Treasurer, and may be reviewed by the Internal Audit Department. Similarly, a member firm's systems and procedures for assuring compliance with margin regulations and the clearance and settlement process is typically the responsibility of the firm's Chief Operations Officer. In addition to the compliance department and risk management department, other groups that typically carry "compliance functions" include the comptroller's or treasurer's office, the legal department, the credit, finance, internal audit and operations departments, and in some firms the human resources department. In addition, in many firms, control function officers with specific monitoring and surveillance or financial control responsibilities are often located within individual business units.[46]

Second, the definition and description also does not draw a clear distinction between the compliance function and supervision. As explained in the White Paper, there is a huge difference between the role of the Compliance Department and its personnel, and the overall broad firm responsibility 'to comply' with applicable rules and regulations. "The Compliance Department plays an integral support function for firm compliance programs, but only senior management and business line supervisors are ultimately responsible" for the effectiveness of the firm's compliance program.[47]

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

Mechanisms Regarding Customer Activity. SIA respectfully disagrees with one aspect of the description of the scope of a compliance function, the statement on pages 6-7 that "[a] compliance function of a firm should also have mechanisms in place to protect the firm from any liability arising from abuses committed by its customers." Broker-dealers in the United States have a well-established obligation to "know their customers," as well as an obligation, imposed on all U.S. financial institutions, to look for and report on potential money-laundering activity. U.S. law also clearly proscribes broker-dealers from colluding with customers to violate the law.[48] However, the above-quoted statement is much broader, suggesting an open-ended surveillance/investigatory obligation of customer behavior, including behavior away from the broker-dealer, in case that customer's behavior in some respect could give rise to "any liability" for the broker-dealer because of

---

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

[47] White Paper at 20.

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

any "abuses committed" by a customer. Due to the fluid scope of private civil liability in the United States,[49] it will be difficult for a U.S. broker-dealer to rule out any prospect of liability for almost any conceivable transgression that a customer might commit that touches in some way upon the customer's account or relationship with the firm. Putting "mechanisms in place to protect the firm from any liability arising from abuses committed by its customers" is therefore unrealistic, and even if it were achievable would be extremely intrusive for customers, giving rise to a host of potential privacy concerns.

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

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

Answer: As this question implies, there is an overlap between the compliance function and the risk management function. Compliance risk has become an integral part of a firm's overall risk management program, and therefore compliance functions may be seen as integral to the organization's program for risk management.[50] Consequently, the White Paper recommends that Compliance Departments "should be alert to risk issues and, if identified, bring them to the attention of Risk Management and work with them in developing remediation steps."[51] Similarly, the risk management function should be informed of compliance risk issues identified by either the legal or internal audit departments. Generally, the role of the compliance function is to assist in development of policies and procedures designed to comply with regulatory requirements and to monitor and advise on the effectiveness of those policies and procedures. Risk management, which is typically closer to the business side, should help harmonize business practices, plans and objectives with these policies and procedures.

It is also important to note that the risk management function is often subdivided between specific activities, such as trading and financial exposure, as well as enterprise-wide risks.[52] These roles may each have their own individual relationships with the compliance function.

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

---

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

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

[51] White Paper at 19.

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

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

These illustrations demonstrate that firms need flexibility to design compliance structures that match their individual size and business model. For this reason, we are concerned that the suggestion in Topic 3 that the "compliance function . . . should report to the board of directors or senior management" will result in regulators becoming hostile to arrangements such as these noted above, even though they have evolved due to the practical requirements of individual firms and have proven effective. The critical point is that officers with ultimate responsibility for compliance functions should have direct access to the Board or senior management, since those individuals bear ultimate responsibility to see that compliance functions are carried out.[53]

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

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

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

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

Answer: Other responsibilities of the compliance function (though not necessarily the compliance department)[54] that are not specifically identified in the Consultation Report (although perhaps implicit in some of its discussion) include:

- Education and training to keep business personnel and other employees apprised of policies, procedures, and regulatory requirements. This training should involve both regularly scheduled updates as well as additional sessions on an as-needed basis to implement new policies or procedures or to communicate recent regulatory developments. The format of this training should be flexible,

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

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

and can include web-based or other electronic training modules as a supplement to in-person training, as well as enhanced training on an as-needed basis for business unit supervisors as well as for new hires;

- Licensing and registration of the firm and its registered personnel are another common compliance function, together with the related role of advising senior management on disciplinary issues, including terminations.[55] Some of these functions may be performed jointly by the compliance department and human resources department;

- Internal inquiries and investigations are a critical compliance function that is not explicitly addressed in the Consultation Report. This role can be played by any or a combination of several control functions within a firm, including the compliance department, the legal department, internal audit or other control areas. These inquiries sometimes involve the use of third parties such as law firms or forensic accounting experts if deemed necessary by senior compliance personnel;

- Monitoring and surveillance of business units to identify potential issues is another important area of the compliance function. This monitoring applies to, among other things, handling of customer accounts, proprietary trading, and employee-related trading and communications; and

- Participating in industry committees and working groups organized by industry trade associations such as SIA, or self-regulatory organizations such as the NYSE or NASD.

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

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

Answer: See answer 9 below.

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

Answer: See answer 9 below.

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

Answer: See answer 9 below.

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

Answer: We will answer questions 6-9 collectively, since they are all closely related. The role of the compliance function is to assist in designing compliance policies and procedures and to monitor, test and

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

advise on the effectiveness of those policies and procedures, rather than to "manage" compliance risk. The responsibility for managing (i.e., implementing and supervising) all aspects of the compliance function belongs to senior management.

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

Responsibility refers to an individual's duties within an organization. Accountability concerns how an organization tracks the performance of those duties and imposes consequences for successfully or unsuccessfully performing them. Liability refers to the regulatory or other legal consequences that can follow when responsibility or accountability break down. Responsibility can be delegated within a firm, and firms should be given wide latitude to delegate responsibility for compliance functions as they see best (as discussed in more detail in answer 1), but accountability and liability cannot be delegated.[56] Within a broker-dealer, these terms can be applied as follows: the board of directors and senior management are ultimately accountable, with respect to the entire firm. Business unit managers have accountability with respect to their particular units. Compliance officers are responsible for creating policies and procedures that are reasonably designed to achieve compliance. They are not generally responsible for implementation of these policies and procedures (except for specific policies where the compliance department has a specific role as executor) and some responsibility for monitoring implementation of the policies (often shared with business units).

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

Answer: Yes. In the United States, NASD Rule 3013 now requires firms to designate a chief compliance officer. However, senior management has the ultimate responsibility for establishing and maintaining a firm's overall compliance effort.[57] This is appropriate, since business line managers have the responsibility to oversee business operations, and the authority to control employee activity to achieve compliance with applicable regulatory requirements. In this regard, the Consultation Report should recognize the central role of senior management in ensuring an effective compliance program. For example, the statement on page 8 of the Report that the compliance function should "enforce effective compliance policies and procedures" could create the false impression that compliance personnel have the authority to discipline all other firm personnel. The ability to terminate or otherwise discipline employees is held by senior management, although compliance personnel often play an important advisory role on such discipline. Therefore, it would be more accurate to say that the compliance function "advises on the enforcement" of compliance policies and procedures.

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

Answer: Allowances should be made for businesses that are owned or operated by just a few people. For example, the NASD permits the compliance function to be performed by the business owner/principal if a firm

---

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

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

only has one such person. Regulators can ensure proper sales and business practices in a "one person" type environment in the same fashion they do for larger organizations - routine audits. It may be necessary or preferable for the audit cycle to be more frequent in this type of scenario to ally the fears and special challenges presented by self-compliance. Due to the size of the firm, the audits should be fairly short in term. In addition, at smaller firms the Chief Compliance Officer may have additional responsibilities.[58] However, supervisors cannot supervise themselves.

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

Answer: We agree that individuals performing both business and compliance activities should not have compliance responsibilities for their own business activities. This follows from the general principle that compliance should not report to a business unit.[59] However, the term "supervision" requires some refinement. There is an important distinction between having compliance responsibility and having overall business responsibility. The NASD, for example, has taken pains to note that compliance responsibility and business line supervision are separate concepts, with the latter "accountable for the discharge of a member's compliance policies and written supervisory procedures."[60]

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

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

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

(a) the budget for the compliance function and compensation for compliance personnel, while linked to the performance of the firm as a whole, should not be directly dependent on the financial performance or revenues of a specific business line, product or transaction overseen by that compliance function or employee;

(b) compliance personnel should have access to any employees, records and other information necessary to carry out their responsibilities; and

(c) compliance personnel should have unrestricted access to the board of directors and senior management to discuss significant compliance matters.[61]

We do not understand the meaning of the statement "The independence of the compliance function may also be undermined if the tenure (i.e., prospects of staff, position) of compliance personnel is dependent on

---

[58] *See* White Paper at 3-4.

[59] *Id*. at 3.

[60] *See* IM 3013, note 17, *supra*.

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

the business lines." If this means that independence is compromised if promotion decisions about anyone involved in compliance functions over a particular business unit can be made or influenced by that unit, we fully agree. If it means that compliance personnel are immune from hiring or wage freezes, or even layoffs and salary reductions, due to a downturn in the firm's overall business lines, then this statement is in conflict with the prior statement that compliance compensation can be dependent on the firm's overall performance.

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

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

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

15. What are the appropriate qualifications for compliance personnel?

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

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

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

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

Answer: The NASD and NYSE both have continuing education requirements.[62] Typically, a firm's compliance department will contribute to the development of the firm element of these requirements, and especially the training for compliance personnel. In addition, some firms have a dedicated position for compliance training, and part of this job function includes evaluating the adequacy of courses, including soliciting feedback from course participants.

---

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

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

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

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

Answer: See answer 22 below.

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

Answer: See answer 22 below.

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

Answer: See answer 22 below.

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

Answer: Since questions 19-22 are closely related, we will answer them collectively. Regarding an external review, the White Paper endorses an independent assessment of a broker-dealer's compliance department, and the Internal Audit Division of SIA has published a guide for conducting such reviews. In addition, there is a regulatory requirement that broker-dealers submit to an annual audit of their compliance with financial responsibility rules.[63] With regard to internal assessments, both the NASD and NYSE require firms to conduct annual assessments of their compliance programs, and the NASD requires that a firm's chief executive officer certify annually that the firm has processes in place to maintain and review compliance procedures and policies.[64]

Apart from these areas, a private external audit of the effectiveness of the compliance function is generally not necessary, since that is a function that the SEC, NYSE, NASD and other federal as well as state regulators perform through their examination programs.[65] The role of these regulators is to examine whether firms have established and maintained policies and procedures reasonably designed to achieve compliance with applicable regulatory requirements. These examinations should be conducted on a frequent basis, based on regulators' judgment of potential risks. Where multiple regulators have oversight of a broker-dealer, it is

[63] Exchange Act Rule 17a-5(d).

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

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

critical that they coordinate their examination programs and share information to avoid unnecessary duplication and inefficient use of both regulatory and internal compliance resources.

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

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

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

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

- Clear communication of compliance priorities to all employees by senior management;
- Sufficient resources devoted to build effective compliance systems;
- Creating incentive structures that reward compliant behavior and penalize behavior that sacrifices compliance principles;
- For firms that have complex organizations or multiple business lines, ongoing reviews of potential conflicts of interest among business lines, products and services, including the effectiveness of systems or procedures to manage or remove those conflicts;
- A willingness on the part of compliance personnel to identify problems independently, work on appropriate solutions to problems that are identified,
- Active participation in industry trade groups such as SIA that provide an opportunity to share best practices, discuss emerging issues, and help shape effective regulatory policy;
- Giving personnel with compliance responsibilities regular and unfettered access to senior management;
- Having procedures and processes in place to enable the compliance function to operate independently; and
- Having sufficient resources devoted to compliance activities.

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

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

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

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

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

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

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

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

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

Conclusion.

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

Sincerely,

Carlos M. Morales

Attachment

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

TD Bank Financial Group

1. ***Do you agree with the definition and description of the scope of a compliance function? Please explain.***
   In general, we agree with the definition. However, given that most large market intermediaries are active in areas that extend beyond the purview of securities exchanges (such as, derivative and structured products, or other off-exchange products), it would be appropriate for the definition to be consistent with the definition developed by other regulators (primarily, bank regulators).

   Post-Enron, regulators have focused on market intermediaries' controls around off-exchange products, as these are certainly considered higher risk, and the compliance function could also be expected to provide guidance and oversight for these activities. In the absence of specific rules and regulations from regulatory bodies, the compliance function could take the lead on establishing "best practice" guidelines for the firm by building on established concepts used for the regulated exchange-traded products (i.e. to ensure ethical conduct and the promotion of fair and orderly markets).

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?***
   Whether the compliance and risk functions are part of or separate is a matter that should not be prescribed, as organization structures will differ from institution to institution.

   However, we do agree that the two functions, if distinct, should work closely together to minimize the overall risk of the firm, whether it is a compliance risk, reputational risk, legal risk, or any other related risk.

3. ***Should a specific organizational structure for compliance be prescribed? Please explain.***
   No, as noted above, a specific organization structure should not be prescribed due to differences from institution to institution in how businesses are organized and the scope of activities carried out by the various intermediaries. However, we do agree that the overall firm compliance function in any organizational structure should be clearly independent of the business being monitored. Even if certain regulatory requirements mandate that the businesses monitor their own compliance with regulations (for example, trade entry, procedures to prevent "front-running", etc.), a separate independent compliance function should exist to monitor and oversee the business's compliance with regulatory requirements to ensure that the business 'self-compliance procedures' are conducted in accordance with regulations.

4. ***Are there any essential roles, responsibilities or activities for the compliance function that should be mandated or otherwise identified by regulators?***
   Given that all large market intermediaries are active in various product lines (such as derivatives, structured products, banking, securities underwriting and trading, etc.) and operate in multiple jurisdictions, it is difficult to mandate specific activities as it may result in conflicts with the specific requirements of different regulatory jurisdictions. Efforts to standardize the compliance requirements being developed by securities regulators and bank regulators are encouraged in order to avoid potential conflicts. In this regard, we would refer you to Principle 7 of the April 2005 Basel Committee on Banking Supervision titled "Compliance and the Compliance Function in Banks" (the "Basel Paper"), which lists the high-level functions of a compliance department as being: giving advice; guidance and education; identification,

measurement and assessment of compliance risk; monitoring, testing and reporting on compliance risk; and acting as a liaison with regulators.

The approach of providing "best practice guidance" via general principles would allow intermediaries in various jurisdictions to tailor the specific compliance roles and responsibilities to address the activities of the particular firm being monitored as well as the various regulatory jurisdictions in which it operates. In our view, the six high-level activities identified in section (b) (1), "*Means for Implementation*" appears adequate.

5. ***Please identify responsibilities other than those described above that are carried out by the compliance function at market intermediaries.***
The compliance function in our organization is also responsible for maintaining firm and staff registrations with the appropriate regulatory body, and for ensuring that a business supervisory structure is in place.

6. ***How and when should the compliance function be responsible for managing compliance risk?***
Managing compliance with regulatory and statutory requirements is the responsibility of everyone operating in regulated market intermediaries and particularly that of the business which is subject to the applicable rules. The compliance function cannot be solely responsible for managing compliance risk. Although the compliance function has an important role in managing compliance risk, it is unreasonable to expect the compliance function to ensure every transaction complies with every regulation. The compliance function's responsibility should be discharged primarily by ensuring that appropriate policies and procedures are implemented, in conjunction with an oversight process to ensure that those policies and procedures are being adhered to (and continue to be appropriate for the business activities being undertaken) by the firm's businesses.

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?***
N/A

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.***
We accept the responsibilities of the Board of Directors, senior management, compliance officers and business unit personnel set out in the Basel Paper.

9. ***Do you distinguish among responsibility, accountability and liability? Please explain.***
We agree with the view of the Securities Industry Association, which we understand to be as follows:

Responsibility refers to an individual's duties within an organization. Accountability concerns how an organization tracks the performance of those duties and imposes consequences for successfully or unsuccessfully performing them. Liability refers to the regulatory or other legal consequences that can follow when responsibility or accountability break down. Responsibility can be delegated within a firm, and firms should be given wide latitude to delegate responsibility for compliance functions as they see best. Accountability and liability cannot be delegated. Compliance officers are responsible for creating policies and procedures that are reasonably designed to achieve compliance. They are not generally responsible for implementation of these policies and procedures.

10. ***Should a senior officer be designated for the day-to-day compliance responsibility? Please explain.***
Yes. Given the importance for market intermediaries to continue to have the ongoing confidence of other market intermediaries, regulators and the public, the firm's compliance function should be headed by a senior enough executive to earn the respect and confidence of the various business leaders. The chief

compliance officer may have day-to-day responsibility via the development of appropriate monitoring processes however, where appropriate business leaders must assume responsibility for ensuring that staff under their supervision that must comply with regulations are appropriately informed of and in compliance with such regulations.

On a regular basis, the chief compliance officer's group should be actively reviewing ongoing business activities, new initiatives, entrance into new jurisdictions, etc. to ensure that detailed policies and procedures continue to be appropriate for the activities being undertaken and the clients / counterparties that the firm deals with.

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

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?***
No, individuals that perform both business and compliance activities should not be allowed to supervise their own business activities in isolation. Although certain regulatory authorities in Canada require the business supervisors to supervise their staff and do compliance work for many of their activities, this should be supplemented by active oversight provided by an independent compliance function. Inherent conflicts of interest exist when compliance officers are also responsible for other activities of the firm. Heightened supervision procedures, more frequent reviews and reviews by an external party may be required to manage these inherent conflicts.

13. ***Are the means for implementation of independence set out above sufficient to achieve independence? Please explain.***
Note: the reference to "… *means for implementation of independence set out above…*" refers to the four items noted in the document (p.17).

In addition to the four items noted in the paper, we would suggest adding in 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 which is outside of the business.

14. ***How do you ensure that compensation of compliance personnel is not subject to undue influence? Please explain.***
In a larger organization with various business segments (like for example, a Retail & Commercial Banking segment that is separate and distinct from a Wholesale Investment Banking and Capital Markets segment), the compensation of the compliance function staff should be tied to the results (net income, not revenues) of the overall firm and not to the specific results of a particular segment. Even if the compliance function is organized, whereby specific responsibilities are assigned for a particular segment, the overall direction and oversight of the group would be a centralized (i.e. Corporate) function, separate and distinct from any business segment.

In market intermediaries that do not have diverse segments, it is more difficult to achieve the clearly independent function since the corporate services areas (including compliance) will ultimately be responsible for only one business segment. In such circumstances it is important that the compliance function have a direct reporting line to the highest management level (CEO) and that compensation not be revenue driven. Note that where the compliance function reports into another independent function (like risk or legal), then that function would need to have the direct reporting line to the CEO.

15. ***What are the appropriate qualifications for compliance personnel?***
As a general comment, it would be appropriate for the Chief Compliance Officer (CCO) to have specific certification requirements. However, at the moment to the best of our knowledge, there are no specific internationally recognized accreditation standards. We would recommend that the IOSCO consider

developing more formal educational and accreditation requirements. The development of a standard syllabus and specific courses for CCOs and their staff would be desirable.

Qualifications required depend on the activities being monitored. If activities are subject to specific exchange regulations that require supervisory functions to pass certain courses, then the compliance staff closest to that direct activity should have the appropriate training, including where appropriate, achieving certain specific educational standards.

Relevant work experience should certainly be taken into consideration: knowledge of the products, market conventions, internal processes, etc. are important. However, it may still be appropriate for individuals at all levels of the compliance function to take and complete certain courses and / or examinations. Furthermore, the appropriate mix of staff of different backgrounds should be left to the determination of the CCO. Diversity of backgrounds among compliance officers is desirable, so staff whose backgrounds differ from those being supervised and from other compliance staff should not be disqualified from their jobs.

16. ***Should the qualifications vary depending on functions, responsibility or seniority?***
Yes, this makes sense. However, it is difficult to prescribe anything specific without also prescribing the necessary organization structure. Accordingly, this may best be left to the Chief Compliance Officer to define and implement the appropriate educational levels for individual staff dependent on the functions being monitored. The final determination should be reviewed and approved by at least the next level of management. The internal compliance function structure and qualifications could also be reviewed by external regulators for appropriateness, although we would not necessarily support an approval level determination by the regulators – i.e. having the regulator officially approve the internal compliance function organizational structure and qualification levels for all compliance staff.

17. ***How do you evaluate the adequacy of courses and training for compliance personnel?***
Given the current lack of specific courses or educational standards, the evaluation of available courses is done by the CCO on an ad hoc basis. As noted in response # 15 above, we would encourage the IOSCO to develop more formal standards and academic requirements, as well as develop specific courses to meet those requirements.

18. ***Who, within or external to a market intermediary, is best placed to assess the effectiveness of the compliance function? Please explain.***
Internally, the internal audit function or other independent internal control function should regularly review the compliance function against the mandate established by the Board of Directors. Other more detailed reviews can be performed to review specified compliance activities depending on the specific type of activities undertaken by the particular market intermediary.

Externally, the home jurisdiction regulator is best suited to assess the effectiveness of the compliance function. The home regulator (or its delegate self-regulatory organization) generally has a consolidated view of the firm and accordingly, should understand all of the market intermediary's activities in all jurisdictions where it is active. External regulators in each jurisdiction would have to determine whether to require a specific review of the compliance function by an independent external party

19. ***What should be the role of an external party in assessing the effectiveness of a compliance function?***
The level of external oversight required to assess effectiveness is a function of the size of the organization and compliance function within the organization. In larger international market intermediaries that have multiple business segments, there should already exist an appropriate level of segregation between the compliance function and the various activities that require monitoring. In such organizations, an external party (regulator or auditor) could focus on the overall mandate of the compliance function, the policies and procedures developed and implemented, and a review of the monitoring activities undertaken by the compliance function, rather than an in-depth transactional level review that would be more appropriate for a smaller market intermediary.

In smaller organizations, which may not have a clearly independent compliance function, the external party would likely need to perform more in depth procedures (for example, sampling actual transactions) rather than relying only on the internal control structure of the organization in question.

20. ***What are the practical concerns of requiring an external party to conduct periodic assessment of a compliance function?***
Primarily, the additional cost and the drain on staff time taken up to meet with, educate, and inform the regulatory staff of the firm's activities. Other considerations might include the lack of knowledge that an external party would have in performing the review. Using a firm's own external auditors might arise as an issue given recent securities commissions' regulations limiting the use of external auditors for non-audit services.

In addition, the compliance function mandate may extend beyond only specific written regulations to include the monitoring of activities that are currently less regulated (such as, derivatives and structured products).

21. ***What should be the scope and frequency of the assessment by an internal party and/or external party?***
Scope would depend on the size and the nature of the compliance function within the market intermediary under review. Internal reviews would need to consider the complexity of the activities undertaken by the market intermediary as part of a risk-based review to determine the particular scope and depth of review. More complex activities, particularly structured products offered to the retail segment of the market (as opposed to more sophisticated counterparties) would require more in-depth reviews and oversight.

From an external perspective, larger organizations would require increased scope however, the depth of the review required would be at a higher level, assuming the external reviewer was satisfied with the internal compliance function's oversight capability and capacity.

In smaller organizations, the scope of review required is narrower, however the depth of testing would likely be more thorough and detailed.

For larger organizations, frequency should not be more than annual, and less frequently if the previous review found the compliance function to be operating effectively (i.e. received a "satisfactory", "good", or higher rating). In smaller organizations, the review would likely have to be annually at a minimum due to the limited ability to have a fully independent compliance function.

22. ***Please identify the methods of monitoring that are the most effective from your perspective and explain why.***
The monitoring of well-established compliance functions in larger organizations should be done by the regulators as part of a regular review of the market intermediary's internal policies and procedures, as well as an assessment of whether such policies and procedures were properly implemented and a review of the results of applying the procedures to the intermediary's activities.

In smaller market intermediaries where the compliance function independence is less clear, there would likely be a need for more focussed reviews. This could either be performed by an external party (such as, the firm's external auditors, regulations permitting) or the regulator, but would likely include sample testing to re-perform established procedures to ensure they were properly carried out.

23. ***What factors are indicative of a strong compliance culture and a weak compliance culture? Please explain.***
Indications of strong compliance culture:
    - Ongoing commitment from executive management to support a clear mandate of the compliance function by dedicating the appropriate level of resources to the function and ensuring business heads under their authority devote an appropriate amount of attention to compliance

requirements. That is, the "tone at the top" should emphasize a strong corporate governance and ethical culture;

- Existence of a clear, well thought-out mandate for the compliance function;
- Internal and external reviews of the compliance function result in consistently good ratings;
- Lack of material or substantive regulatory issues that arise or that have arisen in the past;
- Proactive in the development and promulgation of new industry standards;
- Good working relationship between the compliance function and the businesses being monitored, as demonstrated by providing advice, guidance and direction in the development of appropriate internal procedures to ensure compliance with regulations;
- Ongoing communication between the compliance function and the businesses being monitored, as demonstrated by ongoing education and training to advise businesses of new legislation, involvement during the 'comment period' on any proposed new legislation, etc.;
- Compliance function should have clearly established policies and procedures manuals (that are continuously updated and kept current) for each business activity being monitored;
- Compliance function should have a clear independent role, supported via regular reporting internally to executive management and the Board on the status and results of the compliance function activities;
- Direct reporting lines should be to senior enough individuals and / or committees to provide the appropriate level of authority and visibility to the compliance function; and
- Regular reporting externally to the appropriate regulatory authorities in each of the jurisdictions where the market intermediary is active.

The indications of a weak compliance culture would be the opposite of the above.

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

No, we believe that a program of regular reviews by the regulator, as outlined in our previous comments above, provides the appropriate platform to ensure market intermediaries implement an effective and efficient compliance function.

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.

Primary issue is potential conflicts or differing standards between regulatory jurisdictions – home regulator versus foreign jurisdictions. For example, privacy concerns may arise when the required disclosure of certain information by one regulator can contradict privacy laws in another jurisdiction. For cross-border transactions that are regulated in both jurisdictions, issues may arise as to which regulatory jurisdiction's regulation takes precedence. The coordination of a global compliance function by the Chief Compliance Officer is made more difficult by having to deal with different regulatory standards in multiple locations and may result in "gaps" within global policies and procedures.

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?

For activities that are subject to multiple regulatory regimes (as long as there are no conflicts between the various regulatory requirements), the simplest solution is to ensure a market intermediary develops global internal policies and procedures that comply with the most stringent of similar regulatory requirements.

A centralized compliance function, with global responsibility for the market intermediary's activities is preferred. The centralized compliance function should provide overall direction to the various local compliance functions that should be in place for each jurisdiction where the market intermediary is active. The downside risk of various independent local compliance functions is that it would likely result in diverging practices and possible omissions for cross-border activities.

However, it is important to delegate enough responsibility and accountability to local compliance functions, operating within a set of global standards, policies and procedures, in order to address local business issues on a timely basis. Local compliance functions must have a culture of raising significant or

controversial issues being dealt with locally with the centralized compliance function to ensure such issues are coordinated at a global level within the firm.

CONSULTATION REPORT

COMPLIANCE FUNCTION AT MARKET INTERMEDIARIES

Commentary from
The Australian Compliance Institute
www.compliance.org.au
Email: Mike@compliance.org.au

TECHNICAL COMMITTEE OF THE
INTERNATIONAL
ORGANIZATION OF
SECURITIES COMMISSIONS

APRIL 2005

I. Introduction

Market intermediaries should conduct themselves in a way that protects the interests of their clients and helps to preserve the integrity of the markets.[2] Compliance with securities laws, regulations and rules[3] (referred in this paper as "securities regulatory requirements") is part of the essential foundation of fair and orderly markets as well as investor protection.

The compliance function is intrinsic to the operations of market intermediaries because they must have systems or processes in place to ensure that they are complying with all applicable laws, codes of conduct and standards of good practice in order to reduce their risk of legal or regulatory sanctions, financial loss, or loss to reputation. Market intermediaries should establish effective policies and operational procedures and controls in relation to their day-to-day business operations in order to achieve compliance with all relevant regulatory and legal requirements.[4]

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, which makes the compliance function both increasingly important as well as more complicated.

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 lead to fair and orderly markets and investors' confidence in the markets.

Due to the changing nature and importance of the compliance function, the IOSCO Technical Committee believes it is important to identify and discuss principles that should be considered by all market intermediaries and their regulators. This paper reviews the current IOSCO Principles for Market Intermediaries and recent initiatives by some regulators in the area of compliance. It also proposes supplementary principles and raises some issues for discussion through a consultation process. The Technical

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

[3] These include laws, regulations and rules promulgated by the legislature, regulators and self-regulatoryorganizations (SRO).

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

Committee believes that publication of this paper and consultation with market participants will bring greater clarity and focus on the compliance function.

A. IOSCO Principle

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

> 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].

There should be a balance between separation and independence and the need to imbed compliance responsibility within the business units. It is important that compliance becomes the responsibility of the business and the compliance function supports, advises, monitors and reports.

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].

B. Recent Initiatives by International Regulators Regarding Compliance Function

In Europe, the implementation of the directive on Markets in Financial Instruments that replaces the current Investment Services Directive, and which constitutes the cornerstone of the European Community regulations in the field of securities, will lead to the adoption of so-called "level-2" measures aimed at further convergence of national laws in the European Union through the implementation of a more harmonized regime governing a wide range of conduct of business and organizational issues within investment firms, including the compliance function. In its advice to the European Commission related to compliance, CESR proposes a set of principles – including the role of the compliance function, compliance policies and procedures, the role of senior management, responsibility for compliance oversight – based on the overarching principle that investment firms must maintain a permanent and effective compliance function, which must function independently, have documented status and the necessary authority within the investment firm to discharge its functions.

[5] Id.

[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).

In Australia, recent financial services law reform will subject licensed service providers to specific risk management and compliance obligations. The Australian Securities & Investments Commission (ASIC) expects that, as a minimum to comply with these new specific obligations, all licensed financial service providers will establish and maintain compliance measures, processes and procedures that ensure, as far as reasonably practicable, the provider will comply with all its statutory obligations. Further, ASIC expects, as a minimum compliance measure even where there is not a structurally separate compliance function, that a licensed financial service provider will allocate to a director or senior manager responsibility for overseeing the compliance measures and reporting to the governing body of the provider.

In Canada, the Ontario Securities Commission (OSC), the Autorité des marchés financiers (AMF) and the Investment Dealers Association of Canada (IDA), the SRO for investment dealers, have revised the requirements regarding compliance function at market intermediaries. Under the new requirements, advisers (in Ontario only) and investment dealers must implement a two-level compliance system, with a designated senior officer who is ultimately responsible to the regulators for compliance with securities regulatory requirements and a chief compliance officer who carries out compliance tasks and reports to the designated senior officer. The IDA has also recently introduced a qualifying examination for chief financial officers at investment dealers to help ensure that they understand prudential regulatory requirements, and is also considering a qualifying examination for chief compliance officers.

In the U.S., there has been increased focus on compliance systems. For example, the SEC has adopted new rules that would require investment companies and investment advisers to adopt written compliance procedures, review the adequacy of those procedures annually, and designate a chief compliance officer responsible for their administration[7]. In addition, with respect to broker-dealers, Rule 3013 of the National Association of Securities Dealers, Inc. (NASD) requires each member firm to designate a chief compliance officer[8]. The Rule also requires each member's chief executive officer or equivalent officer to certify annually to having in place a process to establish, maintain, review, modify and test policies and procedures reasonably designed to achieve compliance with NASD and Municipal Securities Rulemaking Board (MSRB) rules, and the federal securities laws. It has also requires the chief executive officer to hold one or more meetings with the chief compliance officer in the preceding 12 months to discuss such process.

In addition, a number of international organizations have conducted studies on compliance functions at firms or have proposed guidance on the compliance function. For instance, the SRO Consultative Committee of IOSCO (SROCC) published its study

[7] Rule 206(4)-7 under the Investment Advisers Act of 1940.

[8] See Securities Exchange Act Release No. 50347 (Sept. 10, 2004), 69 FR 56107 (September 17, 2004).Available at: http://www.sec.gov/rules/sro/nasd/34-50347.pdf.

on the function of compliance officers in October 2003.[9] The Basel Committee on Banking Supervision (Basel Committee) has also published in October 2003 a consultative document entitled "The compliance function in banks," which proposes basic guidance for banks and sets out the banking supervisors' views on compliance in banking organizations.[10]

Given the increased focus on compliance by regulators in different jurisdictions, the IOSCO Technical Committee prepared this paper to set out a number of supplementary principles to Principle 23 with measures for implementation to assist intermediaries to increase the effectiveness of their compliance function. The discussion section identifies current regulatory practices based on a survey of the members of the Technical Committee Standing Committee on the Regulation of Market Intermediaries (SC3) members. This paper is also intended to promote a dialogue between regulators and intermediaries on these issues, and it contains questions in areas where IOSCO would like specific feedback or input from the industry. Commentators are invited to provide feedback on any aspects of this paper, and some or all of the questions identified.

The qualification of compliance professionals, as distinct from compliance knowledge of operations executives, is of key concern. ACI has developed and implemented an Accreditation Program for compliance professionals that goes beyond simple knowledge and application of regulatory requirements. The Accreditation Handbook is attached as it sets out the critical thinking behind the skill sets and levels of knowledge. This is not a licensing regime and is independent of industry. It is expected that organisation and Industry Specific knowledge will be required in addition to that prescribed.

C. Definition of the Compliance Function and Scope

For the purposes of this paper, "compliance function[11]," is defined as follows:

> A function that, on an on-going basis, identifies, assesses, advises on, monitors and reports[12] on a market intermediary's compliance with securities regulatory requirements, including whether there are appropriate supervisory procedures in place.[13]

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. 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 loss to reputation resulting from violation of regulatory requirements. A compliance function of a firm should also have mechanisms

[9] SROCC. The Function of Compliance Officer – Study of What the Regulations of the Member's Jurisdictions Provide for the Function of Compliance Officer(Oct. 2003). Available at: http://www.iosco.org/pubdocs/pdf/IOSCOPD160.pdf. [10] Available at: http://www.bis.org/publ/bcbs103.pdf. [11] In this paper, the expression "function" refers to the staff or group of staff responsible for carrying out specific compliance activities and responsibilities. The expression does not intend to denote any particular organizational structure. [12] "Reporting" in this paper refers to reporting within a market intermediary, and "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. [13] This definition is similar to the definition of "compliance function" for banks. See paper published in October 2003, by the Basel Committee. The Basel Committee incorporates the concept of independence in its definition of compliance function.

in place to protect the firm from any liability arising from abuses committed by its customers.

Market intermediaries range in size from two-people firms to multi-national organizations, and they may carry one simple business offering limited services and products or multiple businesses of different 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 type of its clients, for example retail or institutional;
The structure and diversity of its operations (including the geographical spread of its operations);
The volume or size of transactions for which it is responsible; and
The number of people, registered and unregistered, that it employs or contracts to conduct business.

The principles set forth in this paper are intended to be sufficiently flexible to adapt to the nature, scale and complexity of the market intermediary's business and operations.[14] 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.

Specific Questions for Comment

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

ACI takes a broader view of compliance. The view expressed above is a narrow black letter law approach that will always categories compliance as a cost centre, rather than as a strategic enabler.

Compliance should be a strategic, value adding process that improves organizational performance - not an inefficient supra-system that inhibits the proper operation and purpose of an organisation. Compliance is the management discipline of identifying the ongoing obligations and requirements, exposures, risks and opportunities arising under:

- Laws and Regulations
- Contracts
- Codes (legal & voluntary)
- Fiduciary Duties and
- Stakeholder, Community and Social expectations,

and then designing and implementing an effective assurance system and culture so that the obligations, exposures, risks and opportunities are properly met and managed.

Compliance is more than black letter law - it is the spirit and intent of the law in the context of society's expectations.

In the ideal world compliance is achieved by an organisation through its normal "business as usual systems", without the need to create new and complex structures that add a burden to the organisation.

Achieving effective and efficient compliance requires:

- commitment and leadership from the Board and the CEO;
- analysis of requirements and identification of risks, requirements and exposures;
- development of systems and procedures; and
- the creation of an organisation wide compliance culture.

Cost effective compliance is achieved when the organizational culture integrates compliance into the fabric of how business is conducted.

The primary responsibilities of compliance professionals are founded in the social and business expectation that organisations will be managed in a way that meets, as a minimum, the legal requirements, but more broadly the organisation's codes, values and stakeholder expectations. Compliance management systems form one of the primary platforms for strong corporate governance.

The compliance professional's responsibilities are:

- primary responsibility to the Board to ensure that the organisation has a compliance management framework that is effective and efficient and deals with key compliance risks to the organisation. This is a responsibility that is independent of the business requirements and goes to good corporate governance practices. (There is an emerging trend for Boards to create Compliance Committees separate from the audit function.)
- a responsibility to the Senior Management to assist them in understanding the regulatory and legal obligations from a practical perspective, identify risks and develop appropriate management systems and operational procedures to deal with those risks.

If there is a conflict between compliance requirements and business objectives, it is the compliance professional's responsibility to assess the commercial and legal risks of non-compliance objectively and ensure that the Board and Senior Management are advised of these risks. It is the responsibility of the Board and Senior Management to determine how the compliance risk is to be managed. There should be an independent reporting line between the Board and the Compliance Professional to assist in escalation of these types of issues.

The key objectives of a compliance professional in relation to their organisation are as follows:

- To assist the Board and the Senior Management in the development of an organizational culture that proactively supports compliance activity and to provide current information to the organisation about the "philosophy" of compliance practices and how it is being implemented within an organisation.
- To design and assist in the establishment of a compliance management framework that:
- i*dentifies relevant compliance requirements and understands the risks involved;*
- *codifies the compliance requirements into policies, procedures and controls;*
- *ensures appropriate levels of staff knowledge about compliance requirements;*
- *monitors the effectiveness and efficiencies of compliance procedures and controls; and*
- *provides relevant and appropriate reporting procedures for compliance issues.*
- To provide commercial / practical insight into regulatory and legal compliance requirements that align with business objectives and to generate flexible and innovative solutions to the achievement of compliance requirements within the operational context.

Compliance professionals come from a range of disciplines and backgrounds. Many have legal and accounting degrees, but this is not a prerequisite. Achieving effective compliance is more than just the application of "black letter" law.

The Institute has developed an Accreditation Framework for compliance professionals that accommodates the wide diversity in background and work requirements of members.

Legal compliance

A compliance requirement is any requirement or authorization that is related to the establishment and maintenance of an organization's legal status as issued by a governmental authority (including international, national, state/provincial and local authorities) or other regulatory body and has legal force.

These compliance obligations can take many forms, such as:

- Common law.
- Legislation, including statutes and regulations.
- Decrees and directives.
- Permits, licenses or other forms of authorization.
- Orders issued by regulatory agencies.
- Judgments of courts or administrative tribunals.
- Customary or indigenous law.
- Treaties, conventions and protocols.

Voluntary compliance

An organization may also consider going beyond compliance with existing legal obligations in order to enhance its reputation, gain competitive advantage, anticipate or influence new obligations, improve its performance and improve its relations with the public and relevant authorities.

Depending on its circumstances and needs, an organization may make a commitment to subscribe voluntarily to other obligations. These may include:

- Corporate/company requirements.
- Agreements with public authorities.
- Agreements with customers.
- Non-regulatory guidelines.
- Voluntary principles or codes of practice.
- Voluntary labelling or product stewardship commitments.
- Requirements of trade associations.
- Agreements with community groups or non-governmental organizations.
- Public commitments of the organization or its parent organization.

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?
Compliance & Risk Management

The discipline of risk management involves the identification of the different types of risks that an organisation faces in conducting its business, assessing the impact of those risks on the organisation, determining the risk appetite of the organisation and putting in place appropriate risk management procedures and controls. The risks faced by an organisation are varied and can include operational risk, fiduciary risk, market risk, credit and counterparty risk, legal risk and reputation risk.

- Compliance is about meeting particular acknowledged obligations that may have a mandatory component to them. Risk management does not have a mandatory component to it, as the organisation may determine how it wishes to deal with risky situations.
- Compliance uses risk management techniques to priorities its application but all compliance risks are required to be dealt with in some fashion.
- Risk management deals with issues that are both mandatory and non-mandatory for an organisation to undertake.
- Compliance identifies all the legal obligations and risk management techniques can then be used to priorities them in terms of implementing control procedures, level of monitoring and reporting requirements and resource allocation.

Our recent survey of banks and utilities in Australia has determined there is no distinct pattern. However, even those where there was a single reporting line, there was recognition of the need for separation of technical disciplines, but coordination of approach.

[14] In most of the jurisdictions of SC3 members, it is generally acknowledge that the compliance structures, arrangements, and/or processes will differ among firms based on the nature and complexity of their businesses, although the general requirement of having a structure or processes in place is the same for all firms. In Germany, requirements on compliance function vary based on the nature of a firm's business, for instance whether they possess compliance-relevant facts. Japan, the Netherlands and Pakistan do not have different requirements on the compliance function for firms whose businesses differ in nature and size. The final CESR advice under Article 13(2) of the MiFID requires that firms maintain a permanent and effective compliance function. This particular obligation is not weighted to take account of the firm's size, nature or complexity.

II. Principles and Topics for Discussion and Consultation

One Size Doesn't Fit All

There is no single structure that fits all organisations. Factors that should be taken into account when planning how you will manage your compliance risk include:

- size (number of employees, physical locations, SME)
- operational structure (single entity, multiple business units, head office)
- nature of the business (license, legal exposures and obligations)

Centralized v Decentralized

There is no one right form. In larger organisations it is important to ensure that the operations take responsibility for compliance and does not abdicate its responsibility to the compliance department.

Combining Compliance & Risk

There are logical synergies, but risk management is a different discipline which is used in identifying the compliance exposures and then ranking them. Risk management provides a tool for allocating resources to manage compliance risk in the natural environment where there will never be enough resources to do everything.

Combining Compliance & Audit

It is inadvisable for audit to control the compliance function. Audit must remain independent to ensure that it can conduct arms length reviews.

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 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.

This is too narrow. See previous comments.
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.[15]

Means for Implementation

(a) An effective compliance function should have the necessary authority and resources[16] to properly discharge its functions. agree
(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. agree The compliance function should generally perform the following:
see previous general comments
(1) Identify, measure, and monitor the key securities regulatory requirements of the market intermediary and assist in the management of these requirements and compliance risks;
(2) Establish, communicate, monitor and enforce effective compliance policies and procedures[17] to address compliance requirements and risks;
(3) Provide information to the board of directors[18] and/or senior management on applicable laws and regulations to assist them with their compliance responsibilities;

[15] See Part I.C. on discussion of compliance function and scope for additional discussion. [16] 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. [17] 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. The term "policies and procedures" is used here in a general sense to include, among other things, procedures for supervision and procedures on required and prohibited activities.
(4) Provide assistance, guidance and/or training to business units and staff in relation to compliance; agree
(5) Report periodically to the board of directors and/or senior management on the market intermediary's overall compliance with securities regulatory requirements and internal compliance policies and procedures, including significant breaches; and agree
(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, consider notifying 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) 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.

(d) 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.

Discussion

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.

For large organisations a separate function is necessary because of the breadth and complexity. Senior management should always be responsible, but collective responsibility without specific accountability is flawed.

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

[18] In some jurisdictions, 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. Owing to these differences, the notions of the board and senior management are used jointly in this paper to identify the body that has executive functions in regards to compliance responsibilities.

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 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.

Being informed is essential. Translating that into an organisation wide understanding that changes behaviour is the really critical issue.

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., and US (CFTC and 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. Singapore does not mandate the establishment of a compliance 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.

The Technical Committee has included a question at the end of this section to obtain the industry's view on the necessity of prescribing a specific structure.

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 CFTC).

In Ontario and Quebec (Canada), 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 the US CFTC require registrants to give immediate notice to the regulator if its 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.

<u>Specific Questions for Comment</u>

Should a specific organizational structure for compliance be prescribed? Please explain. No. What should be required is the independence of the compliance function and its ability to have direct access to the Board for the reporting and escalation of issues. ACI surveys have indicated that centralized, decentralized and hybrid systems all work.

Are there any essential roles, responsibilities or activities for the compliance function that should be mandated or otherwise identified by regulators? Mandatory requirements tend to become the lowest common denominator. On the principle that lawyers will prescribe the "absence from a list to mean that it is not required", it is dangerous to prescribe "essential roles and activities". It is more effective to establish outcomes to be achieved, than specific activities.

Please identify responsibilities other than those described above that are carried out by the compliance function at market intermediaries.
As set out before. Compliance is more than just a legal risk management tool. Approached strategically, compliance can provide systems, structures and behaviors that engender compliance without undue emphasis on the narrow legal requirements, but rather the broader issues included in such things as codes of conduct, internal policies and procedures etc. This is summarized in the quote from the CFO from WESTPAC Bank, Phil Chronican who said: "The factors that drive an environment of regulatory compliance and sound corporate governance are the same as those which will support sustainable business practices across the board. Furthermore, sustainability of business practices is essential to the building of long-term shareholder value.

The most important factors are those which legislative prescription cannot address as the core issue for all companies is the organizational climate, or culture that they foster…..however the way to develop an effective culture of compliance varies with organizational climate."

How and when should the compliance function be responsible for managing compliance risk?
The compliance function should be repsonsible for coordinating the identification, codification and planning for the management of compliance risks – regardless of the origin. In achieving this objective, the compliance function will need to work with the business units as they are the ones who own the activities and the associated risks.
It is for the business units to manage the risk and the compliance function to monitor and report against the management of the risks ie compliance with the risk management plan.
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?
There is a trend to complexity that interferes with functionality in the belief that complex manuals of policies and procedures will make the organisation compliant. For smaller intermediaries it is more important to ensure that the operating procedures are inherently designed to engender compliance and that the policies are developed in a manner that is sympathetic to the organisations size and structure. In smaller organisations there is more scope for rapid cultural distortions caused by "key individuals.

Topic 2: Role and Responsibilities of the Board of Directors or Senior Management

Principles:

(a) The board of directors or senior management is responsible for the firm's compliance with securities regulatory requirements.
(b) The board of directors or senior management should establish and maintain a compliance function, and compliance policies and procedures designed to ensure compliance with securities regulatory requirements. The board of directors or senior management should assess whether the compliance policies and procedures are being observed and are appropriate on an on-going basis.

Due to differences in their size and internal organization, market intermediaries will employ different structures to ensure compliance with securities regulatory requirements. Placing ultimate responsibility on the highest 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) The board of directors or senior management 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 at least annually the overall compliance of the market intermediary, including its adherence to internal compliance policies and procedures and the effectiveness of its compliance function, and

Ensuring that any compliance issues are resolved effectively and expeditiously.
(b) The board of directors or senior management should directly oversee the scope, structure and activities of the compliance function[19] to ensure that the compliance function is carrying out its mandate.
(c) The board of directors or senior management should encourage the business units to consult with the compliance function with respect to their operations when appropriate.
(d) 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:

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

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.

Appendix A provides a list of topics that maybe covered in the compliance policies and procedures.

Discussion

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.[20] Seven jurisdictions hold senior management accountable for compliance.[21] 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 noncompliance. Topic 6 also contains discussion on certification requirements on senior management.

Six jurisdictions, including France, Japan, Ontario and Quebec (Canada), Singapore, US (CFTC and SEC), place responsibility for compliance on registered/licensed persons as well as senior management. For example, the US CFTC 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.

[20] The board of directors is ultimately responsible for compliance in Australia, Germany, Italy Mexico, The Netherlands, Pakistan, Singapore, Spain and Switzerland. [21] Senior Management is ultimately responsible for compliance in Ontario and Quebec (Canada), Hong Kong, France, US (CFTC and SEC) and the U.K. The US SEC may hold a board responsible under appropriate circumstances.

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.

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.

The 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.

Specific Questions for Comment

1 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.
The Board is primarily responsible and therefore accountable for:

a. Commitment by the governing body and senior management to effective compliance permeates the whole organization
b. A clearly articulated compliance policy, that is aligned to the organization strategy and business objectives, is endorsed by the governing body
c. Appropriate resources are allocated to develop, maintain and improve the compliance program.
d. Behaviours that create and support compliance are encouraged and behaviours that compromise compliance are not tolerated.

These principles are more fully articulated in Attachment "B" the draft revision of the Australian Standard on Compliance. If the Board has provided impetus and active support for these, then there should be an immunity from prosecution for them at an individual level and a mitigation of penalty for the organisation.

However, if there is a lack of real commitment, an absence of a policy, or inadequate resources (relative to size, complexity and maturity), or where there are extensive policies where there is a culture of "selective non-adherence" then there is no reason to grant immunity.

Senior management in addition to the three general obligations, is responsible for the operational implementation of compliance policy and procedures and thus has more direct accountability for specific actions. Senior management

and operation staff who carry out the actions should be accountable if they have not acted in good faith, or where there is a strict liability accruing and they were careless, or negligent.

Compliance professionals rarely have a direct say in the operations and thus should not be accountable if they have acted in good faith.

Do you distinguish among responsibility, accountability and liability? Please explain.
Responsibility and accountability are interconnected. This should be distinguished from legal liability as distinct from internal disciplinary actions that may attach for failure to perform. Too often a breach with legal liability may be out of the control of the responsible person especially if there is a deliberate act.

Should a senior officer be designated for the day-to-day compliance responsibilities?
Yes. The level of seniority of the compliance manager is critical. It sends signals to the organisation as a whole as to how seriously compliance is taken by the Board and CEO. Seniority is also important as it provides direct power and access through having a "seat at the table" and having both ostensible and actual authority.

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 and should report to the board of directors or senior management.

Independence of the compliance function is critical to ensuring that the board of directors or senior management, who are ultimately responsible to regulators, receive accurate and unbiased reports on the market intermediary's compliance with securities regulatory requirements.

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 level of the organization. In addition, in order to 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 performance and/or opinion 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 functions. 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
(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 compliance function may also be undermined if the tenure (i.e. prospects of staff, position) of compliance personnel is dependent on the business lines.
(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 the board of directors and senior management 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.

Discussion

Independence

About half of the jurisdictions responding to the survey have requirements pertaining to the independence of the compliance function.[22] 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.[23,24] 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 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.[25] 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[26].

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

[23] 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.

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

[25] It is worth noting that the US CFTC and the US SEC both require financial audits and anti-money laundering audits to be completed by independent personnel.

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

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.

Specific Questions for Comment

What requirements relating to independence and ability to act are relevant to a small firm?
It is common for compliance officers in small companies to have multiple roles. Some subsume compliance, risk and audit, others have operational roles. In practical terms independence may be a fiction where the Board and CEO

are controlling shareholders. Where the Board is independent one method for assisting independence is to create a direct reporting line to the independent directors for the compliance officer when acting in that capacity.
Independence is not assisted by simply appointing external providers as their appointment and continued fee income is normally controlled at a level above compliance.

It is possible that there is a role for professional independent compliance committees to be established to support the compliance officer.

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?
No. Self supervision is not adequate. There is an inherent conflict that cannot be managed in any meaningful way.

There needs to be an independent monitoring and reporting function, though primary responsibility for compliance can rest with the operations person.
Are the means of implementation of independence set out above sufficient to achieve independence? Please explain.
How do you ensure that compensation of compliance personnel is not subject to undue influence? Please explain.
In large organisations where there is a decentralized structure, but a central compliance function in support, the final remuneration decision should be established by the central position.
Where all compliance is centralized there is less of a problem,

Remunerating compliance is difficult as performance is difficult to assess.

Topic 4: Qualification of Compliance Personnel
Principle:

Staff exercising compliance responsibilities should have the necessary qualifications, experience and professional and personal qualities to enable them to carry out their duties effectively.

Means for Implementation

Market intermediaries should consider subjecting persons responsible for compliance activities to the following:

(a) Completion of relevant courses and/or training prior to accepting compliance responsibilities;
(b) Successful completion of prescribed examinations that will confirm their knowledge and experience concerning securities regulatory requirements;
(c) Continuing education requirements; and/or
(d) Relevant work experience.

Discussion

Current requirements in the jurisdictions of all 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 US, 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 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.

Specific Questions for Comment

What are the appropriate qualifications for compliance professional?
ACI has developed a comprehensive accreditation framework which is attached. The key principles are:

- Compliance is a complex discipline requiring a broad range of hard and soft skills to enable compliance to be perceived as a valuable strategic asset rather than an impediment to business
- Compliance does not require a law degree, rather an appreciation of how to secure compliant behaviour
- There should be levels of accreditation reflecting the structured nature of the profession. There should also be comprehensive pathways for career development.
- The core compliance skills are common across the globe and across industries and laws. What varies is the legal requirement, or cultural context, but the principles that
- Licensing will lead to a lowering of professional standard. Accreditation allows for defined standards that are internationally transportable.

Should the qualifications vary depending on functions, responsibility or seniority?
Yes. The levels are set out above. There should also be industry specific requirements eg finance, pharmaceutical, health which are added as technical disciplines.

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

ACI has developed a comprehensive set of learning outcomes. These are defined for every subject area. We have also developed a five tier system which sets out the complexity of knowledge required for each subject.
This framework allows ACI assessors to examine a course and rank it as to the level of complexity.
As a rule of thumb a level 1 course is for front line staff who need to be made aware of their obligations, but at a purely operational level.
Level 2 courses are the base line for our entry level of accreditation
Level 3 is for senior compliance staff
Level 4 is for the most senior and is only delivered in a few subject areas.

Existing course providers may have their material assessed. They can also have the learning outcomes provided so that they can redesign their courses to meet higher or lower levels according to eh market requirements.

All courses must be assessed. Attendance is not adequate.

Assessment is carried out after the course (usually the examination becomes available several days after the course as we are assessing retained knowledge). Assessment takes the form of multiple choice, short text and complex assignments depending on the level of the program.

Where possible assessment topics provide the scope for the assignment to be work place based.

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 review by independent third parties, such as the intermediary's external auditors, SROs or regulators.

In order to 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.

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 board of directors 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; and where appropriate, additional training should be provided to compliance personnel.

Discussion

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 US, 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[27].

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.

Specific Questions for Comments:

Who, within or external to a market intermediary, is best placed to assess the effectiveness of the compliance function? Please explain.
ACI has just completed the development to a Compliance Review Protocol. The reviewing process is complex as it is not a simple historical audit and unlike a quality system normally has too small a data set to provide reliable performance measures. In a recent study we completed on Compliance in 7 major Banks, we determined that there is inadequate knowledge on effectiveness and efficiency measures. While there are a number of "existence measures", these alone provide little proven relationship to ultimate effectiveness.

Part of the reason is that compliance is ultimately behavioral outcome and most audits ignore behaviour and behavioral precursors and indicators.

Notwithstanding the above the ACI Protocols provide a guide for not only who should conduct a review, but how it should be conducted. The "who" will depend on the purpose of the review. Is it part of "normal maintenance"? If so then it could be conducted internally by the compliance team, or properly briefed internal audit. If it is in relation to an enforcement action then the independence and qualification of the reviewer become critical.

In all situations, compliance reviews cannot be undertaken by individuals without compliance expertise and preferable practical compliance exposure.

The ACI Compliance Audit Protocol can be provided is required on limited license for IOSCO for the purposes of this study and is not for general distribution.

What should be the role of an external party in assessing the effectiveness of a compliance function?
This is discussed in detail in the protocols.

What are the practical concerns of requiring an external party to conduct periodic assessment of a compliance function?
This is addressed in the protocols. The critical factors are the purpose, the defined scope, the budget and level of access.
What should be the scope and frequency of the assessment by an internal party and/or an external party?
There is no recommended frequency. In practice there will be programmed reviews and reviews triggered by failures or "near misses". The survey indicates annual review, but not of the same part of the compliance framework. The focus may be on new or modified areas, or areas of higher risk, as well as areas which have not been reviewed for some time.

Good practice would suggest that a program of review be coordinated with the internal audit and risk review to minimise disruption to the business .

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

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 arise. 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 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:

(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 on 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[28], of market intermediaries; or
(f) Periodic self-assessment and/or certification by the board of directors or senior management of market intermediaries, which should be filed with the regulators for review.

The above examinations, self-assessments and certifications 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 measures taken to address deficiencies previously identified.

Discussion

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).

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 US, broker-dealers[29] and OTC derivatives

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

[29] Exchange Act Rule 17a-5.

dealers[30] must all file with the US 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 US 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 US SEC and the designated examining authority by report of material inadequacy within 24 hours thereafter. Similar requirements apply to commodity brokers regulated by the US 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 UK, 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.

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[31]. 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

[30] Exchange Act Rule 17a-12.

[31] 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 SEC).

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[32], 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.[33]

In the US, 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 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.

[32] Certification requirements exist in Germany, Pakistan, Spain and Switzerland. The US CFTC requires certification relating to financial compliance.[33] These jurisdictions include Ontario and Quebec (Canada) and Pakistan.

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.

Specific Questions for Comments:
Please identify the methods of monitoring that are the most effective from your perspective and explain why.
What factors are indicative of a strong compliance culture and a weak compliance culture? Please explain.
In many ways it is misleading to single out the compliance culture as if it were separate from the organisation's culture. It is one and the same.

Indicators of a compliance culture include, but are not limited to:

Top management role in encouraging compliance

Top management has a key responsibility for:

- Building awareness and motivating employees by explaining the organization's mission, vision and values in the compliance context.
- Communicating its commitment to the compliance policy.

- Encouraging all persons working for or on its behalf to accept the importance of achieving the compliance objectives and targets for which they are responsible or accountable.
- Encouraging persons working for or on behalf of an organization should be encouraged to make suggestions that can lead to continual improvement in compliance performance.

It is the commitment of individual people, in the context of shared organizational values that transforms a compliance program into an effective process with desired outcomes.

Factors that will support the development of a compliance culture include:

(a) Clear set of published values.

(b) Management actively seen to be implementing the values.

(c) A consistency in reward and punishment for similar actions regardless of position.

(d) The incorporation of compliance performance in every position description.

(e) The linking of performance pay to achievement of compliance obligations.

Evidence of a compliance culture is indicated by an assessment of the degree to which—

- items (a) – (d) above are implemented;
- employees believe that items (a) – (d) above have been implemented;
- employees understand their personal compliance obligations and those of their business unit;
- the obligation for compliance and the remediation of breach is 'owned' by employees; and
- the compliance team is regarded as a valuable resource.

The development of a compliance culture requires the active, visible and consistent commitment of the CEO and management to a common, published standard of behaviour that is required throughout every area of the organization.

Employee commitment to compliance

The organization should ensure that all persons working for it or on its behalf are aware of:
- The importance of conforming to the compliance policy and program.
- Their role and responsibilities within the program.
- Benefits of improved performance and the consequences of departing from the intent of the program.

Behavioural Contributors

An effective compliance program requires a strong behavioural component. Acknowledgement, demonstration and communication of acceptable behaviours in the organization is needed to reduce compliance failures and support the compliance culture.

Behavioural compliance mechanisms should be employed as appropriate. This could include:
- selection processes that includes a high weighting on "values fit" and predisposition to compliance
- induction program with compliance and values occupying a central component
- position description and job requirements clearly setting out the compliance obligations
- fostering an open "no fear" system for feedback and issues management
- ongoing compliance training and regular compliance issues updates
- mentoring, coaching and leading by example
- performance appraisal systems that include assessment of compliant behaviour
- highly visible rewarding of compliant behaviour
- prompt, visible disciplining in the case of either serious or wilful breaches

Are there other means for implementation that we should consider?

Topic 7 Cross-border issues.

Many market intermediaries operate globally. For example, some market intermediaries have branches (i.e. the same legal entity as the market intermediary), affiliates and/or subsidiaries in a number of jurisdictions, while other market intermediaries deal with customers in different jurisdictions through electronic means. Different jurisdictions may have different legal and regulatory requirements. The need to consider and comply with varying legal and regulatory requirements in different jurisdictions creates difficult compliance issues.

Market intermediaries that have cross-border activities should carefully consider the applicable regulatory requirements. Regulators, too, should be cognizant of the implication of cross-border issues for the performance of the compliance function. Regulators should consider whether market intermediaries have arrangements for compliance with all applicable regulatory requirements.

Specific questions for comment

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

Incompatible legal requirements

Incompatible cultural and political requirements

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?

One of the central methods adopted by a number of multinational members of ACI are to clearly identify the highest standard and then setting that as the global benchmark for all activities. While this is seen as a potential competitive disadvantage in local trading, it provides a more cogent and translatable set of messages to all staff and other stakeholders.

In adopting this approach they have reduced the complexity of internal training and communication by distilling the critical substantive messages. They then add specific local issues which are primarily procedural, rather than substantive.

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. The IOSCO Technical Committee 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.

III. Conclusion

It is acknowledged that there is increasing focus on the compliance function. The purpose of this paper is to identify possible supplementary principles to Principle 23 of the IOSCO Objectives and Principles of Securities Regulation and to raise issues for discussion through a consultation process.

You are encouraged to comment on any aspect of this paper. In particular, you are asked to respond to, or otherwise comment on, some or all of the specific questions set out in the paper. These questions are reproduced below.

Do you agree with the definition and description of the scope of a compliance function? Please explain. No. The definition is too narrow and should embrace broader obligations that must be complied with:

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?
Should a specific organizational structure for compliance be prescribed? Please explain.
Are there any essential roles, responsibilities or activities for the compliance function that should be mandated or otherwise identified by regulators?
Please identify responsibilities other those described above that are carried out by the compliance function at market intermediaries.
How and when should the compliance function be responsible for managing compliance risk?
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?
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.
Do you distinguish among responsibility, accountability and liability? Please explain.
Should a senior officer be designated for the day-to-day compliance responsibility? Please explain.
What requirements relating to independence and ability to act are relevant to a small firm?
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?
Are the means for implementation of independence set out above sufficient to achieve independence? Please explain.
How do you ensure that compensation of compliance personnel is not subject to undue influence? Please explain.
What are the appropriate qualifications for compliance personnel?
Should the qualifications vary depending on functions, responsibility or seniority?
How do you evaluate the adequacy of courses and training for compliance personnel?
Who, within or external to a market intermediary, is best placed to assess the effectiveness of the compliance function? Please explain.
What should be the role of an external party in assessing the effectiveness of a compliance function?
What are the practical concerns of requiring an external party to conduct periodic assessment of a compliance function?
What should be the scope and frequency of the assessment by an internal party and/or external party?
Please identify the methods of monitoring that are the most effective from your perspective and explain why.
What factors are indicative of a strong compliance culture and a weak compliance culture? Please explain.
Are there other means for implementation that we should consider?
Please identify the specific issues that arise for the compliance function of a market intermediary if it is operating in more than one jurisdiction.
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?

Appendix ACompliance Procedures Topics

Specific issues that should be considered for the internal compliance policies and procedures of an intermediary are:

Measures to identify and document qualifications of individual employees to provide regulated services;
Training of individual employees regarding securities regulatory requirements and how to comply with such requirements;
Prevention of undue disclosure of confidential information;
Detection, prevention and management of conflicts of interest;
Compliance with conduct of business rules by the firm and its staff;
Monitoring of employees personal transactions;
Supervision of opening of new client accounts;

Supervision of trading practices, including proprietary trading of the firm;
Supervision of portfolio management processes;
Supervision of advice provided to clients;
Supervision of the various duties relating to information to clients and marketing information;
Controlling compliance with prudential rules;
Records and documentation, including safeguards for the privacy protection of client records and information;
Prevention of money laundering;
Dealing with customer complaints;
Reporting and supervisory structure; and
Business continuity plans.