

**Securities Industry Association**

120 Broadway, New York, NY 10271-0080, (212) 608-1500, Fax (212) 608-1604
1401 Eye Street, NW, Washington, DC 20005-2225, (202) 296-9410, Fax (202) 296-9775
info@sia.com, <http://www.sia.com>

LONDON INVESTMENT BANKING ASSOCIATION

6 Frederick's Place, London, EC2R8BT
Tel:0171796 3606 Fax:0171796 4345

LIBA

Mr Eudald Canadell
Secretary General
International Organization of Securities Commissions
PO Box 171, Stock Exchange Tower
800 Square Victoria
42nd Floor, Suite 42 10
Montreal, Quebec H4Z 1C8
Canada

Our ref: DJC/RSKapr9v3/COM14
19th May 1998

Dear Eudald:

RISK MANAGEMENT AND CONTROL GUIDANCE FOR SECURITIES FIRMS AND THEIR SUPERVISORS

The London Investment Banking Association, Securities Industry Association and British Bankers' Association welcome the opportunity to comment on the report by the Technical Committee of IOSCO *"Risk Management and Control Guidance for Securities Firms and their Supervisors"* (the Paper). This letter represents the collective views of the three associations.

Internal controls and risk management are of fundamental importance to securities firms, and of course to their supervisors. Much has been written on this subject as it relates to the financial sector (evidenced by the range of material listed in Appendix A to the Paper) but it remains a complex and difficult one and it is critically important to the industry that a pronouncement with the authority of IOSCO behind it should strike the right balance.

We welcome IOSCO's objective of providing "flexible and nonexclusive" guidance and there is much in the Paper which we support. We believe, however, that, in order for this objective to be achieved, some important statements in the detailed text need to be more prominently placed

and, in most cases, reflected in the Elements themselves. The most significant of these are highlighted below and our detailed comments are set out in the appendix to this letter. Furthermore, we believe that the format of the Paper - and in particular its conflation of the respective roles of supervisor and supervised - reduces the clarity of the underlying messages and therefore needs revision.

1. The objectives of risk management and internal controls

Risk management is an over-arching term of which "control" is only a part. The concept also encompasses the identification and assessment of risk (both financial and non-financial), and the taking of risks in a considered way in conjunction with a determination of the appropriate levels of reward. The Elements in the Paper focus from the outset on the control aspects of risk management and, in doing so, may not allow for this more holistic view. In the comments which follow, we have used the term "control" only where we mean the control aspects of risk management and "risk management" otherwise: we believe that the Elements in the Paper might benefit from a similar change.

At its most fundamental, a system of internal control is "the whole system of controls, financial and otherwise, established by management in order to carry on the business in an orderly and efficient manner". Such controls exist within the broader risk management framework and are established by management and for management, in order to provide them with appropriate reassurance that the business is being conducted in the way they intend, having regard, inter alia, to regulatory benchmarks. Clearly, therefore, internal controls are inextricably linked to a firm's obligations towards shareholders, customers, supervisors and others but cannot be more widely drawn than this.

An inevitable consequence of this analysis is that it is not a function of a firm's internal controls to "protect the financial industry from systemic risk". Indeed, such an objective is unachievable: as Alan Greenspan has observed, "the management of systemic risk is properly the job of the central banks" *. The overall soundness of the system is, of course, a legitimate concern of securities supervisors, and the establishment and effective supervision of appropriate risk management standards across the industry contribute to this, but an expectation that any individual firm's controls can explicitly "protect the financial industry" is no more than wishful thinking. A firm can and should have procedures to control concentrations of exposures to other entities both within and outside the financial - system and the net effect of all firms having such procedures in place may be to diminish systemic risk but any individual firm can only protect itself, not the industry as a whole.

Furthermore, the suggestion that internal controls should be designed to "protect the firm's customers from large financial losses" is too widely drawn. There will be circumstances in which a firm has some form of obligation to protect customers from loss - safeguarding customer assets over which it has custody, for example - but there are many other potential causes of customer losses (including their own behaviour) for which a firm has no responsibility.

Securities firms will have a particular risk appetite, especially as regards market and

credit risk, which is a matter for senior management to decide and for shareholders to review. Risk management functions are needed to make sure that the risks undertaken are effectively identified, measured and monitored in accordance with management's decisions and that returns are appropriate to the risks undertaken, not that risk is minimised or eliminated altogether.

* Remarks before the Conference on Capital Regulation in the 21st Century, Federal Reserve Bank of New York, 26th February 1998.

2. Fundamental attributes of a risk management framework

The "Elements" set out in the Paper focus on the detailed aspects of internal control procedures but give insufficient emphasis to the importance of control culture. Risk management and internal control are essentially attitudes of mind: unless there is a strong control philosophy in a firm, even the best designed system of detailed procedures may be ineffective in practice. These issues are recognised in the discursive part of the Paper (in Section IV) but not explicitly in the "Elements" themselves.

Another critical aspect of an effective risk management system is risk assessment. A firm must be able to identify and assess the risks it faces in order to monitor them, assess returns and design suitable control procedures to reduce risks where appropriate. Again, this is articulated in the body of the Paper but is absent from the "Elements".

Furthermore, it is recognised in the text of the Paper that each firm's risk management framework should be suited to its particular circumstances; in particular, it will depend on the size and complexity of the business and will evolve over time. It is also acknowledged that, in designing an effective risk management system, management must strike a balance between the cost of implementing a particular procedure and the benefits which will result. These are important considerations and should be reflected in the Elements.

3. Respective responsibilities of management and supervisors

The Paper blurs the respective responsibilities of a firm's management and its supervisors in a way which can only be detrimental to both constituencies. One of the reasons that this has occurred is that each of the Elements conflates the different interests of firms and supervisors. Their respective roles would be clearer if they were dealt with in separate Elements.

It is the responsibility of a firm's senior management to put in place a framework of risk management policies that is robust in the context of the specific nature of the firm's business and is consistent with regulatory expectations. Supervisors are responsible for satisfying themselves that appropriate risk management policies are in place in the light of supervisory benchmarks and general industry practice. In doing this, they should explicitly recognise the validity of appropriate delegation and of the costbenefit considerations which are an integral part of sensible risk management: they should also acknowledge that control frameworks operate within tolerances and cannot provide absolute assurances. There will be cases where such an assessment leads to more direct action, but supervisors should not routinely intervene in a firm's decision-making and management processes: in the final analysis, responsibility for the design and

implementation of risk management processes within a firm must rest with management.

The supervisory benchmarks against which firms are measured should be established, in consultation with the industry, at a level which reflects adequacy rather than best practice. They should be framed in a way which encourages each firm to develop its own tailored risk management frame-work which will fit better initially and can evolve over time to meet new risk management challenges that arise as the firm's technology and business activities change - rather than adopting a "one size fits all" approach.

In summary, we believe that the Paper needs to be focussed more sharply on the fundamental aspects of internal controls and risk management whilst moving away from the detail, and to distinguish clearly between management's responsibilities for controls and the supervisors' responsibility to assess those controls.

We would, of course, be happy to discuss these issues further with you, if that would be helpful. I am copying this letter to Richard Britton.

Yours sincerely,

Deborah Chesworth

Deborah Chesworth
Director

Appendix: detailed comments on the Paper

I Detailed comments on sections I and IV

Section I (Introduction) and IV (Elements of a risk management and control system) are dealt with together because both cover the twelve "Elements" proposed by IOSCO as benchmarks for firms and supervisors.

1.1 Introductory paragraphs in section I

- a) We support the intention that the Paper's recommendations should be flexible and non-exclusive but believe that much of the detail of the document undermines this approach; many of our comments below relate to this issue.
- b) We understand the sentiments behind the statement (in the press communique) that "risk management and controls ... are not a substitute for adequate capital requirements" but we believe that this needs to be qualified by a recognition that there is a relationship between the risks which a firm wishes to take, the quality of its risk management and the level of capital which is "adequate" to support its business.

- c) The introductory paragraphs - which set the scene for everything that follows - need to acknowledge that:
- whilst supervisors have a role in setting appropriate internal control standards, these cannot be mandated at a detailed level because internal controls must be suited to the particular circumstances of each firm and must be adapted over time to reflect market and business developments;
 - risk management and controls cannot - and should not - eliminate risk entirely for two reasons: firms which do not take any risks cannot make money; and there is a balance to be struck between cost and benefit;
 - no internal control system can provide absolute assurance.

These themes are well covered in section IV (in the first paragraph below Elements 3 to 5 on page 16) and this text could usefully be given more prominence by its inclusion in the Introduction.

- d) The second paragraph of the Introduction defines "controls" as comprising basic internal accounting controls and risk management policies and procedures. This under-estimates the importance of over-arching aspects of the control framework - control culture and risk, assessment, for example - and we would prefer to see a broader definition (the standard one being *"the whole system of controls, financial and otherwise, established by management in order to carry on the business of an enterprise in an orderly and efficient manner, ensure adherence to management policies, safeguard the assets, and secure as far as possible the completeness and accuracy of the records"*).
- e) The Introduction could also usefully clarify the respective responsibilities of firms and supervisors with respect to internal controls.

1.2 Control environment Elements

1 Firms need to establish a mechanism to ensure that they have internal accounting controls and risk management controls^(b) . Supervisors need to establish a mechanism to ensure that the entities they regulate have internal accounting controls and risk management controls^(b) . The supervisory mechanism need not^(c) prescribe specific and detailed controls, but rather provide general guidance^(d) to firms.

2 Firms and supervisors need to determine that controls are set and monitored at the senior management level at a firm and responsibility for monitoring controls is clearly defined.

Comments:

- a) It is surprising that the Elements focus immediately on detailed internal controls. They should cover explicitly the importance of a strong control culture (without which all other controls may be ineffective) and of risk assessment (which is a necessary first step in the design of an internal control system).
- b) Both occurrences of the phrase "internal accounting controls and risk management controls" in Element 1 should be preceded by "adequate"; it is adequacy, rather than best practice, which is needed.
- c) The last sentence of Element 1 should read "The supervisory mechanism should not prescribe specific and detailed controls but may ...". Guidance provided by supervisors must be sufficiently general to accommodate implementation by each firm's management in the way which best suits the needs of their business, and to allow controls to be adapted over time to reflect changing markets and technologies.
- d) The suggestion that supervisors could provide general guidance to firms is not unreasonable per se but it does raise questions about the status of such pronouncements. General guidance must be precisely that: supervisors may suggest broad principles to the firms they regulate but it must remain the responsibility of the management of each firm to determine an appropriate internal control structure. In addition, firms must not be punished for failing to comply with a regulator's retrospective or unpublished interpretation of general guidance into detailed rules.
- e) The Paper has a strong emphasis on documentation which begins to emerge in section IV under these two Elements. We recognise that good documentation of internal controls is highly desirable and makes it easier to reinforce and demonstrate a strong control environment. The statement (in Section IV under Element 7) that "the absence of written evidence of controls should be a warning ... that a weak control environment may exist" is undeniable but it is not *necessarily* the case that a strong control environment cannot exist without documentation, particularly in smaller firms.

1.3 *Elements on the nature and scope of controls*

- 3 Firm guidance and guidance from supervisors^(a) should cover both internal accounting controls and risk management and controls.**
- 4 Internal accounting controls for firms should include books and records requirements, segregation of duties, and controls that are designed to safeguard assets of the entity and to safeguard customer property^(b).**
- 5 Risk management and control for firms should include controls for overall firm and individual trading desk limits^(c), market risk, credit risk, legal risk, operational risk, and liquidity risk.**

Comments:

- a) See 1.2(d) above on guidance from supervisors.
- b) It needs to be clear in Element 4 that it is only customer property *over which the firm has custodial* control which can plausibly be subject to safeguard controls operated by the firm.
- c) Element 5 could be read to imply that there should be monetary limits over all the risks listed but this is clearly impractical for operational and legal risk. The drafting could be clearer simply by reversing the order of the sentence: "Risk management and controls for firms should cover market, credit, legal, operational and liquidity risk and should include, for relevant risk types, controls for overall firm and individual trading desk limits.

1.4 Implementation Elements

- 6 Firm guidance from senior management to the business units regarding controls should contain general guidance at the most senior levels and specific and detailed guidance as the information flows to smaller business units and individual trading desks^(a).**
- 7 Firms should have and supervisors should require written documentation about their control procedures.**

Comments:

- a) The intended meaning of Element 6 is unclear. If it is saying that senior management should be responsible for setting broad policies which should be subject to detailed implementation at operating level, then it seems reasonable but some redrafting would be helpful.

1.5 Verification Elements

- 8 Firms and supervisors need to determine that controls, once established by management, are effectively operating as designed on a continuous^(a) basis.**
- 9 Firms and supervisors^(c) need to establish mechanisms to verify that controls, once established, are being followed. The verification procedures should include internal audits, which should be independent of the trading desks and the revenue side of the business, and external audits^(d) by independent accountants. For supervisors, additional verification would be accomplished through an examination process.**

Firms need to determine that recommendations by auditing bodies and supervisors are properly implemented.

- 10 Firms and supervisors need to determine that controls, once established, keep pace with new products and industry technology.**

Comments:

- a) It is impossible to "*determine* that controls ... are effectively operating as designed on a *continuous* basis" (our italics). Verification procedures are intended to provide reasonable assurance that controls are being performed regularly and conscientiously as designed but this is quite different from what is called for in Element 8.
- b) The supporting text in section IV implies (on page 18) that internal audit must necessarily be carried out by employees of the firm. This may be inappropriate in group situations or where internal audit is outsourced (as may be the case for smaller, national firms).
- c) As regards Element 9, it is not normally the function of supervisors to "verify that controls ... are being followed" - their role is to satisfy themselves that management perform this function (an element of which may be to identify and raise with management any risks not covered by existing controls), otherwise they run the risk of interfering in the management of the business. The statement - on page 18 - that supervisors are a "level of defense" in the oversight of control procedures is inappropriate.
- d) Also in Element 9, there seems to be a misunderstanding about the role of external auditors (if, by this, IOSCO means the statutory auditors). Their function is to form an opinion on the financial statements and, in doing so, they will look at some but not all internal controls in order to assess whether they can rely on them for the purposes of the audit. This is completely different to the Paper's assertion - on page 18 - that "external auditors are responsible for making independent checks on the control system".

In some jurisdictions, external firms of accountants (but not necessarily the external auditors) do have a distinct function within the regulatory framework to review certain internal controls. In order to maximise the effectiveness of this role, its precise nature must vary between different supervisory regimes - and to some extent - from firm to firm. We do not therefore agree that it is necessarily helpful for supervisors to mandate annual reviews by external auditors of "at least the internal accounting control systems"; this could devalue the status of *internal* audit and making such a review annual - particularly if full scope - is likely to be both impractical and unnecessary in many cases.

1.6 Reporting Elements

- 11 Firms need to establish and supervisors should require mechanisms to report material inadequacies or breakdowns in controls to senior management and supervisors^(a) on a timely basis.**
- 12 Firms should be prepared to provide supervisors with relevant information about controls. Supervisors should have mechanisms to share information about controls with each other^(b).**

Comments:

- a) The level of materiality at which control inadequacies and breakdowns need to be reported to supervisors is much higher than that at which senior management need to be informed. This needs to be clear in Element 11.
- b) We agree that there should be mechanisms for supervisors to exchange information but these should not be unfettered powers. Disclosure should be constrained by appropriate professional secrecy rules and should not be permitted unless it is regarded as necessary for the proper exercise of one or both of the respective supervisors' functions.

2 Detailed comments on section II

2.1 Functions of internal risk management controls

- a) The first paragraph of Section II suggests four functions for internal risk management controls, of which two are seriously flawed:
 - *to protect the financial industry from systemic risk*: whilst, in a general sense, appropriate industry standards of internal control contribute to the safety of the financial system, an individual firm's internal controls cannot protect the system as a whole from systemic risk. Controls can go some way towards insulating a firm from the possible effects of a systemic incident (using concentration limits, for example) but even this will not be watertight;
 - *to protect the firm's customers from large financial losses*: it is not the purpose of investor protection to protect customers from financial loss as such, nor is it a purpose of a firm's internal controls. For example, the wholesale markets operate by and large on the principle of caveat emptor, and firms do not - and should not - generally have a responsibility for establishing the suitability of a particular product for a particular wholesale customer. There will be some situations - in the retail sector, where a firm has advised on suitability, discretionary management and custody, for example - where a firm has some sort of responsibility for protecting a customer from large losses but this is quite different from the sweeping over-generalisation proposed in the Paper.
- b) There are some passages in Section II where the Paper seems to suggest that the objective should be to minimise or eliminate financial risks (for example, "credit risk can be minimised by..."). Of course, a firm which does eliminate financial risks will not make money the real objective is to limit financial risks to acceptable levels determined by management.
- c) It needs to be acknowledged in the Paper that not all risks are internally generated and that some risks cannot be "controlled" in the conventional sense of being able to measure them quantitatively or prevent them from occurring.
- d) The explanations provided of the different risk types tend to restrict their meaning in a way which is undesirable (for example, the passages on credit

risk implicitly assume that all exchange-traded transactions are free of credit risk). Furthermore, we do not find the case studies cited in Section II helpful, as they tend to oversimplify both the nature of the risk and its implications.

2.2 Systemic risk

- a) Systemic risk may well be a supervisory concern but it does not - except in the most general terms - relate to the supervision of an individual firm and it cannot be managed by an individual firm's internal controls. This section is therefore completely out of place in a paper on firms' internal controls and should be removed.
- b) The suggestion - in the second paragraph - that OTC derivatives contribute particularly to Systemic risk is flawed and objectionable. Firstly, derivatives can - and do - reduce systemic risk by providing risk reduction tools and, secondly, it is risk which can cause the problem, not the fact that it happens to be packaged up in a particular way (ie a derivative). None of the statements in this paragraph apply uniquely to derivative transactions.

3 Detailed comments on section III

3.1 Firms

- a) The first sentence of this section - "The ultimate goal of a control system is to maximize safeguarding of assets and capital by minimizing the exposures that have the potential to unexpectedly deplete such firm resources" - is an incomplete description. It needs to be counterbalanced by acknowledgement that firms must take a degree of risk in order to make money and that there is a balance to be achieved between the cost of implementing a control and the benefit it brings.

- b) *Risk management and control strategy*

It is impossible to "perform independent evaluations ... to *ensure* compliance" with strategies and policies (first paragraph). The correct objective of evaluation of controls is to provide *reasonable assurance* the policies and procedures are being complied with.

The description of the process for setting a risk management and control strategy (in the second paragraph) would benefit from a recognition that part of that process is determining the risk appetite of a firm.

- c) *Policies and procedures to accomplish the strategy*

There is a discussion of independent risk management and control functions in the latter part of the first paragraph. Whilst this text is not, of itself, objectionable, it could usefully be supplemented by an acknowledgement that the existence of such a function is not a substitute for control functions carried out within the front office - every trader must have a responsibility for staying within limits (or obtaining the necessary approvals for

exceeding them), for example.

The last sentence of the second paragraph focusses on "formalized - written communication" - see comments above under sections I and IV on documentation.

We do not understand the phrase "whether the compliance function is being met" at the end of the fourth paragraph.

In the fifth paragraph, there is a fundamental misunderstanding of the role of external audit ("As part of this work, external auditors will form a view on the effectiveness of the system of internal control") - see 1.5(d) above. In addition, the suggestion that internal audit should report "directly to the governing body" needs to be qualified by a phrase such as "or suitably designated committee thereof".

d) *Risk measurement methodologies*

The first sentence is inaccurate. It is unreasonable - and, arguably, dangerous - to suggest that all risks can be measured. Some would assert that values can be attributed to legal, operational and reputational risks but many firms would disagree and, in any event, such techniques need to be used with extreme caution. Perhaps this sentence should refer to "all identified *financial* risks"?

3.2 Supervisors

a) *Oversight of the risk management and controls process*

The section fails to capture the essential difference between the responsibilities of management and those of supervisors. It suggests a blurring of the two roles in a way which is highly undesirable from both a regulatory and industry perspective. To quote just a few examples:

- *"Thee advantage to supervisors is the ability to directly administer major aspects of the oversight of the risk management and control function"* implies that it is appropriate for supervisors to become directly involved in making management decisions. It is well-established that it is management's role to run the business and that of supervisors to assess whether the way in which the business is run satisfies the relevant regulatory rules;
- *"Supervisors could promulgate the establishment of management controls indirectly through standardsetting groups such as accounting and auditing principles boards"*. Accounting and auditing standard-setters do not - and should not - seek to set standards for internal controls. The accounting bodies set standards for financial reporting which may include *descriptions of* the internal controls which exist and auditing bodies determine the work needed for auditors, to give an opinion on the financial statements - which may involve a review of the internal controls which exist - but neither determines what controls should exist and supervisors should not seek to arrogate them to this end;
- *"A future possibility might be a requirement for auditors to examine risk*

management and controls as part of an audit of a firm in the securities industry". As the paper goes on to acknowledge, this is an area fraught with difficulty and supervisors should not even contemplate such an approach unless and until the auditing profession has resolved the issue for companies generally.

IOSCO risk management and control guidance

Detailed LIBA/SIA/BBA comments: 19th May 1998 (ref: DJC/RSKapr6v3/COM14)