

**RISK MANAGEMENT AND CONTROL GUIDANCE**  
**FOR**  
**SECURITIES FIRMS AND THEIR SUPERVISORS**



**A Report by the Technical Committee**  
**of the**  
**International Organization of Securities Commissions**

**May 1998**

## TABLE OF CONTENTS

<b>I.</b>	<b>Introduction.....</b>	<b>1</b>
<b>II.</b>	<b>The Role of Risk Management and Controls.....</b>	<b>4</b>
<b>III.</b>	<b>Firm and Supervisory Considerations .....</b>	<b>8</b>
<b>IV.</b>	<b>Elements of a Risk Management and Control System.....</b>	<b>13</b>
	<b>Appendix A</b>	
	<b>    Significant Risk Management and Control Papers.....</b>	<b>19</b>
	<b>Appendix B</b>	
	<b>    Risk Management and Control Self-Assessment Grid .....</b>	<b>27</b>

## I. Introduction

This paper provides guidance about controls to securities firms and their supervisors. The primary concern of the paper is guidance relating to risk management and control policies and procedures and internal control systems. The objective of this paper is to promote domestic and international risk management and control structure awareness for firms and regulators. The paper's recommendations are intended to be flexible and non-exclusive, allowing each jurisdiction and firm to implement appropriate policies and procedures. In addition, implementation of the papers' recommendations should be appropriate for the size, complexity and nature of a firms' business and the markets in which it operates. The paper is based on the premise that, although risk management and controls are an integral part of a well run securities firm and the industry as a whole, they are not a substitute for adequate capital requirements. While much has been published on controls from a firm's perspective, this paper addresses controls from a supervisory perspective.

The term "controls" as used in this paper refers to basic internal accounting controls and risk management policies and procedures. Basic internal accounting controls refer to systems which are designed to provide reasonable assurance that transactions are properly recorded and verified including appropriate segregation of duties. Risk management and control systems refer to systems to manage market risk, credit risk, legal risk, operational risk, and liquidity risk.<sup>1</sup>

The nature and scope of risk management and controls by necessity must fit the organization they are going to protect which means they can not be dictated in much detail from without, but must be designed from within to meet the needs of the organizational structure as well as a firm's business practices and appetite for risk. Irrespective of design and implementation, controls can provide only reasonable assurance with respect to fulfilling a firm's control objectives.

The twelve "*Elements of a Risk Management and Control System*" discussed in Section IV constitute the control guidance for firms and supervisors. They are intended to be benchmarks which can be used by firms and supervisors in each jurisdiction to measure the adequacy of their control systems. The elements are grouped under five categories which are considered to be critical elements of any control system:

### **The Control Environment**

- 1. Firms need to establish a mechanism to ensure that they have internal accounting controls and risk management controls. Supervisors need to establish a mechanism to ensure that the entities they regulate have internal accounting controls and risk**

---

<sup>1</sup> These controls refer to the structure of the control environment, the nature and scope of risk management and internal controls, implementation, verification, and reporting taken as a whole. It is a framework by which management of a firm can independently monitor and verify the activities of its revenue producing and support operations.

management controls. The supervisory mechanism need not prescribe specific and detailed controls, but rather provide general guidance to firms.

2. Firms and supervisors need to determine that controls are set and monitored at the senior management level at a firm; responsibility for monitoring controls is clearly defined; and senior management promotes a culture of controls at all levels within a firm.

### **Nature and Scope of Controls**

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

### **Implementation**

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.
7. Firms should have and supervisors should require written documentation about their control procedures.

### **Verification**

8. Firms and supervisors need to determine that controls, once established by management, are effectively operating as designed on a continuous basis.
9. Firms and supervisors 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 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.

## **Reporting**

- 11. Firms need to establish and supervisors should require mechanisms to report material inadequacies or breakdowns in controls to senior management and supervisors 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.**

The recommendations in this paper are designed to help securities firms and their supervisors protect against the risks inherent in the financial and securities activities. The recommendations represent prudent standards that should be compared to the existing firm controls and supervisory frameworks.

The rapid growth and complexity of traditional financial and securities activities requires that their associated risks be identified, monitored, and managed. The recommendations set forth in this paper apply to all types of financial and securities activities.

## II. The Role of Risk Management and Controls

The implementation of strong and effective risk management and controls within securities firms promotes stability throughout the entire financial system. Specifically, internal risk management controls provide four important functions:

- to protect the firm against market, credit, liquidity, operational, and legal risks;
- to protect the financial industry from systemic risk;
- to protect the firm's customers from large non-market related losses (e.g., firm failure, misappropriation, fraud, etc.); and
- to protect the firm and its franchise from suffering adversely from reputational risk.

Sound and effective risk management and controls promote both securities firm and industry stability which, in turn, inspires confidence in the investing public and counterparties. Securities firms have economic and commercial incentives to employ strong risk management internal control systems. Without such controls, a firm is vulnerable to risk.

The importance of effective risk management and controls in protecting against serious and unanticipated loss is perhaps best illustrated by some recent cases where risk management and controls broke down or were not properly implemented, as follows:

### **Market Risk**

Market risk inherent in any investment is the risk that the investment will not be as profitable as the investor expected because of fluctuations in the market. Market risk involves the risk that prices or rates will adversely change due to economic forces. Such risks include adverse effects of movements in equity and interest rate markets, currency exchange rates, and commodity prices. Market risk can also include the risks associated with the cost of borrowing securities, dividend risk, and correlation risk.

An example of the danger inherent of market risk is highlighted in the bankruptcy of Orange County. Orange County's Treasurer used the Orange County Investment Pool's resources to invest in a significant amount of derivative securities, namely "structured notes" and "inverse floaters". When interest rates rose, the rates on these derivatives securities declined along with the market value of those notes (since they were at rates below those generally available in the market). This resulted in a \$1.7 billion loss to the Orange County Investment Pool.

Gibson Greetings, Inc. ("Gibson") faced similar market risk when it began aggressively purchasing interest rate derivatives to take advantage of falling rates. When interest rates began to climb, Gibson sustained a \$20 million loss on its derivatives contracts. Likewise, Procter & Gamble ("P&G") took a \$157 million charge to unwind interest rate derivative contracts that were tied to interest rates in Germany and the United States. When the interest rates rose in both countries above the derivative's contractual hurdle rate (which required P&G to pay interest rates

that were 1 412 basis points above the then commercial paper rate), the leveraged derivatives became too costly for P&G.

### **Credit Risk**

Credit risk involves the possibility that one of the parties to the contract will not perform on its obligations. Credit risk comprises risk of loss resulting from counterparty default on loans, swaps, options, and during settlement. Securities firms are faced with credit risk whenever they enter into a loan agreement, an OTC contract, or extend credit. Credit risk can be minimized by risk management and controls and procedures that require counterparties to maintain adequate collateral, make margin payments, and have contractual provisions for netting.

Credit risk has been recently highlighted in the many U.S. banks who reported in January 1998 that their latest quarterly results were hurt by the Pacific Rim economic crisis. For example, J.P. Morgan reclassified approximately \$600 million of its loans as “non-performing” due to the turmoil in Asia. Its fourth quarter profits fell to \$1.33 a share from \$2.04 a year earlier (35% lower than last year), which were below market expectations of \$1.57 a share.

### **Liquidity Risk**

Liquidity risk is the risk that a party to a securities instrument may not be able to sell or transfer that instrument quickly and at a reasonable price, and as a result, incur a loss. Liquidity risk includes the risk that a firm will not be able to unwind or hedge a position.

An example of liquidity risk is illustrated by the March 1994 \$600 million loss of Askin Management. Askin specialized in mortgage-backed debt instruments known on Wall Street as “toxic waste” because they carried the highest credit and interest rate risk. When interest rates rose sharply, trading in these debt instruments ceased. No market participant would quote Askin a price on his positions anywhere near what he had paid for them. Furthermore, Kidder, Peabody & Co. lost \$25.5 million loaned to Askin to leverage these positions.

### **Operational Risk**

Operational risk is the risk that improper operation of trade processing or management systems will result in financial loss. Operational risk encompasses the risk of loss due to the breakdown in controls within the firm including, but not limited to, unidentified limit excesses, unauthorized trading, fraud in trading or in back office functions including inadequate books and records and a lack of basic internal accounting controls, inexperienced personnel, and unstable and easily accessed computer systems.

The importance of operational risk management and controls is highlighted by the collapse of Barings in February of 1995. Britain’s Board of Banking Supervision concluded that Barings’ failure was due to immense losses from unauthorized and hidden derivatives trading of an employee of Barings Futures Pte. Limited in Singapore, that went virtually undetected by management. The trader had been left unsupervised in his dual role as head of futures trading settlements. Barings’ failure to independently monitor the trader’s activities, as well as its failure

to separate front and back office functions, created operational risk which resulted in large losses and, ultimately, the total collapse of the firm.

Similar poor management led to even larger losses at Japan's Daiwa Bank Ltd. ("Daiwa") in the bond market. In 1995, it was discovered that a bond trader at Daiwa was able to conceal approximately \$1 billion in trading losses because of his access to Daiwa's accounting books. As with Barings, the Daiwa trader was in control of accounts as well as trading activities. Separation of trading and support functions, a fundamental risk management practice, was violated in both.

Another example of operational risk can be found in the situation involving allegations of \$350 million in false trading profit of government securities in Kidder, Peabody & Co. in Spring 1994. At that time, Kidder had determined that nearly \$350 million in "profits" that had been attributed to a trader's trading activity were phantom and arose out of manipulation of the firm's trading and accounting system. This incident resulted in the sale of Kidder's assets to a competitor and ultimately Kidder's liquidation.

Maintaining adequate books and records and internal controls is essential to effectively managing operational risk. In its effort to strengthen its internal control structure, Salomon Inc., in mid-1993, commissioned a detailed review because of some unreconciled differences reported internally by the Company's Financial Division staff and its independent auditors, Arthur Andersen LLP, of material general ledger accounts of Salomon Inc. This review's objective was to ensure the general ledger accounts were properly supported and that appropriate reconciliation procedures were in place. The detailed account review uncovered significant unsupported balances which required pre-tax charges against earnings of \$303 million in 1994. Subsequently, the company has made improvements in its reconciliation and control procedures.

In January 1996, strong risk management controls at Salomon Inc. revealed trading losses arising from mismarked options positions. The trader had assigned incorrect volatilities to mask trading losses. The firm's internal control structure, which included routine spot checks carried out by its risk management area, reacted as it was intended by catching these discrepancies and minimizing the losses to \$15 million.

Operational risk is controlled through proper management procedures including adequate books and records and basic internal accounting controls, a strong internal audit function which is independent of the trading and revenue side of the business, clear limits on personnel, and risk management and control policies. Had proper management oversight, as well as the fundamental risk management and control practice of separating backroom and trading functions, been in place, the losses at Barings and Daiwa could perhaps have been avoided, or at the very least, minimized. The obvious importance of maintaining proper risk management and controls is underscored by these financial failures.

### **Legal Risk**

Legal risk arises from the possibility that an entity may not be able to enforce a contract against another party. Legal risk arises from possible risk of loss due to an unenforceable contract or an

“ultra vires” act<sup>2</sup> of a counterparty. Legal risk involves the potential illegality of the contract, as well as the possibility that the other party entered into the contract without proper authority. For example, the U.K. decision in Hazell v. Hammersmith & Fulham L.B.C., 2 W.L.R. 372 (1991), ruled that swaps transactions entered into by local government authorities were ultra vires, and therefore legally unenforceable contracts. This ruling cost banks approximately \$1 billion in defaulted swap payments. The need for legal clarity is highlighted by the fact that legal counsel in Hazell had made continuous assurances that the swaps contracts were legal and enforceable.

Currently, Orange County has asserted an ultra vires claim in its suit against Merrill Lynch claiming that Merrill Lynch should have known that the contract violated several provisions of the California Constitution, hence rendering the contracts unenforceable.<sup>3</sup> In today’s global environment, major securities firms are faced with substantial litigation both as plaintiff and defendant because of the nature and scope of their business activities.

### **Systemic Risk**

Systemic risk refers to (1) the scenario that a disruption at a firm, in a market segment, or to a settlement system could cause a “domino effect” throughout the financial markets toppling one financial institution after another or (2) a “crisis of confidence” among investors, creating illiquid conditions in the marketplace. Systemic risk encompasses the risk that failure in one firm or one segment of the market would trigger failure in segments of or throughout the entire financial markets.

Over-the-counter derivatives illustrate the supervisory concern with respect to systemic risk. The fact that some financial and securities activities are concentrated in a small number of financial institutions and can be used for unhedged, proprietary speculation creates the potential for a domino effect of systemic risk if a major financial institution is collapsing. This risk is more than a possibility due to the potential for substantial market and trading losses which can result in rapid, global transmission of defaults to the counterparties. This risk is further exacerbated by the interconnection of obligations among the same institutions and with the cash markets.

Although the domestic and international financial markets have withstood large firm losses as seen in the Barings and Daiwa cases, these isolated defaults occurred in the absence of significant market movement. Defaults of unprecedented nature and magnitude could occur in the event of heavy volatility across capital markets, such as currency and equity crashes.

Systemic risk is perhaps the greatest challenge to supervisors and to the financial markets. A uniform, flexible framework of risk management and controls, coupled with adequate capital standards is essential to the continued orderly operation of the global financial markets.

---

<sup>2</sup> An *ultra vires* act is defined as any act performed without legal authority because such act is beyond the scope of powers granted to a corporation, state or municipality.

<sup>3</sup> The California Constitution provides that debts of the country which exceed the revenue for the current year must be approved by two thirds of the voters. (California Const. art. XVI, section 18.)

### **III. Firm and Supervisory Considerations**

#### **A. FIRMS**

The ultimate goal of a control system<sup>4</sup> is to maximize safeguarding of assets and capital by minimizing the exposures that have the potential to unexpectedly deplete such firm resources. The specific components of an effective risk management and control system will vary considerably in sophistication based on the size and complexity of a firm's business operations. However, a well-developed risk management and control system generally should include a comprehensive risk management and control strategy. That would include policies and procedures to accomplish this strategy, risk measurement and control methodologies, compliance monitoring and reporting, and on-going assessment of the effectiveness of the strategies, policies and procedures. The components of an effective risk management and control system are discussed below.

#### **Risk Management and Control Strategy**

The governing body (i.e., a board of directors or its equivalent) of a firm has the ultimate responsibility and accountability for the level of risk undertaken and should function in an oversight capacity. The governing body should approve overall business strategies and risk management and control policies of a firm, and perform independent evaluations (through the internal audit function) to ensure compliance and continuing suitability of established strategies and policies. Firms that have adopted systems of matrix management should have clearly defined lines of reporting at all levels.

The first step in setting a risk management and control strategy is a formal analysis of firm's business activities and the risks of these activities to the firm, ultimately in terms of the risk to capital. From this analysis, quantitative risk exposure limits for each major business activity or product and specifications of the scope of permitted activities should be developed and supported by adequate capital. Once developed, ongoing reviews of the activities and risks of a firm should be conducted on a regular basis and periodic reevaluation of strategies considered based on changes in business and markets. As discussed below, the results of internal and external audits should be reported directly to the governing body.

The level of technical knowledge necessary for governing body members to have or obtain in order to fulfill their duties will vary based on the complexity of the firm's operations and products. In a larger and more complex entity, it would be desirable for members of the governing body to have industry expertise.

---

<sup>4</sup> These controls refer to the structure of the control environment, the nature and scope of risk management and internal controls, implementation, verification and reporting taken as a whole. It is a framework by which management of a firm can independently monitor and verify the activities of its revenue producing and support operations.

### **Policies and Procedures to Accomplish the Strategy**

Once risks have been identified and the general policies toward those risks have been established, firms can develop the detailed and specific guidelines to be used in the day-to-day and long-range operations of the business. Policies and procedures to accomplish the governing body's guidance should include designated lines of authority in the risk management and control process and responsibility for compliance with risk exposure policies, effective internal accounting controls, and internal and external audit. In the case of larger and more complex entities, it may be desirable to establish a centralized and autonomous risk management and control function. Of primary importance is that the risk management and control functions are staffed at an appropriate level of expertise and are independent of risk-generating activities.

Since a control structure is only as effective as the people who operate it, a strong commitment by all personnel within an organization is a prerequisite. In developing the lines of authority and responsibility for the risk management and control process, a primary consideration should be the separation of responsibility for the measurement, monitoring and control of risk from the execution of transactions giving rise to the risk. Senior management should ensure that there is appropriate segregation of duties and that personnel are not assigned conflicting responsibilities. However, humans are fallible and internal control breakdowns can be due to errors, mistakes and collusion. Also of particular importance is formalized written communication throughout the organization of authorized activities, transactions, and risk tolerances.

Effective internal accounting controls and audit procedures are the underlying support for a risk management and control system. Basic internal controls such as authorization for transactions, segregation of duties, safeguards over assets and records, documentation standards and independent verification controls should be consistent between firms. In terms of risk management and capital protection, the most consequential internal controls involve the segregation of duties between the trading function and the internal control and risk management functions and the authorization of transactions.

While defining the respective roles of internal and external auditors is beyond the scope of this paper, it should be stressed that it is important for the supervisor to make judgments on the degree of independence of the respective functions, their relationships with the corporate governance structure, and whether the compliance function is being met.

The internal audit function should be independent of the trading and revenue side of the business and compensation should not be dependent on revenues generated. External auditors operate independently of a firm and their purpose is primarily to express an opinion on the financial statements. As part of this work, external auditors will form a view on the effectiveness of the system of internal control. Internal auditors, by contrast, are not independent of the firm they are auditing, but should be "independent" within the firm by reporting directly to the governing body. Internal auditors are able to tailor their audits to address both financial and operational functions.

Although it may not be suitable for external auditors to report on the general appropriateness of risk management and control policies, the frequency, scope and findings of internal and external auditors are an important independent check on the effective functioning of an established risk management and control system and internal control systems. While each generally has different audit purposes, internal and external auditors often rely on the other's work in determining the nature and extent of audit work to be performed.

### **Risk Measurement Methodologies**

Systems to measure risk must include a methodology that encompasses all identified risks in terms of the firm's positions, markets, currencies and counterparties. Value-at-risk ("VAR") and other mathematical models should be validated frequently, including the assumptions going into the models, and subjected to continued back-testing of the data generated. This methodology should include both sensitivity analysis and stress testing. As an adjunct to a stress testing system, a contingency plan to be followed in adverse circumstances and worst-case scenarios should be developed.

### **Systems for Reporting Compliance with Established Policies and Procedures**

Firms should have in place a risk management and control reporting and review process. This process should include a review mechanism for reporting compliance with established policies and procedures and addressing exceptions. Generally, exposures and profit and loss results should be reported daily to management responsible for risk monitoring who, in turn, should brief senior management responsible for day-to-day operations of the firm.

### **Assessment of the Effectiveness of the Strategies, Policies and Procedures**

Assessment of the effectiveness of established strategies, policies and procedures should be performed regularly. The evaluation should consider the results of established policies, changes in business activities and changes in markets. Material changes to methodologies, models, and assumptions of risk management and control policies should be reviewed by the governing body. Policies and procedures should require that the risk management and control functions be involved in the review of new business products and activities.

## **B. SUPERVISORS**

Supervisors should concern themselves with understanding the control environment of each firm and satisfying themselves as to the adequacy of controls established by management. Supervisors are responsible for regulating the activities of securities firms in order to protect investors in the securities markets and ensure the integrity of those markets. To this end, supervisors must be proactive, rather than reactive, in devising high quality supervision of the dynamic securities industry. In general, supervisors should not be involved in setting specific control standards at each firm. The guidance in this paper is not intended to limit a firm's management from exercising its proper responsibilities. This is not intended to preclude supervisors that have determined controls have fallen below acceptable levels of international

standards or minimum standards in their jurisdictions from setting detailed requirements for a particular firm.

### **Oversight of the Risk Management and Control Process**

While the best method of achieving supervisory goals will depend on the legal, political, and regulatory environments in a jurisdiction, the following are suggestions to supervisors concerning oversight of the risk management and control process.

Supervisors could promulgate regulations requiring the establishment of specified risk management and controls at regulated entities and require periodic reports and examinations of compliance with the regulations. The advantage to supervisors is the ability to directly administer major aspects of the oversight of the risk management and control function. However, this approach may be complicated by legal, jurisdictional and political considerations.

Supervisors could consider a tiering of capital requirements based on the level and sophistication of risk management and controls. This has the advantage of relating the level of capital to the level of capital protection procedures in place. However, universal standards of controls are not practical and the determination of the sufficiency of controls and their actual execution in practice is judgmental and time-consuming to assess.

Supervisors could work with industry associations to advocate certain risk management and control standards for members. The advantage of this recommendation is a “peer pressure” approach to compliance. However, the industry group would be primarily geared to the interests of its members and adherence to suggestions of an industry group would be strictly voluntary. Thus the supervisor would have limited enforcement abilities.

Supervisors could promulgate the establishment of management controls indirectly through standard-setting groups such as accounting and auditing principles boards. The collaboration of the IOSCO Technical Committee with the International Accounting Standards Committee and the International Auditing Practices Committee to establish global accounting and auditing standards for international securities issuers is a concrete example of an effective alliance between supervisors and standard setters. 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. This might motivate the establishment of additional controls if the lack of adequate controls would increase audit time and cost or be mentioned in management or audit reports. However, the difficulty of agreement between the auditing profession and the securities industry about the necessity of such examinations and the lack of objective standards for risk management and control procedures might be road blocks to the prompt adoption of such a standard.

The globalization of firms, markets and systems across geographic and functional boundaries necessitates that supervisors formally harmonize and coordinate regulatory requirements and efforts. The activities of IOSCO’s Technical Committee and the Basle Committee on Banking Supervision are the leading example of the collaboration of supervisors in promoting the stability of financial markets. In June 1996, a Joint Statement concerning cooperation between banking and securities regulators identified significant principles of supervisory cooperation. These included information sharing, supervision of capital, special supervisory arrangements for

diversified firms, the need of supervisors to receive accurate reports of operations and early warnings, and the necessity for periodic enhancements to the supervisory process.

## IV. ELEMENTS OF A RISK MANAGEMENT AND CONTROL SYSTEM

It is generally accepted within the financial industry that a key component for the successful management of risk is a strong and effective risk management and controls structure within each securities firm. The following elements of a sound and effective system of risk management and controls are suggested benchmarks that firms and supervisors in each jurisdiction can use to test the adequacy of the control environment for securities business activities:

### The Control Environment

- 1. Firms need to establish a mechanism to ensure that they have internal accounting controls and risk management controls. Supervisors need to establish a mechanism to ensure that the entities they regulate have internal accounting controls and risk management controls. The supervisory mechanism need not prescribe specific and detailed controls, but rather provide general guidance to firms.**
- 2. Firms and supervisors need to determine that controls are set and monitored at the senior management level at a firm; responsibility for monitoring controls is clearly defined; and senior management promotes a culture of controls at all levels within a firm.**

The control environment is a representation of the attitude, awareness, and actions of a securities firm's governing body and senior management toward the safeguarding of the firm's financial resources and the integrity of internally generated information. The control culture should also be expanded to all staff levels, with a view to promoting a widely shared control culture within the firm. As an example of this concept, Statement of Auditing Standards No. 78 states that the control environment sets the tone of an organization, influencing the control consciousness of its people; it is the foundation for all other components of internal control, providing discipline and structure.<sup>5</sup>

The control environment's effectiveness is influenced by several variables, including:

- Management's attitudes, beliefs, and practices;
- Organizational structure and accountability;
- Nature and scope of the governing body and management committees; and
- Degree of external oversight.

A strong control environment is the essential basis of a firm's efforts to protect itself from unanticipated losses and erosion of capital. When working properly, the internal accounting

---

<sup>5</sup> American Institute of Certified Public Accountants, "Statement of Auditing Standards No. 78, *Consideration of Internal Control in a Financial Statement Audit*", paragraph .07a.

controls and risk management and controls can spot and identify potential problems early on and, while it may not prevent unanticipated losses (nor should it be so extensive as to prevent losses), it can bring such situations quickly to light within the governing body and senior management's thresholds (e.g., Solomon Inc.'s pricing controls described under "operational risk" above). When a firm lacks an adequate control environment, it is at the mercy of unscrupulous employees to take advantage of the firm and, in some instances, with terminal consequences (e.g., the collapse of Barings PLC). The lack of an adequate control environment and "control consciousness" on the part of a firm's governing body and senior management has been at the root of such recent losses at Barings, Daiwa, Kidder Peabody, and NatWest.

The governing body has the ultimate responsibility to a securities firm's owners for understanding the risks and exposures facing a securities firm and ensuring that senior management takes the necessary steps to monitor and control these risks and ascertaining the effectiveness of the risk management and control systems<sup>6</sup>. Senior management, in turn, has the responsibility for day-to-day oversight of the firm's activities, implementing appropriate risk management and control policies, and monitoring risks and exposures to the firm. Both the governing body and senior management are responsible for promoting high standards of ethical conduct.

Supervisors of firms as well as the firms themselves have to be control conscious. Supervisors must be satisfied that the firms they oversee have adequate control environments and that senior management sponsors a culture of control at all levels within a firm. In order to do this, supervisors must have the tools and mechanisms (e.g., statutory authority, financial means, human resources, etc.) to be able to satisfy themselves with respect to the control environment. Certain aspects of this, such as identifying material weaknesses or inadequacies in the system of internal accounting controls may involve the use of independent external auditors. Supervisors should not craft a "one size fits all" detailed control framework, as each institution has unique aspects and characteristics to its organization and the way it conducts business. Rather, supervisors should provide broad, general guidance which is flexible and adaptable to firms as they see fit. This is not intended to preclude supervisors that have determined controls have fallen below acceptable levels of international standards or minimum standards in their jurisdictions from setting detailed requirements for a particular firm.

It is incumbent upon supervisors to ensure that firms' risk management and internal accounting control environment is consistent with the general framework. Each firm should have its control environment documented and approved by its governing body. By documenting the control environment, a firm can clearly illustrate to supervisors and external third parties that it has policies and procedures in place to ensure that the assets and capital of the firm are safeguarded from unauthorized use.

---

<sup>6</sup> This should be read in the context of the legislative and regulatory frameworks in each jurisdiction which may differ in the high level governance and management structures and obligations they impose upon firms at the highest levels.

### **Nature and Scope of Controls**

- 3. Firm guidance and guidance from supervisors 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.**
- 5. Risk management and controls for firms should include controls for overall firm and individual trading desk limits, market risk, credit risk, legal risk, operational risk, and liquidity risk.**

The nature and scope of risk management and controls by necessity must fit the organization they are going to protect which means they can not be dictated in much detail from without, but must be designed from within to meet the needs of the organizational structure as well as a firm's business practices and appetite for risk. Irrespective of design and implementation, controls can provide only reasonable assurance with respect to fulfilling a firm's control objectives.

To be effective, risk management and controls must cover certain basic elements. The basic control elements which should be disseminated as firm guidance by management and guidance from supervisors should cover both internal accounting controls, which include basic books and records requirements, and risk management and controls. Basic internal accounting controls for firms should include books and records requirements which have controls that are designed to safeguard assets of the entity and to safeguard customer property. This needs to be accomplished in an environment where duties are segregated (*i.e.*, front office and back office responsibilities must be separated). Segregation of duties is necessary to reduce the opportunities to allow one person to be in a position to both create and conceal errors in the normal course of business. It is therefore important to assign different people the responsibilities of authorizing transactions, recording transactions, and maintaining custody of assets. For example, this may require the independent verification of pricing securities positions and other information.

Risk management and controls for firms should include controls for overall firm and individual trading desk limits, market risk, credit risk, legal risk, liquidity risk, and operational risk (as discussed in detail above in Section II, "*The Role of Risk Management and Controls*"). The degree of risk that a firm takes is generally not a concern of the regulator. A regulator needs to have a clear understanding of the risk appetite of the firm to review the control structure appropriateness.

### **Implementation**

- 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.**
- 7. Firms should have and supervisors should require written documentation about their control procedures.**

Implementation procedures need to be performed to effectively carry out management's wishes regarding the controls that need to be established in an entity. Without effective implementation procedures the best system of controls will be nothing more than a facade. We have seen examples of this in some recent high profile losses that have been reported by financial institutions where the existence of control systems were documented, but were not properly implemented by the organization.

It is the responsibility of senior management to provide general guidance to the most senior levels and specific and detailed guidance as the information flows to smaller business units and individual trading desks. This can be accomplished with the use of written documentation about control procedures at each level of the control hierarchy. The absence of written evidence of controls should be a warning to firms and supervisors that a weak control environment may exist, which would pose significant risks to a firm, its customers, and institutional counterparties.

The existence of written procedures alone is not assurance that an adequate control environment exists without additional evidence of proper implementation and verification by firm management at all levels and examination procedures by regulators. This means in part that line managers must be actively involved in controls and their frequent use. The procedures that need to be put in place to properly implement a system of internal controls is best left to individual firms. Senior management is responsible for creating an appropriate risk management and control structure within a firm. It must be cost effective. Any implementation procedures in order to be effective must involve management at all levels and should be strictly enforced with severe penalties to employees that circumvent or ignore control directives.

### **Verification**

- 8. Firms and supervisors need to determine that controls, once established by management, are effectively operating as designed on a continuous basis.**
- 9. Firms and supervisors 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 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.**

Verification is an essential element of any risk management and control system. Without a comprehensive set of verification procedures by firms and supervisors the risk of a breakdown in controls somewhere in an organization increases. Firms and supervisors need to determine that controls, once established by management, are operating as designed and keep pace with new products and industry technology.

For firms, the verification procedures must include internal audits conducted by employees that are properly trained and have adequate resources. For supervisors, verification procedures should include to the extent possible examination procedures that allow for some testing of firm controls.

In addition, external audits by independent accountants which cover at least the internal accounting control systems should be part of a firm's annual procedures and should also be mandated by the supervisory authority responsible for firm oversight. In some jurisdictions the use of external auditors may supplement the examination process and may be engaged to do special purpose audits for special problems or concerns. The mix of supervisor exams and special purpose exams by external auditors is left to the decision of each jurisdiction.

Verification procedures relating to controls should be a function of internal and external oversight with four levels of defense:

- Internal day-to-day management;
- an internal audit function;
- external auditors; and
- supervisors.

Line managers are responsible for monitoring and ensuring the effectiveness of controls daily. Internal auditors are responsible for making periodic checks of the system. External auditors are responsible for making independent checks of the control systems. Without taking away or diminishing from the responsibilities of these three groups (line managers, internal and external auditors) supervisors, based upon their individual statutory and regulatory authority, will also use high level review, examination procedures, and other oversight processes to satisfy themselves that no gaps are present in the control environment.

### **Reporting**

**11. Firms need to establish and supervisors should require mechanisms to report material inadequacies or breakdowns in controls to senior management and supervisors 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.**

Reporting on the adequacy of risk management and controls is necessary to maintain an effective and efficient control environment. Firms need to establish and supervisors should require mechanisms to report material inadequacies or breakdowns in controls to senior management and supervisors on a timely basis. Without timely reporting procedures about breakdowns in controls, the effectiveness of controls would be diminished due to the loss of essential and timely information that may be crucial to the decision making process of management and regulators.

Effective reporting procedures can only be maintained if the firm has in place a good information system which will permit accurate and detailed information to be retrieved in a timely and reliable manner. Supervisor's ability to gather and accurately interpret necessary financial and operational information relating to the control environment is critical to effective supervision.

Firms should be prepared to provide supervisors with relevant information about the use of controls in each firm and about control failures under routine and in emergency situations. Supervisors should have mechanisms to share information about controls with each other during these situations. Supervisors' information needs relating to controls will often be sharply focused and potentially very detailed in any emergency situation. While the primary information needs in an emergency situation will be firm-specific, there may also be a need for information relating to depositories, exchanges, and clearing organizations.

## Appendix A. Significant Risk Management and Control Papers

The following is a listing of significant issues papers offering additional firm and supervisory guidance and insight concerning risk management and controls:

### **1997 International Standards on Auditing 400: Risk Assessment and Internal Controls**

The purpose of this International Standard on Auditing is to establish standards and provide guidance on obtaining an understanding of the accounting and internal control systems and on audit risk and its components: inherent risk, control risk and detection risk.

### **July 1997 European Monetary Institute: Internal Control Systems of Credit Institutions**

Basic principles for a sound internal control system. The report is intended to assist banking supervisors in assessing the adequacy of the internal control systems of credit institutions. It draws upon the practical experience of banking supervisors in the European Union and incorporates comments made to a number of international accounting firms.

### **June 1997 Global Supervision of Financial Institutions and Markets Study Group: The Group of Thirty, Global Institutions, National Supervision and Systemic Risk (“Study”)**

The rapid evolution of financial institutions, products and markets is increasingly challenging the effectiveness of management oversight, market discipline, and official supervision. That concern prompted the creation of this study group on the global supervision of financial institutions and markets by the Group of Thirty.

Managing an expanding range of complex products and varied services around the globe and around the clock is a daunting challenge, but it has become business as usual for globally active firms. This operating environment places a premium, as never before, on understanding and managing risk. A key to understanding and managing a firm’s own risk is evaluating how effectively counterparty firms understand and manage theirs; a task that is, if anything, more challenging than the first because of the limited grounds on which to base such a judgment. Most daunting of all is the difficult task facing national supervisors who are charged with setting supervisory requirements for the global operations of complex financial conglomerates while operating within the limits of national legal jurisdiction and supervisory charters. Even as progress is being made in strengthening the international supervisory framework for financial services, the significance of the institutional and geographic boundaries that define the existing framework continues to diminish.

The Study first examines the potential for systemic risk arising from the gap between the global operations of financial institutions and markets and nationally based systems of accounting, reporting, law, and supervision. It then proposes actions that the financial services industry, the accounting profession, supervisors, and legislators should take to promote the continued stability and efficiency of global institutions and markets.

**1996 Deloitte & Touche, “Internal Control Issues In Derivatives Usage: An Information Tool for Considering the COSO Internal Control - Integrated Framework in Derivatives Applications”**

Deloitte & Touche developed this report using published and internal sources supplemented by input from the Project Advisory Council and other interested persons. This report’s purpose is to serve as a reference document, illustrating how the COSO Internal Control - Integrated Framework (“COSO Report”) can be employed by end users to evaluate the effectiveness of internal controls surrounding the use of derivative products.

The Committee of Sponsoring Organizations of the Treadway Commission, commonly referred to as COSO, issued a document in September 1992 (and reissued it in July 1994 - see the “COSO Report” below). COSO believes that COSO Report is useful in assessing control systems and determining how to improve them. In recent years, there have been reports of large, unauthorized losses arising from the use of financial derivatives products. COSO, believing the COSO Report can be used as a basis for reviewing the adequacy and effectiveness of controls over derivatives, requested that Deloitte & Touche LLP author an information tool that would assist organizations in applying the Framework to the control of derivatives.

**November 1996 U.S. General Accounting Office (“GAO”), Report to Congressional Committees, “Financial Derivatives - Actions Taken or Proposed Since May 1994”**

This report is a follow-up to a report the GAO issued in May 1994, “Financial Derivatives: Actions Needed to Protect the Financial System” (see below) that responded to questions regarding derivative products. This report reveals that, although many concerns still remain in the oversight and management of derivatives-related risk, many U.S. market participants and regulators have improved the management and oversight of their derivatives activities consistent with the GAO’s 1994 recommendations. U.S. industry surveys show that dealers and end-users of derivatives have strengthened their risk management and control systems. Other market participants have proposed recommended practices to improve internal control systems and intend to implement such recommendations in the future. In June 1996 an additional six organizations signed the agreement.

**March 15, 1996 Declaration on Cooperation and Supervision of International Futures Markets and Clearing Organizations**

Information-sharing memorandum of understanding signed by 49 futures and option exchanges and clearing houses. The intent was to establish a framework for information sharing between exchanges and clearing houses in the event of certain destabilizing market events.

In June 1996, an additional six organization signed the agreement. Also, the Futures Industry Association issued a final report of “Financial Integrity Recommendations”.

**January 1996 Coopers & Lybrand, Generally Accepted Risk Principles (“GARP”)**

Written by C&L’s Capital Markets and Risk Management practice in consultation with a review panel comprised of representatives from industry (Barclays, JP Morgan and Bank of England) and regulators (CFTC, SEC, SFA and SIB).

A checklist of 89 *Risk Management Principles*, categorized into five broad groups:

- **Risk Management Strategy:** an integrated framework of responsibilities and functions driven from the governing body down to operational levels which identifies, quantifies, and manages the risks of the business. Suggests that a risk management group independent of risk generating functions (such as trading activities) be established, reporting to the executive committee of the governing body;
- **Risk Management Function:** a group charged with the day-to-day responsibility for risk monitoring, measurement and evaluation;
- **Risk Measurement, Reporting and Control:** the development and use of risk and performance measures to ensure that business activities are being managed in accordance with the defined risk management strategies;
- **Operations:** operational controls over front, middle, and back office operations regarding the authorization and reporting of transactions; and
- **Risk Management Systems:** real-time information reporting the results of each risk system.

**December 1995 American Institute of Certified Public Accountants, *Statement on Auditing Standards No. 78 (“SAS 78”): “Consideration of Internal Control in a Financial Statement Audit”***

This statement provides the independent external auditor with guidance on how to assess an entity’s internal control structure during an audit of financial statements in accordance with generally accepted auditing standards (“GAAS”). An assessment of an entity’s internal control system is necessary for the auditor to be able to assess the level of control risk for the assertions set forth in the financial statements, which in turn will determine the extent of testing to be done.

Note that SAS 78 amended SAS 55, *“Consideration of the Internal Control Structure in a Financial Statement Audit”* to recognize the definition and description of internal control contained in *“Internal Control - Integrated Framework”* published by the Committee of Sponsoring Organizations of the Treadway Commission (“COSO Report” - see below). The definition of internal control contained therein is a revision to the second standard of fieldwork of the ten generally accepted auditing standards.

**December 1995 Futures & Options Association, Managing Derivatives Risk - Guidelines for End-Users of Derivatives**

Advisory guidelines for users on procedures and controls necessary in managing derivatives risk.

**July 18, 1995 Report of the Board of Banking Supervision Inquiry into the Circumstances of the Collapse of Barings**

Detailed explanation and analysis of the circumstances and the reasons for the Barings collapse. Presents lessons to be learned by management and regulators involving internal controls, accountability for profits, risk and operations, and failure to follow-up on warning signals (see discussion above regarding “Operational Risk”).

**July 1995 The Tripartite Group of Bank, Securities and Insurance Regulators, The Supervision of Financial Conglomerates**

A cross-industry report written by an international group of banking, securities, and insurance regulators addressing the particular problems in the supervision of financial conglomerates (any group of companies under common control whose exclusive or predominant activities consist of providing significant services in at least two different financial sectors such as banking, securities, or insurance).

The report suggested that the five main areas of interest to supervisors involved capital adequacy, cooperation and exchange of information between supervisors, the impact of individual entities within the conglomerate on the financial stability of the group and of markets, intra-group transactions, and counterparty concentrations on a consolidated basis.

**June 1995 Futures Industry Association Global Task Force on Financial Integrity, Financial Integrity Recommendations for Futures and Options Markets and Market Participants**

Participants from 17 countries cooperated in the issuance of 60 recommendations on exchange-traded derivatives, including those directed at exchanges / clearing houses, brokers / intermediaries, and customers.

In March 1996, an information-sharing memorandum of understanding was reached in a follow-up to the recommendations. In June 1996, a final report of *Financial Integrity Recommendations* was issued (see above).

**May 1995 Basle Committee on Banking Supervision and the Technical Committee of the International Organization of Securities Commissions, Framework for Supervisory Information About the Derivatives Activities of Banks and Securities Firms (“Framework”)**

Basle and IOSCO issued to banking and securities firm supervisors worldwide a framework for supervisory information on the derivatives activities of banks and securities firms. The Framework consisted of a catalogue of data on derivatives activities, broken down into the areas of credit risk, liquidity risk, market risk, and earnings, from which supervisors could draw from

as they expanded and improved their reporting systems. The Framework also included a recommendation that supervisors have available to them a minimum subset.

**April 1995 Basle Committee on Banking Supervision (“Committee”), Planned Supplement to the Capital Accord to Incorporate Market Risks and An Internal Model-Based Approach to Market Risk Capital Requirements**

The Committee proposed to permit banks to use VAR models to determine capital requirements for market risk (“Basle Standard”). During 1994, the Committee investigated the possible use of banks’ proprietary in-house models for the calculation of market risk capital as an alternative to a standardized measurement framework. The proposed approach for a model-based supervisory capital requirement was based on the definition of a series of quantitative and qualitative standards that banks would have to meet in order to use their own systems for measuring market risk, while leaving a necessary amount of flexibility to account for different levels of detail in the systems.

**March 1995 UK Auditing Practices Board “Accounting and Internal Controls Systems and Audit Risk Assessments”, Statement of Auditing Standards 300**

The objective of the statement is to establish standards and provide guidance on audit risk and its components and also on the auditors approach to obtaining an understanding of the accounting and internal control systems.

**March 1995 Derivatives Policy Group (“DPG”), Framework for Voluntary Oversight: A Framework for Voluntary Oversight of the OTC Activities of Securities Firm Affiliates to Promote Confidence and Stability in Financial Markets (“Framework”)**

The DPG was formed to address the regulatory issues arising from the unregulated activities of securities firms. Specifically, the DPG focused on the use of capital at risk models to measure market risk. The Framework provided for the use of proprietary models to measure capital at risk due to OTC derivatives activities but not as a method for calculating minimum capital standards for the DPG.

The DPG defined risk of loss or “capital at risk” to be the maximum loss expected to be exceeded with a probability of one percent over a two-week period. The Framework provided that each firm’s model must capture all material sources of market risk which might impact the value of the firm’s positions. The Framework identified nine specific material sources of risk, or core risk factors, based on interest rate shocks, changes in equity values, and changes in exchange rates.

The Framework also sets forth common audit and verification procedures of the technical and performance characteristics of the models. Each firm’s modeling procedures will undergo an internal and external audit by independent auditors.

**September 1994 Euro-currency Standing Committee of the Central Banks of the Group of Ten countries, A Discussion Paper on Public Disclosure of Market and Credit Risks by Financial Intermediaries**

This report dealt with disclosure issues relating to the risk exposures and risk management performance of trading activities of financial intermediaries. This report is based on the premise that the markets function most efficiently when participants have access to information that facilitates the prompt and accurate pricing of assets. The intent of this report was to stimulate debate on the purpose and scope of public disclosures by all financial intermediaries and encouraging an evolution of disclosures practices that will improve the functioning of financial markets.

**July 1994 The Committee of Sponsoring Organizations of the Treadway Commission (“COSO”), originally issued September 1992, Internal Control - Integrated Framework (COSO Report)**

This report deals with the needs and expectations of management and others. It defines: internal controls; what internal controls can do and cannot do; the organizational roles and responsibilities. The report is organized into four volumes: an Executive Summary; the Framework; Reporting to External Parties and Evaluation Tools.

Note that this report’s definition of internal control revised the second standard of fieldwork of the ten generally accepted auditing standards. This revision caused the issuance of SAS 78, “Consideration of Internal Control in a Financial Statement Audit” (see above) to recognize the new definition and description of internal control, which amended SAS 55.

**July 1994 Basle Committee on Banking Supervision, Risk Management Guidelines for Derivatives and the Technical Committee of the International Organization of Securities Commissions, Operational and Financial Risk Management Control Mechanisms for Over-the-Counter Derivative Activities of Securities Firms**

Basle and IOSCO recommended risk management and control guidelines for derivatives traders in their respective industries. The guidelines built on work already in progress by banking and securities regulators in some of the more advanced financial markets as well as the report issued by the G-30 in 1993. Specifically, the guidelines apply to both dealers and end-users and cover such themes as governing body oversight, internal controls, continuous risk monitoring and audit procedures. Both papers issued the same conclusion: sound internal risk management and control is essential for both banks and securities firms in promoting the stability of the financial markets worldwide.

**May 1994 U.S. General Accounting Office (“GAO”), Financial Derivatives: Actions Needed to Protect the Financial System**

The GAO report (“Report”) was a result of concerns from Congress, federal regulators, and some market participants that knowledge of how to manage and oversee risks associated with derivatives may not have kept pace with their increased use. These concerns were heightened by reports of major losses from derivatives use at that time.

The GAO concluded that no comprehensive industry or federal regulatory requirements existed to ensure that U.S. OTC derivatives dealers followed good risk management and control practices. The GAO stated that primary responsibility for risk management and controls rests with a firm's governing body and senior management. However, there was no regulatory mechanism in place to bring all major OTC dealers into compliance with risk management and control guidelines already issued by regulators.

The GAO further noted that accounting standards for derivatives, particularly those used in hedging, were incomplete and inconsistent and have not kept pace with business practices.

However, the DPG initiative in the U.S. specifically addressed some of the GAO's concerns about the lack of federal oversight of large, non-banking OTC derivatives dealers by volunteering to abide by risk management and control systems that the DPG, Securities and Exchange Commission ("Commission"), and Commodities Futures Trading Commission ("CFTC") all agreed would enhance the risk management and controls within the six firms. Accordingly, since 1995, the Commission and the CFTC have received quarterly information from five of the six DPG members regarding their OTC derivatives affiliates' trading revenues, individual counterparty exposures, credit concentrations, and estimated amounts of capital at risk. This type of disclosure provides a basis for supervisors to assess the adequacy of capital.

In November 1996, the GAO issued a follow-up report (see above).

**July 1993 Global Derivatives Study Group: The Group of Thirty ("G-30"), Derivatives: Practices and Principles ("Study")**

The Study is the first comprehensive study of successful management approaches over derivatives activity. The general goal of the Study was to define a set of sound risk management and control practices for those involved in financial derivatives activity.

Twenty recommendations were offered as a benchmark against which brokers and dealers could measure their own practices. The Study concluded that derivatives by their nature do not introduce risks of a fundamentally different kind or of a greater scale than those already present in the financial markets. Hence, systemic risks are not appreciably aggravated, and supervisory concerns can be addressed within present regulatory structures and approaches. Therefore, the Study concluded the role of the regulators should be to clarify legal uncertainties and resolve legal inconsistencies between countries that may impede risk-reduction procedures such as "netting". The G-30 also concluded that not all industry participants were following the principals presented in the Study.

However, the SEC survey issued to the major U.S. broker-dealers after the G-30 report found these firms substantially in compliance with the G-30 recommendations.

**October 1992 Report of the IOSCO Technical Committee, "Principles for the Supervision of Financial Conglomerates"**

This paper sets out principles which the Technical Committee believes should govern the supervision of financial conglomerates. The principles address the following eight areas:

- Group-Based Risk Assessment
- Investments in Other Group Companies
- Intra-Group Exposures
- Structure of Financial Conglomerates
- Relationships with Shareholders
- Management
- Supervisory Cooperation
- External Auditors

The principles are intended to provide a framework which the Technical Committee believes should guide the development of regulatory practices in this area both in individual countries and in relation to international regulatory cooperation. The paper also discusses the ability of securities regulators to obtain an overview of risks involved, which is different in each case, and the techniques which may need to be employed to this end.

## Appendix B. Risk Management and Control Self-Assessment Grid

The following is a blank self-assessment form which is based upon the twelve Elements of a Risk Management and Control System, as discussed above in part IV of this document. Each country is encouraged to complete the form so that their approach can be published in the confidential section of the IOSCO Web Site as part of this Appendix.

<b>CONTROL ELEMENTS</b>	<b>RESPONDING COUNTRY APPROACH</b>
<p data-bbox="240 785 594 816"><b><u>The Control Environment</u></b></p> <ol data-bbox="240 863 824 1640" style="list-style-type: none"><li data-bbox="240 863 824 1304">1. Firms need to establish a mechanism to ensure that they have internal accounting controls and risk management controls. Supervisors need to establish a mechanism to satisfy themselves that the entities they regulate have internal accounting controls and risk management controls. The supervisory mechanism need not prescribe specific and detailed controls, but rather provide general guidance to firms.</li><li data-bbox="240 1350 824 1640">2. Firms and supervisors need to determine that controls are set and monitored at the senior management level at a firm; responsibility for monitoring controls is clearly defined; and senior management promotes a culture of controls at all levels within a firm.</li></ol> <p data-bbox="240 1724 643 1755"><b><u>Nature and Scope of Controls</u></b></p> <ol data-bbox="240 1801 824 1940" style="list-style-type: none"><li data-bbox="240 1801 824 1940">3. Firm guidance and guidance from supervisors should cover both internal accounting controls and risk management and controls.</li></ol>	

<b>CONTROL ELEMENTS</b>	<b>RESPONDING COUNTRY APPROACH</b>
<p data-bbox="240 352 824 571">4. Internal accounting controls for firms should include books and records requirements and segregation of duties controls that are designed to safeguard assets of the entity and to safeguard customer property.</p> <p data-bbox="240 617 824 835">5. Risk management and controls for firms should include controls for overall firm and individual trading desk limits, market risk, credit risk, legal risk, operational risk, and liquidity risk.</p> <p data-bbox="240 915 456 947"><b><u>Implementation</u></b></p> <p data-bbox="240 993 824 1283">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.</p> <p data-bbox="240 1329 824 1434">7. Firms should have and supervisors should require written documentation about their control procedures.</p> <p data-bbox="240 1514 402 1545"><b><u>Verification</u></b></p> <p data-bbox="240 1591 824 1770">8. Firms and supervisors need to determine that controls, once established by management, are effectively operating as designed on a continuous basis.</p> <p data-bbox="240 1816 824 1992">9. Firms and supervisors need to establish mechanisms to verify that controls, once established, are being followed. The verification procedures should include internal audits, which should</p>	

<b>CONTROL ELEMENTS</b>	<b>RESPONDING COUNTRY APPROACH</b>
<p>be independent of the trading desks and the revenue side of the business, and external audits 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.</p> <p>10. Firms and supervisors need to determine that controls, once established, keep pace with new products and industry technology.</p> <p><b><u>Reporting</u></b></p> <p>11. Firms need to establish and supervisors should require mechanisms to report material inadequacies or breakdowns in controls to senior management and supervisors on a timely basis.</p> <p>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.</p>	