# Statement of Guidance

### Internal controls – Securities Investment Business

## 1. Statement of Objectives

To set standards of best practice regarding internal controls.

## 2. Management Control Culture and Oversight

2.1. A licensee must ensure that its internal controls and systems are adequate for the size, nature and complexity of its activities.

2.2. The governance and control environment as established by the Board of the licensed entity, must set the culture and permeate every business activity and operational aspect of the entity. It must demand a high level of control consciousness and expect every employee to contribute to its effectiveness.

2.3. Compliance

Internal controls should facilitate compliance with applicable laws, regulations, policies and guidelines of the Authority and the licensee's own policies and procedures. In addition, the licensee should review whether its policies, practices and controls remain sufficient and appropriate for the business. A licensee should establish and maintain at all times effective systems of internal control and must be able to describe and demonstrate the objectives and operation of the systems to its auditor, reporting accountant and the Authority.

2.4. Management Oversight and the Control Culture

2.4.1 Board of Directors

The board of directors should have responsibility for approving and periodically reviewing the overall business strategies and significant policies of the licensee; understanding the major risks run by the

licensee, setting acceptable levels for these risks and ensuring that senior management takes the steps necessary to identify, measure, monitor and control these risks; approving the organisational structure; and ensuring that senior management is monitoring the effectiveness of the internal control system. The board of directors is ultimately responsible for ensuring that an adequate and effective system of internal controls is established and maintained.

a) The board of directors provides governance, guidance and oversight to senior management. Board members should be objective, capable, and inquisitive, with a knowledge or expertise of the activities of and risks run by the bank. The board should consist of some members who are independent from the daily management of the bank. A strong, active board, particularly when coupled with effective upward communication channels and capable financial, legal, and internal audit functions, provides an important mechanism to ensure the correction of problems that may diminish the effectiveness of the internal control system.

b) The board of directors should include in its activities (1) periodic discussions with management concerning the effectiveness of the internal control system, (2) a timely review of evaluations of internal controls made by management, internal auditors, and external auditors, (3) periodic efforts to ensure that management has promptly followed up on recommendations and concerns expressed by auditors and supervisory authorities on internal control weaknesses, and (4) a periodic review of the appropriateness of the licensee's strategy.

2.4.2  Senior Management

Senior management should have responsibility for implementing strategies and policies approved by the board; developing processes that identify, measure, monitor and control risks incurred by the

licensee; maintaining an organizational structure that clearly assigns responsibility, authority and reporting relationships; ensuring that delegated responsibilities are effectively carried out; setting appropriate internal control policies; and monitoring the adequacy and effectiveness of the internal control system.

a) Senior management is responsible for carrying out the directives of the board of directors, including the implementation of strategies and policies and the establishment of an effective system of internal control.

b) It is important that senior management take steps to ensure that activities are conducted by qualified staff that have appropriate experience and technical capabilities. The allocation of duties and responsibilities should ensure that there are no gaps in reporting lines and that an effective level of management control is extended to all levels of the licensee and its various activities.

c) Staff in control functions must be properly remunerated. Staff training and skills should be regularly updated. Senior management should institute compensation and promotion policies that reward appropriate behaviours and minimise incentives for staff to ignore or override internal control mechanisms.

2.4.3 Control culture
The board of directors and senior management are responsible for promoting high ethical and integrity standards, and for establishing a culture within the organisation that emphasises and demonstrates to all levels of personnel the importance of internal controls. All personnel need to understand their role in the internal controls process and be fully engaged in the process.

a) An essential element of an effective system of internal control is a strong control culture. This includes the ethical values that

management displays in their business dealings, both inside and outside the organisation. The Board and senior management, through their words, attitudes and actions, affect the integrity, ethics and other aspects of the licensee's control culture.

b) In varying degrees, internal control is the responsibility of everyone in the organisation. Almost all employees produce information used in the internal control system or take other actions needed to effect control. An essential element of a strong internal control system is the recognition by all employees of the need to carry out their responsibilities effectively and to communicate to the appropriate level of management any problems in operations, instances of non-compliance with any code of conduct, or other policy violations or illegal actions that are noticed. This can best be achieved when operational procedures are contained in clearly written documentation that is made available to all relevant personnel. It is essential that all personnel within the entity understand the importance of internal control and are actively engaged in the process.

c) In reinforcing ethical values, entities should avoid policies and practices that may inadvertently provide incentives or temptations for inappropriate activities. Examples of such policies and practices include undue emphasis on performance targets or other operational results, particularly short-term ones that ignore longer-term risks; compensation schemes that overly depend on short-term performance; ineffective segregation of duties or other controls that could allow the misuse of resources or concealment of poor performance; and insignificant or overly onerous penalties for improper behaviours.

d) While having a strong internal control culture does not guarantee that an organisation will reach its goals, the lack of such a culture

provides greater opportunities for errors to go undetected or for improprieties to occur.

# 3. Risk Recognition and Assessment

3.1. An effective internal control system requires that the material risks that could adversely affect the achievement of the entity's goals are being recognised and continually assessed. This assessment should cover all risks facing the entity.

    3.1.1 SIB businesses are in the business of risk-taking. Consequently it is imperative that, as part of an internal control system, these risks are being recognised and continually assessed. From an internal control perspective, a risk assessment should identify and evaluate the internal and external factors that could adversely affect the achievement of the SIB's performance, information and compliance objectives. This process should cover all risks faced by the SIB and operate at all levels within the SIB.

    3.1.2 In order for risk assessment, and therefore the system of internal control, to remain effective, senior management needs to continually evaluate the risks affecting the achievement of its goals and react to changing circumstances and conditions. Internal controls may need to be revised to appropriately address any new or previously uncontrolled risks.

# 4. Control Activities and Segregation of Duties

4.1. Control activities should be an integral part of the daily activities of a SIB. An effective internal control system requires that an appropriate control structure is set up with control activities defined at every business level. These should include: top level reviews; appropriate activity controls for different departments or divisions; physical controls; checking for compliance with exposure limits and follow-up on non-compliance; a system of approvals and

authorisations; and, a system of verification and reconciliation.

4.2. Control activities are designed and implemented to address the risks that the SIB identified through the risk assessment process described previously. Control activities involve two steps: (1) the establishment of control policies and procedures; and (2) verification that the control policies and procedures are being complied with.

4.2.1 Top level reviews – Boards of directors and senior management often request presentations and performance reports that enable them to review the SIB's progress toward its goals. For example, senior management may review reports showing actual financial results to date versus the budget. Questions that senior management generates as a result of this review, and the ensuing responses of lower levels of management, represent a control activity which may detect problems such as control weaknesses, errors in financial reporting or fraudulent activities.

4.2.2 Activity controls – Department or division level management receives and reviews standard performance and exception reports on a daily, weekly or monthly basis. Functional reviews occur more frequently than top-level reviews and usually are more detailed. As with the top-level review, the questions that are generated as a result of reviewing the reports and the responses to those questions represent the control activity.

4.2.3 Physical controls – Physical controls generally focus on restricting access to tangible assets, including cash and securities. Control activities include physical limitations, dual custody, and periodic inventories.

4.2.4 Compliance with exposure limits – An important aspect of internal controls is a process for reviewing compliance with such limits and

follow-up on instances of non-compliance.

4.2.5 Approvals and authorisations – Requiring approval and authorisation for transactions over certain limits ensures that an appropriate level of management is aware of the transaction or situation, and helps to establish accountability.

4.2.6 Verifications and reconciliations – Verifications of transaction details and activities and the output of risk management models used by the SIB are important control activities. Periodic reconciliations, such as those comparing balances and positions with exchanges, approved exchanges, clearing houses and intermediate brokers as recorded by the SIB with the position statement issued by the exchange may identify activities and records that need correction. Consequently, the results of these verifications should be reported to the appropriate levels of management whenever problems or potential problems are detected.

4.2.7 Control activities are most effective when they are viewed by management and all other personnel as an integral part of, rather than an addition to, the daily activities of the SIB. When controls are viewed as an addition to the day-to-day activities, they are often seen as less important and may not be performed in situations where individuals feel pressured to complete activities in a limited amount of time. In addition, controls that are an integral part of the daily activities enable quick responses to changing conditions and avoid unnecessary costs.

4.2.8 Senior management must regularly ensure that all areas of the SIB are in compliance with stated policies and procedures and ensure that existing policies and procedures remain adequate. This is usually a major role of the internal audit function.

4.3. An effective internal control system requires that there is appropriate segregation of duties and that personnel are not assigned conflicting

responsibilities. SIB's have fiduciary responsibilities to their clients, internal controls should ensure that no conflict of interest exists.

4.3.1 Assigning conflicting duties to one individual (for example, responsibility for both the front and back offices of a trading function) gives that person access to assets of value and the ability to manipulate financial data for personal gain or to conceal losses. Consequently, certain duties within a SIB should be split, to the extent possible, among various individuals in order to reduce the risk of manipulation of financial data or misappropriation of assets.

4.3.2 At all times, client transactions must take precedent over personal trades and client assets must be clearly segregated from the assets of the licensee.

4.3.3 In order to reduce potential areas of conflict, entities should have in place systems:

a) to monitor client's requests for purchases and sales;
b) for recording receipts from clients;
c) for the approval of the disbursement of funds and the actual disbursement;
d) to provide information to customers about their positions while marketing to the same customers; and
e) any other areas where significant conflicts of interest emerge and are not mitigated by other factors.

4.3.4 Areas of potential conflict should be identified, minimised, and subject to careful monitoring by an independent third party. There should also be periodic reviews of the responsibilities and functions of staff to ensure that they are not in a position to conceal inappropriate actions.

# 5. Information and Communication

5.1. An effective internal control system requires that there are adequate and comprehensive internal financial, operational and compliance data, as well as external market information about events and conditions that are relevant to decision making. Information should be reliable, timely, accessible, and provided in a consistent format.

5.1.1 Adequate information and effective communication are essential to the proper functioning of a system of internal control. From the SIB's perspective, in order for information to be useful, it must be relevant, reliable, timely, accessible, and provided in a consistent format. Information includes internal financial, operational and compliance data, as well as external market information about events and conditions that are relevant to decision making. Internal information is part of a record-keeping process that should include established procedures for record retention.

5.1.2 An effective internal control system requires that there are reliable information systems in place that cover all significant activities of the SIB. These systems, including those that hold and use data in an electronic form, must be secure, monitored independently and supported by adequate contingency arrangements.

5.1.3 A critical component of a SIB's activities is the establishment and maintenance of management information systems that cover the full range of its activities. This information is usually provided through both electronic and non-electronic means. SIBs must be particularly aware of the organisational and internal control requirements related to processing information in an electronic form and the necessity to have an adequate audit trail. Management decision-making could be adversely affected by unreliable or misleading information provided by systems that are poorly designed and controlled.

5.1.4 Electronic information systems and the use of information technology

have risks that must be effectively controlled by SIBs in order to avoid disruptions to business and potential losses. Controls over information systems and technology should include both general and application controls. General controls are controls over computer systems (for example, mainframe, client/server, and end-user workstations) and ensure their continued, proper operation. General controls include in-house backup and recovery procedures, software development and acquisition policies, maintenance (change control) procedures, and physical/logical access security controls. Application controls are computerised steps within software applications and other manual procedures that control the processing of transactions and business activities. Application controls include, for example, edit checks and specific logical access controls unique to a business system.

5.1.5 In addition to the risks and controls above, inherent risks exist that are associated with the loss or extended disruption of services caused by factors beyond the SIB's control. In extreme cases, since the delivery of corporate and customer services represent key transactional, strategic and reputational issues, such problems could cause serious difficulties for SIB's and even jeopardise their ability to conduct key business activities. This potential requires the SIB to establish business resumption and contingency plans using an alternate off-site facility, including the recovery of critical systems supported by an external service provider. The potential for loss or extended disruption of critical business operations requires an institution-wide effort on contingency planning, involving business management, and not focused on centralised computer operations. Business resumption plans must be periodically tested to ensure the plan's functionality in the event of an unexpected disaster.

5.2. An effective internal control system requires effective channels of communication to ensure that all staff fully understand and adhere to policies

and procedures affecting their duties and responsibilities and that other relevant information reaches the appropriate personnel.

5.2.1 Without effective communication, information is useless. Senior management of SIB's need to establish effective paths of communication in order to ensure that the necessary information is reaching the appropriate people. This information relates both to the operational policies and procedures of the SIB as well as information regarding the actual operational performance of the organisation.

5.2.2 The organisational structure of the SIB should facilitate an adequate flow of information – vertical and lateral. Two-way communication facilitates goal congruence and effective information dissemination.

# 6. Monitoring Activities and Correcting Deficiencies

6.1. The overall effectiveness of the SIB's internal controls should be monitored on an ongoing basis. Monitoring of key risks should be part of the daily activities of the SIB as well as periodic evaluations by the business lines and internal audit.

6.1.1 Since securities business is a dynamic, rapidly evolving industry, licensees must continually monitor and evaluate their internal control systems in the light of changing internal and external conditions, and must enhance these systems as necessary to maintain their effectiveness. In complex, multinational organisations, senior management must ensure that the monitoring function is properly defined and structured within the organisation.

6.1.2 Monitoring the effectiveness of internal controls can be done by personnel from several different areas, including the business function itself, financial control and internal audit. Senior management should clearly identify those personnel who are responsible for monitoring

functions. Monitoring should be part of the daily activities of the SIB but also include separate periodic evaluations of the overall internal control process. The frequency of monitoring different activities of a SIB should be determined by considering the risks involved and the frequency and nature of changes occurring in the operating environment.

6.1.3 Ongoing monitoring activities can offer the advantage of quickly detecting and correcting deficiencies in the system of internal control. Such monitoring is most effective when the system of internal control is integrated into the operating environment and produces regular reports for review. Examples of ongoing monitoring include the review and approval of trade entries.

6.1.4 Although typically retrospective, separate evaluations allow an organisation to take a fresh, comprehensive look at the effectiveness of the internal control system and specifically the monitoring activities. Separate evaluations of the internal control system often take the form of self-assessments. The documentation and the results of the evaluation is then reviewed by senior management.

6.2. There should be an effective and comprehensive internal audit of the internal control system carried out by operationally independent, appropriately trained and competent staff. The internal audit function, as part of the monitoring of the system of internal controls, should report directly to the board of directors or its audit committee, and to senior management. Reports of the internal audit function should be available to the Authority.

6.2.1 The internal audit function is an important part of the ongoing monitoring of the system of internal controls because it provides an independent assessment of the adequacy of, and compliance with, the established policies and procedures. It is critical that the internal audit function is independent from the day-to-day functioning of the SIB and that it has access to all activities conducted by the licensee, including,

where applicable, at its branches and subsidiaries.

6.3. Internal control deficiencies, whether identified by business line, internal audit, or other control personnel, should be reported in a timely manner to the appropriate management level and addressed promptly. Material internal control deficiencies should be reported to senior management and the board of directors.

6.3.1 Internal control deficiencies, or ineffectively controlled risks, should be reported to the appropriate person(s) as soon as they are identified, with serious matters reported to senior management and the board of directors. The internal auditors should conduct follow-up reviews or other appropriate forms of monitoring and immediately inform senior management or the board of any uncorrected deficiencies. In order to ensure that all deficiencies are addressed in a timely manner, senior management should be responsible for establishing a system to track internal control weaknesses and actions taken to rectify them.

6.3.2 The board of directors and senior management should periodically receive reports summarising all control issues that have been identified. Issues that appear to be immaterial when individual control processes are looked at in isolation, may well point to trends that could, when linked, become a significant control deficiency if not addressed in a timely manner.