Securities and Exchange Commission, Thailand

Internal Control and Compliance - Guidelines for Sound Practice

June 2000

Contents

Overview

The primary objective of this Guideline is to improve the understanding of what is sound practice in internal control and regulatory compliance amongst market participants/intermediaries.

It is recognised that securities regulation in Thailand is still in a development phase and it is recognised that more depth and guidance is required in support of the regulations to assist rather than set hurdles for the intermediaries. It is recognised further, that the development of a mature set of regulations tailored for a market at a particular stage in its development is no simple matter and is not one that may be addressed at very short notice. Rather it is something which evolves. Accordingly these "Internal Control and Compliance - Guidelines for Sound Practice" should not be seen as a quasi regulation. Rather, they should be seen as a set of principles that embody sound practice and may assist as a learning aid within intermediary organisations and in setting up an infrastructure around which a culture of compliance may develop within the market.

It must be noted also that whilst these principles try to assist with the "how-to" elements of internal control and compliance, there is no single correct method or blueprint for being fully compliant. Some compliance departments are "watchdogs", some are "bloodhounds" and some operate as consultative "centres of excellence", but one must not be fooled by "form over substance", regardless of which model is being applied, the best houses understand the need for compliance and have built a culture of sound practice in internal control and compliance throughout the organisation and for which every person in the organisation is responsible.

Responsibility for compliance within an intermediary is not just the responsibility of the Compliance Department, it is the responsibility of every member of the organisation and often even beyond, to their families. Accordingly, each and every staff member should be familiar with what guidelines constitute sound internal control and compliance practice and understand how that affects them in the performance of their duties and in their interaction with clients, family, friends etc. outside of the organisation.

Accordingly, as far as possible, the principles should be simple and straightforward and provide meaningful guidance for staff and management to follow and reflect accurately the SEC's expectations in relation to internal controls and compliance.

As such, in total, these principles should seek to ensure that the company will have an appropriate internal management system which can identify, monitor and control risks in relation to its securities business, both in its existing product lines and planned new business.

Adherence to such principles should provide investors with confidence that such a company is a safe and worthy one with which to do business.

The organisation of this document

This document is organised into three parts and a brief description of the content and purpose of each part is provided below:

Part I – Understanding and analysing the securities business

Part I outlines company-wide issues which emphasise the need to develop:

- capabilities in core organisational areas
- an effective communication programme to keep employees informed of the company's operating environment, internal control and regulatory compliance requirements

In short, the company should ensure:

- an effective organisational structure (e.g. well-defined roles and responsibilities with clear reporting lines and segregation of duties)
- comprehensive and effective policies and procedures in all operational areas
- a sound management information system and the ability to use the company systems effectively
- employees having the right qualifications, skills and experience to implement internal control and compliance procedures

Part II – Sound practices for internal control and compliance

Part II deals with the operational areas and issues pertinent to the securities industry (e.g. Confidentiality policy, Chinese walls and front and back office procedures). Each section contains:

- sound practice recommendations
- explanation of the topic or recommendations; and
- examples of controls, where it is deemed appropriate

It also contains sound practice recommendations on business conduct and professional ethics for employees engaged in client advisory and front office work as well as for compliance professionals.

Part III – Preventive and detective measures against breaches in compliance

Part III outlines those instances where fraud and breaches in regulatory reporting occur and recommends sound practices to deal with the situation. However, recommendations in Part III are equally relevant in dealing with other breaches in compliance and internal control. Thus, the company can view the "features of good practice" as a checklist to assess its adequacy in internal control and compliance procedures.

Part I Understanding and analysing the securities business

1. The business and related inherent risks

1.1 Organisational structure

The Board of Directors has the ultimate responsibility for establishing an effective organisational structure in order to ensure that business operations are conducted in a sound, efficient and effective manner.

Appropriate segregation of duties

1.1.1 The Board of Directors should ensure that, where practical, supervisory and internal review functions, including internal audit and compliance, are effectively segregated from line operations in order to reduce the risk of manipulation of financial data and misappropriation of assets. Policy, procedural or control development would normally be overseen by a Controls Committee but this Committee would include representations from line management.

1.1.2 There should be proper segregation of duties within the key operational functions including, but not limited to, front office, middle office, and back office minimising the potential for conflicts, errors or abuse. The extent to which the proper segregation of duties is employed is contingent, in part, upon the size of the business. Examples of duties which are normally segregated may include the following:

- the broking function is independent of and properly segregated from the corporate finance / investment banking function
- trade confirmation process is independent of the sales and trade execution function
- the settlement of trade process is independent of the sales and trade execution function
- the research function is properly segregated from the corporate finance and broking function
- the proprietary trading function is properly segregated from the corporate finance function and the client broking function

1.1.3 Segregation of duties should also address those instances where an individual assumes conflicting responsibilities e.g. where an individual is responsible for the approval of the disbursement of funds and the actual disbursement itself.

1.1.4 As far as possible, the Compliance Function and Internal Audit should be segregated from, and independent of, operational and related supervisory functions. It is important that the Compliance Function and Internal Audit have access to the Board of Directors, either directly or via the Audit and Compliance Committees.

1.1.5 Areas of potential conflict should be identified and carefully monitored. There should also be a periodic review of the responsibilities and functions of key individuals to ensure that they are not in a position to conceal inappropriate actions.

Skills, qualifications and training

1.1.6 The Board of Directors should ensure that positions are filled by employees with the appropriate level of skills and qualifications. This is especially important for senior and supervisory roles where industry knowledge and experience is key to the effective discharge of their duties.

1.1.7 There should be on going and relevant on and off-the-job training for employees in order to keep them abreast with industry knowledge and skill requirements.

Well-defined roles and responsibilities and clear reporting lines

1.1.8 Every position in the company, especially senior and supervisory positions, should have well-defined roles and responsibilities with clear reporting lines. This not only ensures employees understand the scope and objectives of their job functions, but more importantly, how and to whom to escalate issues as and when such issues arise.

Effective communication

1.1.9 There should be regular and effective communication within the company to ensure that staff have access to the company's organisational structure and understand their roles and responsibilities within the organisation. At a minimum, the following information must be available to employees either through the company's operation manuals or the intranet:

- organisation chart of the company and each department
- roles and responsibilities of each department
- job descriptions (at least for senior and supervisory positions)
- Business Code of Conduct (if available)
- Compliance Manual (if available)

1.2 Products and services

Products and services and their characteristics should be documented and communicated to staff in order to improve staff awareness and knowledge.

1.2.1 Senior management should ensure that an appropriate department with the required knowledge is assigned the responsibility to document and update information on products and services.

1.2.2 Product and services information should be accessible by employees and would ideally be documented in the company's operations manuals or intranet and may include:

- product name and type (equity, equity warrant, debt, futures and etc.)
- exchange traded or OTC

- name of Exchange, Clearing houses and central depositories
- settlement period and mechanisms
- board lot, tick size and contract specifications
- information on brokerages, stamp duty and other charges
- types of services (advisory, underwriting, broking and etc.)

1.2.3 Changes in product characteristics or new products should be approved by a New Products Committee or senior management and updated within the company's operations manuals or Intranet before being launched or the changes taking effect.

1.3 Company history and information

Relevant information about the industry and the company as part of the industry should be communicated to staff.

1.3.1 Information relating to the industry and the company can be documented and distributed in staff newsletters or the annual report. This includes:

- history of the securities industry
- the role of the securities industry in the economy and its significance in the global and domestic markets e.g. market share, contribution to national output and number of people employed
- challenges and issues facing the industry e.g. deregulation, disintermediation, globalisation and internet trading
- history of the company and its involvement in the securities industry

1.3.2 In order to improve compliance culture, management should communicate to employees the importance of internal control and compliance through staff newsletters or the annual report. Such communications may include:

- importance of internal control and compliance
- the role of the compliance and internal audit function
- the role of the regulator, both within the industry and within the company itself
- expectation of the company on each employee in relation to internal control and compliance
- the need and benefits of specific internal control and compliance initiatives, proposed or undertaken by the company. This can be used as a more illustrative example to further improve staff awareness on internal control and compliance

1.4 Human resource policies and practices

Human resource policies and procedures should be in place to ensure staff are suitable, observe high standards of integrity, are adequately trained and properly supervised to perform the duties for which they are employed.

1.4.1 As part of the recruitment process, management should carry out background checks on all candidates recommended for hire. These may entail obtaining references from the candidate's previous employers and independently checking with relevant self-regulating bodies or government agencies about the candidate.

1.4.2 If there are any doubts concerning a candidate's "fitness and propriety", the manager in-charge of recruitment should consult the Compliance Function for advice and further investigative actions prior to hiring.

1.4.3 Recruitment criteria should be carefully planned by the Human Resource department together with the management of each specific business unit. Recruitment criteria can include such as:

- possession of the necessary registration
- fit and proper
- academic qualification, skills and training
- entrepreneurship
- work experience and track record
- reference and testimonials
- leadership quality

1.4.4 At all times, management should make clear to employees the consequences of breaching applicable laws, regulations and company policies.

Suitability

1.4.5 There should be appropriate policies and procedures in place to ensure that the company recruits people with relevant and appropriate skills for the job and that such persons are duly registered with all applicable bodies as required.

High standards of integrity

1.4.6 The company should employ persons who are fit and proper to perform the duties for which they are employed.

Adequate training

1.4.7 Management should ensure that all employees receive adequate structured training and on-the-job training suitable for their specific duties both initially and on an on-going basis.

Proper supervision

1.4.8 There must be appropriate senior management supervision and sign-off for key tasks performed by the staff.

1.5 Operating system

The operating system employed by the company should be appropriately designed in order to reflect the complexities of the business and should be documented and defined in sufficient detail to properly record the key operating systems of the business, for the purposes of management control and to improve staff understanding.

1.5.1 The operating system of the company is the combination of manual, semi-manual and computer systems that together help run the operations of the company.

1.5.2 An overview depicting all systems used and system interfaces is essential to foster better understanding. Where possible, the input, computer / manual processes and output should be appropriately detailed.

1.5.3 The systems should be differentiated between those that relate to the company's business and supporting functions to improve staff understanding of business critical systems and assist in inter-system reconciliation planning.

1.6 Applicable laws & regulations

There should be policies and procedures in place which ensure that all employees understand the legal and regulatory environment in which the company operates and which assist in ensuring that the company remains in compliance with such laws and regulations.

1.6.1 The Compliance Function of the company should be responsible for designing and implementing a compliance programme to educate employees on applicable laws and regulations that the company must comply with.

1.6.2 The Compliance Programme may include:

- compliance policies for the company and specific departments
- compliance briefing / training as and when required. Ideally employees should be briefed at the time of induction into the company and at least on an annual basis
- the Compliance Programme may have common or differing content based on staff seniority and job functions and responsibilities

1.6.3 In general, employees should understand the nature and relevant laws and regulations governing the securities industry that are relevant to their business activity, e.g.:

Acts governing Companies

Securities & Exchange Commission Act B.E. 25

Laws concerning foreign companies (if applicable)

Rules and regulations of the Stock Exchange of Thailand

Rules and regulations of the Securities Depository Centre including any other regulatory body relevant to the business of the company

1.7 Social influence

Information on the social influence of the company should be communicated to staff to improve awareness.

1.7.1 The company and the securities industry as a whole have great social influence on the economy and investor confidence. Thus, staff should be aware of the importance of maintaining the integrity of the industry and companies within it at all times. Social influence includes:

- reputation of the financial system of the country
- transparency / accountability of the financial system
- market discipline of participants
- investor protection against unfair trading practices
- fair competition for all participants

2. Information systems environment

A critical component of the company's operations is the establishment and maintenance of information systems that cover the full range of its activities. This information is usually provided through both electronic and non-electronic means. The company must be particularly aware of the organisational and internal control requirements related to processing information in an electronic form.

The Board of Directors and senior management of the company should ensure that the company's operating and information management systems (including electronic data processing (EDP) systems) meet the company's needs and operate in a secure and adequately controlled environment.

As the use of electronic information systems and information technology have risks, the Board of Directors and senior management should implement effective controls and disaster recovery planning in order to avoid disruptions to business and potential losses.

2.1 Management information system (MIS)

Senior management must ensure that there are appropriate information systems in place that cover all activities of the company. These systems, including those that hold and use data in an electronic form, must be secure and periodically tested.

2.1.1 Management information systems include front and back office systems, accounting systems, PC based systems (e.g. spreadsheets) and other computer systems that provide management with information to run the company's business.

2.1.2 Senior management should ensure that the company's management information systems meet the company's needs and are able to provide timely and accurate management information without requiring excessive manual intervention.

2.1.3 Where fragmented systems are used and the need for manual intervention is unavoidable, controls such as daily inter-system reconciliations must be carried out to ensure data integrity.

2.1.4 Senior management should ensure that appropriate employees have access to information regarding the company's systems which include:

- linkages and interface between different systems
- input, computer processes / manual interventions and output of each system
- brief information of the respective systems e.g. hardware, operating platforms, software and version
- management information / report specifications from each system (e.g. report name, frequency, originator of the report, person responsible for preparing the reports and users)

2.2 Client MIS policy & monitoring

There must be policies and procedures to govern and monitor client access to the company's information systems through Internet or other means.

2.2.1 The channels where clients can have access to the company's systems and the level of access should be approved by senior management.

2.2.2 Management information available to clients through the internet or on-site computer terminals may include:

- market information e.g. online quotes, charts and public information relating to listed companies
- account information specific to each client e.g. trading and account balance information
- company's research materials that are approved by the Research Department for client distribution and viewing

2.2.3 The type and level of access should be client specific and protected by password.

2.2.4 The relevant business unit / department should ensure that clients are made aware of the company's policies and procedures regarding client MIS prior to granting access to the company's information systems and databases.

2.2.5 The relevant business unit / department should check at the end of day if there are breaches in client access to predetermined database and systems and inform management of any breaches. Immediate corrective actions must be taken to rectify any violations including the tightening up of system controls.

2.3 Control aspect for the information system environment

Policies and procedures should be established to ensure the integrity and security of the company's information systems, data and other form of documentation.

2.3.1 Management of information, both in physical and electronically stored form, should be assigned to qualified and experienced personnel.

2.3.2 Management reporting requirements should be clearly defined to ensure the adequacy and timeliness of internal and external reports including regulatory reports.

2.3.3 Key components of the information management system design and implementation programme should be adequately documented and regularly reviewed for effectiveness.

2.3.4 Controls should be established to prevent and detect unauthorised access to and alteration of the company's information systems and data. Examples of controls include but are not limited to the following:

- Heads of Departments and IT should authorise computer access (to specific computer

systems and/or functions) based on the job requirements and information needs of every employee or employee groups. Similar rationale should also extend to physical documentation.

- Management to sign-off new computer users created and access changes based on system generated reports on a daily basis. The Internal Audit function should randomly check to ensure new users or access changes have been authorised by the appropriate personnel.
- Information systems should be programmed to generate exception reports for the attention of appropriate personnel and/or the client, when the client static data is amended. This should also apply to information such as settlement data, counterparty information and commission rates.

2.3.5 Management establishes and maintains effective record retention policies, covering computer and physical records, which ensure that all relevant legal and regulatory requirements are complied with, and which enable the firm, its auditors and other interested parties, e.g. exchanges, clearing houses and the Commission, to carry out routine and ad hoc comprehensive reviews or investigations.

2.3.6 Controls over information systems and technology should include both general and application controls.

- General controls are controls over the computer system (i.e. mainframe and end-user terminals) and which ensure its continued, proper operation. For example, general controls include back-up and recovery procedures, and access security controls.
- Application controls are computerised steps within software applications and other manual procedures that control the processing of transactions. Application controls include, for example, edit checks and computer matching.

2.4 Back-up, recovery and contingency planning

The IT architecture and policies of the company should define adequate back-up and recovery procedures to ensure that the company can withstand failures of hardware, software or telecommunications with an acceptable level of disruption. Full contingency plans should be in place in the event of failure.

2.4.1 Disaster recovery procedures should be in place and well tested so that in the event of a technical failure, systems can be restored either at a remote location or on a different machine given an acceptable delay in time. This could be achieved, for example, by the use of 'shadowed' disks and mirrored or replicated databases.

2.4.2 A degree of fault tolerance should be built into the systems for example to cover one-off surges in volume over normal volume ranges, so that system integrity can be maintained in the event of technical failures. An example of this is where a system is designed to process a certain number of transactions within a prescribed timeframe. For instance, high volume transactions which are subject to volume peaks and troughs during volatile periods within a trading day. It is recommended that any system, which is subject to such processing extremes, has a sufficient default tolerance (buffer) above the maximum anticipated trading volumes.

2.4.3 Appropriate back-ups and archiving should be done at least on a daily basis, moving to a near instantaneous back up of database driven systems.

2.4.4 Appropriate technical resources should be available 24 hours a day to identify and action any fault that occurs.

2.4.5 All back-up and recovery procedures should be fully documented and thoroughly tested both prior to live operations, and on a periodic basis thereafter.

2.4.6 In addition to the system based disaster recovery or contingency plans described above, the necessary operational procedures should be in place to cater for a total systems shutdown.

3. The Internal control environment

Internal control is a process effected by the Board of Directors, senior management and all levels of personnel. It is not solely a procedure or policy that is performed at a certain point in time, but rather it is continually operating at all levels within the company.

The Board of Directors and senior management are responsible for establishing the appropriate culture to facilitate an effective control process and for continuously monitoring its effectiveness; however, each individual within the company must participate in the process.

The main objectives of the internal control process can be categorised as follows:

- efficiency and effectiveness of operations (operational objectives)
- reliability and completeness of financial and management information (information objectives)
- compliance with applicable laws and regulations (compliance objectives)

3.1 The structure of corporate governance system

The Board of Directors is fully responsible for good corporate governance. The Compliance Function and Internal Audit only play secondary roles.

3.1.1 Corporate governance may be broadly summed up as those processes and structures which encompass the following:

- the protection of shareholders' interest
- transparency of management's and company's actions
- prudent risk management
- the safeguarding of the company's assets
- compliance with laws and regulations

3.1.2 Corporate governance extends beyond the duties and responsibilities of the company directors, for it seeks to achieve objectives beyond the compliance with laws and regulations by the company and its officers. For example, an indicator of good corporate governance would be the establishment of an internal code that discusses the workings of some or all of the following processes:

- Board of Directors (such as the composition, responsibilities and conduct of meetings)
- Remuneration Committee
- Audit Committee
- Compliance Committee
- Internal Control

- Internal Audit
- Code of conduct
- Relations with shareholders
- Financial and other reporting

3.1.3 The company should be headed by an effective board which should lead and control the company. The board should include a balance of executive directors and non-executive directors (including independent non-executives) such that no individual or small group of individuals can dominate the board's decision making.

3.1.4 The heads of each department / operating unit should report to the Board of Directors, at least annually, on the effectiveness of the company's regulatory compliance and system of internal control. This may be achieved by the 'Control Self-Assessment' approach (refer to Appendix A - Glossary), which permits management to reconfirm to the Board that the procedures and controls within the organisation are operating as intended and that no significant weaknesses are evident.

3.1.5 Senior management, must ensure there is suitable review over the adequacy of internal controls and of the monitoring mechanisms which provide ongoing assurance of compliance effectiveness at least annually. This may be done by the use of specific work / review programmes and 'Control Self-Assessment' (refer to Appendix A - Glossary). If senior management is unclear as to what may be involved in such a review they should enlist professional assistance at least in the development of a self-assessment program and process.

3.1.6 Effective control over compliance is a key element of good corporate governance and ensuring that the compliance strategy fits into the integrated control framework is a matter that requires the attention of the Board of Directors and senior management.

3.2 The approach to controls

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.

3.2.1 It is important that the Board of Directors and senior management not only emphasise the importance of internal control through their words but by their actions as well. This includes the ethical value the Board of Directors and senior management display in their business dealings, both inside and outside the company.

3.2.2 All levels of personnel in the company need to understand their role in the internal control process and be fully engaged in the process.

3.2.3 Employees should be encouraged to report to management any internal control deficiencies, or ineffective policies or procedures as soon as they are identified. Once deficiencies or ineffective policies and procedures are reported, management should correct the deficiencies on a timely basis.

3.2.4 The Internal Audit function should conduct follow-up reviews and immediately inform

the Board of Directors, Audit Committee and senior management of any uncorrected deficiencies.

3.2.5 A system of tracking internal control weaknesses should be established in order to ensure all deficiencies are addressed in a timely manner. This can be done by developing a log to document such issues / weaknesses and to plan / control remedial actions. These issues may be of particular focus in subsequent reviews by Internal Audit.

3.3 Establishing shared ethical value

Values are essential to bind employees together, guide them through difficulties and uncertainties and provide assurance that they serve clients with high standards of integrity and conduct.

3.3.1 The company should establish and ingrain in employees a set of values that are built on ethics, integrity, and devotion to client service.

3.3.2 Shared values should be aimed at providing a uniform emphasis for employee behaviour and approach to difficulties and uncertainties, especially in situations where they need to exercise ethical judgement.

3.3.3 Employees should understand that as an industry participant, the company and its employees are obliged to protect the integrity of the market and prevent clients from abusing it. It is important that the company and its employees do not turn a blind eye to such abuses.

3.4 An atmosphere of mutual trust

The company and its employees should conduct its business in the highest professional standards and to put the trust of its clients and regulators first.

3.4.1 Employees should uphold the letter as well as spirit of the company's business principles, sound practice guidelines and applicable laws and regulations.

3.4.2 In general, employees should first seek clarification from management or the Compliance Function on any activity which is not expressly prohibited by applicable laws and regulations but is incompatible with the spirit of proper business conduct. They should not cause themselves, thereby the company, to be in situations where their integrity as professionals can be questioned.

3.4.3 The company should always view the trust of its clients and regulators as paramount.

3.5 Management's organisation

An appropriate and effective management should be established to implement strategies approved by the Board of Directors; set appropriate internal control policies; and monitor the effectiveness of the internal control system.

3.5.1 Senior management is responsible for carrying out directives approved by the Board of Directors, including implementation of strategies and policies and the establishment of an effective system of internal control.

3.5.2 Senior management should delegate the responsibility for establishing more specific internal control policies and procedures to those responsible for a particular unit's activities or functions.

3.5.3 It is important for senior management to ensure that the managers to whom they have delegated these responsibilities develop and enforce appropriate policies and procedures in consultation with the affected departments.

3.6 Framework of management control

Management should establish and maintain effective operational procedures and controls for the company's day-to-day business operations.

3.6.1 Effective operational procedures and controls should be established to ensure:

- the integrity of client and counterparty information. (e.g. controls such as mandatory fields in computer input screens and sending out static data confirmations to clients and counterparties for verification should be implemented)
- timely and appropriate disclosures of required information to clients and counterparties. (e.g. operational procedures to achieve this include computer generated messages to clients and counterparties and/or mandatory acknowledgements from clients and counterparties prior to account activation)
- the integrity of the company's business practices, including the treatment of all clients in a fair, honest and professional manner. Examples of operational procedures and controls include effective Confidentiality, Restriction, Chinese Walls and Client Order Priority policies
- the safeguarding of both the company's and its clients' assets. An example of control to achieve this is to have timely asset reconciliation procedures and resolution of reconciling items (refer to Part II, Section 7.4 and Part III, Section 2.2)
- the maintenance of proper records and the integrity of the information used within the company or for publication (refer to Part I, Section 2 and Part II, Section 7.6)
- the compliance by the company and its employees, with relevant legal and regulatory requirements

3.7 Effectiveness of the internal audit department

An audit policy and related review functions should be established and maintained which objectively examines, evaluates and reports on the adequacy, effectiveness and efficiency of the company's management, operations and internal controls.

3.7.1 The Board of Directors should establish an independent and objective Internal Audit function which is free of operating responsibilities and staffed with competent, well-trained individuals who have clear understanding of their roles and responsibilities.

3.7.2 Internal Audit should report to the Board of Directors, directly or through the Internal Audit Committee to ensure the function is able to report information that is unbiased and unaltered in any way by the levels of management that the reports cover.

3.7.3 Internal Audit should perform periodic independent assessment of the adequacy of, and compliance with, the established system of internal controls.

3.7.4 There should be clearly prescribed terms of reference which set out the scope, objectives, approach and reporting requirements of the Internal Audit function. The frequency and extent of internal control review and testing of internal controls should be consistent with the nature, complexity and risk of business activities.

3.7.5 Internal Audit should ensure there is adequate planning, control and recording of all audit and review work performed; timely reporting of findings, conclusions and recommendations to management; and matters of risks highlighted in the relevant reports are followed up and resolved satisfactorily.

3.8 Effectiveness of internal control system

Control activities are most effective when they are viewed by management and other employees as an integral part, rather than an addition to, the daily operations of the company.

3.8.1 Controls that are an integral part of the daily operations enable quick responses to changing conditions and avoid unnecessary costs.

3.8.2 Management should set up an appropriate control culture to ensure effective internal controls and defining the control activities at every business level. These should include:

- senior management reviews
- appropriate activity controls for different business units
- physical and computer access controls
- periodic checking for compliance with exposures limits (e.g. credit limit, single client and single securities limits)
- establishing an early warning system to monitor regulatory capital compliance in order to correct any weaknesses upon detection

- a system of approvals and authorisation
- a system of verification and reconciliation

3.8.3 It is not sufficient to establish appropriate policies and procedures, management should periodically ensure that all areas of the company are in compliance with internal control policies and procedures and also determine that existing policies and procedures remain adequate.

4. Terms of reference – Compliance Function

The Compliance Function (refer to Appendix A – Glossary) acts as the business advisor to the company on technical compliance matters, including the interpretation of applicable laws and regulations. It should work closely with other business units to solve compliance problems which may arise from new products, new business or changes in laws and regulations. Additionally, it is possible in certain business process models for the Compliance Function to be directly responsible for ensuring institutional compliance.

It is essential for the Compliance Function to establish an appropriate regulatory compliance framework to achieve regulatory compliance and in order for this to be achieved, the following steps should be implemented (further guidance is also set out in Part II, Section 1.1 on Compliance Charter): -

Step 1: Identification and maintenance of applicable laws and regulations. It is imperative that the Compliance Function remains up-to-date with any proposed changes to applicable laws and regulations.

Step 2: Assessment of the 'compliance risk' (refer to Appendix A – Glossary) associated with each facet of the company's business and development of a compliance work plan. In order to understand and assess the compliance risks inherent within the organisation, the Compliance Function will be required to assess the various business activities and functions within the company and map them against internal policies and external regulatory obligations. Thereafter, the compliance risk of each activity should be assessed in terms of high, medium or low risk (or other appropriate methods) based on factors such as:

- complexity of the business activity
- introduction of new products or services
- complexity of applicable laws and regulations
- changes in applicable laws and regulations that require the company to be compliant over a relatively short space of time
- adequacy of internal control of the business activity and related processes
- staff familiarity with the business activity or applicable laws and regulations
- business areas that are understaffed or have high staff turnover
- business areas that have frequent regulatory breaches
- fragmented and inadequate information systems (e.g. the back office system is not able to produce timely failed settlement reports)
- business areas where regulatory breaches attract heavy penalties

Once the assessment is complete, a checklist of "work to be performed" by the Compliance

Function can be prepared into a work plan. This work plan shall form the basis in determining the type and amount of compliance work that would be performed over the company's activities. It should be pointed out however, that the work programme should change over time in order to properly address the compliance risks within the company.

4.1 Expectations of stakeholders

The Compliance Function should understand the expectations of stakeholders, within and outside the company.

4.1.1 Although stakeholders may have different and sometimes conflicting interests as detailed below, it is vital that the Compliance Function acts independently in discharging its duties. Only through acting independently, will it be able to meet the expectations of all stakeholders.

Expectation of shareholders

4.1.2 Shareholders' investments are preserved and enhanced over time when the company is able to fulfil its business objectives uninterrupted and unhindered by regulatory reprimand, suspensions and loss of reputation resulting from non-compliance with laws and regulations.

Expectation of regulators

4.1.3 The company and its employees, through observing high standards of market conduct and complying with applicable laws and regulations, will protect customers and help to increase market confidence.

Expectation of clients

4.1.4 Clients can have the comfort that they will always be afforded a fair deal and their assets and interests protected by the company because its employees are in compliance with applicable laws and regulations and act with honesty, integrity and diligence.

Expectation of the Board of Directors

4.1.5 Assisting the Board of Directors in ensuring that the operations of the company are conducted with integrity, comply with applicable laws and regulations including statement of sound practice, and are conducted in accordance with the highest ethical standards.

4.2 Expectations of company administrators

Expectation of management of other departments / business units

Working closely with management to cultivate a company-wide compliance culture, to provide advice on technical compliance matters and to develop solutions to compliance

problems.

4.2.1 The Compliance Function should proactively involve itself in what is going on in the company. This may entail visiting each department / business unit / branch in order to understand and have a feel for business and operational issues. It is only with this knowledge that the Compliance Function will be able to ensure that it can ask the right questions, receives the right information and provides appropriate advice and guidance.

4.2.2 A sound and smooth working relationship between the Compliance Function and other departments / business units / branches will ensure:

- new products / new business are implemented in conjunction with appropriate input from the Compliance Function
- compliance reviews are performed at a mutually convenient time so that department / business unit staff will not be disrupted from their duties

Expectation of Internal Audit

Working closely with Internal Audit to ensure that the integrated control framework (i.e. the control environment established by the finance department, Compliance Function and Internal Audit) is effective.

4.2.3 The Compliance Function should co-ordinate with Internal Audit to ensure that no overlapping of work occurs.

4.2.4 An interactive reporting process should be established to ensure that the Compliance Function is informed, on a timely basis, of all compliance irregularities identified by Internal Audit.

4.3 Reporting responsibilities

Reporting responsibilities to the Board of Directors

Key compliance issues should be submitted to the Board of Directors.

4.3.1 The Compliance review report should focus on enhancing the existing regulatory compliance framework.

4.3.2 The Compliance Function should follow-up on the Board of Directors' decisions to enhance the regulatory compliance framework to ensure corrective actions are effected without delay.

Reporting responsibilities to regulators

Identification and Escalation policies and procedures should be in place to ensure that the company brings to the attention of the regulators any matters that qualify for disclosure.

4.3.3 The Identification and Escalation policies and procedures specify "when" and "who" to contact within the company when regulatory and/or internal breaches occur.

4.3.4 The Compliance Function should ensure that relevant staff understand the Identification and Escalation policies and procedures.

4.3.5 Senior management and the Compliance Function should be alerted immediately when breaches occur so that independent verification can be performed.

4.3.6 The Compliance Function must maintain a positive and pro-active relationship with regulatory bodies which govern the operations of the company.

4.3.7 The Compliance Function should advise senior management of matters which may require disclosure to the regulators. Senior management should ensure that the company meets its regulatory obligations by bringing to the attention of the regulators any matters that qualify for disclosure.

Reporting responsibilities to Internal Audit

The Compliance Function should share with Internal Audit, findings from compliance reviews and work closely with Internal Audit in resolving any non-compliance detected.

4.3.8 In organisations where the Compliance Function is independent of Internal Audit, both departments should work together closely to resolve any non-compliance detected and leverage on each other's resources and skills.

4.3.9 Interactive reporting should be established to ensure that Internal Audit is informed, on a timely basis, of all compliance irregularities identified by compliance reviews.

Part II Sound practices for internal control and compliance

1. Structure and roles of the Compliance Function

The objective of the Compliance Function is to instil in the employees of the company, from senior management down to the most junior member of staff, a sense of "regulatory awareness" in connection with the type of business that is being performed. Once this understanding has been achieved and an appropriate culture developed, the role of the Compliance Function may be looked upon by the business units as a business advisor role, rather than as a procedural critic.

When establishing the Compliance Function, the Board of Directors or the Compliance Committee should consider the following sound practices:

a) The compliance structure is designed, with due consideration to the size, type and complexity of the business, to support compliance officers to perform their task effectively and efficiently.

b) There are clear policies to ensure that the Compliance Function covers all relevant aspects of the company's operations, including the unfettered access to necessary records and documentation.

c) The organisational structure, roles and responsibilities of the Compliance Function are clearly defined in writing and are reflected within the Compliance Charter. (Refer to Part II, Section 1.1)

d) The Compliance Function is an independent unit, segregated from other operational and business functions.

e) Staff performing the Compliance Function, in conjunction with management, establish, maintain and enforce effective compliance procedures. These procedures should cover:

- legal and regulatory requirements including, where applicable, registration / licensing and capital adequacy requirements
- record keeping (for management and regulatory reporting, audit and investigations)
- business practices (e.g. codes of conduct; commission rebates and preparation, approval and dissemination of research reports)
- internal control matters relating to the operations (e.g. internal controls in the front and back offices)
- compliance with the relevant client, proprietary and staff dealing requirements

f) The Compliance Function can have multiple reporting lines to the Chief Executive Officer, Board of Directors or Compliance Committee but the circumstances and requirements to report to different authorities must be clearly defined.

g) The role of the Compliance Function should be communicated to employees to ensure full and open co-operation is given to compliance staff to inspect records and activities and request for clarification and information.

h) The Compliance Function should act as the centre of contact between employees and regulators on compliance and regulatory issues. In general, employees should always consult with the Compliance Function first before taking any further action.

i) The Compliance Function and senior management should enlist external legal or other

independent professionals (e.g. financial regulatory consultants)to review company activities when they consider this necessary in order to minimise material risk of loss due to breaches of regulations or failure to anticipate regulatory changes. Such advice may be relevant prior to the company entering into complex business transactions or launching of new products.

j) Prior to entering into new trading activities, senior management must ensure that authorisation has been received from the regulators and systems are in place to comply with the relevant regulations.

1.1 The charter of the Compliance Function

The Compliance Function should develop a Compliance Charter, which clearly defines the organisational structure of the Compliance Function, the roles and responsibilities of the compliance staff (including reporting lines) and embodies realistic objectives that it sets out to achieve.

1.1.1 Depending on the preference of the Compliance Function, the Compliance Charter may be a simple statement and may include some or all of the following topics:

- the Mission Statement of the Compliance Function
- management structure and corporate governance
- structure of the Compliance Function and the Compliance Committee
- benefits of having a Compliance Function
- performance measures
- resource requirements
- responsibilities and accountability
- lines of communication and relationships with other departments (e.g. Internal Audit) and regulators and etc.

1.1.2 The Compliance Charter is useful as a guide to compliance staff in their daily work, and a reminder as to "why" the Compliance Function exists.

1.1.3 Compliance performance measures may include:

- the number of compliance breaches or complaints received and comparing actual figures with previous years' statistics or industry average;
- time and resources required to resolve compliance matters;
- obtaining assessment from other departments / business units on the effectiveness and helpfulness of the Compliance Function etc.

1.2 Composition of compliance officers

Compliance officers should be able to work closely and effectively with company employees and deal with regulators in an open co-operative manner.

1.2.1 Compliance officers should work closely and effectively with company staff of all levels. Specifically,

- acting honestly, with integrity and diligence in order to earn the trust of employees
- able to work "independently" and have the eagerness to uncover root causes of non-compliance
- knowledgeable and capable enough to deal with management, traders and marketing personnel in discharging compliance functions

1.2.2 Compliance officers should be able to deal with regulators in an open and co-operative manner. Specifically:

- able to assess the severity of regulatory breaches and make disclosure to regulators as appropriate
- facilitating communications between the company and the regulators
- contributing constructive ideas to regulators to improve the compliance culture in the industry

1.3 Independence issues & policy

The Board of Directors or the Compliance Committee should establish and maintain an appropriate and effective Compliance Function (having due regard to the overall size of the organisation) independent of all operational and business functions and which reports directly to the Board of Directors or through the Compliance Committee.

1.3.1 The Compliance Function should be an independent unit, segregated from other operational and business functions.

1.3.2 The Compliance Function can have multiple reporting lines to the Chief Executive Officer, Board of Directors or Compliance Committee but the circumstances and requirements to report to different authorities must be clearly defined.

1.3.3 The Compliance Function should establish policies and procedures covering appropriate reporting actions under various circumstances and for different degree of regulatory breaches e.g. reporting to the Chief Executive Officers for minor regulatory breaches, but also reporting to higher authorities (the Board of Directors or Compliance Committee) and the regulators for serious breaches like trading abuses and insufficient net capital.

1.3.4 The company must establish policies to emphasise that all employees are responsible for compliance not just the Compliance Function. The company's senior management, which includes the Board of Directors, Chief Executive Officer or other senior managers, together with registered persons / licensed traders are responsible for ensuring the company's business activities

are conducted in compliance with applicable laws and regulations at all times.

1.3.5 Senior management should encourage every employee to consult the Compliance Officers with his / her concerns and assure employees that any concerns they raise to the Compliance Function will be handled with sensitivity and discretion.

2. Compliance professionals

2.1 Code of professional ethics

Compliance professionals should act with integrity and employ effectively the resources and procedures for the proper performance of the compliance function.

2.1.1 Notwithstanding that compliance professionals may be from different professional backgrounds and discipline, they should always act with integrity, honesty and perform their duties with high professional standards. Specifically:

- employ effectively the resources and procedures that the company expects from them to perform the compliance function
- act with due skill, care and diligence; and perform their duties in accordance with applicable laws, regulations and company policies
- escalate issues in a timely manner to regulators as appropriate and work with regulators to achieve their resolution

2.1.2 Compliance professionals should ensure that they observe any code of professional ethics or any guidelines on ethics as may be issued by regulators from time to time, in Thailand.

2.2 Standard knowledge and skills for compliance professionals

The Compliance Function should be fully-staffed and possess the necessary skills and qualifications to enable them to effectively execute their duties.

2.2.1 The size of the Compliance Function will normally be in proportion to the size, type and complexity of the underlying activities of the company. The most appropriate method of determining the number of compliance personnel is to first carry out an assessment of the compliance risks within the company and to prepare the necessary work programmes. The Head of Compliance should seek to recruit a sufficient number of qualified personnel in order to ensure that compliance risks are properly addressed. This process should be approved by the Board of Directors and reflected in the Compliance Charter.

2.2.2 Compliance officers should possess the necessary skills, qualification and experience, for example:

<u>Knowledge</u>

- Strong knowledge and understanding of applicable laws and regulations
- Knowledge of the industry's business process and operations
- Good understanding on financial products, principles and risk concepts
- Good knowledge and understanding of computer systems

Skills

- Able to effectively diagnose internal control and compliance problems
- Able to communicate effectively with regulators and staff to ensure consistent understanding of applicable laws and regulations
- Able to identify resourcing needs and staffing issues to achieve efficient and effective internal control and compliance

Qualification

- University degree/ formal coursework in finance, accounting, or law
- Possess relevant work experience as a compliance officer

2.3 Continuing professional development for compliance professionals

Proper training, both internally and externally, should be held for compliance professionals on a regular basis.

2.3.1 In order to ensure that compliance professionals are able to provide the highest quality advice, they should be kept fully informed and remain up-to-date on applicable laws and regulations.

2.3.2 As compliance monitoring involves a diverse range of skills, regular training on legal, accounting and financial principles should be held for compliance professionals, either by in-house experts or outside professionals.

2.3.3 Some relevant areas of training are detailed below:

Ongoing product training

Compliance professionals need to have good knowledge of financial products including structures of financial transactions. This knowledge is equally important to enable them to deal with traders confidently and effectively. Other areas of training may include new market structure and electronic trading systems.

Basic risk management training

Basic risk management training (e.g. on techniques for managing operations, credit and market risks) equips compliance professionals with the knowledge to independently assess the adequacy of risk management in the company and whether it is likely to post a threat to compliance going forward.

Money laundering training

It is important to recognise that combating money laundering requires different knowledge and skills, therefore compliance professionals should be trained formally and attend seminars in this area to assist them in reviewing possible money laundering instances brought to their attention by management. Seminars that are conducted by bankers and lawyers can be very helpful.

Law firms' circulars

Reading circulars and case studies by international law firms on regulatory breaches may help the Compliance Officer to prevent similar occurrences from happening at his / her company.

Conferences

Attending conferences offers good opportunities to find out what goes on in the industry.

3. Conflicts of interest and confidential information policies

Employees must respect and preserve the confidentiality of information received in the course of their jobs in order to maintain the trust and confidence of clients, to protect sensitive information of the company and to comply with applicable laws and regulations. Confidential information may only be used for the business purpose for which it was provided and by employees who "need to know" in order to perform their duties. It should not be used by any employee for personal profit or gain.

In general, the company and its employees should either avoid any conflict of interest arising or, where conflicts arise, should ensure fair treatment to all clients by disclosure, internal rules on confidentiality, declining to act, or otherwise. A person should not unfairly place its interests above those of its clients, and, where a properly informed client would reasonably expect that the person would place the client's interest above its own, the person should live up to that expectation.

3.1 Confidential information defined

Confidential information, in the context of a securities company, can be broadly defined as material non-public "inside" information which is not generally available to the public but provided to the company on a confidential basis by an external source or information originating from within the company through its research efforts and other corporate activities.

3.1.1 Securities companies often receive privileged confidential information when performing corporate finance, advisory or underwriting work and other business dealings with its clients.

3.1.2 Information is material if the dissemination of such information is likely to have an effect on the market price of the securities in question or is likely to be considered to be important by reasonable investors in deciding whether to trade the securities. Examples of material information include but are not limited to: proposed dividends, earnings estimates, write-downs of assets or additions to reserves for bad debt, proposed mergers, acquisitions and management buy-outs, major litigation, liquidity problems and re-capitalisation.

3.1.3 Whilst the degree of confidentiality may be different from one company to another, depending on the nature of the information and business performed by the company, the company may wish to be particularly conservative when dealing with confidential information concerning its clients.

3.1.4 Confidential information concerning the company's clients is also referred to as "inside" information. The company possesses this information only because it has a business relationship with the client and is not expected to have the information if the business relationship does not exist.

3.1.5 Inside information includes, but is not limited to:

- information received from corporate finance, advisory and underwriting work with the

client

- the client's account information such as its past and proposed transactions, its account performance and balance
- information about the client in general. e.g. business strategy or trading intent

3.1.6 Research information, whether from public or private sources, should be treated as confidential but not necessarily "inside" information. This information may have strategic and legal implications on the company and proper authorisation should be obtained prior to its release or use.

3.2 Policy regarding confidential information

Policies and procedures should be established to ensure client information is treated as confidential and confined to those staff members who must have such information in order to carry out their duties or client instructions effectively.

3.2.1 There should be controls over client information, both physical and computer access controls, to ensure only relevant staff members have access to the information.

3.2.2 Chinese Walls should be maintained to restrict the flow of confidential information amongst the various departments / business units.

3.2.3 Client information stored in the company databases and records includes, but is not limited to the following:

- client agreements and other legal documents
- contract notes, statements and ledgers
- tape recorded conversations with clients
- client correspondences

3.2.4 Employees should treat confidential information with care and diligence and ensure client information is not released to the public inadvertently or available in inappropriate areas e.g. confidential information should not be left in photocopy rooms, meeting rooms or public areas.

3.2.5 Employees including front and back office personnel should refrain from discussing confidential information in public areas such as elevators, restaurants or public transports.

3.2.6 Employees should exercise care when using mobile phones, email and other modes of public communication to discuss / exchange confidential information as these may not be 100% secure.

3.3 The Chinese Wall approach/policy

Chinese Wall policies and procedures should be established to ensure price-sensitive information privy to the employees in a particular department is not available to employees outside the department, except on a "need to know" basis for control or compliance purposes.

3.3.1 The Chinese Wall is an approach that restricts the flow of confidential information in order to avoid apparent and potential conflicts of interests between the client and the company.

3.3.2 Chinese Wall policies and procedures should ensure that the department in possession of confidential or "inside" information is responsible for the flow of information within the department and for controlling the dissemination of the information outside the department.

3.3.3 Thus, if the Chinese Wall is effective and properly maintained, it allows the company to perform agency trades, corporate finance, underwriting and research work simultaneously despite the fact that each business unit possesses confidential information that may cause conflicts of interests between the client and the company.

3.3.4 Confidential or "inside" information should be communicated inside a Chinese Wall on a "need to know" basis. i.e. Should only be communicated for work purposes.

3.3.5 Outside the Chinese Wall, recommendations based on confidential information should not be given to or exchanged amongst any front offices, research or proprietary trading personnel unless given in accordance with the Chinese Wall policies and procedures.

3.3.6 When the Chinese Wall policies and procedures permit confidential information to be given, the recipient must be informed that the information is confidential and warned of any dealing restrictions.

3.3.7 An employee crossing the Chinese Wall will be subject to the duty of confidentiality and restrictions on staff dealing. Similarly, a proprietary trader who crosses the Chinese Wall is prohibited from using the information to benefit the company.

3.3.8 If a member of staff suspects that there might be a breach of Chinese Wall policies and procedures, he / she should report the matter immediately to the Compliance Officer.

3.3.9 Code of ethics related to confidential or inside information should be clearly communicated to all employees and vigorously implemented.

3.3.10 Effective Chinese Wall policies and procedures should ensure clear segregation of duties, physical separation and restricted access to premises and information systems between staff members of different departments.

Segregation of duties

Staff performing corporate finance or research should not be involved in any dealing activities. There should also be separation of dealers handling agency accounts from those handling proprietary and/or staff accounts.

Physical separation

Corporate Finance and Research should be separated from each other and from other departments to ensure price-sensitive information privy to Corporate Finance and/or Research staff is not available to staff outside those departments. Ideally, Corporate Finance and Research should be located on a different floor from Proprietary and Agency dealing. Please also refer to Section 9.2 on the physical separation of Proprietary trading.

Restricted access to premises

Physical access to the Corporate Finance and Research offices should be controlled by using electronic pass cards.

Restricted access to systems and databases

In general, staff from other departments should not be given computer access to Corporate Finance and Research databases that contain confidential and price-sensitive information.

3.3.11 In situations where physical separation is not possible, the Compliance Function should perform compensating controls to check that the Chinese Wall is intact. For example:

- vigorously checking proprietary and staff positions against the Grey, Restricted and Research lists
- being present in the dealing areas
- issuing ad-hoc instructions to lock all doors and filing cabinets at the end of the day (However, the Compliance Function should make clear to the Board of Directors that these are temporary measures and long-term solutions should be urgently effected.)

3.3.12 The Compliance Function should review the effectiveness of Chinese Wall policies and procedures periodically. Any non-compliance noted should be promptly brought to the attention of the Board of Directors, either directly or through the Compliance Committee. (Also refer to Section 3.3.4 to 3.3.7 and Section 3.3.10 for effective Chinese Wall policies and procedures.)

3.4 Gifts and benefits in kind

Employees should not accept any gifts or benefits in kind of material value from any sources and should not offer any gifts or benefits in kind to any persons unless this has been disclosed to the management and written approval of acceptance has been obtained and recorded.

3.4.1 In general, an employee should not accept any gifts or benefits in kind of material value from any sources which affects or may be perceived to affect, how the employee will discharge his / her duties.

3.4.2 In circumstances when this is unavoidable, the employee should disclose the gifts or benefits in kind to the management and obtain their approval.

3.4.3 Employees should not offer any gifts or benefits in kind to any persons if this could reasonably be construed as intending to influence the recipient to place business with the company except with prior approval from the management.

3.4.4 Policies relating to receiving and offering of gifts and benefits in kind should not apply to normal social entertaining on a scale, which is reasonable and appropriate. e.g. New Year celebrations.

3.4.5 Employees who are in doubt about the policies should seek guidance from the Department Head or the Compliance Function.

3.5 Introductions to other Group companies

Employees should deal with other Group companies at arms length and ensure preferential treatments are not afforded to other group companies that will place other clients at a disadvantage or cause conflicts of interest between the company and the client.

3.5.1 Dealings with other Group companies, whether they are the company's clients or not, should be conducted at arms length and with high professional ethics and conducts. Employees should not treat other Group companies differently from normal clients.

3.5.2 Employees should be aware that because the company is part of the Group, conflicts of interest between the company and the client may arise as a result of affording preferential treatments to other Group companies. Preferential treatments may include but are not limited to:

- giving confidential information to other Group companies
- giving priority to orders from other Group companies
- allowing other Group companies to breach account opening and settlement rules

3.5.3 On the other hand, employees should also treat information about other Group companies as confidential, whether they are the company's clients or nor. For example, employees should not leak such confidential information to clients with the intention of inducing clients to trade thereby earning more commissions.

3.5.4 Employees should notify and consult with Senior Management or the Compliance Function on business dealings or conduct that could give rise to conflicts of interest.

3.6 Conflicts monitoring system

Management should establish an appropriate and effective conflicts monitoring system to identify, verify and police apparent and potential conflicts.

3.6.1 An appropriate and effective conflicts monitoring system is not one that is full of restrictions, built on paranoia or purposefully set up to stop staff interaction. It should employ tactics, intelligent methods and latest technology and have a good staff education programme.

3.6.2 Every employee should understand the consequences of breaching conflicts of interest

policies i.e. the company and other fellow employees will be affected and he / she will face severe disciplinary actions, inside and outside of the company as well.

3.6.3 Proper account opening procedures should be in place to verify the identity and particulars of new clients.

3.6.4 There should be IT mechanisms to check for unusual trading patterns of client and staff accounts including checks on trading on Grey, Restricted and Research list securities. For example, a dormant client account suddenly having large trading volume on a Restricted list stock should be flagged automatically for the attention of management and the Compliance Function.

3.6.5 Management and the Compliance Function should monitor closely those employees who have records of breaching company policies and behaving in a recalcitrant manner. Equally important is for management and the Compliance Function to carry out immediate and thorough verification when breaches are discovered or rumoured.

3.6.6 Management should encourage "whistle blowing" amongst staff and assures staff that any concerns they raise to management or the Compliance Function will be handled with sensitivity and discretion.

3.6.7 Management and the Compliance Function should monitor closely news and market activities, including excessive price / volume swings, especially those concerning public listed companies for which the company is performing research or advisory work and use this as a basis for random checks.

3.6.8 All forms of client correspondences (e.g. letters, faxes and emails) should be properly kept and telephone conversations in the front office recorded for random checks and investigation purposes. At a minimum, records of telephone conversations should be kept for a period in accordance with applicable laws and regulations.

3.6.9 Management should establish guidelines on taking client instructions by mobile phones and taking "off-premise" orders. In general, marketing staff and dealers should avoid using mobile phones to take client instructions or accepting "off-premise" orders, and if this is unavoidable, they should promptly call back the client on a taped line to confirm the client's instructions.

3.6.10 Management and the Compliance Function should monitor closely accounts that have frequent settlement failures and those clients who often request to settle differently e.g. clients who often change bank accounts or request the company to issue "uncrossed" cheques when receiving payments.

4. Restriction policies

Employees in possession of confidential or "inside" information should preserve the confidentiality of such information until the information is fully disclosed and made public through proper channels.

They should not trade or recommend trading in securities to which confidential information relates, either for their own account, the company's account or advise others to trade. They should not communicate such information to anyone whom he / she believes will deal in the securities until the inside information is fully disclosed and made public.

4.1 Grey list

The Compliance Function should maintain a Grey list covering securities of companies for which the company is mandated to perform advisory, corporate finance and underwriting work that is not yet made public. This list should also include securities of companies where the company may be pitching for potential deals.

4.1.1 The Compliance Function is responsible for maintaining the Grey list with the co-operation from the Corporate Finance, Advisory and Underwriting departments.

4.1.2 The Grey list is strictly confidential and access to this list should be limited to the Compliance Function and personnel authorised to have the information.

4.1.3 Dealings in securities in the Grey list are prohibited for employees in the Corporate Finance department and any other department as determined by the company who may be in possession of inside information.

4.1.4 Employees who are not restricted by the Grey list, may trade these securities for their own accounts subject to staff dealing rules and practices.

4.1.5 The Compliance Function should review references made to companies on the Grey list in any research material to ensure that it does not contain any inside information or breach regulatory requirements.

4.2 Restricted list

A Restricted list should be maintained by the Compliance Function covering securities of companies for which the company is performing advisory, corporate finance and underwriting work where a public announcement has been made. However, the company feels, that despite its "Chinese Wall" policy, the situation is deemed too sensitive to trade or issue research materials in those particular securities.

4.2.1 Dealings in securities in the Restricted list are prohibited both for proprietary trading and staff trading until the securities are dropped from the list.

4.2.2 The Compliance Function shall maintain the Restricted list with the co-operation from the Corporate Finance, Advisory and the Underwriting departments.

4.2.3 The Compliance Function shall distribute the Restricted list to traders handling proprietary trading, staff dealing and designated Heads of Departments.

4.2.4 Prior to executing staff orders, designated dealers handling staff trading should check to ensure the securities are not on the Restricted list.

4.2.5 The Research Department should not print any research materials on securities in the Restricted list until the securities are dropped from the list or prior approval is obtained from the Head of Corporate Finance, Underwriting or Advisory.

4.3 Research list

The Compliance Function should maintain a Research list covering all securities recommended (buy, sell or hold) in research materials that are produced by the company.

4.3.1 Dealings in securities in the Research list are prohibited for staff trading until the date specified in the list. Proprietary trading positions however, should not be materially altered based on that research information alone and proper Chinese walls (including physical separation) should be established and maintained to segregate research and proprietary trading.

4.3.2 The Compliance Function shall maintain the Research list with the co-operation from the Research Department.

4.3.3 The Compliance Function shall distribute the Research list to staff handling proprietary trading and staff trading, and designated Heads of Departments.

4.3.4 Prior to executing staff orders, designated dealers handling staff trading should check to ensure the securities are not on the Research list.

4.4 Insider trading

Insider trading is unlawful.

4.4.1 Insider trading involves trading or recommending trading in securities on the basis of material non-public "inside" information which is not generally available to the public but provided to the company on a confidential basis by an external source.

4.4.2 Staff who are in possession of such inside information must not trade, either for their own account, the company's account or providing advice to others to trade until the information is disclosed and made public.

4.4.3 An employee who is in doubt, whether he / she possesses inside information, should clarify and consult with the Compliance Function.

4.4.4 Management and the Compliance Function should ensure all employees, especially

those who are engaged in Corporate Finance, Underwriting and Advisory work, understand the law and regulations governing insider trading and the penalty for breaching the law.

4.4.5 The Compliance Function should factor in insider trading practices when establishing and designing the company's conflicts monitoring system. Set out below are examples of controls to prevent and monitor insider trading:

- implementing an effective compliance programme to promote compliance awareness throughout the company
- establishing policies and procedures for operational areas and professional conduct e.g. Confidentiality, Chinese Walls, Trading restriction and Staff dealing
- checking by the Compliance Function and Internal Audit to ensure company policies and procedures are adhered to
- installing devices to tape front office telephone conversations and forbidding the use of mobile phones in the front office
- monitoring unusual trading patterns in the market and staff / client accounts
- maintaining a presence in the dealing areas on a random basis and be observant of dealers' behaviours and rumours
- listening to taped telephone conversations, either randomly or based on unusual trading patterns and suspicions
- encourage whistle blowing amongst staff
- working closely with regulators to investigate any suspected insider trading practices

4.4.6 When insider trading is suspected, management and the Compliance Function should seek legal advice and determine if any appropriate disclosure to the regulators should be made.

4.5 Churning

It is gross misconduct to generate commissions through excessive transactions on a client account.

4.5.1 Marketing and dealing staff should only trade for the client account when instructed by the client and take reasonable steps to ensure client orders are executed in accordance with client instructions. (Also refer to Part II, Section 6.3)

4.5.2 Management and the Compliance Function should ensure Marketing and dealing staff understand the law and regulations governing churning and the penalty for breaching the law.

4.5.3 The Compliance Function should factor in churning when establishing and designing the company's conflicts monitoring system. Examples of such measures include :

- Monitoring accounts with high volume of transactions versus the size of client portfolio or account value. Ideally, the back office system should have the functionality to set parameters to generate exception reports for review.
- Printing the Compliance or Operations Department telephone numbers for clients to

lodge complaints on account statements.

- The client agreement and other account opening documentation should highlight that discretionary trading is prohibited and that all orders are based on client instructions only.
- If churning is suspected, the Compliance Function could listen to taped telephone conversation to investigate if a dealer has churned any accounts.

4.5.4 Management and the Compliance Function should investigate immediately when churning is detected and take appropriate disciplinary actions against the staff involved.

4.6 Front running

Client needs and interests should take priority over the company's interests.

4.6.1 Front running client orders constitutes gross misconduct, is unethical and constitutes a major conflict of interest.

4.6.2 Employees may not time transactions in employee accounts to take advantage of possible market action caused by a client order or place an order, knowing that a sizeable order is being entered or about to be entered for any client account.

4.6.3 Marketing and dealing personnel should ensure client orders are executed efficiently and in a reasonable time.

4.6.4 Management and the Compliance Function should ensure Marketing and dealing personnel understand the law and regulations governing front running and the penalty for breaching the law.

4.6.5 The Compliance Function should factor in front running when establishing and designing the company's conflicts monitoring system. For example:

- Recording time and content of client instructions by taping telephone conversations.
- Ensure client orders are time stamped (either on a deal ticket or recorded in the system). The Compliance Function should carry out surprise checks at the front office to ensure all deal tickets are time stamped or recorded in the system without delay.
- Checking the time order was received against execution, either randomly or based on any unusual trading patterns.
- Monitoring trading activity in client and employee accounts in the same stocks.

4.6.6 Management should refer to the Compliance Function any unusual execution delays or significant trade disputes.

5. Securities business rules and practices

Business should be conducted in accordance with regulatory requirements, and any actual or potential problems followed up and corrective actions taken where necessary. This duty extends throughout the organisation from senior management through all employees.

All employees

5.1.1 Employees should be aware of and comply with applicable laws, regulations and internal compliance policies of the company at all times.

5.1.2 Employees should consult the Compliance Function immediately when they are in doubt of the application of applicable laws, regulations and internal compliance policies.

5.1.3 Employees should direct all enquiries from regulators to the Compliance Function and not attempt to provide answers or information to regulators without first consulting with the Compliance Function.

5.1.4 Employees should act honestly and fairly in their dealings with clients, regulatory bodies, the general public and other employees and observe high standards of integrity.

5.1.5 Employees should act with due skill, care and diligence and protect the interests of the company and its business. They should strive at all times to promote and maintain the reputation of the company and industry and should not do anything that will injure this reputation.

5.1.6 Employees should observe all duties of good faith and fair dealing owed to clients and others. They should avoid any conflict of interests and when it can not be avoided, employees should ensure fair treatment to all affected clients. Employees should not unfairly or unreasonably place the interests of themselves or the company above those of a client.

5.1.7 Employees should obtain information about a client's financial situation and other relevant circumstances, investment experience and objectives appropriate to the services requested.

5.1.8 Employees should disclose any information known to them (except that of a confidential nature) which may be material to a client's decision-making processes. Employees should take reasonable steps to ensure that this information is given in a timely and comprehensive way.

Management

5.1.9 Management should ensure any employees who should be registered with relevant regulatory bodies are properly licensed prior to engaging in any activities which will require a license.

5.1.10 Management and the Compliance Function should ensure new products / businesses have the necessary approval from relevant regulatory bodies prior to commencement of business.

5.1.11 Management should keep relevant employees informed of requirements and progress on new business activities.

The Compliance Function

5.1.12 The Compliance Function is responsible for the timely updating of any legal, regulatory and internal compliance policy changes and for circulating these updates within the company to ensure that employees perform their duties according to the latest requirements.

5.1.13 The Compliance Function should conduct staff training to implement complex rules or changes involving extensive modifications to business processes.

5.1.14 Where the company has control of or is otherwise responsible for safeguarding assets belonging to a client, suitable protection should be arranged for the client in accordance with the appropriate regulatory, contractual or fiduciary responsibility which has been accepted.

6. Front office practices

6.1 The procedure for new customers

The company should take all reasonable steps to establish the true and full identity of its clients, and the client's financial situation, experience and objectives relevant to the services to be provided.

6.1.1 The company should establish proper account opening procedures consistent with applicable laws, regulations and internal policies.

6.1.2 Proper account opening procedures are important for the company to gather appropriate information about its clients and to prevent the company from being used for money laundering by counterparties who are involved in criminal activities.

6.1.3 Before opening an account, the company should take reasonable steps:

- to establish the identity of the client for example getting relevant copies of passports or official I.D. cards
- to obtain satisfactory documentation in order to verify the client's credit records, financial situation and solvency
- to avoid accepting physical cash as deposits i.e. the client should pay deposits or make payments for purchases by cheque or other payment medium (e.g. bank transfer)
- to explain to the client the content of the standard risk disclosure statement and asking the client to sign it

6.1.4 As appropriate, additional due diligence, reference checks and credit searches should be performed where the client is not well known to the company.

6.1.5 Staff in-charge of account opening should ensure proper execution of contractual and regulatory documents which include:

- Client agreement
- Risk disclosure statement (if appropriate)
- Custody agreement (if appropriate)

6.1.6 Copies of all documents, supporting documentation and specimen signatures should be treated with confidentiality and appropriately filed as soon as possible.

6.1.7 As part of the account opening procedures, the company should provide information regarding the company's policies that include, services to be provided, the nature and scope of fees, penalties and other relevant terms and conditions.

6.1.8 New accounts should be reviewed and approved by the appropriate senior management prior to becoming active.

6.1.9 It is important to ensure that the whole account opening process is completed within the time specified in internal policy and management should be informed immediately when delay occurs.

6.1.10 Front office personnel should not begin trading for new accounts until the proper completion of all account opening procedures and the client information is maintained in the respective systems.

6.1.11 Regarding all of the above, the Compliance officer should be involved in the setting of policy and the design of the procedures to satisfy the above. Additionally, the Compliance Function must review and periodically check both that such controls are working as they were designed and constitute an effective control. Such review / testing will probably be part of the broader internal control / compliance reviews that will take place and may be done by the Compliance Function itself or in consultation with Internal Audit.

6.2 Type of client account

Information and requirements regarding each type of client account should be clearly documented for the benefits of the client and internal reference.

6.2.1 At a minimum, the following information for each type of account should be established:

- basic requirements of each type of account (e.g. how to have a margin account)
- basic features of each type of account
- limits (i.e. trading, credit or margin limits)
- settlement mechanism and methods (e.g. , including force-selling, buy-in and use of margin financing to pay for purchases)
- fees and charges
- particulars of designated dealer
- how to lodge a complaint

6.2.2 The types of client account currently available in Thailand include:

- Cash account
- Margin account
- Internet account

6.3 Dealing on client orders

Unless otherwise approved by management or the client, the company should only trade on behalf of the client when instructed by the client to do so.

6.3.1 In general, the company should only trade on behalf of the client when instructed by the client to do so saved for the following situations:

- when management orders to "force sell" or "buy-in" against the client account in

accordance with applicable laws and regulations e.g. when the client fails to settle any open positions falling due

- the client consents and authorises the company in writing to operate his / her account under specific circumstances (e.g. when the client is abroad). Such requests must be accompanied by specific instructions detailing whether to buy or sell, the name of the securities, the price and volume of the transaction and any special conditions e.g. limit or market order. The Compliance Function should ensure that there are policies and procedures around such arrangements and all undertakings are in accordance with applicable laws and regulations

6.3.2 Only properly registered staff should handle client orders, respond to enquiries from them or approach prospective clients. Depending on the company's front office organisation, client orders can be received through the following methods:

- Client instructions are received by a Marketing staff who then passes the order to a Dealing staff for execution. Under this method, the Marketing Staff should record the client's verbal instructions at the time the order is received and the Dealing staff should in turn, record instructions from the Marketing staff.
- Where a Marketing staff is also a registered Dealer, the same staff should record the client's verbal instructions at the time the order is received and prior to executing the order in the market.

Notwithstanding the differences, there should always be a clear audit trail that links client instructions to the staff who received it and the execution of the order.

6.3.3 All verbal instructions received from the client to trade must be recorded in written or electronic record as soon as possible by the company's Marketing or Marketing/Dealing staff who received them. At a minimum, the following information should be recorded:

- client's identity
- time and date when the order is placed
- stock
- price
- the nature of the order and any particular instructions for executing the order and reporting its execution

6.3.4 Unless otherwise directed by or agreed with the client, orders must be entered as soon as practical after receipt.

6.3.5 Marketing or Marketing/Dealing staff should check the status of the client account (active, closed or on 'watch list'), available funds, credit or securities in the relevant account and applicable limitations at the time of receiving client instructions or prior to executing the client order. (Refer to Appendix A – Glossary for the definition of watch list)

6.3.6 If a client order is not filled within a short period of time, whether because of market conditions or the nature of the order, the Marketing or Marketing/Dealing staff shall keep the client informed accordingly until such time as the order is filled entirely, or it becomes clear that it is not possible to do so, or the client withdraws or amends the order.

6.4 Dealing errors

There should be policies and procedures to ensure dealing errors are identified and brought to the attention of the appropriate personnel immediately.

6.4.1 Polices and procedures on dealing errors should be established to:

- ensure errors are identified and reported immediately for risk management
- avoid error positions being held in company accounts that may breach applicable laws and regulations (e.g. in situations where applicable laws and regulations require error positions to be closed out within a specific time period after trade date in order to calculate net capital position accurately)
- identify and monitor the causes of errors to enable corrective actions to be taken

6.4.2 In general, all errors should be reported immediately by the employee who identified the error to the relevant Head of Dealing or persons identified in the company's error policy.

6.4.3 Dealing staff should not attempt to rectify dealing errors without the express approval of the Head of Dealing or persons identified in the company's error policy.

6.4.4 The Head of Dealing or other responsible persons should close out any error positions as quickly as possible.

6.5 Client order priority

The company should give priority to client orders and ensure that clients are treated fairly at all times.

6.5.1 Client orders should be dealt with fairly and in the order which they are received. In general, client orders should be executed strictly in order of receipt unless the client specifies conditions as to how its order is to be executed, e.g. a price limit or a period over which the order is to be executed.

6.5.2 Client orders should always be entered first and take precedence over any orders entered for the personal accounts of an employee.

6.5.3 The Compliance Function should factor in checks in the company's conflicts monitoring system to ensure client order priority. Examples of controls to check for client order priority include:

- taping telephone conversations in the front office
- time stamping client orders
- checking the time order was received against execution, either randomly or based on unusual trading pattern
- monitoring client complaints or checking with appropriate market participants on the company's reputation on trade execution

6.5.4 Management and the Compliance Function should investigate and take disciplinary actions when client order priority policies are breached.

6.6 Aggregation of orders and allocation

Client orders should only be aggregated in accordance with applicable laws and regulations.

6.6.1 Where applicable laws and regulations allow orders from different clients to be aggregated (bunched together) for trade execution, the company should ensure client orders are aggregated for the purpose of improving trade execution only and any trades executed will be allocated fairly between the clients.

6.6.2 Order aggregation should only be performed for clients who understand that aggregation may work for or against their orders (e.g. institutional clients).

6.6.3 As a general rule, employee orders should not be aggregated with or entered ahead of client orders.

6.6.4 Where orders have been aggregated, the company should allocate executions fairly and not give unfair preference to a specific client or itself. If all orders can not be satisfied then it should give preference to satisfying client orders first.

6.7 Average price trades

Average price trades should be booked and reported to the Exchange in accordance with applicable laws and regulations.

6.7.1 Where a client instructs the company to aggregate a series of buys or sells throughout the course of a single business day in order to achieve a single confirmation and settlement at an average price:

- each separate execution should be booked and reported to the Exchange in accordance with applicable laws and regulations
- the client should receive a single confirmation with a remark that the company acted on the client instructions and information on the client order e.g. order date and average price

6.8 Warehousing

Warehouse trades (for example, large block institutional orders which may require to be executed over a number of days) should be booked, confirmed and settled on a daily basis unless otherwise permitted by applicable laws and regulations.

6.8.1 Generally, trades executed on one or more consecutive days in order to fill a single client order should be booked, confirmed and settled on a daily basis unless otherwise permitted by a formal company policy and applicable laws and regulations.

6.8.2 The company should not hold, on behalf of a client, positions in a principal trading or internal suspense account of any kind unless in accordance with an approved company policy.

6.8.3 Management should establish arrangements to ensure that dividend, financing and settlement procedures are in place in order to handle warehousing with any financing and stock loan charges being built into the pricing of the trade.

6.8.4 In order to protect the company's interest and avoid disputes, the client consent to the company's policies on warehousing and client instructions on warehousing should be evidenced.

6.8.5 Individual executions (market side) should be booked and reported to the Exchange and regulators in accordance with applicable laws and regulations.

6.8.6 Individual execution (client side) should be booked daily into a segregated "average price" account clearly attributed as belonging to the client. This is to avoid the semblance of securities being warehoused at the company's risk on behalf of the client and to segregate client from the company's positions.

6.8.7 The client should receive a daily confirmation by fax or telex of partial executions completed on their behalf, as per a normal trade.

6.8.8 The final trade booking and confirmation should include a remark that the company acted on the client instructions and information on the client order, e.g. order date and average price.

6.8.9 All warehouse trades should be booked out from the average price account to the client account in accordance with applicable laws and regulations.

6.8.10 The Compliance Function should be informed immediately when there are disputes between the client and the company regarding warehouse trades.

7. Back office practices

7.1 Trade processing

All approved transactions should be processed in a timely manner, with an audit trail that links the transaction to the initiator and the trade time.

7.1.1 Transaction processing controls should be in place to ensure that the risk of error is minimised:

- sufficient records should be maintained to identify each transaction's terms and counterparties
- systems should provide a complete audit trail to the accounting records, and include any errors, exceptions, corrections or changes
- the Compliance Function should ensure that systematic, periodic review of such controls takes place and remedial action is taken where controls are found to be inadequate

7.1.2 Transaction processing should take place as soon as possible after trade execution to ensure records are up to date.

7.1.3 Controls should be in place to ensure the completeness and accuracy of trades e.g. reconciliation of the front and back office systems and/or with the Exchange reports, where applicable. Specifically, trade documentation should include a unique trade number, details of the transaction, the time the trade was recorded and the initiator of the trade.

7.1.4 Trade volume statistics and error log should be circulated to management to aid the identification of process weaknesses.

7.1.5 Senior back office management should regularly review all outstanding items and aged analysis of such items.

7.2 Trade amendments

Any cancellation or correction to a trade required after trade date should be approved by the appropriate personnel to ensure the cancellation or correction is genuine.

7.2.1 Any cancellation or correction to a trade required after trade date that is caused as a result of a data entry or booking error by the front office and which involves a change of beneficial ownership , should be approved by the appropriate personnel to ensure that it is:

- in accordance with the terms of the original order and execution
- not to the deliberate detriment or favour of one client over another client or the company

7.2.2 Any amendment involving a substantial change of terms to the client's advantage or disadvantage should be discussed with the client beforehand.

7.2.3 Trade amendments, cancellations and unusual trades should be subject to additional scrutiny and authorisation by senior staff. In particular:

- changes should be linked to the original trade
- periodic reviews of trade amendments should be carried out including reviewing trends in product type, trader identification and trade times

7.2.4 In general, changes in trade date are not allowed as trade date has settlement implications.

7.3 Trade confirmations / contract notes

All transactions should be confirmed independently of the trading function with the trading counterparty on trade date.

7.3.1 Back office-to-back office confirmation of trades should take place on trade date by fax, telex or electronic messages.

7.3.2 Outgoing confirmations should be verified with the original trade and authorised by the appropriate personnel. The following should be noted in particular:

- a trade should be confirmed at the time of trading or as soon as possible thereafter according to the applicable market practices
- confirmation should be performed independently of the trading and payment functions

7.3.3 Incoming confirmations should be received independently of the front office and matched to the original trade ticket or system reports to review for accuracy and discrepancies. Specifically:

- the back office should monitor the consistency between the terms of a transaction as originally agreed and the terms as subsequently confirmed
- discrepancies in incoming confirmations should be monitored and resolved by the back office and appropriately reviewed by senior management and the Compliance Function

7.3.4 Periodically, management should review aged analyses of outstanding and disputed client confirmations.

7.3.5 Back office should ensure that valid confirmation notes, containing all necessary details as required by regulations, are dispatched to clients in accordance with applicable laws and regulations.

7.3.6 There should be controls to ensure the completeness and timeliness of confirmation notes dispatched. Back office staff should not accept any requests by clients to "hold" confirmation notes, unless such requests have been approved by the appropriate senior management.

7.3.7 Any confirmation notes returned should be investigated immediately including telephoning the client to reconfirm correspondence details.

7.4 Reconciliation

Independent reconciliations should be carried out with third parties on a regular basis (consistent with the level of transactions) and internal reconciliations should be performed as appropriate. Timely reconciliations are a critical part of ensuring regulatory compliance.

7.4.1 Reconciliations are required to ensure the company's systems and databases are internally consistent, and to verify that these records are consistent with those recorded by external parties. In summary:

- Internal systems reconciliations should be prepared at least daily. Front office systems should be reconciled with the back office database and internal reconciliations should also be performed for inter-company balances e.g. where balances may exist between different companies or business units and where compensating balances are set up in the accounting systems.
- The general ledger should be reconciled with operational databases and regulatory reports.
- Reconciliations to external parties' statements should be prepared on a regular basis with periodic supervisory review.
- There should be procedures setting out how reconciling items are investigated, explained, documented and cleared and how any required adjustments are distributed to end users of the data (e.g. traders, compliance, credit, regulatory, accounting etc.) note 1 (see end of 7.4)

7.4.2 Formal management review and reporting is required:

- management should evidence that all reconciliations have been properly and accurately prepared
- periodic management meeting should include details of any long outstanding reconciling items

7.4.3 Reconciliations of cash and custody positions should be performed with third parties. Specifically:

- reconciliations to third party statements should be performed by independent staff
- cash reconciliations should be performed, generally on a daily basis, by staff independent of the payments and receipts, trading and confirmation functions
- custody reconciliations should be performed independently of the trading, confirmation and settlement functions
- all third party statements should be received independently of the trading and payment functions
- to ensure agreement between records of the third party (broker, depository, bank etc.) and the records of the company, reconciliations should cover positions, valuations and money movements
- reconciliations should also be performed for intra-group accounts

Note 1:

It should be noted that we have already stated that all employees in the organisation are responsible for compliance. Very often those employees will maintain compliance through monitoring financial or other consolidated information within the company e.g. net capital, position in a particular security, etc. Accordingly the Board, the Compliance Function and other employees are dependent on timely and accurate data to ensure that the company remains compliant. Such information may come from a variety of diverse sources.

Where the reconciliation process shows differences between the data being used to ensure compliance and any 'mirror' or supporting data source, each individual difference must be identified promptly. Once identified, each individual difference must be followed up or investigated, to ensure (amongst other things) that the information source being used to ensure compliance is accurate. Once the explanation is apparent a number of courses of action may be appropriate: -

- the data source being used for compliance purposes may be incorrect. It should be corrected and cleared forthwith and users of the data for compliance purposes informed, particularly with regard to any regulatory reporting that may be in process
- the third party, 'mirror' or support data may be incorrect and the error should be corrected and cleared
- the difference may be a timing difference. This should correct itself in a future period and should be kept on the reconciliation until that time. Meanwhile, any impact that the timing difference may have on regulatory compliance should be considered and monitored
- in all cases the explanation should be documented with the reconciliation to satisfy future reviews by the Compliance Function, Internal and External Audit and the regulators

Procedures for all aspects of reconciliation, identification of differences and subsequent investigation, explanation, clearance and documentation should be developed and clearly documented.

7.5 Segregation of client assets

Controls should exist to ensure that client assets are safeguarded and segregated from company assets at all times.

7.5.1 Client assets include cash and securities held on behalf of clients for settlement, collateral or custody purposes.

7.5.2 Client assets should be kept in a secured area with restricted access and protected from fires.

7.5.3 Procedures should be in place to ensure that client assets are segregated from company assets, or assets of other Group companies or other assets held by the company which are not client assets.

7.5.4 Client assets should be applied only:

- for purposes of completing transactions on behalf of clients
- pursuant to the terms of the client account agreement
- pursuant to client instructions

7.5.5 Systems and procedures should be in place to ensure that client funds are promptly paid into segregated bank accounts and the company's money is not paid into segregated bank accounts except in cases where restitution is required.

7.5.6 Management should prevent segregated bank accounts from becoming overdrawn, and procedures should be implemented to ensure that the money of one client is not used to satisfy the debt of another. Examples of preventative and detective controls include:

- enabling the system to earmark client money for settlement purposes when the client has open positions and informing the client immediately to make payment for any shortfall, failing which, the client position may be subject to force selling
- daily reconciliation of the client segregated account with bank statement to ensure clients with debit balances are issued with debit notes immediately

7.5.7 Detailed records should be maintained and reconciled of each client's balances and transactions:

- reconciliation should be performed regularly to ensure that client money is held securely
- periodic statements should be sent to clients disclosing their balances and transactions

7.5.8 Physical counts and inspection of client assets should be performed on a periodic basis by staff independent of the custody or record keeping functions. (e.g. securities in scrip form)

7.6 Record keeping

Company records should be kept and accessible in accordance with applicable laws and regulations.

7.6.1 An efficient record keeping system should be established to:

- comply with applicable laws and regulations
- to improve the consistency and speed of preparing regulatory returns and other internal reports
- allow post facto review and inspection of regulatory and other reports
- promotes knowledge continuity and information sharing within the company

7.6.2 Department heads should consult the Compliance Function on:

- the type of documents for retention purposes
- the length of time to keep records

Generally, all documents that pertain to a complete and proper audit trail (of a trade) are retained in the office or at an off-site location (but which is readily accessible). These records would include (but are not limited to):

- dealers' blotters
- deal slips
- trade confirmations
- settlement records
- copies of client statements / instructions
- accounting records reflecting the trading activities of the company

7.6.3 Factors that should be considered when establishing record keeping policy and procedures include:

- statutory requirements (i.e. tax authorities minimum period for record retention)
- level of details required (i.e. types of documents)
- when and how to duplicate information already kept elsewhere in the organisation
- efficient use of computer media to store / share information
- level of access
- physical storage and computer backups
- protection from fires and other hazards

8. Good advice and recommendations

When advising or acting on behalf of a client, employees should ensure that any representations made and information provided to the client are accurate and not misleading.

8.1.1 Employees providing investment advice or other business advisory services to clients must be authorised and properly registered to do so.

8.1.2 In providing advice and recommendations, employees should observe high standards of integrity and fair dealing by acting honestly, fairly and in the best interest of the client.

8.1.3 Any advice and recommendations made to clients should have a reasonable basis, are suitable for the client's business objectives, investment experience and financial position.

8.1.4 Employees should adhere strictly to the company's confidentiality policies.

9. Marketing and sales practices

9.1 Discretionary accounts

Discretionary accounts should only be accepted if the company is licensed to do so.

9.1.1 Securities companies in Thailand are allowed to accept discretionary accounts if these accounts are managed under the Private Fund Management License.

9.1.2 Management should ensure that clients who opened discretionary accounts have been informed of and understand the company's policies, procedures and the risk in discretionary investment.

9.1.3 Clients who opened discretionary accounts should complete and sign appropriate discretionary account opening documents, including the standard risk disclosure statement, where applicable.

9.1.4 Only dealers approved by senior management and those having the necessary experience should handle discretionary accounts.

9.2 Company dealing

Proprietary trading should be segregated from other business units and traders should adhere to applicable laws, regulations and internal policies in order to avoid conflicts of interest between the company and its clients.

9.2.1 Staff performing proprietary trading should not be involved in other client servicing tasks and should not have access to computer systems, databases or physical records containing individual client's information. However, access to trade flows information in aggregate is not prohibited

9.2.2 Proprietary trading staff should adhere to applicable laws and regulations as per other employees and should avoid acts that will cause conflict of interest between the company and its clients.

9.2.3 Staff performing proprietary trading should adhere to the company's policies on Chinese Walls, Restrictions and Confidentiality. (Also refer to Part II, Section 3.3, 3.6 and 4)

9.3 Staff dealing rules & practices

Employees and their associated persons who wish to carry out securities transactions should first open staff accounts with the company.

9.3.1 Staff dealing rules are applicable to all employees and for those who are in positions to receive and obtain "inside" information, the rules shall also extend to their spouses and associated persons.

9.3.2 Employees in corporate finance, underwriting, advisory and research are likely to receive and obtain "inside" information but the Compliance Function should identify other employees who may also possess such information.

9.3.3 The term "associated persons" means:

- the spouse, partner and any child under the age of 20 of an employee
- any child over 20, or relatives of the employee who invest based on the employee's advice
- any other person who invest based on the employee's advice

9.3.4 In general, employees should refrain from speculation or invest for short term trading gains as such activities may interfere with their work. Management and the Compliance Function may consider setting minimum holding period for securities purchased by employees as a way to monitor speculative activities. Examples of speculative securities transactions include highly leveraged financial futures and options contracts or intra-day positions initiated solely for purposes of speculation or short term trading gains.

9.3.5 For purposes of avoiding conflicts of interests, employees and their associated persons should not trade in securities in which the company is engaged in any corporate finance, underwriting or advisory work prior to the time restriction is lifted. (Also refer to Part II, Section 4)

9.3.6 Employees and their associated persons who wish to carry out securities transactions should first obtain management's approval and ensure:

- the approval is documented
- the Compliance Function is informed of the approval
- the approval is valid for a specific time frame e.g. 24 hours
- the securities is not in any restriction lists of the company

9.3.7 Management approving staff dealing should ensure :

- the company's staff dealing rules, including ad-hoc rules imposed by the Compliance Function, are adhered to
- the securities are not in any restriction lists of the company at time of approval
- the company's policies on Confidentiality, Restrictions and Chinese Walls are adhered to

9.3.8 Designated dealers handling staff dealing should check for the necessary approval prior

to executing employee orders.

9.3.9 The Compliance Function should ensure that staff dealing rules are consistent with applicable laws, regulations and relevant code of business conduct.

9.3.10 The Compliance Function should factor in staff dealing restrictions when establishing and designing the company's conflicts monitoring system. For example, linking restricted securities to the front end and back office systems so that staff accounts with restricted securities will be flagged automatically.

9.3.11 Management and the Compliance Function should keep employees informed on a timely manner if there are certain securities transactions that are not subject to staff dealing rules or do not require pre-clearance e.g. authorised unit trusts and mutual funds.

9.3.12 In order to avoid front running practices and conflicts of interest, client orders should be given priority over employee orders. In general, employee trades should not receive a more favourable execution than that given to clients.

9.4 Complaints handling

Complaints should be referred to senior management and the Compliance Function immediately for prompt resolution in accordance with company policies, applicable laws and regulations.

9.4.1 Complaints should be referred to senior management and the Compliance Function immediately to ensure:

- complaints are dealt with fairly and promptly
- the client is given any further avenues for complaint as required by applicable laws and regulations
- reporting requirements to regulators, together with record keeping requirements are fulfilled
- management approval is given to any remedial steps taken to resolve the complaint
- a letter is sent to the client in response stating and confirming any proposed remedial actions as appropriate

9.4.2 The Compliance Function should inform and consult with the Legal Department if legal proceeding is served or if legal action is likely.

9.4.3 Once a complaint is received, all responses and communications with the client should be sanctioned and supervised by the Compliance Function.

9.4.4 The Compliance Function should be responsible for co-ordinating any investigations by the various departments and settling the matter to the satisfaction of the parties involved.

9.4.5 Verbal complaints should be recorded in writing and all documents instituting legal or arbitration proceedings should be passed to the Compliance Function immediately.

9.4.6 A Register of Complaints together with full records of each complaint should be kept

by the Compliance Function.

9.5 Dealings with customers

When performing their duties, the company and its employees should observe high standards of integrity and fair dealing by acting honestly, fairly and in the best interest of its clients and in a manner, which contributes to the maintenance of a fair and orderly market.

9.5.1 Dealing and marketing staff should take all reasonable steps to provide clients with the best execution and put client interest ahead of the company or self.

9.5.2 When advising or acting on behalf of a client, employees shall ensure that any representations made and information provided are accurate and not misleading.

9.5.3 Dealings with clients, and the charges, mark ups or fees shall be fair and reasonable under the particular business context and always be characterised by good faith.

9.5.4 The company and its employees should make adequate disclosure of relevant material information or required to be disclosed by law in dealings with clients.

9.5.5 The company should establish policies and procedures for solicitation via 'cold calling' (refer to Appendix A – Glossary).

9.6 Public relations & advertising

Public relations activities and advertisements should be reviewed by the Compliance Function to ensure that the format, disclaimer and general contents comply with company policies, applicable laws and regulations.

9.6.1 Public relations and advertisements include events and activities promoting the company's financial products and services in all print and electronic media for general distribution to clients, prospective clients and the general public.

9.6.2 The placing of information on the Internet is also considered to be advertisement and may require compliance with applicable laws and regulations.

9.6.3 All public relations activities, including events and information, and advertisements should obtain clearance from the Compliance Function prior to implementation or publication to ensure relevant company policies and applicable laws and regulation have been complied with.

9.6.4 Only authorised staff should communicate with the media on behalf of the company or use the name of company in the media.

9.6.5 In general, use of the company name or logo, including endorsing third party products or services, should be reviewed by the Compliance Function first.

Part III Preventative and detective measures against breaches in compliance

1. Introduction

Breaches in compliance can result for a number of reasons. These may include, but are not limited to:

- inadequate internal control, for example in the area of segregation of duties
- fragmented and inadequate information systems
- inadequate training or inexpert personnel preparing compliance returns
- inadequate training or inexpert personnel checking and submitting compliance returns
- inadequate investment in and attention to compliance generally
- substantial change in the requirements to be compliant over a relatively short space of time
- human error
- wilful fraud and/or collusion

It is fair to say that all of the above with the exception of fraud may be systematically addressed and virtually eliminated (i.e. breaches either prevented or identified in a timely manner) by a combination of both preventative and detective measures and indeed many of the foregoing chapters in this 'manual' have stressed the need for adequate internal controls to eliminate, effectively, breaches in compliance and we will not seek to cover these again in this section, but rather focus on some basic principles to observe in the area of internal control to ensure adequate preventative and detective measures are in place.

Wilful fraud is a different matter however. It is well recognised that a fraud can be almost impossible to prevent, particularly if there is collusion (rendering management's best efforts at segregating duties relatively useless). However, a positive control environment exercised by management, together with strong internal controls discourage fraud, assist with detection and help to ensure that subsequent action is taken in an efficient and effective manner.

The remainder of this section is split into two parts:

1. The Fraud Control Environment
2. Principles for Preventing and Detecting Breaches in Regulatory Reporting Compliance

2. The fraud control environment

2.1 Management commitment towards control and malpractice

- Without clear direction from senior management to demonstrate the company's attitude towards fraud any controls are likely to be ineffective. It is necessary for both employees and third parties to recognise in the clearest terms the position to be taken by the company should a fraud be committed. There should be no room for any misinterpretation of the company's policy towards any malpractice. Should management's attitude to control or malpractice be unclear, it may give the wrong signals to employees who may be tempted to obtain some pecuniary advantage, whether criminal or not, to the company's loss.
- The policy of the company should also be clear as regards any malpractice which may be committed by management that amounts to a fraud on others but is of benefit to the company. People's motives for committing frauds are sometimes unclear but this should not be allowed to obscure management's attitude towards control and malpractice.

Features of good practice

- A formal written policy endorsed by the board of directors that sets out high standards of ethical behaviour and clearly indicates the circumstances in which employees will be dismissed and criminal and civil remedies sought.
- Responsibility for preventing and detecting frauds to be allocated to a nominated senior member of management who is able to report direct to the board of directors or a suitably independent senior committee of management (ideally a body of non-executive directors or audit committee).
- A clearly designated internal control and investigation function with an administrator to monitor control procedures and to carry out investigations. The administrator should be independent of the company's day-to-day operations.
- Investigations personnel properly trained in areas such as the rules of evidence so as not to hinder any subsequent criminal proceedings.

2.1.1 Management awareness of the risk of fraud facing the company

- Owing to their very nature, little is known about many of the frauds that are committed. However, management must be cognizant of the risk of fraud. Senior management must be aware of the fraud risks facing the company if they are to institute effective prevention and detection controls to minimise these risks.

Features of good practice

- Clearly stated accounting control procedures matching the needs of the business, which are reviewed and updated regularly.
- Sufficient numbers of people within the accounts department and other operational departments to enable a proper segregation of duties to exist.
- Personnel with adequate training and specialised skills for the complexity of the company transactions for which they are responsible.
- The inspection and internal audit departments to be adequately staffed and to have a high reputation within the company.
- Effective responses by management to the internal control problems that have been identified previously.
- Liaison between the company and other institutions and regulatory and prosecution authorities to ensure that risk areas are kept under review.

2.1.2 Effective personnel policies

- Even the best designed systems will not deter a determined fraudster: effective personnel policies should however limit the risks either that one will be recruited or that existing employees will be tempted.

Features of good practice

- Recruitment procedures to ensure that personnel have the right skills and experience and that independent checks are made to verify personal details and references.
- Conditions of employment detailed in a policy booklet which reflects a high code of ethics.
- Written policies to cover the conditions attaching to personal loans to staff and the appropriate monitoring and reporting of such indebtedness.
- Ensure the disclosure of all financial interests / holdings of staff and ban any own account trading in any situation that may give rise to conflict of interest. Institute policy that accounts may only be opened at the company of the employee.
- Proper training given to staff, including inspectors and security staff.
- Fidelity insurance cover taken out where circumstances warrant.
- Regular evaluation and counselling of staff.
- A record of low turnover of staff and low absences due to sickness.

2.1.3 Management review procedures

- Senior management can help limit the risk of fraud going undetected by monitoring the effectiveness of the accounting systems and controls and by being alert in their review of management information to matters that require further examination.

Features of good practice

- Potential weaknesses in the company's operations identified by management and exception reports designed to lessen the associated risks.
- Regular review of management information carried out by senior management in sufficient detail to highlight irregularities.
- Regular reviews undertaken to check that control procedures are carried out on a day-to-day basis and are not being circumvented for ease of operation or other reasons.
- In-depth analyses of certain areas of control performed by independent inspectors or internal auditors.
- The effectiveness of exception reports and management information kept constantly under review and updated to meet any new risks, for example, to meet the requirements of Money Laundering Guidelines.
- All suspicions of fraud or possible malpractice reported directly to the senior official nominated to deal with fraud.

2.2. Fraud issues facing management

2.2.1 Theft of assets (from either the company or its' clients)

- The principal risk of theft as it applies to companies is in relation to securities, negotiable instruments, cash and, increasingly, confidential information. Thefts may involve an employee passing relevant information on customer accounts to fraudsters who subsequently obtain customers' money by deception; other thefts may involve supplying the company with false information, so as to fraudulently obtain advances or to obtain valuable securities. There is also the risk of theft perpetrated by the unauthorised use of electronic funds transfer.
- The principal protection against such frauds is a suitable mix of authorisation, physical and computer security controls over access to information, cash and securities coupled with effective segregation of duties and rotation of personnel.

Features of good practice

- Physical security measures to protect:
  - Access to premises and secure areas
  - Computer installations and equipment
  - Vaults and deposits for securing cash, valuable securities and documents of title
  - Unused company drafts, cheque books, travellers cheques and other negotiable instruments
  - Accounting records and supporting documentation.
- Computer security measures to protect:
  - Computer software from any unauthorised manipulation
  - Computer data files from unauthorised access or amendment, especially of standing data.
- Adequate segregation of duties, especially between operational or dealing functions, authorisation and confirmation functions and accounting functions .
- Records of all valuable assets accurately maintained and their existence checked on both a regular and spot check basis. Where documents of title for security purposes are in a possession of a third party, for example where property deeds are held by solicitors, proper undertakings are received and follow up procedures exist to ensure the timely recovery of such documents.
- • Dealers and other senior officers prevented from taking advantage of price sensitive information before its public release (`front running', `insider trading').
- All dealing transactions fully documented, authorised and confirmed, where necessary, in accordance with laid down procedures and limits.
- All payments, including electronic fund transfers, properly authorised and controlled.
- Senior management review of exception reports such as:
  - Detailed analysis of profit and loss account and key operating ratios, for example any significant, otherwise unexplained, single month reverses or declines in client assets or commissions to deal volume statistics.
  - Analysis of credit risks and interest and currency exposures
  - Large and unusual transactions.
- Close control exercised over dormant or slow moving accounts which tend to be vulnerable to fraud.
- Regular statements sent to customers and any queries dealt with by an independent section within the company.
- Reconciliations of trading positions regularly and on a spot check basis.
- Full reconciliations of any suspense accounts carried out frequently and explanations promptly obtained for any outstanding items.

2.2.2 Risk of loss on loans and other transactions

- The principal risk of loss on loans (i.e. margin lending and any other form of credit extension e.g. non DVP, delays over cheque clearing) and other transactions lies in advancing funds or being party to a transaction based upon false representations or information, for example, where the security in reality is poor or non-existent or the transaction has no substance.
- The principal protection lies in effective authorisation and confirmation procedures and dealing with known counterparties.

Features of good practice

- Proper evaluation of loan applications in accordance with laid down procedures concerning identification, documentation etc.
- Loans authorised at the appropriate level of the authorisation hierarchy.
- Any security independently valued and legal charges registered prior to any advance being made.
- All paper transfers of ownership properly authorised.
- Dealing restricted to authorised counterparties. The terms of treasury or other dealing transactions should be properly authorised and in accordance with predetermined counterparty limits.
- All deals independently confirmed prior to transfer of any funds.
- Individual customer transactions, balances and standing data held on computer files protected from unauthorised amendment.
- Any late repayments or extended credit terms properly authorised.

2.2.3 Risk of illicit use of assets for private benefit

- The risk mainly lies in the use of computers, office services and equipment and cars. However, a sense of proportion is needed in restricting and monitoring the use of certain assets e.g. photocopiers and telephones. There is also a risk in financial institutions that officers may use their positions to obtain free or low interest loans or to trade on their own account using a disguised account or that of a co-conspirator.
- The principal protection are clear policies and guidelines on conduct together with a suitable mix of security and operational controls.

Features of good practice

- Clear personnel policies on the use of assets for private benefit.
- Effective procedures over computer operations to prevent unauthorised access and use.
- Physical security measures to protect computer equipment and other assets, especially easily portable equipment.
- Effective controls over the grant and operation of margin loans with abnormal interest margins.
- Policies to ban, or at the very least to restrict severely and report, any trading for private benefit. This would include dealing with any company in which management has an interest.
- Exception reports to identify any large or unusual transactions or significant trading with particular parties.

2.2.4 Risk of diversion of proceeds due to the company in whole or in part

- The principal risk lies in opportunities to divert funds or securities or to misrecord cash receipts. Where cash is involved it is often difficult to detect fraud: preventative controls are therefore essential.
- The principal protection is a suitable mix of physical measures (e.g. limiting receiving and handling points, immediate recording and securing of cash and valuable securities), segregation of duties and regular reconciliations.

Features of good practice

- Measures to prevent or detect unauthorised access to premises, assets and accounting records.
- Tight controls over receipts, including physical security over the cashier area.
- Regular reconciliations and surprise counts of cash tills and valuable securities.
- Regular valuation of securities.
- Any differences to be written off on reconciliations authorised by senior management and monitored.
- Segregation of duties between staff handling cash and securities and those accounting for transactions and authorising write offs.

2.2.5 Risk of payments made for goods, services, assets or benefits either not received or at excessive prices

- The principal risk arises in poorly controlled payment and payroll systems. Risks of collusion with outsiders is high, for example, a deal may be made at an off-market price, and bribery and corruption may be a problem. Payments may be disguised, for example, a payment made for participating in a particular transaction may be shown as consultancy advice etc.
- The principal protection lies in effective authorisation of payments (and adjustments), particularly those of a large or unusual nature.

Features of good practice

- Exception reporting of deals made at off-market prices.
- Effective authorisation controls over normal purchase transactions.
- Exception reporting procedures to obtain specific authority over large or unusual payments.
- Controls to identify unusual invoices, for example, not from a regular supplier, no VAT registration, photocopied invoice, or payment request to an offshore company account.
- Procedures to cancel invoices and other documents properly to avoid double payment.
- Effective controls over the amendment of computer standing data, particularly payroll.

2.2.6 Risk of falsification of the accounting records to conceal evidence of theft

- The principal risk is that by amending or destroying the accounting records and supporting documentation or by processing a false document, evidence of theft will not be apparent, or will be identified too late to prevent loss.
- The principal protection lies in controlling and limiting access to accounting records and supporting documentation and in having effective segregation of duties.

Features of good practice

- Physical controls to limit access to accounting records and supporting documentation.
- Effective procedures to safeguard computer operations and to prevent unauthorised access to data files.
- Computer records which identify any unauthorised attempts to access financial records.
- Control procedures such as reconciliations and exception reporting carried out on a timely basis and any follow up work not delayed.

- Any amendments to the accounting records fully documented with a full audit trail. This is particularly relevant as regards computerised records.

3. Principles for preventing and detecting breaches in regulatory reporting compliance

The following represent basic principles for preventing and detecting the occurrence of breaches in regulatory compliance.

3.1 Adequacy of staff

Personnel responsible for regulatory compliance (basically each member of the company) should be suitably briefed as to their roles and responsibilities within the company and should be thoroughly briefed and trained as regards their particular responsibilities regards compliance and in the company's compliance policies and procedures.

With regard to the preparation of regulatory returns the following principles should be adhered to:

- Staff preparing regulatory returns must understand the returns which they are preparing and the data sources used to prepare the returns.
- Such staff should be experienced in the preparation of these and similar returns.
- Procedures for the preparation of regulatory returns should be accurately documented and maintained.
- Adequate cover should be arranged for the preparation of regulatory returns in the event of sickness and/or holiday; the cover personnel should also be suitably trained and experienced in the preparation of such returns.
- There should be a more experienced person checking and submitting the returns, they should have prior experience in the preparation of such returns.

3.2. Adequacy of systems

The systems employed by the company should be adequate for conducting the business of the company and should be configured to take due consideration of all regulatory reporting requirements. Ideally,

- Systems should be designed and implemented having full regard to regulatory reporting requirements in addition to normal business requirements
- Where manual intervention is necessary in the preparation of regulatory returns, suitable controls need to be constructed around the procedures of preparing regulatory returns.
- Where spreadsheets are used in the preparation of regulatory returns, the spreadsheet program should be documented and reviewed (at least once per year) to ensure that it is resulting in accurate regulatory reporting.

- All the regulatory reporting procedures must be documented and regular review by external auditors (specialising in regulatory reporting) is recommended to ensure that the procedures are suitable to ensure accurate regulatory reporting, for example to ensure that reconciliation procedures are adequate in the event of the late processing of journals after a period end.
- Documentation of systems and procedures should include due consideration of the escalation and remedial actions necessary in the event of a breach or potential breach.

3.3. Internal control

It is the responsibility of management to design a system of internal controls which eliminates as far as possible the potential incidence of compliance breach. This will include but is not necessarily limited to:

- Adequate segregation of duties.
- A suitable organisation chart understood by all personnel
- Clear documentation of roles and responsibilities.
- A management team stressing the virtue of good practice in compliance.
- Clear detailed documented systems, procedures and manuals (including compliance).
- Adequate training for all staff in the organisation and particularly with regard to their responsibilities in the area of compliance.
- Significant use of internal audit in ensuring that compliance controls are adequate, effective and in good working order.
- Use of external audit regulatory advisors where necessary to continuously "up the ante" in terms of good regulatory practices and improving internal control accordingly.

Appendix A

Glossary

This appendix provides descriptions/definitions of certain terms or phrases used in this Guideline for which clarification was requested during the hearing process.

Compliance Function

Depending on the internal organisation of each company, the Compliance Function may comprise non-executive directors at the Board level, directors and senior management at the Compliance Committee level and the Compliance Department. A comprehensive regulatory compliance framework, incorporating compliance strategy and policies, is determined by the top levels and implemented by the Compliance Department. The framework ensures the company is in compliance with applicable laws and regulations at all times.

Compliance risk

The risk of breaching applicable laws and regulations. Compliance risk is sometimes increased by factors such as:

- complex business activities
- new products or services
- complex laws and regulations
- changes in applicable laws and regulations that require the company to be compliant over a relatively short space of time
- inadequate internal control
- inexperience staff
- business areas that are understaffed or have high staff turnover
- fragmented and inadequate information systems (e.g. the back office system is not able to produce timely failed settlement reports)

Control self-assessment

Control self-assessments usually adopt the "questions and answers" format where questions are asked about the state of process and key controls of a particular business activity. Normally, for each question, a sound practice will be used as an example of the expected answer and for comparison purposes. Respondents go through the questionnaire and detail the current state of control and compare that to sound practices. Respondents are also expected to agree with their superiors on any remedial actions to bridge any gaps between the current state and the ultimate state of control.

Watch list

The watch list is a tool for monitoring clients that have trading / settlement records. Normally, marketing and marketing/dealing staff need to clear with senior management when watch list clients want to take on bigger positions. Thus, senior management is informed when this happens and allowed time to assess each case separately and able to avoid increasing the risk to the company if it does not warrant to do so.

Cold calling

Where marketing and marketing/dealing staff approach potential customers who have no prior knowledge of the purpose of the call or the company.