TOPIC 6 - OVERVIEW

1. INTRODUCTION

- Topic 5: External relationships, particularly with clients
- Topic 6: Internal operations and controls

2. INTERNAL CONTROL GUIDELINES (ICG)

- Full title: **Management, Supervision and Internal Control Guidelines for Persons Licensed by or Registered with the Securities and Futures Commission**

- The ICG identifies eight key areas of business controls:
  - Management and supervision
  - Segregation of duties and functions
  - Personnel and training
  - Information management
  - Compliance
  - Audit
  - Operational controls
  - Risk management

- SFC recognizes that **small entities** may not have a complicated system of functional segregation or any compliance/internal audit departments

- **Internal controls** refer to the entire system of policies, procedures, checks, controls and division of responsibilities which a licensed/registered person has installed to the run the business

- A licensed/registered person should use internal controls to provide itself with reasonable assurance that it is able to:
  - Operate its business in an orderly and efficient manner
  - Safeguard the assets of its clients and its own
  - Maintain proper records, and reliable financial and other information that it produces
  - Comply with all applicable laws and regulatory requirements

2.1 Management and Supervision

2.1.1 Objective

- Management should establish and operate an effective management and operational structure which ensures that the business is conducted in a sound, efficient and effective manner

2.1.2 Control Guidelines

- Management are responsible for:
  - Development, implementation and ongoing **effectiveness of the Internal Controls**
  - Establishing **regular communication of control information** to various levels of management, including risks, detected weaknesses, non-compliance with laws and regulations, and any deviations from business principles
  - Identifying **clear reporting lines** with reporting responsibilities
  - Detailed **definitions of authorities** for key positions
  - Assignment of management functions to **suitably qualified and experienced persons**

2.2 Segregation of Duties and Functions

2.2.1 Objective

- Incompatible duties and functions should be segregated, particularly those which, when performed by the same person, may provide opportunities for abuse or result in the overlooking of errors, thereby exposing the intermediary and its clients to risks

2.2.2 Control Guidelines

- Line operations staff should not conduct the following duties:
  - Policy making
  - Supervision/advisory
  - Compliance
  - Internal audit
- Sales/dealing/accounting/settlement functions should be segregated from each other
- Research functions should be segregated from sales and dealing
- Where practical, research and corporate finance functions should be segregated
- Compliance and internal audit should be separate/independent, reporting directly to Management

2.3 Personnel and Training

2.3.1 Objective

- Recruitment and training policies and procedures should be established and implemented to ensure compliance with the intermediary's operational and internal control policies and procedures, and all applicable legal and regulatory requirements

2.3.2 Control Guidelines

- There should be procedures to employ fit and proper persons and to have them licensed/registered where necessary
- Provision of comprehensive and up-to-date information to staff covering policies and procedures
- Provision of adequate training for specific duties and to meet CPT requirements

2.4 Information Management

2.4.1 Objective

- Policies and procedures should be established to ensure the integrity, security, availability, reliability and completeness of all information and documentation relating to the business, in whatever form it is stored

2.4.2 Control Guidelines

- Features of good information management are:
  - Information (physical or electronic) should be managed by qualified and experienced staff
  - The systems should be adequate and operated in a secure and controlled environment
  - Reporting requirements should be clearly defined to ensure that that internal and external reports are produced in time and contain the necessary information
  - Systems specifications are sufficiently documented and regularly reviewed for adequacy and effectiveness
  - Adequate and effective data security policies
  - Effective record retention policies which ensure that all legal and regulatory requirements are complied with

2.5 Compliance

2.5.1 Objective

- Policies and procedures shall be established to ensure that the intermediary and its staff comply with all applicable laws and regulations and with the intermediary's own internal policies and procedures

2.5.2 Control Guidelines

Management should:

- Establish and maintain an effective compliance function, independent of all operational and business functions
- Ensure compliance staff have the necessary skills, qualifications and experience
- Establish and enforce policies and procedures to provide compliance staff with full access to all necessary records and documentation
- Assist compliance staff to establish effective compliance procedures
- Establish proper complaint handling procedures (in writing)
- Establish prompt reporting to Management by compliance staff of material breaches of:
  - Legal and regulatory requirements
  - The intermediary's own policies and procedures
- Promptly report cases of material non-compliance with legal and regulatory requirements by the intermediary and its staff to the appropriate regulators

2.6 Audit

2.6.1 Objective

- To establish and operate an audit policy and review function which independently examines, evaluates and reports on the adequacy, effectiveness and efficiency of the intermediary's management, Internal Controls and operations. The review functions can be performed by internal staff or external consultants, such as firms of accountants who may be asked to carry out ad-hoc or regular reviews

2.6.2 Control Guidelines

- Management should establish internal audit as an independent function free of operating responsibilities, reporting directly to management
- The persons performing the internal audit function should have the necessary technical competence and experience
- Clearly defined terms of reference should set out the scope, objective, approach and reporting requirements
- Responsibilities and working relationship between internal and external auditors may be defined with the agreement of the external auditor
- Management should ensure adequate planning, control and recording

2.7 Operational Controls

2.7.1 Objective

- To have effective policies, procedures and controls over day-to-day business operations which ensure:
  - Communications between the intermediary and its clients are in line with the Code of Conduct
  - The integrity of the intermediary's dealing practices and the fair, honest and professional treatment of clients
  - The safeguarding of client/intermediary assets
  - Reliable and accurate records/information are kept
  - Compliance with relevant legal and regulatory requirements

2.7.2 Control Guidelines

- Management is required to establish policies and procedures to:
  - Obtain and confirm the true identity of every client, the beneficial owner of each client account and the persons authorized to give instructions for its operation
  - Obtain information regarding the client's financial position, experience and objectives
  - Establish precise terms and conditions for operating discretionary accounts, which should be communicated to the client
  - Ensure that any investment advice given for remuneration is supported by a contractual advisory agreement, and investment recommendations are made after thorough analysis, are suitable for the client, and are properly documented
  - Minimize the potential for conflicts of interest
  - Ensure that whenever the intermediary or its staff have a material interest in a transaction with a client, the fact is disclosed to the client prior to executing the transaction
  - Ensure that client orders are handled in a fair manner
  - Ensure that complete audit trails are created with records and times of orders received from clients or orders generated internally
  - Ensure that there is fair and timely allocation of client orders
  - Prevent the intermediary or staff from taking advantage of price-sensitive information or from participating in insider dealing
  - Prevent or detect errors, omissions, fraud and other unauthorized or improper activities
  - Protect the assets of clients and the intermediary from theft, fraud and other acts of misappropriation
  - Ensure that regular reconciliations of the intermediary's records with external records and reports are carried out

2.8 Risk Management

2.8.1 Objective

- To establish and maintain effective policies and procedures to:
  - Ensure the proper management of risks
  - Identify and quantify risks
  - Provide timely/adequate information to enable Management to take action to contain and manage risks

2.8.2 Control Guidelines

- The control guidelines provide for the establishment of:
  - a risk management function with suitably qualified and experienced professionals;
  - procedures to limit the exposure of the intermediary to risk of suffering loss to acceptable levels;
  - trading and position limits for proprietary trading and their monitoring at the end of the trading day;
  - comprehensive risk-focused reviews at suitable intervals or whenever there are significant changes in the business, operations or staff;
  - regular reporting of exposures and significant variances to management; and
  - risk policy defined by management including risk measurement and reporting methodologies

2.8.3 SFC Risk Criteria

- The SFC uses the following risk criteria in assessing intermediaries:
  - **Credit risk**: risk of a client or counterparty defaulting on an obligation
  - **Market risk**: risk of an intermediary suffering a loss due to adverse movements in asset/liability market values
  - **Liquidity risk**: risk that a product may not be sold in the short term without material loss
  - **Operational risk**: risk of losses from fraud, errors, omissions and other operational/compliance matters

3. PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING

Money Laundering

Activities and processes by which property obtained as a result of illegal activities is altered so that it is given the appearance of coming from a legitimate source

- Four pieces of legislation and one SFC Guideline:
  - Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance (**AMLO**)
  - Drug Trafficking (Recovery of Proceeds) Ordinance (**DTRPO**)
  - Organised and Serious Crimes Ordinance (**OSCO**)
  - United Nations (Anti-terrorism Measures) Ordinance (**UNATMO**)
  - Guideline on Anti-Money Laundering and counter-Terrorist Financing (**GAML**)

3.1 Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance

- Objective is to enhance Hong Kong AML regime for the financial sector, including banking, securities, insurance and remittance and money changing. Primary concerns are:
  - customer due diligence (CDD) requirements
  - record-keeping requirements
  - powers of relevant authorities (SFC & HKMA) to investigate and supervise LCs and RIs for AMLO compliance and then to discipline, if appropriate
  - establishment of a disciplinary review panel
- A breach of the AMLO is a criminal offence
- Employees/managers of LCs/RIs who knowingly cause/permit the corporate entity to breach the AMLO, are committing a criminal offence – maximum penalty is HK$1m and 2 years in prison
- If fraud is involved, the maximum penalty will be a fine of HK$1m and 7 years in prison
- A breach of the AMLO by a LC/RI can lead to regulatory discipline

3.2 Drug Trafficking (Recovery of Proceeds) Ordinance

- It is an offence to deal with property known to, or believed to, represent the proceeds of drug trafficking
- Any person who knows or suspects that property relates to drug trafficking, should report it to a police officer, a customs and excise officer, or the Joint Financial Intelligence Unit (JFIU) – **failure to disclose is an offence**
- It is an offence to disclose to another person that a disclosure has been made, as above
- A person making a disclosure is excused from any resulting contract breach or professional obligation

3.3 Organised and Serious Crimes Ordinance

- Provisions are similar to DTRPO
- Police are given powers to obtain a court order to compel a person to provide information or material relating to the investigation
- Requirements to disclose and to submit to searches override any duties of secrecy and confidentiality

3.4 United Nations (Anti-terrorism Measures) Ordinance

- It is a criminal offence to provide/collect property or financial services to/from terrorists or their associates
- Terrorist property can be frozen/forfeited
- It is an offence not to report knowledge or suspicions of terrorist property to an authorized officer

3.5 SFC Regulations – Guideline on Anti-Money Laundering and Counter-Terrorist Financing (GAML)

- As empowered by the AMLO, the SFC has issued guidance on implementing policies, procedures and controls to comply with the AMLO

- The GAML describes 3 common stages identified by the SFC in the process of money laundering:
  1. **Placement**: physical disposal of cash derived from illegal activities
  2. **Layering**: separation of the illicit proceeds from the source by creating a number of financial transactions (layers) – the most likely point at which a licensed corporation could become involved in a money laundering scheme
  3. **Integration**: creating an impression of legitimacy by bringing the proceeds back into the general financial system (without being connected with the illegal activity)

- The **GAML requires** licensed corporations to:
  - **Issue policies** and procedures to staff reflecting GAML provisions
  - Ensure that **staff understand** the GAML
  - **Regularly review** anti-money laundering policies and procedures through the compliance and audit functions
  - **Appoint** a money laundering reporting officer as a central reference point

3.5.1 GAML Detailed Guidelines

Client Identification

- Client risk should be considered when carrying out CDD, taking the following into account:
  - Services that provide more anonymity
  - Non face-to-face account opening
  - Background/profile(eg politically exposed persons)
  - Unduly complex ownership structure
  - Nature of business – sensitive or high-risk activities
  - Nationality/place of incorporation
  - Means/types of payments
  - Countries with critical deficiencies in their anti-money laundering systems

Ongoing Monitoring

- Client activities should be subject to ongoing monitoring to detect unusual or suspicious activities
- Activities of higher risk clients should be subject to more frequent and more intensive monitoring

Record-keeping and Retention

- There should be a satisfactory audit trail
- **Customer documents** and information should be kept throughout the business relationship and for a period of **six years** after the end of the business relationship
- **Transaction documents** and information should be kept for **six years** irrespective of whether the business relationship ends during the period

Recognition and Reporting of Suspicious Transactions

- Senior management and the money laundering reporting officer should be able to detect unusual or suspicious activities promptly
- Suspicious transactions will be unusual in relation to the client's business/financial circumstances

Examples of Suspicious Transactions

- GAML provides a list of situations that might give rise to suspicions of money laundering activity:

  Customer-related

  - Requests for investment management services where source of funds are unclear or not in line with customer's financial background
  - Opening of multiple accounts with same beneficial owners

  Trading-related

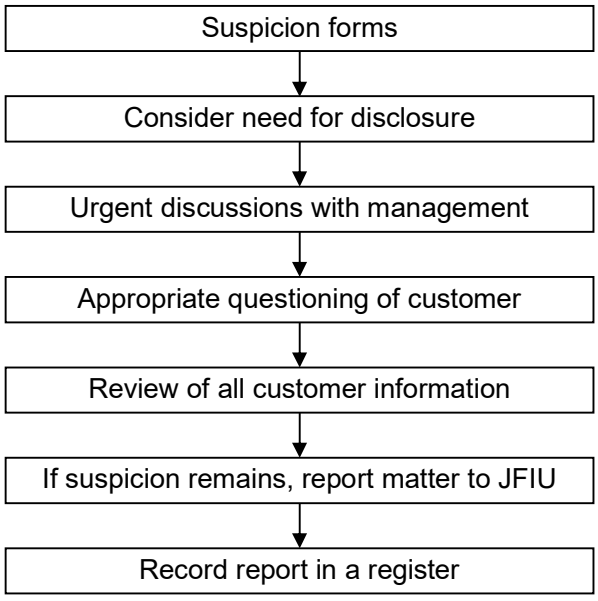
  - Buying/selling activities with no obvious purpose
  - Frequent small cash transactions followed by one sale transaction to a third party

  Settlement/custody/transfers-related

  - Large or unusual settlements in cash
  - Idle client funds held by licensed corporation
  - Frequent fund transfers/cheque payments to/from unverified third parties

- **Involving employees**
  - Changes in lifestyle: high spending or not taking holidays
  - Unusual or unexpected increase in an employee's sales performance
  - Forwarding addresses used for clients such as staff or persons connected to staff

Procedures for Disclosure (as suggested by JFIU)



Education and Training

- Licensed corporations are required to regularly give staff information and training to keep them aware of:
  - Their obligations and potential liabilities
  - Policies and procedures relating to money laundering, including identification and reporting of suspicious transactions
  - New and emerging ways of money laundering

4. ELECTRONIC TRADING

- Internet activities are treated the same as any other form of securities and futures business

4.1 Conduct Requirements of Electronic Trading in Code of Conduct and its Application

Para 18 and Schedule 7 of the Code of Conduct set out the conduct requirements of electronic trading. A licensed or registered person conducting electronic trading of securities that are listed or traded on an exchange must abide by the conduct requirements

Electronic trading includes internet trading, direct market access and algorithmic trading.

4.1.1 Responsibility for Orders

- A licensed or registered person is responsible the settlement and financial obligations of orders and implementation of policies and procedures to supervise the orders

4.1.2 Management and Supervision

- A licensed or registered person should manage and supervise the design and operation of the electronic trading system, including
  - written internal policies and procedures
  - at least one responsible/executive officer responsible for the overall management and supervision of the system
  - adequate qualified staff, technology and financial resources

4.1.3 Adequacy of System

- To ensure the reliability, security and capacity of the system, the following controls should be adopted:
  - Prevention of system generating and sending orders to the market and cancelation of any unexecuted orders in the market
  - Initial system testing should be followed by regular reviews. Any material system interruptions should be promptly reported to the SFC
  - Appropriate security controls to avoid system abuse
  - A licensed/registered person should monitor capacity usage and keep a record of spare capacity planned
  - System capacity should be regularly stress tested and findings documented
  - There should be contingencies for client orders that exceed system capacity ensuring that alternative means of order execution are available

4.1.4 Record Keeping

- Proper records should be kept covering system design and development, risk management controls and audit logs for a period not less than 2 years

4.2 Specific Requirements on Internet Trading and Direct Market Access (DMA)

4.2.1 Risk Management

- A licensed or registered person that provides internet trading or direct market access (DMA) services must ensure that all client orders are transmitted to its infrastructure. Client orders must be subject to the following:
  - Appropriate automated pre-trade risk management controls
  - Regular post-trade monitoring to identify any manipulative or abusive order instructions/transactions

4.2.2 Minimum Client Requirements for DMA Services

- DMA clients should be vetted before any service is provided. Comfort should be gained that the client:
  - Has appropriate arrangements in place to ensure its users are competent in using the relevant systems
  - Understands and complies with applicable regulatory requirements
  - Is able to monitor the orders entered through the DMA services
- A licensed or registered person should regularly evaluate minimum client requirements, given current market conditions, and consider whether clients using its DMA services continue to meet minimum client requirements

Note: DMA refers to market access for a client through a licensed or registered person's identifier whereby the client transmits orders, directly or indirectly, to the market's trading system for execution

4.3 Algorithmic Trading System and Trading Algorithms

- Algorithmic trading is computer generated trading created by a predetermined set of rules aimed at delivering specific execution outcomes. The trading system can be a system designed and developed in-house or by a third-party service provider

4.3.1 Qualification

- Controls should ensure that only suitably qualified persons are involved in the design and development of an algorithmic trading system as well as the use of the system. Training should be provided where required

4.3.2 Testing

- There should be adequate testing of an algorithmic trading system to ensure that it operates as designed and that it will cope with changing market conditions
- The system and algorithms should be reviewed and tested at least annually

4.3.3 Risk Management

- Reasonably designed controls should ensure the integrity of an algorithmic trading system and should ensure that it operates in the interest of the market

5. ALTERNATIVE LIQUIDITY POOLS (ALP)

- ALP means an electronic system operated by a licensed/registered person allowing crossing/matching of orders involving Hong Kong and overseas listed securities
- Code of Conduct applies to ALP operators

5.1 Management and Supervision

- An ALP operator should have written policies and procedures to ensure that:
  - There is at least one responsible/executive officer responsible for overall ALP management and supervision
  - There are controls to manage the risks of ALP operations
  - There is a formal governance process with input from risk and compliance functions
  - There are clearly defined reporting lines
- Regarding access to and operation of ALPs, an ALP operator should:
  - Ensure only qualified investors can become ALP users
  - Ensure client orders have priority over proprietary orders
  - Revise/update as necessary the ALP Guidelines

5.2 Adequacy of Systems

- An ALP system should restrict the visibility of trading information available to staff of the ALP operator, including:
  - Restricting staff access to ALP trading information
  - Keeping the SFC informed of the identities of staff with access to the ALP
  - Maintaining a log with details of staff access to the ALP
  - Ensuring that staff members who originate proprietary orders in the ALP do not have access to ALP trading/transaction information

5.3 Record Keeping

- An ALP operator should keep proper records covering the design, development, deployment and operation of the ALP
- SFC should be kept informed of any changes to ALP operation

6. PERSONAL DATA (PRIVACY) ORDINANCE (PDPO)

- The PDPO protects the privacy of individuals in relation to personal data
- The Privacy Commissioner for Personal Data is an independent public officer appointed to enforce and promote compliance with the PDPO
- Data users must comply with six data protection principles

6.1 Data Protection Principles

Principle 1 - Purpose and manner of collection of personal data

- Data shall only be collected for a lawful and relevant purpose
- The purpose of collecting the data should be disclosed

Principle 2 - Accuracy and duration of retention of personal data

- Personal data should be accurate, up to date and kept no longer than necessary and should be rectified if incorrect

Principle 3 - Use of personal data

- Without the consent of the subject, the data should not be used for any purpose other than for which it was collected

Principle 4 - Security of personal data

- All measures should be taken to ensure that personal data are protected against unauthorized access, processing, erasure, etc

Principle 5 - Information to be generally available

- A data user's policies and practices relating to the data should be available

Principle 6 - Access to personal data

- A data subject should be able to get access (at a reasonable fee) to the data held and request corrections to it

7. COMPLIANCE AND RELATED ISSUES

- An intermediary should ensure that a good compliance philosophy is established and that directors and employees meet the highest expectations of:
  - Clients
  - The market
  - Regulators
  - The Government

7.1 Roles of Senior Management

- Senior management must provide leadership to drive the promotion of good compliance practices by installing:
  - Good line and reporting structures
  - Clearly defined functions and responsibilities
  - Effective communications
  - Appropriate transparency and disclosure practices
  - Well-defined policies, practices and procedures….in writing
  - Distinctions between supervisory/review functions and operational/line functions
  - Good relationships with external agencies, such as regulators and auditors
  - Open access for complaints, which should be dealt with promptly
  - Good corporate governance

7.2 Corporate Governance

- Corporate governance is concerned with the **system by which companies are directed and controlled** to ensure the proper relationship between a company's management, its board and its shareholders
- The Organisation for Economic Co-operation and Development (**OECD**) has issued a **set of core principles** for corporate governance practices to include:
  - Fairness
  - Transparency
  - Accountability
  - Responsibility
- An objective of good corporate governance is to avoid management taking improper advantage of its position to the detriment of the company's interests

- Corporate governance can be improved through:
  - Installing appropriate **checks and balances**, such as separating the functions of **Chairman and CEO**, appointment of **non-executive directors**, establishment of **independent audit committees** and setting up of **remuneration and benefit committees**
  - Increasing transparency and disclosures to shareholders / stakeholders /public
  - Adopting international accounting/auditing standards
  - Installing strong protective structures for minority shareholders, creditors and other lenders
  - Identifying and penalizing corporate wrongdoing

- Corporate governance deficiencies can lead to insider dealing, fraud and connected transactions which are undervalued

8. OTHER MATTERS CONCERNING BUSINESS OPERATIONS AND PRACTICES

8.1 Insurance Cover

- Insurance cover by a licensed corporation is a necessary licensing requirement
- The Securities and Futures (Insurance) Rules do not apply to licensed corporations which may not hold client assets and are not exchange participants
- The SFC may approve master policies of insurance
- The risks covered are the loss of client assets by the licensed corporation (including assets held by its associated entity) attributed to fraud or theft
- An example of the amount of cover required is HK$15m for each of:
  - Dealing in securities
  - Dealing in futures contracts
  - Securities margin financing

8.2 Common Reporting Standard (CRS)

- In 2014, the OECD developed the CRS to enhance tax transparency and combat tax evasion
- Under the CRS, Hong Kong has introduced legislation requiring licensed corporations/registered institutions to undertake due diligence necessary to identify financial accounts held by tax residents of reportable jurisdictions
- Such accounts need to be reported to the Inland Revenue Department on an annual basis