INSTITUTE OF SINGAPORE CHARTERED ACCOUNTANTS

Global Mindset, Asian Insights

Anti-Money Laundering and Countering the Financing of Terrorism

A Summary of Requirements and Guidelines for Professional Accountants in Singapore

Anti-Money Laundering and Countering the Financing of Terrorism

A Summary of Requirements and Guidelines for Professional Accountants in Singapore

Every year, criminals launder anywhere between US$800 billion and US$2 trillion worldwide. The global impact is staggering. Expectations of professional accountants to combat money laundering are rising. Internationally, there are increasing calls for professional accountants to adopt measures that are at least up to the international standards recommended by the Financial Action Task Force (FATF)[1].

In response, ISCA has developed a new Ethics Pronouncement (EP) 200, *"Anti-Money Laundering and Countering the Financing of Terrorism – Requirements and Guidelines for Professional Accountants in Singapore"*, which covers the following areas:

(a) Legal obligations of professional accountants under the existing Singapore legislations, which include the reporting of suspicious transactions; and

(b) New requirements and guidelines on the anti-money laundering (AML) and countering the financing of terrorism (CFT) systems, controls and measures that professional firms[2] should have in place, including enhanced measures for high risk services. These requirements and guidelines are in line with the standards set by the FATF.

Which Requirements and Guidelines are Relevant to You?

EP 200 sets out the scope of its respective sections as follows:

Section/ Category of Professional Accountants	Reporting and Tipping-off (Section 2)	Systems and Controls (Section 3)	Customer Due Diligence (CDD) and Records Keeping (Section 4)	Reporting, Training, Compliance, Hiring and Audit (Section 5)
Professional accountants in business	Mandatory	Not Applicable	Not Applicable	Not Applicable
Professional accountants in public practice and professional firms, providing services other than designated high risk services[3]	Mandatory	Mandatory	Good Guidance	Good Guidance
Professional accountants in public practice and professional firms, providing any designated high risk service	Mandatory	Mandatory	Mandatory	Good Guidance

Section 2 – Reporting and Tipping-off

A professional accountant is required under Singapore law[4] to lodge a suspicious transaction report with the Suspicious Transaction Reporting Office, Commercial Affairs Department of the Singapore Police Force (STRO) if he knows or has reasonable grounds to suspect that transactions are related to money laundering or terrorist financing, and if such

---

[1] The Financial Action Task Force (FATF) is an inter-governmental body established in 1989 to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorism financing and other related threats to the integrity of the international financial system. Singapore is a member of FATF.

[2] A professional firm is an accounting corporation, an accounting firm or an accounting LLP approved under the Accountants Act; or an entity owned or controlled by a professional accountant or professional accountants, that provide professional services. Professional services are services requiring accountancy or related skills performed by a professional accountant including accounting, auditing, taxation, management consulting and financial management services. These include the designated high risk services described in footnote 3.

[3] The designated high risk services are:
(a) Buying and selling of real estate;
(b) Managing of client money, securities or other assets;
(c) Management of bank, savings or securities accounts;
(d) Organisation of contributions for the creation, operation or management of companies; and
(e) Creation, operation or management of legal persons or arrangements, and buying and selling of business entities.

[4] In Singapore, the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act, Cap. 65A (CDSA) is the legislation which sets out criminal offences directly in relation to money laundering. The Terrorism (Suppression of Financing) Act, Cap. 325 (TSFA), sets out the criminal offences directly in relation to terrorist financing.

knowledge or suspicion arose in the course of his trade, profession, business or employment[5]. All suspicious transactions, including attempted transactions, shall be reported regardless of the amount of the transaction. Failure to report is a criminal offence.

Where a professional accountant knows or suspects that investigations by the authorities are underway, the professional accountant should exercise caution not to disclose related information to the alleged perpetrator (or any other parties) so as to avoid tipping off. It is an offence under the Singapore law if doing so is likely to prejudice an investigation or impending investigation[6].

Confidentiality and Statutory Immunity

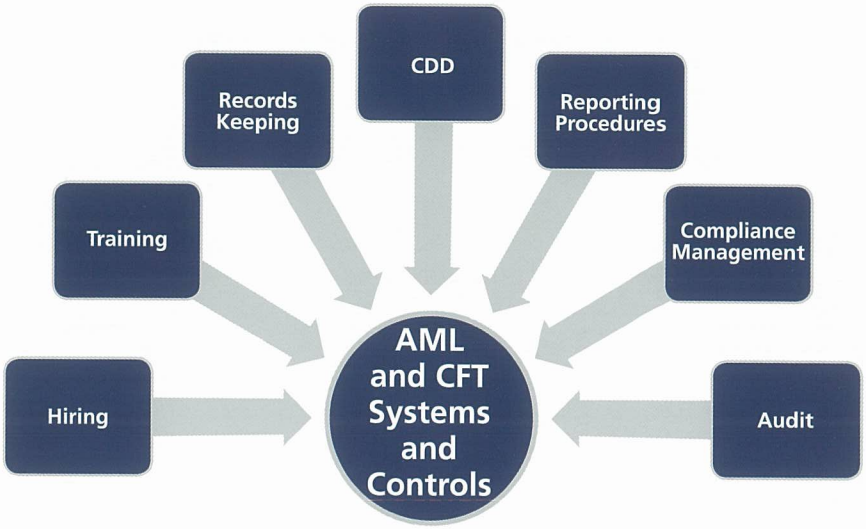
The statutory obligation to report suspicious transactions to the authorities overrides any duty of confidentiality to a client.

Statutory immunity is granted from any legal action, criminal or civil, for breach of confidence arising from having reported suspicions of money laundering and terrorist financing to the STRO, provided the report is made in good faith, and even if no criminal activities have been found upon subsequent investigation. Statutory immunity is similarly granted to the professional accountant who reports any knowledge or suspicion of money laundering or terrorist financing to an appropriate partner of the professional firm through its internal reporting channel.

Section 3 – Systems and Controls

All professional firms shall have in place systems and controls to address money laundering and terrorist financing concerns.

A risk-based approach towards establishing AML and CFT systems and controls shall be adopted. The type and extent of the measures taken in each of the areas (see diagram on right) shall be appropriate having regard to the risk of money laundering and terrorist financing and the size and nature of the business. Where the risks are higher, enhanced measures shall be taken to manage and mitigate those risks. Conversely, if the risks are lower, simplified measures may be permitted.



For professional firms which have branches and/or subsidiaries, the firms shall also develop and implement group-wide programmes on AML and CFT, including policies and procedures for sharing information within the group.

Section 4 – CDD and Records Keeping

The CDD and records keeping measures are covered in Section 4 of EP 200. These measures are mandatory for professional firms when they provide any designated high risk service. When other services, such as audits are performed, these measures are good guidance that can be implemented.

CDD

The primary objective of CDD is to enable effective identification and reporting of suspicious activities. Unless one truly knows his clients, and well enough to understand and anticipate their behaviour, one can neither reasonably nor effectively distinguish unusual suspicious activity from usual behaviour.

The **CDD measures** to be taken are:
(a) Identifying the client;
(b) Identifying the beneficial owner;
(c) Verifying the identity of the client using reliable, independent source documents, data or information;
(d) Verifying the identity of the beneficial owners using reasonable measures;
(e) Understanding and obtaining information on the purpose and intended nature of the business relationship; and
(f) Conducting ongoing due diligence on any continuing business relationship and scrutiny of transactions undertaken during the course of the relationship.

Application and Timing of CDD

The CDD measures shall be undertaken when establishing business relations; carrying out occasional transactions; when there is a suspicion of money laundering or terrorist financing; or where there are doubts about the veracity or adequacy of

[5] Section 39 of the CDSA and Section 8 of the TSFA.

[6] Section 48 of the CDSA and Section 10(B) of the TSFA.

previously obtained client identification data. Generally, the verification of the identity of the client and the beneficial owner should be performed before or during the course of establishing the business relationship.

Conducting CDD [Know Your Client (KYC)]

The information usually obtained when conducting CDD are as follows:

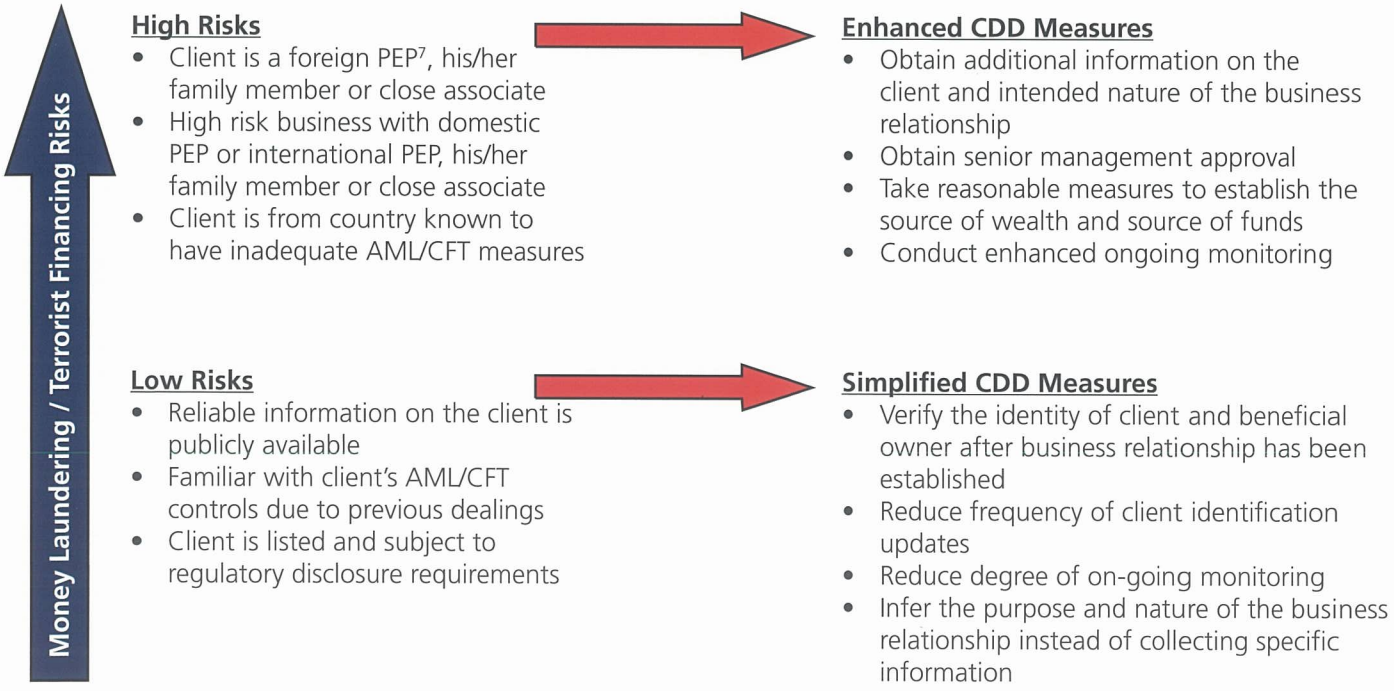
Identification and verification of client's identity	Identification and verification of beneficial owner's identity
Name, legal form and proof of existence – A certificate of incorporation, a certificate of good standing, a partnership agreement, a deed of trust, or other appropriate documentation from a reliable independent source	**For legal persons –** (in the following order) The identity of the natural persons who ultimately have a controlling ownership interest in a legal person; The identity of the natural persons (if any) exercising control of the legal person or arrangement through other means; or The relevant natural person who holds the position of senior managing official.
The powers that regulate and bind the legal person or arrangement – Memorandum and articles of association of a company, as well as the names of the relevant persons having a senior management position in the legal person or arrangement	**For legal arrangements –** Trusts – the identity of the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust (including through a chain of control/ ownership) Other types of legal arrangements – the identity of persons in equivalent or similar positions
The address of the registered office, and, if different, a principal place of business	-

Non-compliance with CDD Requirements

Where the professional firm is unable to carry out the CDD measures, for example, due to client's refusal to provide evidence of identity or other information, business relations shall not commence/shall be terminated; and consideration shall be made as to whether a suspicious transactions report is necessary.

The Risk-Based Approach to CDD

All the CDD measures shall be applied. However, the extent of such measures would depend on the risks of money laundering and terrorist financing.



[7] Politically exposed person (PEP) – An individual who is or has been entrusted with prominent public functions.

Prohibited Relationships

Professional firms shall comply with prohibitions issued by relevant authorities and shall also check the names of clients or potential clients against the list of persons subject to prescribed restrictions in the regulations issued by the Monetary Authority of Singapore, and the list of terrorist names under the First Schedule of the TSFA.

Such screening shall be done when, or as soon as reasonably practicable after, the business relations have been established with the client; on a periodic basis after the establishment of business relations; and when there are any changes or updates to the lists and information provided by the relevant authorities.

Reliance on third parties

Professional firms may rely on third parties to perform the CDD measures, provided certain criteria are met. However, third parties cannot be relied upon to perform ongoing monitoring of clients, unless the third party is part of the professional firm's group or network. The ultimate responsibility for CDD measures remains with the professional firm.

Records Keeping

Professional firms shall prepare, maintain and retain documentation on all its business relations with, and transactions for, its clients such that:

(a) All requirements imposed by law are met;

(b) Any individual transaction can be reconstructed so as to provide, if necessary, evidence for prosecution of criminal activity;

(c) The relevant authorities are able to review the professional firm's business relations, transactions, records and CDD information and assess the level of compliance with relevant laws and compliance with EP 200; and

(d) The professional firm can satisfy, within a reasonable time or any more specific time period imposed by law or by any requesting authority, any enquiry or order from the relevant authorities for information.

Unless otherwise imposed by law or request from relevant authorities, all information obtained through CDD measures, account files and business correspondence, including the results of any analysis undertaken, shall be retained for a period of at least 5 years after the termination of business relations.

All records relating to a transaction, including any information needed to explain and reconstruct the transaction, shall be retained for a period of at least 5 years following the completion of the transaction.

Section 5 – Reporting, Training, Compliance, Hiring and Audit

Section 5 of EP 200 covers measures on reporting procedures, training, compliance management, hiring and audit. These measures are good guidance that should be implemented by professional firms.

Reporting Procedures

Professional firms should implement appropriate internal policies, procedures and controls to meet its reporting obligations under the law, including what is expected of their employees who form suspicions or obtain knowledge of possible money laundering or terrorist financing. A single reference point [the appointment of a Money Laundering Reporting Officer (MLRO)] should be established within the organisation. Employees could promptly refer all suspicious transactions, for possible reporting to the STRO, to the MLRO who will then determine whether a report to the STRO is necessary.

Training

Professional firms should establish an on-going training programme, tailored to their size, nature and complexity. Staff should be reminded of their responsibilities with respect to AML and CFT and kept informed of related new developments through refresher training, or through other forms of internal communication. Refresher training should be held at least once every 2 years, or more regularly where there have been significant developments such as new regulatory requirements or changes to key internal processes.

Compliance Management

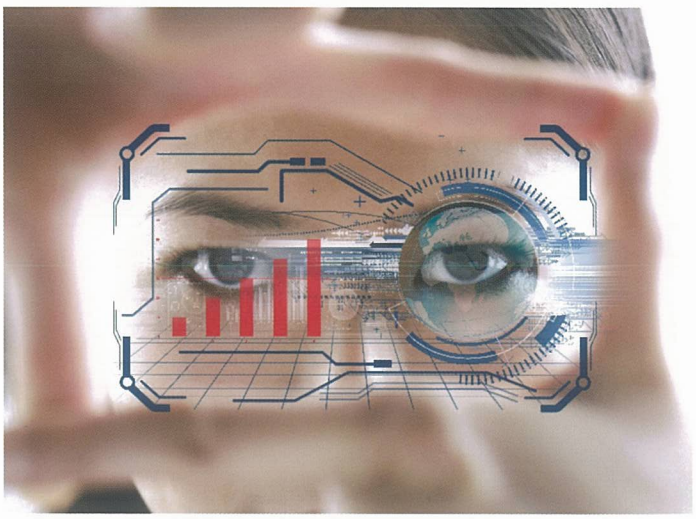
It is important to develop appropriate compliance management arrangements to monitor the firm's compliance with its AML and CFT policy and procedures. This includes the appointment of a compliance officer at the management level who would report to senior management on compliance and address any identified deficiencies.

Hiring

Professional firms should have adequate screening procedures in place to ensure high standards when hiring employees.

Audit

There should be an adequately resourced and independent audit function to regularly assess the effectiveness of the professional firm's internal policies, procedures and controls, and its compliance with AML and CFT requirements.



About the Institute of Singapore Chartered Accountants

The Institute of Singapore Chartered Accountants (ISCA) is the national accountancy body of Singapore. ISCA's vision is to be a globally recognised professional accountancy body, bringing value to our members, the profession and wider community.

Established in 1963, ISCA shapes the regional accountancy landscape through advocating the interests of the profession. Possessing a Global Mindset, with Asian Insights, ISCA leverages its regional expertise, knowledge, and networks with diverse stakeholders to contribute towards Singapore's transformation into a global accountancy hub. Our stakeholders include government and industry bodies, employers, educators, and the public.

ISCA is the Administrator of the Singapore Qualification Programme (Singapore QP) and the Designated Entity to confer the Chartered Accountant of Singapore - CA (Singapore) - designation.

It aims to raise the international profile of the Singapore QP, a post-university professional accountancy qualification programme and promote it as the educational pathway of choice for professional accountants seeking to achieve the CA (Singapore) designation, a prestigious title that is expected attain global recognition and portability.

For more information, please visit www.isca.org.sg

About ISCA Technical Standards Development and Advisory

The Technical Standards Development and Advisory (TSDA) team is part of the Technical Knowledge Centre and Quality Assurance division of ISCA. It is committed to supporting the Institute in advancing and promoting technical developments within the accountancy profession as part of the effort to transform Singapore into a leading global accountancy hub by 2020.

ISCA TSDA engages external stakeholders in soliciting meaningful feedback on accounting, auditing and ethics related issues to develop a consistent approach to addressing industry issues identified. It also prescribes auditing and assurance standards and the ISCA Code of Professional Conduct and Ethics that are closely aligned to international standards, champions thought leadership initiatives with key stakeholders and drives projects in collaboration with various ISCA technical committees.

It actively engages international standard setters and strives to be an advocate of matters pertinent to the development of Singapore's accountancy profession. Furthermore, it aims to cultivate a mindset change and raises awareness of new and revised standards through the publication of articles authored by the team.

Additionally, ISCA TSDA seeks to empower members and the profession at large to achieve their aspirations by equipping them with relevant technical expertise and this is achieved through the development of a range of resources that they can tap on.

Knowledge sharing with the accountancy profession is facilitated through a variety of print and online channels including the sharing of regular updates and thought leadership articles via in-house publications like the journal, "IS Chartered Accountant", the E-newsletter, "ISCA Weekly", and various online knowledge centres and a technical forum. Seminars and workshops are regularly organised and ISCA TSDA also provides value-added technical clarification services to assist the profession in resolving accounting, auditing and ethics related issues.

Disclaimer

This document contains general information only and ISCA is not, by means of this document, rendering any professional advice or services. This document is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a professional advisor. Whilst every care has been taken in compiling this document, ISCA makes no representations or warranty (expressed or implied) about the accuracy, suitability, reliability or completeness of the information for any purpose. ISCA, its employees or agents accept no liability to any party for any loss, damage or costs howsoever arising, whether directly or indirectly from any action or decision taken (or not taken) as a result of any person relying on or otherwise using this document or arising from any omission from it.