INSTITUTE OF SINGAPORE CHARTERED ACCOUNTANTS

Ethics Pronouncement EP 200

Anti-Money Laundering and Countering the Financing of Terrorism – Requirements and Guidelines for Professional Accountants in Singapore

This Pronouncement was issued by the Council of the Institute of Singapore Chartered Accountants (ISCA) on 29 October 2014.

This Pronouncement is effective 1 November 2014.
The establishment of, and any improvement to, systems and controls to meet the requirements and guidance in Sections 3, 4 and 5 shall be implemented by 1 May 2015.

All ISCA Members are required to comply with the requirements in this Pronouncement. Apparent failure to do so may result in an investigation into the member's conduct by the Investigation Committee of ISCA.

ANTI-MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM – REQUIREMENTS AND GUIDELINES FOR PROFESSIONAL ACCOUNTANTS IN SINGAPORE

(This Pronouncement is effective 1 November 2014. The establishment of, and any improvement to, systems and controls to meet the requirements and guidance in Sections 3, 4 and 5 shall be implemented by 1 May 2015)

CONTENTS

ANTI-MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM – REQUIREMENTS AND GUIDELINES FOR PROFESSIONAL ACCOUNTANTS IN SINGAPORE

PREAMBLE

1. Singapore has established a strict and rigorous anti-money laundering (AML) and countering the financing of terrorism (CFT) regime through its comprehensive and sound legal, institutional, policy and supervisory frameworks to ensure that Singapore is not a safe haven for money launderers and terrorist financiers.

2. The Financial Action Task Force (FATF) is an inter-governmental body established in 1989 to set standards and to promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and the financing of proliferation, and other related threats to the integrity of the international financial system. Singapore is committed to the fight against money laundering and terrorist financing and is a member of several international AML/CFT organisations, including FATF. As a member of FATF, Singapore is committed to comply with and implement the "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation" issued by the FATF (FATF Recommendations).

3. The AML and CFT legislations in Singapore provide a framework for discouraging money laundering and terrorist financing by, for example, establishing criminal sanctions for such activities and requiring the reporting of suspicious transactions to the authorities.

4. These legislations have implications on the responsibilities of professional accountants, including the risk of criminal liability on professional accountants for non-compliance.

5. The purpose of this Pronouncement is to provide information about our current AML and CFT legislations, and guidance on compliance with those legislations, as well as additional requirements and guidelines on AML and CFT to the professional accountants in Singapore.

SECTION 1 – ABOUT THIS PRONOUNCEMENT

Introduction

1.1 Money is "laundered" to conceal criminal activity associated with it, including the crimes that generate the money, for example, drug trafficking, fraud and criminal breach of trust. The term “money laundering” covers any activity by which the apparent source and ownership of money representing the proceeds of crime are changed so that the money appears to have been obtained legitimately. Terrorist financing refers to the direct or indirect act of providing or collecting property for terrorist acts, providing property and services for terrorist purposes, using or possessing property for terrorist purposes, and dealing with property of terrorists. A brief description of money laundering and terrorist financing is set out in Appendix A.

1.2 This Pronouncement takes into consideration the following primary AML and CFT legislations in Singapore:

(a) Primary legislation setting out criminal offences directly in relation to money laundering which apply to any person, regardless of the capacity in which he or she is acting. These offences are set out in the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act, Cap. 65A (CDSA). The CDSA also imposes a duty on a person, who in the course of his or her professional duties comes to know or suspect that any property represents the proceeds of drug trafficking or criminal conduct, to report the knowledge or suspicion to the relevant authorities. A summary of the key provisions is set out in Appendix B;

(b) Primary legislation setting out criminal offences directly in relation to terrorist financing which apply to any person, regardless of the capacity in which he or she is acting. These are set out in the Terrorism (Suppression of Financing) Act, Cap. 325 (TSFA). The TSFA also imposes a duty on a person who has possession, custody or control of terrorist property, or information regarding a transaction in terrorist property, to report such information to the relevant authorities. Furthermore, a person who has information which can prevent the commission of a terrorist financing offence, or assist in the apprehension, prosecution or conviction of a person for a terrorist financing offence, is required to immediately inform the relevant authorities. A summary of the key provisions is set out in Appendix C; and

(c) Primary legislation setting out criminal offences indirectly in relation to money laundering which apply to any person, regardless of the capacity in which he or she is acting. These offences are set out in Sections 107, 108, 108A and 108B of the Penal Code, Cap. 224. A summary of the key provisions is set out in Appendix D.

Definitions

1.3 For purposes of this Pronouncement, the following terms have the meanings attributed below:

(a) Beneficial owner – The natural person(s) who ultimately owns or controls a client and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.

(b) Branch – An extension of the parent and is not a legal entity separate from the parent.

(c) Group – A parent and its subsidiaries and/or branches.

(d) Legal arrangement – Express trusts or other similar arrangements.

(e) Legal person – Any entities other than natural persons that can establish a permanent client relationship with a professional firm or otherwise own property. This can include companies, bodies corporate, foundations, partnerships, or associations and other relevantly similar entities.

(f) Professional accountant – An individual who is a member of the Institute of Singapore Chartered Accountants (ISCA).

(g) Network – A larger structure that is aimed at co-operation, and that is clearly aimed at profit or cost sharing or shares common ownership, control or management, common quality control policies and procedures, common business strategy, the use of a common brand-name, or a significant part of professional resources.

(h) Network firm – A firm or entity that belongs to a network.

(i) Politically exposed person (PEP) – A foreign PEP, domestic PEP or international organisation PEP.

Foreign PEPs are individuals who are or have been entrusted with prominent public functions by a foreign country, for example Heads of State or of government, senior politicians, government ministers, senior civil or public servants, judicial or military officials, senior executives of state owned corporations, senior political party officials and members of the legislature.

Domestic PEPs are individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, government ministers (including Second Minister and Minister of State), senior civil or public servants[1], judicial or military officials, senior executives of state owned corporations, senior political party officials[2] and members of the legislature.

International organisation PEPs are persons who are or have been entrusted with a prominent function by an international organisation such as members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions. International organisation means an entity established by formal political agreements between member countries that have the status of international treaties, whose existence is recognised by law in member countries and who is not treated as a resident institutional unit of the country in which it is located.

The definition of PEPs is not intended to cover middle ranking or more junior individuals in the foregoing categories.

(j) Family member of a PEP – An individual who is related to a PEP either directly (consanguinity) or through marriage or similar (civil) forms of partnership.

(k) Close associate of a PEP – An individual who is closely connected to a PEP, either socially or professionally.

(l) Professional accountant in business – A professional accountant employed or engaged in an executive or non-executive capacity in such areas as commerce, industry, service, the public sector, education, the not for profit sector, regulatory bodies or professional bodies, or a professional accountant contracted by such entities.

(m) Professional accountant in public practice – A professional accountant irrespective of functional classification (for example, audit, tax or consulting) in a professional firm.

[1] Senior civil or public servants include:
(a) Senior Parliamentary Secretary
(b) Parliamentary Secretary
(c) Permanent Secretary
(d) Second Permanent Secretary
(e) Director–General
(f) Heads of statutory boards
(g) Chairman & Chief Executive Officer of government bodies excluding Government-Linked Corporations (GLC)

[2] Senior political party officials include:
(a) Head or
(b) Secretary General

(n) Professional firm – A professional firm is:

(i) An accounting corporation, an accounting firm or an accounting LLP approved under the Accountants Act; or

(ii) An entity, other than those in (i) above, owned or controlled by a professional accountant or professional accountants, that provide professional services.

(o) Professional services – Services requiring accountancy or related skills performed by a professional accountant including accounting, auditing, taxation, management consulting and financial management services. These include the services described in paragraph 1.5.

Scope

1.4 The table below illustrates the scope of this Pronouncement:

Section/ Category of Professional Accountants	**2**	**3**	**4**	**5**
Professional accountants in business	Mandatory	Not applicable	Not applicable	Not applicable
Professional accountants in public practice and professional firms, providing services other than those described in paragraph 1.5	Mandatory	Mandatory	Good Guidance	Good Guidance
Professional accountants in public practice and professional firms, providing any service described in paragraph 1.5	Mandatory	Mandatory	Mandatory	Good Guidance

1.5 When professional accountants in public practice and professional firms which prepare for or carry out transactions for their clients concerning the following situations, there are specific measures on customer due diligence and records keeping under the FATF Recommendations which they have to follow, which are set out in Section 4:

(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;

(e) Creation, operation or management of legal persons or arrangements, and buying and selling of business entities.

1.6 However, this Pronouncement:

(a) Does not address issues beyond those set out in this Pronouncement which may arise when providing professional services to financial institutions, such as providing reports to a regulator or other authority which may be required in relation to these entities' arrangements to prevent and detect money laundering and terrorist financing, their compliance with legislations and regulations, or their systems of controls more generally;

(b) Does not constitute legal advice, which a professional accountant shall consider obtaining to address specific situations that the professional accountant faces, such as if the professional accountant wishes to adopt legal interpretations that are different from those set out in this Pronouncement; and

(c) Shall not be regarded as guidance on foreign legislations. Professional accountants who perform services outside Singapore shall consider the need to familiarise themselves with the foreign AML and CFT legislations in order to mitigate the risk of committing offences in that foreign country.

SECTION 2 – REPORTING AND TIPPING-OFF

The relevant legislations in Singapore make it mandatory for a person, who in the course of his or her trade, profession, business or employment, to lodge a suspicious transaction report to the Suspicious Transaction Reporting Office, Commercial Affairs Department (CAD) of the Singapore Police Force (STRO) if one knows or has reasonable grounds to suspect transactions related to money laundering or terrorist financing. One is also prohibited from disclosing any information to any person if doing so is likely to prejudice an investigation or proposed investigation under the CDSA or TSFA. This Section provides a summary of the related criminal offences and guidance on reporting and tipping-off which is applicable for all professional accountants in Singapore.

Criminal Offences

2.1 Details of the criminal offences under the CDSA, TSFA and Penal Code are summarised in Appendices B, C and D respectively.

2.2 Professional accountants shall ensure that they are sufficiently aware of the main provisions of the AML and CFT legislations. In particular, the professional accountants' attention is drawn to the following matters:

(a) *Unknowingly assisting an offence*. Services provided by professional accountants could be of value to a successful criminal transaction. These include expertise in creating corporate vehicles, trusts and other legal arrangements that facilitate money laundering or terrorist financing, and the provision of financial and fiscal advice that is often an important element in criminal schemes.

Therefore, a professional accountant could be used by criminals resulting in a risk that the professional accountant being held liable for assisting in the crime, notwithstanding that the assistance was provided unknowingly. The prosecution need not prove that a person had actual knowledge of the relevant facts (e.g. knowing that the criminal's proceeds are from drug trafficking or other criminal conduct). Instead, a person can be held liable based merely on evidence showing that he had "reasonable grounds to believe" (e.g. that the proceeds were derived from criminal conduct).

Statutory defences are available. However, professional accountants shall note that the burden of establishing those statutory defences is upon the defendant, who must satisfy the Court on the balance of probabilities.

(b) *Statutory reporting responsibilities*. It is a criminal offence for failing to report money laundering to the authorities. Reporting is mandatory even in cases where a professional accountant merely has reasonable grounds to suspect that money laundering has occurred. Similarly, a professional accountant who fails to report terrorist financing faces the prospect of criminal liability.

(c) *Tipping-off offence*. It is an offence to disclose any information to any person if doing so is likely to prejudice an investigation or proposed investigation under the CDSA or TSFA.

2.3 When considering whether or not a professional accountant acted in a reasonable way, the Court could have regard to the requirements of this Pronouncement. Therefore, all professional accountants shall be familiar with and apply the requirements in the relevant Sections of this Pronouncement.

2.4 The offence of "assisting" may become relevant to professional accountants when suspicions of money laundering or terrorist financing exist. In normal circumstances, fulfilment of the professional accountant's responsibilities does not give rise to risk of committing the offence, even if subsequently money laundering or terrorist financing is found to have taken place. However, where the professional accountants discover information which could indicate to them that money laundering or terrorist financing is occurring or has occurred, they shall complete their assessment of whether there are reasonable grounds to suspect money laundering or terrorist financing is

occurring or has occurred (and, if appropriate, to report to the STRO) as discussed later in this Section before completing their professional responsibilities, for example, issuing their auditor's report on the client's financial statements.

2.5 To avoid the risk of being held to have assisted a money laundering or terrorist financing activity, professional accountants shall report any knowledge or suspicion of money laundering or terrorist financing through the professional firm's usual internal channels to an appropriate partner of the professional firm (where applicable), who will then determine whether a report to the STRO is necessary, or to the STRO directly.

Reporting and Tipping-off

2.6 A professional accountant faces the prospect of criminal liability for failing to report to the authorities suspicious transactions relating to money laundering or terrorist financing. All suspicious transactions, including attempted transactions, shall be reported regardless of the amount of the transaction.

2.7 Suspicious transactions shall be reported to the STRO and using as a recommendation, the Suspicious Transaction Reporting (STR) template available on the CAD website[3], "Guidelines on STR reporting and other AML/CFT requirements" section. The version updated as at the issuance date of this Pronouncement is in Appendix F. It is therefore critically important that professional accountants make a careful assessment of matters which put them on notice of money laundering or terrorist financing, in order to determine what type of activity may be involved and what obligations or consequences arise.

In the event that urgent disclosure is required, particularly where a transaction is known to be part of an ongoing investigation by the relevant authorities, professional accountants shall give initial notification to the STRO by telephone or email and follow up with such other means of reporting as the STRO may direct.

2.8 Professional accountants shall consider whether the following circumstances are suspicious that warrant a report to the STRO. Such considerations and conclusions shall be documented:

(a) The professional accountant is for any reason unable to complete the CDD measures; or

(b) The client is reluctant, unable or unwilling to provide any information requested by the professional accountant, decides to withdraw from establishing business relations or a pending engagement, or to terminate existing business relations.

2.9 Professional accountants shall keep watch for suspicious transactions in the course of conducting screening against lists of terrorist suspects as may be required by law or by any relevant authority. The professional accountant shall consider filing a suspicious transaction report even though there is no positive match against any name if the surrounding circumstances raise sufficient suspicions.

Knowledge and Suspicion

2.10 Suspicion is not defined in the existing legislations. Case law and other sources indicate that suspicion is more than speculation but it falls short of proof or knowledge. Suspicion is personal and subjective but will generally be built on some objective foundation.

2.11 Generally speaking, knowledge or reasonable grounds to suspect is likely to include:

(a) Actual knowledge;

(b) Shutting one's mind to the obvious;

(c) Deliberately refraining from making inquiries, the results of which one might not care to have;

[3] http://www.cad.gov.sg/content/cad/en/aml-cft/suspicious-transaction-reporting-office--stro-/suspicious-transaction-reporting.html

(d) Deliberately deterring a person from making disclosures, the content of which one might not care to have;

(e) Knowledge of circumstances which would indicate the facts to an honest and reasonable person; and

(f) Knowledge of circumstances which would put an honest and reasonable person on inquiry and failing to make the reasonable inquiries which such a person would have made.

2.12 Suspicion is a subjective concept which may be caused by a transaction or transactions or set of circumstances which to the professional accountants appear unusual or out of context. It can arise from a single transaction or from on-going activity over a period of time.

2.13 Reasonable grounds to suspect shall not be confused with the existence of higher than normal risk factors which may affect certain sectors or classes of persons. Whilst a particular sector or business may be subject to a greater degree of inherent risk of criminal activities than another sector, or the assessment of control risk in a particular entity may raise the overall risk of fraudulent, illegal or unauthorised transactions, an assessment that there is a higher than normal risk of money laundering or terrorist financing is not the same as suspecting money laundering or terrorist financing. For example, cash-based businesses or complex overseas trust and company structures may be capable of being used to launder money, but this capability in itself is not considered to constitute “reasonable grounds”. Existence of higher than normal risk factors require increased attention to gathering and evaluation of “know-your-client” information, and heightened awareness of the risk of money laundering or terrorist financing in performing professional work, but do not of themselves require a report of suspicion to be made.

2.14 In order for a suspicion to be acted upon, there must be a reasonable basis in fact, so that the person concerned can show that the suspicion that money laundering or terrorist financing has occurred is honestly held and arrived at in good faith. Therefore, for reasonable grounds to suspect to come into existence, there needs to be sufficient information to advance beyond speculation that it is possible that someone is laundering money or financing terrorism, or a generalised assumption that low levels of crime (e.g. not declaring all cash takings) are endemic in particular sectors.

2.15 The following three points may be of assistance in determining whether there are reasonable grounds for knowledge or suspicion that someone is committing a money laundering offence:

(a) Does the conduct under scrutiny fall within that which is potentially criminal?

(b) If so, is the person or entity in question suspected of having been involved in that conduct or arrangement?

(c) What factors and information have led to the formation of knowledge or suspicion, i.e. how will the grounds for the report be described to authorities?

2.16 In considering factors which may put professional accountants on notice that there is a risk that money laundering or terrorist financing may be occurring, two situations can be distinguished:

(a) *The entity is involved knowingly and/or actively*: Professional accountants consider the effect of such factors, where they exist, on their assessment of risk for the purposes of determining the work necessary for the services they provide. For example, factors indicating an increased risk of money laundering occurring are often similar to those indicating an increased risk of fraud; and

(b) *The entity is inadvertently involved*: Such involvement may occur in one of two ways. The entity's directors or management may realise that an unusual transaction is taking place but have no evidence to suggest that the unusual transaction involves money laundering or terrorist financing. Alternatively, the directors or management may not even suspect that anything unusual is happening. Factors indicating an increased risk of such “third party” money laundering or terrorist financing are likely to be more difficult to distinguish

from routine innocent transactions, particularly if the amounts concerned are comparatively small in the context of the entity's financial statements.

2.17 An illustrative list of indicators which may give rise to suspicious transaction is set out in Appendix E. Such indicators may not come to the attention of professional accountants where they are not significant or material in the context of the financial statements of the entity, nor is the existence of an individual indicator necessarily sufficient of itself to give rise to suspicion: legitimate reasons arising in the ordinary course of business may give rise to many of the circumstances listed.

2.18 Money laundering or terrorist financing activity may first be identified in relation to comparatively small amounts. However, a continuous use of apparently immaterial transactions may be used to give apparent legitimacy to significant amounts of criminal proceeds. Professional accountants shall be alert to circumstances in which a combination of indicators may give rise to suspicion and, when suspicion arises, to determine whether the matter ought to be reported to the STRO.

2.19 Professional accountants shall also bear in mind that they may not be able to identify the source of the funds, and therefore may not be able to ascertain whether the funds relate to one of the predicate serious crimes (including terrorist financing) and drug trafficking offences. In case of doubt, professional accountants may wish to take legal advice and, subject to that advice, to report the matter to the STRO.

Procedures When Possible Money Laundering or Terrorist Financing is Discovered or Suspected

Suspicious Transactions Reporting – Considerations for the Professional Accountant

2.20 When professional accountants become aware of a possible breach of law or regulations, the professional accountants usually discuss the matter with appropriate members of management and the board of directors. However, this step shall not be taken if the professional accountants have concluded that they no longer have confidence in the integrity of the directors. Indications that the directors are aware of or involved in the criminal activity would be grounds for this conclusion. In addition, professional accountants shall be aware that they are under a statutory obligation not to disclose related information to the directors (or other parties) if doing so is likely to fall within the definition of tipping-off. Hence to avoid any risk of tipping-off it is important that the professional accountants only go so far as to establish to their own satisfaction whether there is a suspected case of money laundering or terrorist financing involving the directors and to consider the consequences for the professional services they provide.

2.21 Similarly, where the entity or its customers, suppliers or other business associates are suspected of being involved in the criminal activity, professional accountants undertake their assessment of the circumstances with care so as not to alert the entity's management or anyone else to these suspicions in case tipping-off occurs. Consequently, professional accountants shall exercise caution in determining with whom, amongst the management and directors, the suspicions can be discussed and they may conclude that none would be suitable. In cases of doubt, legal advice would normally be sought.

2.22 Preliminary enquiries to verify the precise nature of a transaction will not give rise to a tipping-off offence unless professional accountants know or suspect that an investigation is underway or is proposed and that the enquiries by the professional accountants are likely to prejudice that investigation. Where it is known or suspected that a report has already been made or is being made to the STRO, great care is necessary to ensure that the perpetrator does not become aware that the matter has been brought to the attention of the law enforcement agencies. When the professional accountants conclude that further enquiries are necessary as part of their work, they shall consider obtaining legal advice as to the extent and possible effect of those enquiries before undertaking further work.

2.23 The actions taken when considering whether to report suspicions of money laundering or terrorist financing will have a different emphasis depending on whether the entity is actively or passively involved in money laundering or terrorist financing, though this may be a difficult decision to make. In cases of doubt, it may be prudent to assume the entity is actively involved. If the entity appears to be actively involved, great care shall be taken not to alert it to the entity's suspicions. If the entity appears to be only passively involved, the entity's directors need to take appropriate steps to prevent further involvement; in addition, depending upon the size and complexity of the entity, its control procedures might have been expected to prevent the event occurring and so the directors need to be alerted to any weakness in the systems. However, great care shall still be taken in case some of the entity's staff are involved or the entity alerts the third party.

Confidentiality, Statutory Immunity and Legal Privilege

2.24 A professional accountant's duty of confidentiality under the ISCA *Code of Professional Conduct and Ethics* (Ethics Code) imposes an obligation on the professional accountant to refrain from disclosing confidential information acquired as a result of professional and business relationships. However, in certain circumstances, that duty of confidentiality is overridden by statute, law or by courts of law. When professional accountants become aware of a suspected or actual non-compliance with law and regulations which give rise to a statutory duty to report, they shall make a report to the appropriate authority without undue delay.

2.25 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[4]. It also means that professional accountants, acting in good faith, are able to report suspicious transactions to the STRO without the threat of subsequent legal action even if, on further investigation, it were found that there had been no offence. 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.

2.26 Legal privilege can provide a defence for a professional legal adviser to a charge of failing to report suspicions of money laundering. This only applies under privileged and restricted circumstances. There may be situations where a professional accountant comes into possession of legally privileged information, such as where it has been instructed by a lawyer on behalf of the entity in respect of legal proceedings. If a suspicious transaction report required under law would result in the disclosure of that information, the professional accountant shall on a case-by-case basis obtain legal advice to ascertain whether the information and the professional accountant, under the specific circumstances, qualifies for protection for non-disclosure on grounds of legal privilege, or whether a suspicious transaction report has to be made.

[4] The protection generally relates to reporting knowledge or suspicion of the crime, and may not extend more widely, for example to disclosure of audit working papers to an investigating officer. Professional accountants shall consider legal advice in order to avoid a breach of confidentiality where such further disclosure is requested without a court order made under the relevant law.

SECTION 3 – SYSTEMS AND CONTROLS

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

The professional accountants in public practice who own or control the professional firm shall take reasonable efforts to ensure that the firm has the necessary AML and CFT systems and controls as set out in this Section.

A professional accountant in public practice shall comply with the policies, procedures and controls implemented by his/her professional firm.

Establishing Policies, Procedures and Controls

3.1 All professional firms shall develop and implement internal policies, procedures and controls to address money laundering and terrorist financing concerns and communicate these to its employees. The policies, procedures and controls shall include the following:

(a) Risk assessment and management (i.e. a risk-based approach);

(b) Group policy (if a group exists);

(c) Customer due diligence (CDD);

(d) Records keeping;

(e) Reporting procedures;

(f) Ongoing training;

(g) Compliance management and appointment of compliance officer;

(h) Hiring; and

(i) Independent audit function.

3.2 The type and extent of the measures taken in each of the area described in paragraph 3.1 shall be appropriate having regard to the risk of money laundering and terrorist financing and the size and nature of the business. Some of the factors to be considered include:

(a) The nature, scale and complexity of the professional firm's business;

(b) The diversity of a professional firm's operations, including geographical diversity;

(c) The professional firm's customer, product and activity profile;

(d) The volume and size of the transactions;

(e) The degree of risk associated with each area of the professional firm's operations; and

(f) The extent to which the professional firm is dealing directly with the customer or is dealing through intermediaries, third parties, correspondents, or non-face to face access.

Risk-Based Approach

3.3 The risk-based approach is a general and underlying principle of all AML/CFT systems. The general principle of a risk-based approach is that, where there are higher risks, professional firms shall take enhanced measures to manage and mitigate those risks; and that, correspondingly, where the risks are lower, simplified measures may be permitted.

3.4 The risk-based approach is an effective way to combat money laundering and terrorist financing. By adopting a risk-based approach, professional firms would be able to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified, and would enable them to make decisions on how to allocate their own resources in the most effective way.

3.5 In implementing a risk-based approach, professional firms shall have in place processes to identify, assess, monitor, manage and mitigate money laundering and terrorist financing risks.

3.6 Professional firms shall:

(a) Take appropriate steps to identify and assess their risks (for clients, countries or geographic areas; and products, services, transactions or delivery channels);

(b) Document the risk assessments in order to be able to demonstrate their basis;

(c) Keep these assessments up to date; and

(d) Have appropriate mechanisms to provide risk assessment information to relevant authorities.

The nature and extent of any assessment of the risks shall be appropriate to the nature and size of the business.

3.7 When assessing risk, professional firms shall consider all the relevant risk factors before determining what is the level of overall risk and the appropriate level of mitigation to be applied. Professional firms may differentiate the extent of measures, depending on the type and level of risk for the various risk factors (e.g. in a particular situation, normal CDD could be applied for client acceptance measures, but enhanced CDD for ongoing monitoring, or vice versa).

3.8 Enhanced CDD shall be applied to clients from higher risk countries for which this is called for by the FATF.

3.9 Professional firms shall:

(a) Have policies, controls and procedures that enable them to manage and mitigate effectively the risks that have been identified;

(b) Monitor the implementation of those controls and enhance them, if necessary;

(c) Ensure that the policies, controls and procedures are approved by senior management; and

(d) Ensure that the measures taken to manage and mitigate the risks are consistent with relevant laws and regulations and this Pronouncement.

3.10 Professional firms may refer to the Singapore National Money Laundering and Terrorist Financing Risk Assessment Report issued by the Ministry of Home Affairs, Ministry of Finance and the Monetary Authority of Singapore (MAS) to understand the money laundering and terrorist financing risks in Singapore for professional accountants, as well as other sectors that the professional accountants have dealings with. This helps professional firms better assess the adequacy of their internal AML and CFT systems and controls in mitigating the risks identified, and to strengthen these controls where necessary.

Group Policy

3.11 This sub-section on group policy applies when a professional firm has branches and/or subsidiaries, i.e. where the professional firm exercises control over another entity and/or establish a branch, including foreign entities and branches. This is contrasted with a network scenario, where an entity within a network do not exercise control over another entity/entities within the network but is a larger structure aimed at co-operation. The requirements in this sub-section do not apply to a professional firm which does not have branches and/or subsidiaries but is part of a network firm.

3.12 Where a professional firm has branches and/or subsidiaries, the professional firm shall develop and implement group-wide programmes on AML and CFT, including policies and procedures for sharing information within the group required for the purposes of CDD and money laundering and terrorist financing risk management. Adequate safeguards on the confidentiality and use of information exchanged shall be in place.

3.13 Where a professional firm has a branch or subsidiary in a country or jurisdiction known to have inadequate AML/CFT measures (as determined by the professional firm for itself, those notified and required of the professional firm by any relevant authority, or those called for by the FATF), the professional firm shall ensure that the group policy on AML/CFT is strictly observed by the management of that branch or subsidiary.

3.14 Where the minimum AML/CFT requirements of the country of the branch/subsidiary are less strict than those in Singapore, professional firms shall ensure that their branch/subsidiary implements the requirements of Singapore, to the extent that host country laws and regulations permit. If the country of the branch/subsidiary does not permit the proper implementation of the AML/CFT measures, professional firms shall apply appropriate additional measures to manage the money laundering and terrorist financing risks.

SECTION 4 – CUSTOMER DUE DILIGENCE AND RECORDS KEEPING

This Section covers measures on customer due diligence and records keeping.

This Section is mandatory for professional firms when providing any service described in paragraph 1.5. Professional accountants in public practice who own or control such a professional firm shall take reasonable efforts to ensure that the firm has the necessary measures in place.

Professional firms which do not provide any service described in paragraph 1.5 may refer to this Section as good guidance that can be implemented.

A professional accountant in public practice shall comply with the customer due diligence and records keeping measures implemented by his/her professional firm.

Customer Due Diligence (CDD)

What is Customer Due Diligence and Why it is Important

4.1 An important element in any effective AML/CFT measure is CDD. The primary objective of CDD is to enable effective identification and reporting of suspicious activities. The underlying assumption is that, unless you truly know your client, and well enough to understand and anticipate that client's business behaviour, you can neither reasonably nor effectively distinguish unusual and possibly suspicious activity from usual and customary behavior.

4.2 CDD requires or recommends developing a thorough understanding, through appropriate due diligence, of the true beneficial parties to transactions, the source and intended use of funds and the appropriateness and reasonableness of the business activity and pattern of transactions in the context of the business.

4.3 Professional firms will have other client acceptance and continuance procedures, for example to ensure compliance with independence requirements and to avoid conflicts of interest. The CDD requirements may either be integrated with those procedures or addressed separately. Initial CDD information assists in client acceptance decisions and also enables the professional firms to form expectations of their client's behaviour which provides some assistance on detecting potentially suspicious behavior during the business relationship.

4.4 The following CDD measures shall be taken:

(a) Identifying the client;

(b) Identifying the beneficial owner;

(c) Verifying that client's identity using reliable, independent source documents, data or information, and taking reasonable measures to verify the identity of the beneficial owner, such that the professional firm is satisfied that it knows who the beneficial owner is. For legal persons and arrangements, this shall include professional firms understanding the ownership and control structure of the client;

(d) Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship; and

(e) Conducting ongoing due diligence on any continuing business relationship and scrutiny of transactions (if any) undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the professional firm's knowledge of the client, their business and risk profile, including, where necessary, the source of funds.

When Customer Due Diligence Measures are to be Performed

Application of Customer Due Diligence Measures

4.5 Professional firms shall undertake CDD measures when:

(a) Establishing business relations;

(b) Carrying out occasional transactions;

(c) There is a suspicion of money laundering or terrorist financing; or

(d) Where there are doubts about the veracity or adequacy of previously obtained client identification data.

4.6 The CDD measures apply to all new clients. Professional firms shall also apply the CDD measures to existing clients[5] on the basis of risk, and shall conduct due diligence on such existing relationships at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained.

Timing of Customer Due Diligence Measures

4.7 Professional firms shall verify the identity of the client and beneficial owner before or during the course of establishing a business relationship or carrying out occasional transactions. If the money laundering and terrorist financing risks are effectively managed and if it is essential not to interrupt the normal conduct of business, the verification can be performed subsequent to establishing business relations with the client. However, the professional firm shall adopt internal risk management policies and procedures concerning the conditions under which such business relations may be established prior to verification and such verification shall be completed as soon as reasonably practicable.

4.8 Examples of reasonable timeframe are:

(a) Such verification are completed no later than 30 working days after the establishment of business relations;

(b) Suspension of business relations with the client and refraining from carrying out further transactions if such verification remains uncompleted 30 working days after the establishment of business relations; and

(c) Terminating business relations with the client if such verification remains uncompleted 120 working days after the establishment of business relations.

The professional firm shall factor what it considers as reasonable timeframe in their internal policies, procedures and controls.

4.9 Examples where it may be essential not to interrupt the normal course of business are urgent insolvency appointments, and urgent appointments that involve ascertaining the legal position of a client or defending the client in legal proceedings.

4.10 The application of CDD measures set out in paragraph 4.4 does not imply that professional firms have to repeatedly identify and verify the identity of each client every time the client, with an existing business relationship, enters into a new engagement with the professional firm. The professional firm is entitled to rely on the identification and verification steps that it has already undertaken, unless it has doubts about the veracity of that information. Examples of situations that might lead to doubts could be where there is a suspicion of money laundering or terrorist financing in relation to that client, or where there is a material change in the client's activities, which is not consistent with the client's business profile.

[5] Existing clients as at the date that this Pronouncement is effective.

Conducting Customer Due Diligence

Know Your Client (KYC)

4.11 Professional firms shall identify and verify the client's identity. The type of information that would normally be needed to perform this function would be:

(a) Name, legal form and proof of existence – verification could be obtained, for example, through a certificate of incorporation, a certificate of good standing, a partnership agreement, a deed of trust, or other documentation from a reliable independent source providing the name, form and current existence of the client;

(b) The powers that regulate and bind the legal person or arrangement (e.g. the 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 (e.g. senior managing directors in a company, trustee(s) of a trust); and

(c) The address of the registered office, and, if different, a principal place of business.

4.12 Professional firms shall also identify the beneficial owners of the client and take reasonable measures[6] to verify the identity of such persons, through the following information:

(a) For legal persons:

(i) The identity of the natural persons (if any – as ownership interests can be so diversified that there are no natural persons (whether acting alone or together) exercising control of the legal person or arrangement through ownership) who ultimately have a controlling ownership interest in a legal person; and

(ii) To the extent that there is doubt under (i) as to whether the person(s) with the controlling ownership interest are the beneficial owner(s) or where no natural person exerts control through ownership interests, the identity of the natural persons (if any) exercising control of the legal person or arrangement through other means.

(iii) Where no natural person is identified under (i) or (ii) above, professional firms shall identify and take reasonable measures to verify the identity of the relevant natural person who holds the position of senior managing official.

(b) For legal arrangements:

(i) 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).

(ii) Other types of legal arrangements – the identity of persons in equivalent or similar positions.

4.13 Where a person purports to act on behalf of a client, the professional firm shall identify and verify the identity of the person and shall verify that the person is so authorized, by obtaining for example, the appropriate documentary evidence that the client has appointed the person to act on its behalf, and the specimen signatures of the person appointed.

[6] In determining the reasonableness of the identity verification measures, regard should be had to the money laundering and terrorist financing risks posed by the client and the business relationship.

4.14 It is not necessary to identify and verify the identity of any shareholder or beneficial owner if the client is:

(a) A Singapore Government entity;

(b) A foreign government entity;

(c) An entity listed on the Singapore Exchange;

(d) An entity listed on a stock exchange outside of Singapore that is subject to regulatory disclosure requirements[7];

(e) A majority-owned subsidiary of a company in (c) or (d);

(f) A financial institution that is licensed, approved, registered (including a fund management company registered under paragraph 5(1)(i) of the Second Schedule to the Securities and Futures (Licensing and Conduct of Business) Regulations (Rg. 10)) or regulated by the MAS but does not include:

(i) Holders of stored value facilities, as defined in section 2(1) of the Payment Systems (Oversight) Act (Cap. 222A); and

(ii) A person (other than a person referred to in paragraphs 4.14(g) and (h)) who is exempted from licensing, approval or regulation by the MAS under any Act administered by the MAS, including a private trust company exempted from licensing under section 15 of the Trust Companies Act (Cap. 336) read with regulation 4 of the Trust Companies (Exemption) Regulations (Rg. 1);

(g) A person exempted under section 23(1)(f) of the Financial Advisers Act (Cap. 110) read with regulation 27(1)(d) of the Financial Advisers Regulation (Rg. 2);

(h) A person exempted under section 99(1)(h) of the Securities and Futures Act (Cap. 289) read with paragraph 7(1)(b) of the Second Schedule to the Securities and Futures (Licensing and Conduct of Business) Regulations;

(i) A financial institution incorporated or established outside Singapore that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF; or

(j) An investment vehicle where the managers are financial institutions:

(i) Set out in paragraphs 4.14 (f)-(h); or

(ii) incorporated or established outside Singapore but are subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF,

unless the professional firm has doubts about the veracity of the CDD information, or suspects that the client, business relations with, or transaction for the client may be connected with money laundering or terrorist financing activities.

4.15 The relevant identification data may be obtained from a public register, from the client or from other reliable sources. Copies of all reference source documents, data or information used to verify the identity of the client shall be retained. Where the client is unable to produce original documents, the professional firm may consider accepting documents that are certified to be true copies by an independent, qualified person, such as a network firm, a notary public, or an external law firm.

[7] It is recommended that the foreign stock exchanges of FATF member countries qualify for the purpose of paragraph 4.14 (d).

Ongoing Monitoring

4.16 Professional firms shall monitor on an ongoing basis, its business relations with its clients.

4.17 Documents, data or information collected under the CDD process shall be kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher-risk categories of clients.

4.18 The need to update CDD information shall be considered at appropriate times, using a risk-based approach, based on the professional firm's knowledge of the client and changes in its circumstances or the nature of services provided by the professional firm. A professional firm may also wish to consider this need on a more regular basis, for example, when planning for recurring engagements, when there is a change of control and/or ownership of the client or when there is a material change in the level, type or conduct of business.

4.19 Where there are reasonable grounds for suspicion that existing business relations with a client are connected with money laundering or terrorist financing, and where the professional firm considers it appropriate to retain the client, the professional firm shall substantiate the reasons for retaining the client and document them; and the business relations shall be subjected to commensurate risk mitigation measures, including enhanced ongoing monitoring. Where the client or the business relations with the client is assessed to be of high risks, enhanced CDD shall be conducted, including obtaining the approval of senior management to retain the client.

Non-compliance with Customer Due Diligence Requirements

4.20 Where the professional firm is unable to comply with the CDD requirements under paragraph 4.4 (subject to appropriate modification of the extent of the measures on a risk-based approach), for example, due to client's refusal to provide evidence of identity or other information, the professional firm shall not commence business relations or perform the transaction; or shall be required to terminate the business relationship; and shall consider making a suspicious transactions report in relation to the client.

The Risk-Based Approach to Customer Due Diligence

4.21 Professional firms shall apply each of the CDD measures under paragraph 4.4, but shall determine the extent of such measures using a risk-based approach.

4.22 Professional firms shall take into consideration the risks of money laundering and terrorist financing that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products. Such a risk assessment shall take place prior to the launch of the new products, business practices or the use of new or developing technologies and take appropriate measures to manage and mitigate those risks.

Simplified Customer Due Diligence Measures

4.23 Where the risks of money laundering or terrorist financing are lower, professional firms are allowed to conduct simplified CDD measures, which shall take into account the nature of the lower risk. The simplified measures shall commensurate with the lower risk factors (e.g. a lower risk for identification and verification purpose at the client acceptance stage does not automatically mean that the same client is lower risk at the ongoing monitoring stage). Examples of possible simplified measures are:

(a) Verifying the identity of the client and the beneficial owner after the establishment of the business relationship.

(b) Reducing the frequency of client identification updates.

(c) Reducing the degree of on-going monitoring and scrutinising transactions, based on a reasonable monetary threshold.

(d) Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transactions or business relationship established.

4.24 Simplified CDD measures are not acceptable whenever there is a suspicion of money laundering or terrorist financing, or where specific higher-risk scenarios apply, for example, where the clients are from or in countries and jurisdictions known to have inadequate AML/CFT measures, as determined by the professional firm for itself, those notified and required of the professional firm by any relevant authority, or those called for by the FATF.

4.25 Professional firms shall set out clearly in their internal procedures what is considered to constitute reasonable grounds to conclude that a client can be subject to simplified CDD measures. Where simplified CDD measures are performed, the details of the risk assessment and the nature of the simplified CDD measures shall be documented.

4.26 The following are some examples where professional firms may adopt simplified CDD measures:

(a) Reliable information on the client is publicly available.

(b) The professional firm is familiar with the client's AML/CFT controls due to previous dealings with the client.

(c) The client is a listed company that is subject to regulatory disclosure requirements, or a financial institution that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by FATF.

4.27 The extent of knowledge a professional firm will have regarding a client will generally grow within the context of an ongoing relationship with that client. Information on such matters that the professional firm obtains may come from, for example:

(a) The reasons for the proposed appointment of the professional firm and non-reappointment of the previous firm.

(b) Communications with existing or previous providers of professional services to the client, and discussions with other third parties.

(c) Inquiry of other firm personnel or third parties such as bankers, legal counsel and industry peers.

(d) Background searches of relevant databases.

Enhanced Customer Due Diligence Measures

4.28 In situations where PEPs may be involved or in other situations where there is a higher risk of money laundering or terrorist financing, professional firms shall take enhanced CDD measures.

Politically Exposed Persons (PEPs)[8]

4.29 Professional firms shall have appropriate risk management systems in place to determine whether clients or beneficial owners are foreign PEPs, and if so, to take enhanced CDD measures to determine if and when they are doing business with them.

This means that proactive steps must be taken, such as assessing clients on the basis of risk criteria, risk profiles, the business model, verification of CDD information, and the professional firm's own research, to determine whether a client or a beneficial owner is a foreign PEP.

[8] Additional guidance on PEPs can be found in the *"FATF Guidance – Politically Exposed Persons (Recommendations 12 and 22)".* This is a guidance tool issued by FATF based on the experiences of countries, international organisations, the private sector and non-governmental organisations which may assist in implementation of requirements relating to PEPs.

4.30 Professional firms shall also take reasonable measures, based on the assessment of the level of risk, to determine whether a client or beneficial owner is a domestic PEP or an international organisation PEP.

This means reviewing, according to relevant risk factors, CDD data collected. The risk of the business relationship shall be determined and, in low risk cases, no further steps to determine if a customer is a PEP is required.

4.31 The different sets of requirements to detect PEPs (paragraph 4.29 for foreign PEPs and paragraph 4.30 for domestic/international organisation PEPs) reflect that the level of risks are different. In practice, professional firms may choose to use one client on-boarding procedure for all clients.

4.32 In cases of foreign PEPs or high risk business relationship with domestic PEPs, international organisation PEPs, or PEPs who have stepped down from their prominent public functions, taking into consideration the level of influence such persons may continue to exercise after stepping down from their prominent public functions (whether as client or beneficial owner), professional firms shall, in addition to performing normal CDD measures, perform enhanced CDD measures. This includes:

(a) Obtaining senior management approval for establishing (or continuing, for existing clients) such business relationships;

(b) Taking reasonable measures to establish the source of wealth and source of funds[9]; and

(c) Conducting enhanced ongoing monitoring of the business relationship.

4.33 The enhanced CDD requirements for a PEP shall also apply to family members and close associates of such a PEP.

4.34 In cases of lower risk business relationship with domestic PEPs, international organisation PEPs or PEPs who have stepped down from their prominent functions, their family members and close associates, the professional firm may adopt a risk-based approach in determining whether to perform enhanced CDD or the extent of enhanced CDD to perform.

4.35 When considering whether to establish or continue a business relationship with a PEP, his/her family members and close associates, the focus shall be on the level of money laundering and terrorist financing risk, and whether the professional firm has adequate controls in place to mitigate the risk so as to avoid the professional firm from being abused for illicit purposes.

4.36 Existing clients may have become PEPs after they enter a business relationship, so it is essential that professional firms periodically monitor their existing client base for a change in the PEP status and update client information. Such ongoing monitoring shall be based on the level of risk.

Other High Risk Categories

4.37 Professional firms shall examine, as far as reasonably possible, the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose. Where the risks of money laundering or terrorist financing are higher, enhanced CDD measures shall be conducted, consistent with the risks identified. In particular, they shall increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious. This includes business relationships and transactions with clients from higher risk countries known to have inadequate AML/CFT measures, as determined by the professional firm for itself, those notified and required of the professional firm by any relevant authority, or those called for by the FATF. Examples of enhanced CDD measures that could be applied for higher risk business relationships include:

[9] The source of wealth and source of funds must be verified by some documentary means.

(a) Obtaining additional information on the client (e.g. occupation, volume of assets, information available through public databases, internet, etc.), and updating more regularly the identification data of client and beneficial owner.

(b) Obtaining additional information on the intended nature of the business relationship.

(c) Obtaining information on the source of funds or source of wealth of the client.

(d) Obtaining information on the reasons for intended or performed transactions.

(e) Obtaining the approval of senior management to commence or continue the business relationship.

(f) Conduct enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.

(g) Requiring the first payment to be carried out through an account in the client's name with a bank subject to similar CDD standards.

Prohibited Relationships

4.38 Professional firms shall comply with prohibitions, that are required of them, issued by any relevant authority in respect of any person or country. Directions may be given not to enter into business relationships or transactions with these parties or proceed with any such arrangements already in progress.

4.39 Professional firms shall also check the names of clients or potential clients against:

(a) The lists of persons subject to prescribed restrictions in the United Nations Regulations, enacted to give effect to the sanctions requirements of the United Nations resolutions adopted by the Security Council; and

(b) The list of terrorist names under the First Schedule of the TSFA.

4.40 Professional firms shall perform screening against the lists and information provided by the relevant authorities under paragraphs 4.38 and 4.39 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

4.41 In a third party reliance scenario, the third party will usually have an existing business relationship with the client, which is independent from the relationship to be formed between the professional firm and the client. For example, a third party introduced a new client to the professional firm resulting in direct business relations between the professional firm and the new client. Thus, if the third party has already performed its own CDD on the new client, the professional firm can then dispense with performing CDD on the new client if the criteria in paragraph 4.42 are satisfied. This is contrasted with an outsourcing or agency scenario, in which the outsourced entity applies the CDD measures on behalf of the professional firm, in accordance with its procedures, and is subject to the professional firm's control of the effective implementation of those procedures by the outsourced entity. This sub-section on reliance on third parties is not intended to cover such outsourcing scenarios.

4.42 Professional firms may rely on third parties to perform the CDD measures set out in paragraph 4.4(a)-(d), provided that the criteria set out below are met. However, the ultimate responsibility for CDD measures remains with the professional firm. The criteria that shall be met are as follows:

(a) A professional firm relying upon a third party shall immediately obtain the necessary information concerning the CDD measures set out in paragraph 4.4(a)-(d)[10];

(b) Professional firms shall take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to the CDD requirements will be made available from the third party upon request without delay;

(c) The professional firm shall satisfy itself that the third party is regulated, supervised or monitored for, and has measures in place for compliance with CDD and record-keeping requirements in line with standards set by the FATF; and

(d) When determining in which countries the third party that meets the conditions can be based, professional firms shall have regard to information available on the level of country risk.

4.43 When a professional firm relies on a third party that is part of the same group or a network, the professional firm may be considered to have applied measures in paragraph 4.42(b) and (c) through its group or network programme and that paragraph 4.42(d) is not a necessary precondition to reliance when higher country risk is adequately mitigated by the group's or network's AML/CFT policies if:

(a) That group or network applies CDD and record-keeping requirements, as well as programmes against money laundering and terrorist financing, in line with standards set by the FATF; and

(b) The effective implementation of those CDD and record-keeping requirements and AML/CFT programmes is supervised at a group or network level by a competent authority.

4.44 The professional firm may take a variety of measures, including but not limited to the following in determining whether the third party satisfies the criteria in paragraph 4.42(c):

(a) Referring to any publicly available reports or material on the quality of AML/CFT supervision in the jurisdiction where the third party operates (such as mutual evaluation reports of the FATF and its associated bodies, or assessment reports made under the Financial Sector Assessment Programme of the International Monetary Fund and the World Bank);

(b) Referring to any publicly available reports or material on the quality of that third party's compliance with applicable AML/CFT rules;

(c) Obtaining professional advice as to the extent of AML/CFT obligations to which the third party is subject by the laws of the jurisdiction in which the third party operates; and

(d) Examining the AML/CFT laws in the jurisdiction where the third party operates and determining its comparability with the AML/CFT laws of Singapore.

4.45 Professional firms shall not rely on third parties to conduct ongoing monitoring of clients, except where the third party is part of the professional firm's group or network.

[10] Where there are time lags in acquiring the CDD documentation from the third party, the professional firm shall seek confirmation from the third party that the CDD has been performed, verified and is true and accurate.

4.46 Where a third party is relied on to perform the CDD measures, the professional firm shall justify that the criteria in paragraph 4.42 have been met and shall take considerable care when deciding if a third party is one on whom the professional firm can safely rely on to perform the CDD measures. The professional firm shall document the basis for its satisfaction that the criteria have been met except where the third party is a:

(a) Financial institution under paragraph 4.14(f) but does not include:

(i) Financial advisers licensed under section 6 of the Financial Advisers Act (Cap. 110) which only provide advice by issuing or promulgating research analyses or research reports, whether in electronic, print or other form, concerning any investment product; and

(ii) Insurance brokers registered under the Insurance Act which, by virtue of such registration, are exempted under section 23(1)(c) of the Financial Advisers Act which only provide advice by issuing or promulgating research analyses or research reports, whether in electronic, print or other form, concerning any investment product;

(b) Person exempted from section 23(1)(f) of the Financial Advisers Act read with regulation 27(1)(d) of the Financial Advisers Regulation (Rg. 2) except those which only provide advice by issuing or promulgating research analyses or research reports, whether in electronic, print or other form, concerning any investment product; and

(c) A person under paragraph 4.14(h).

Records Keeping

4.47 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 in Singapore 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 this Pronouncement; 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 in Singapore for information.

4.48 Subject to paragraph 4.53 and any other requirements imposed by law, a professional firm shall, when setting its record retention policies, comply with the following document retention periods:

(a) A period of at least 5 years following the termination of business relations for all information obtained through CDD measures (e.g. copies or records of official identification documents like passports, identity cards, driving licences or similar documents), account files and business correspondence, including the results of any analysis undertaken (e.g. inquiries to establish the background and purpose of complex, unusual large transactions); and

(b) A period of at least 5 years following the completion of the transaction for records relating to a transaction, including any information needed to explain and reconstruct the transaction.

4.49 Professional firms may retain documents, data and information as originals or copies, in paper or electronic form or on microfilm, provided that they are admissible as evidence in a Singapore court of law.

4.50 Professional firms shall maintain a complete file of all internal suspicious transactions reports (which can take any form specified by the professional firms) filed by individual professional accountants in public practice and staff to their professional firm's Money Laundering Reporting Officer (MLRO), whether or not these were subsequently reported by the professional firm to the STRO, together with all internal findings and analysis done in relation to them.

4.51 Internal reports would usually include details of the professional firm's handling of the matter, the professional firm's requests for further information, assessment of the information received, decisions as to whether to conclude immediately or to wait for further developments or information, proper justification for internal suspicious transactions reports not subsequently reported to the STRO, and any advice given to engagement teams as regards to the continuation of work.

4.52 It is recommended that the internal reports are held by the MLRO and excluded from client files. The obligations to report suspicious transactions is not part of providing professional services to the clients and accordingly, such reports are not required in client files. Exclusion of such information also assists in avoiding inadvertent or inappropriate disclosure of information and provides some protection against the threat of tipping off.

4.53 A professional firm shall retain records of documentation, data and information on all its business relations with or transactions for a client pertaining to a matter which is under investigation or which has been the subject of a suspicious transaction report for such longer period as may be necessary in accordance with any request or order from the STRO or from other relevant authorities in Singapore.

SECTION 5 – REPORTING, TRAINING, COMPLIANCE, HIRING AND AUDIT

This Section covers measures on reporting procedures, training, compliance management, hiring and audit.

This Section is not mandatory on the professional firms but provides good guidance that can be implemented.

A professional accountant in public practice shall comply with the reporting, training, compliance management, hiring and audit measures implemented by his/her professional firm.

Reporting Procedures

5.1 Professional firms should keep in mind the provisions in the CDSA and TSFA that provide for the reporting of suspicious transactions to the STRO, and implement appropriate internal policies, procedures and controls for meeting its obligations under the law, including what is expected of their employees who form suspicions or obtain knowledge of possible money laundering or terrorist financing.

5.2 Professional firms should establish a single reference point within the organisation to whom all employees are instructed to promptly refer all transactions suspected of being connected with money laundering or terrorist financing, for possible reporting to the STRO, i.e. the appointment of a MLRO who is a person of sufficient seniority and authority. (Sole practitioners who do not employ any staff will not be required to have internal reporting procedures or an MLRO). The MLRO will then determine whether a report to the STRO is necessary.

5.3 The professional firm's internal process to evaluate whether a matter should be referred to the STRO should be completed without delay, unless the circumstances are exceptional or extraordinary.

Ongoing Training

5.4 The statutory definition of money laundering and terrorist financing can be complex. There can be wide variation in what constitutes unusual and suspicious activity and legally reportable conditions of suspicious transactions.

5.5 Professional firms should therefore establish an on-going training programme and take appropriate steps to ensure that all levels of professional staff have undergone such training. Staff should be reminded of their responsibilities and kept informed of new developments through refresher training, or through other forms of internal communication, at regular intervals. 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.

5.6 A professional firm's training programme should be tailored to its size, nature and complexity. Training would as a minimum be expected to emphasise the following:

(a) Requirements of the AML and CFT legislations;

(b) Prevailing techniques, methods and trends in money laundering and terrorist financing;

(c) Indications of money laundering and terrorist financing;

(d) Risks of tipping-off;

(e) The professional firm's internal policies, procedures and controls on AML and CFT and the roles and responsibilities of professional accountants in public practice in combating money laundering and terrorist financing; and

(f) The need to obtain legal advice in situations where there is doubt about the legal framework and requirements.

5.7 When considering which staff may require training, professional firms should consider not only those who have involvement in client work, but also, where appropriate, those who deal with the professional firm finances, and those who deal with procuring services on behalf of the professional firm and who manage those services. Accordingly, all client-facing staff and at least the senior support staff are likely to be considered relevant. Professional firms may decide to provide comprehensive training for all relevant staff, or may choose to tailor its provision to match more closely the role of the staff concerned. In particular, the MLRO may require supplementary training, and members of senior management may also benefit from a customised approach or some supplementary training.

5.8 To help ensure the effectiveness of training, professional firms should monitor attendance at such training and take appropriate follow-up action in relation to staff who absent themselves without reasonable cause.

5.9 When any staff has knowledge or suspicion of money laundering or terrorist financing, the staff would be expected to follow the professional firm's internal reporting procedures. Junior staff may be the first to spot evidence of crime. This reinforces the need for professional firms to have clear procedures which are communicated to all personnel. Staff ought to report any suspicions to the MLRO. This will discharge their personal reporting responsibility.

5.10 Training does not need to be performed in-house. Attendance at conferences, seminars and training courses run by external organisations, or participation in computer based training courses, may be taken to represent an effective method of fulfilling the training obligations. However, professional firms should ensure the appropriateness of those courses, seminars or conference.

5.11 It is recommended that evidence of assessment of training needs and steps taken to meet such needs are retained and that such records be kept for at least 5 years, in line with the record retention policy required for the documentation on the professional firm’s business relations and transactions with its clients.

Compliance Management

5.12 Professional firms should develop appropriate compliance management arrangements to monitor the professional firm’s compliance with its AML/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.

5.13 Professional firms should ensure that the compliance officer, as well as any other persons appointed to assist him, has adequate resources and timely access to all client records and other relevant information which they require to discharge their functions.

Hiring

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

Independent Audit Function

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

APPENDIX A

DESCRIPTION OF MONEY LAUNDERING AND TERRORIST FINANCING

A1. Professionals, such as accountants, are at risk of being used by criminals for money laundering or terrorist financing purposes because their services could be of value to a successful criminal transaction or they may be used merely to give the appearance of legitimacy to a criminal transaction.

Money Laundering

A2. Money laundering is the funneling of cash or other funds generated from illegal activities through financial institutions and businesses to conceal or disguise the true ownership and source of the funds.

A3. Although money laundering can be defined and the main characteristics of money laundering can be identified, money laundering comes in widely varying forms and degrees. Usually the process of money laundering occurs in many phases and through many different transactions, thereby making identification of the process difficult if not impossible. Although the activities and methods of money laundering have become increasingly complex and ingenious, its "operations" tend to consist of three basic stages or processes — placement, layering and integration.

(a) *Placement* is the process of disposing the proceeds from drug trafficking or criminal conduct, for example by transferring the illegal funds into the financial system in a way that financial institutions and government authorities are not able to detect. Money launderers pay careful attention to national laws, regulations, governance structures, trends and law enforcement strategies and techniques to keep their proceeds concealed, their methods secret and their identities and professional resources anonymous.

(b) *Layering* is the process of generating a series or layers of transactions to distance the proceeds from their illegal source and to obscure the audit trail. Common layering techniques include outbound electronic funds transfers, usually directly or subsequently into a "bank secrecy haven" or a jurisdiction with lax record-keeping and reporting requirements, and withdrawals of already-placed deposits in the form of highly liquid monetary instruments, such as money orders or travelers checks.

(c) *Integration*, the final money-laundering stage, is the unnoticed reinsertion of successfully laundered, untraceable funds into an economy. This is accomplished by spending, investing and lending, along with cross-border, legitimate-appearing transactions.

Terrorist Financing

A4. Terrorist financing refers to the direct or indirect act of providing or collecting property for terrorist acts, providing property and services for terrorist purposes, using or possessing property for terrorist purposes, and dealing with property of terrorists. Properties refer to assets of every kind, whether tangible or intangible, movable or immovable, including bank credits, travellers cheques, bank cheques, money orders, shares, securities, bonds, drafts and letters of credit.

A5. Given its nature, signs of suspicious activities relating to terrorist financing are generally less observable. The assets involved in the transaction may not necessarily be proceeds from criminal activities. These assets could also be derived from lawful activities but intended for use in support of terrorist.

A6. A terrorist refers to any person who commits or attempts to commit any terrorist act, or participates in or facilitates the commission of any terrorist act. A terrorist act includes, among others, actions that involve violence against a person, serious damage to property, endangering a person's life, creating a serious risk to the health or the safety of the public, the use of firearms or explosives, and releasing into the environment dangerous, hazardous, radioactive or harmful substance.

APPENDIX B

SUMMARY OF BASIC CRIMINAL OFFENCES UNDER ANTI-MONEY LAUNDERING LEGISLATION

B1. This summary is not a reproduction of the actual wordings in the legislation. It is only intended to provide a broad description of the key legal provisions and, therefore, does not constitute authoritative legal interpretation of the legislation. Legal counsel shall be sought where appropriate or necessary.

B2. The Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (CDSA) contains seven basic offences directly in relation to money laundering:

(a) Laundering own benefits from drug trafficking or criminal conduct;

(b) Assisting another to launder benefits from drug trafficking or criminal conduct;

(c) Laundering by acquisition;

(d) Assisting another to retain or control the benefits of drug trafficking or criminal conduct;

(e) Failure to report suspicious transactions;

(f) Tipping-off offence; and

(g) Failure to co-operate with law enforcement agencies.

B3. Drug trafficking includes offences relating to the manufacturing, importation and exportation of controlled drug, and cultivation of cannabis, opium and coca plants. Criminal conduct refers to serious crimes as defined under the CDSA. There are many offences that have been defined as serious offences under the CDSA and these include bribery, corruption, criminal breach of trust, theft, misappropriation of property, cheating and tax evasion.

B4. The professional accountants' attention is specifically drawn to the extra-territorial provisions of the CDSA. The terms "drug trafficking" and "criminal conduct" include offences that are committed outside Singapore, as defined under the CDSA.

B5. The following sets out a summary of the seven basic offences.

Laundering own benefits from drug trafficking or criminal conduct

B6. It is an offence for a person[11] to conceal or disguise property which is, in whole or in part, directly or indirectly, represents, his own benefits from drug trafficking or criminal conduct. The offence extends to steps to convert or transfer that property, or to remove it from the Singapore jurisdiction, or to acquire, possess or use that property.

B7. There are no statutory defences. Upon conviction, the accused faces a fine not exceeding $500,000, or imprisonment for a term not exceeding 10 years, or both. If the accused person is not an individual, he shall be liable upon conviction to a fine not exceeding $1 million.

[11] The legislation's use of the term 'person' indicates that commission of an offence by a legal body, as well as by an individual, is not excluded.

Assisting another to launder benefits from drug trafficking or criminal conduct

B8. Any person who, knowing or having reasonable grounds to believe that any property is, in whole or in part, directly or indirectly, represents, another person's benefits from drug trafficking or criminal conduct:

(a) Conceals or disguises that property; or

(b) Converts or transfers that property or removes it from the Singapore jurisdiction,

shall be guilty of an offence.

B9. Upon conviction, the accused faces a fine not exceeding $500,000 and/or imprisonment for a term not exceeding 10 years. If the accused person is not an individual, he shall be liable upon conviction to a fine not exceeding $1 million.

Laundering by acquisition

B10. It is an offence to acquire or has possession of or use any property, knowing or having reasonable grounds to believe that the property represents another person's benefits of drug trafficking or criminal conduct.

B11. Upon conviction, the accused faces a fine not exceeding $500,000 and/or imprisonment for a term not exceeding 10 years. If the accused person is not an individual, he shall be liable upon conviction to a fine not exceeding $1 million.

Assisting another to retain or control the benefits of drug trafficking or criminal conduct

B12. It is an offence for a person to enter into or otherwise be concerned in an arrangement knowing or having reasonable grounds to believe that by that arrangement:

(a) It will facilitate the retention or control of benefits of drug trafficking or criminal conduct by/on behalf of; or

(b) The benefits of drug trafficking or criminal conduct are used to secure funds or acquire property (by way of investment or otherwise) for,

another person (whom the person knows or has reasonable grounds to believe has been/is involved in, or has benefited from, drug trafficking or criminal conduct).

B13. The following are statutory defences to charges of committing the above offence:

(a) The person proves that he did not know and had no reasonable ground to believe that the arrangement related to any person's proceeds from drug trafficking or criminal conduct, or facilitated the criminal to use, retain or control the property;

(b) Before acting in connection with any arrangement, the person discloses the knowledge or suspicion of money laundering to either (i) an authorised officer; or (ii) to an appropriate person/partner following the professional firm's internal procedure and, thereafter, if that person only acts with the consent of the authorised officer;

(c) Where the person has begun to act/has acted in connection with any arrangement, the person discloses the knowledge or suspicion on his own initiative and as soon as it is reasonable to either (i) an authorised officer; or (ii) to an appropriate person/partner following the professional firm's internal procedure; or

(d) The person proves that he intended to disclose his suspicion or belief of money laundering to an authorised officer[12] and that there is a reasonable excuse for his failure to do so.

The term "reasonable excuse" permits a Court to take account of any factor which would be considered reasonable in all the circumstances of a particular case. Justifiable fear of physical violence or other menaces may be regarded as reasonable in this context: however, the meaning of the term "reasonable excuse" is wider than physical distress and may include other factors, depending upon the circumstances - for example, practical difficulties of making a report or deciding to obtain further information before doing so.

Failure to report suspicious transactions

B14. It is mandatory for all persons who, in the course of their trade, profession, business or employment, know or have reasonable grounds to suspect that any property representing the proceeds of drug trafficking or criminal conduct or was used (or is intended to be used) in connection with drug trafficking or criminal conduct, to disclose such knowledge or suspicion to an Suspicious Transaction Reporting Officer as soon as is reasonably practicable after it comes to his attention.

B15. Failure to report the knowledge or suspicion is an offence punishable by a fine of up to $20,000.

Tipping-off offence

B16. It is an offence to disclose any information to any person if doing so is likely to prejudice an investigation or proposed investigation under the CDSA. Disclosure in such circumstances is also known as 'tipping-off'.

B17. The offence is committed if a person knows or has reasonable grounds to suspect:

(a) That an authorised officer is acting/proposing to act in connection with an investigation which is being or is about to be conducted; or

(b) That a disclosure has been made or is being made to an authorised officer,

and he discloses any information to any person which is likely to prejudice any investigation or proposed investigation, as the case may be.

B18. Tipping-off offence is punishable by a fine of up to $30,000, or imprisonment of up to three years, or both.

B19. It is a defence for a person accused of tipping-off to prove that he did not know or had no reasonable grounds to suspect that the disclosure was likely to be prejudicial to such an investigation or that he had lawful authority for making the disclosure.

Failure to co-operate with the law enforcement agencies

B20. An authorised officer can apply to the Court for a production order requiring a person to produce relevant materials or allow authorised officers to have access to such materials. The CDSA also empowers the Court to issue a warrant authorising an authorised officer to enter and search a specified premises.

B21. It is an offence to contravene a production order issued by the Court, or obstruct or hinder any authorised officer acting in the discharge of his duty under the CDSA.

[12] Under the CDSA, an "authorised officer" is defined to mean any officer of the Central Narcotics Bureau appointed under the Misuse of Drugs Act; any special investigator of the Corrupt Practices Investigation Bureau appointed under the Prevention of Corruption Act; any Commercial Affairs Officer appointed under the Police Force Act 2004; any police officer; and any officer authorised by the Minister under the CDSA. Officers of the Commercial Affairs Department (CAD) are authorised officers under the Act. Reports should normally be made to the Suspicious Transaction Reporting Office (STRO) of the CAD, which provides a national reception point for all reports concerning known or suspected money laundering and terrorist financing.

APPENDIX C

SUMMARY OF BASIC CRIMINAL OFFENCES UNDER TERRORIST FINANCING LEGISLATION

C1. This summary is not a reproduction of the actual wordings in the legislation. It is only intended to provide a broad description of the key legal provisions and, therefore, does not constitute authoritative legal interpretation of the legislation. Legal counsel shall be sought where appropriate or necessary.

C2. The Terrorism (Suppression of Financing) Act (TSFA) contains seven basic offences:

(a) Providing or collecting property for terrorist acts;

(b) Providing property and services for terrorist purposes;

(c) Using or possessing property for terrorist purposes;

(d) Dealing with property of terrorists;

(e) Failure to report terrorist financing offences;

(f) Tipping-off offence; and

(g) Failure to co-operate with the law enforcement agencies.

Terrorist financing offences include conspiracy, inciting another and attempting to commit, and aiding, abetting, counselling or procuring the commission of, offences C2(a) to C2(d).

C3. The term "property" means assets of every kind, whether tangible or intangible, movable or immovable. This means that money, property, bank credits, travellers cheques, bank cheques, money orders, shares, securities, bonds, drafts and letters of credit, would all constitute property under the TSFA. A property is deemed to be terrorist property if the property is used, in whole or in part, in order to commit any terrorist act.

C4. A "terrorist" refers to any person who commits/attempts to commit any terrorist act, or participates in or facilitates the commission of any terrorist act and includes any person set out in the First Schedule under the TSFA. One can check the list of terrorist names under the First Schedule to determine if he is in possession, custody or control of property belonging to any person identified to be terrorists.

C5. A "terrorist act" includes, among others, actions that involve violence against a person, serious damage to property, endangering a person's life, creating a serious risk to the health or the safety of the public, the use of firearms or explosives, and releasing into the environment dangerous, hazardous, radioactive or harmful substance.

C6. The professional accountants' attention is specifically drawn to the extra-territorial provision of the TSFA. It provides for extra-territorial jurisdiction for offences C2(a) to C2(c) committed outside Singapore by any person. Where a Singapore citizen commits an offence outside Singapore relating to the dealing with terrorist property or failure to report terrorist financing (that is, offences C2(d) and C2(e)), he may be dealt with as if the offence had been committed in Singapore.

C7. The following sets out a summary of the seven basic offences.

Providing or collecting property for terrorist acts

C8. It is an offence for any person to directly or indirectly, wilfully and without lawful excuse, provides or collects property:

(a) With the intention that the property be used; or

(b) Knowing or having reasonable grounds to believe that the property will be used,

to commit any terrorist act.

C9. Upon conviction, the accused faces a fine of up to $500,000, or imprisonment of up to 10 years, or both.

Providing property and services for terrorist purposes

C10. It is an offence for any person to, directly or indirectly, collect property, provide or invite a person to provide, or make available property or financial or other related services:

(a) Intending that they be used, or knowing or having reasonable grounds to believe that they will be used for the purpose of facilitating or carrying out any terrorist act, or for benefiting any person who is facilitating or carrying out such an activity; or

(b) Knowing or having reasonable grounds to believe that they will be used by or will benefit any terrorist or terrorist entity.

C11. Upon conviction, the accused faces a fine of up to $500,000, or imprisonment of up to 10 years, or both.

Using or possessing property for terrorist purposes

C12. It is an offence for any person to:

(a) Use property, directly or indirectly, for the purpose of facilitating or carrying out any terrorist act; or

(b) Possess property intending that it be used or knowing or having reasonable grounds to believe that it will be used, directly or indirectly, for the purpose of facilitating or carrying out a terrorist act.

C13. Upon conviction, the accused faces a fine of up to $500,000, or imprisonment of up to 10 years, or both.

Dealing with property of terrorists

C14. Except where specific exemption (subject to terms and conditions) is granted by a lawful authority under the TSFA, no person in Singapore and no citizen of Singapore outside Singapore shall:

(a) Deal, directly or indirectly, in any property that he knows or has reasonable grounds to believe is owned/controlled by or on behalf of any terrorist or terrorist entity, including funds derived or generated from property owned/controlled, directly or indirectly, by any terrorist or terrorist entity;

(b) Enter into or facilitate, directly or indirectly, any financial transaction related to a dealing in property referred to in paragraph (a); or

(c) Provide any financial services or any other related services in respect of any property referred to in paragraph (a) to, or for the benefit of, or on the direction or order of, any terrorist or terrorist entity.

C15. Upon conviction, the accused faces a fine of up to $500,000, or imprisonment of up to 10 years, or both.

Failure to report terrorist financing offences

C16. The TSFA imposes a duty on every person in Singapore and every Singapore citizen outside Singapore who has possession, custody or control of terrorist property, or information regarding a transaction/proposed transaction in terrorist property to disclose such information to the authorities.

C17. The TSFA also requires every person in Singapore who has information which he knows or believes may be of material assistance in preventing a terrorist financing offence, or in securing the apprehension, prosecution or conviction of a person for a terrorist financing offence, to immediately inform the authorities.

C18. Failure to report is an offence punishable by a fine of up to $50,000, or imprisonment of up to 5 years, or both.

C19. It is a defence for a person who failed to disclose the information to the authorities to prove that he had a reasonable excuse for not informing the Commissioner of Police[13].

Tipping-off offence

C20. It is an offence to disclose any information to any person if doing so is likely to prejudice an investigation or proposed investigation under the TSFA. Disclosure in such circumstances is also known as 'tipping-off'.

C21. The offence is committed if a person knows or has reasonable grounds to suspect:

(a) That a police officer is acting/proposing to act in connection with an investigation which is being or is about to be conducted; or

(b) That a disclosure has been made to an authorised officer,

and he discloses any information to any person which is likely to prejudice any investigation or proposed investigation, as the case may be.

C22. Tipping-off offence is punishable by a fine of up to $30,000, or imprisonment of up to three years, or both.

C23. It is a defence for a person accused of tipping-off to prove that he did not know or suspect that the disclosure was likely to be prejudicial to such an investigation or that he had lawful authority for making the disclosure

Failure to co-operate with the law enforcement agencies

C24. The TSFA has provisions allowing the Court to issue search warrants, seizure warrants, forfeiture orders or restraint orders against terrorist property. The TSFA also empowers the relevant authorities to require a person to furnish such information or particulars as the relevant authorities think fit in relation to a report of terrorist financing offence.

C25. Failure to co-operate in relation to those matters is an offence.

[13] Commissioner of Police includes (a) any police officer; and (b) any other person authorised by the Commissioner of Police to act for him for the purposes of section 8 of the TSFA.

APPENDIX D

SUMMARY OF BASIC CRIMINAL OFFENCES UNDER THE PENAL CODE

D1. This summary is not a reproduction of the actual wordings in the legislation. It is only intended to provide a broad description of the key legal provisions and, therefore, does not constitute authoritative legal interpretation of the legislation. Legal counsel shall be sought where appropriate or necessary.

D2. The primary legislation in Singapore contains the offence of abetment indirectly in relation to an offence. The nature of this offence is summarised below.

D3. The offence of abetment is set out in Sections 107, 108, 108A and 108B of the Penal Code. Abetment involves the active involvement of a person with the principal culprit towards the commission of an offence. There are three forms of abetment, namely:

(a) Abetment by instigation;

(b) Abetment by conspiracy; and

(c) Abetment by aid.

D4. A person who knowingly aids an offence or facilitates an offence would be liable for abetment of that offence. In the case of *Mavuthalayan (1934) 58 Mad 86* it was held that a person who knowingly aids in the disposal of stolen property is an accomplice to the offence. Therefore, for example, a person who knowingly disposes of, or conceals, (that is, launders) the proceeds of an illegal gambling house may be liable for abetting an offence under the Common Gaming Houses Act (Cap. 49).

D5. Depending on the facts and circumstances, a person who launders money may be convicted for abetment by aid.

APPENDIX E

INDICATORS OF SUSPICIOUS TRANSACTIONS

E1. Money launderers use many different and sophisticated types of schemes, techniques and transactions to accomplish their ends. While it would be difficult to describe all money laundering methodologies, the following are the more frequently observed signs of suspicions:

(a) Broadly, transactions that appear inconsistent with a client's known legitimate (business or personal) activities or means; unusual deviations from normal account and transaction;

(b) Any situation where personal identity is difficult to determine;

(c) Unauthorised or improperly recorded transactions; inadequate audit trails;

(d) Unconventionally large currency transactions, particularly in exchange for negotiable instruments or for the direct purchase of funds transfer services;

(e) Apparent structuring of transactions to avoid dealing with identification requirements or regulatory record-keeping and reporting thresholds;

(f) Transactions passed through intermediaries for no apparent business reason; and

(g) Introduction of a client by an overseas associate or financial institution based in a country or jurisdiction known for drug trafficking and production, other financial crimes and “bank secrecy”.

E2. The following sets out examples of common indicators of suspicious transactions. Indicators to help establish that a transaction is related to terrorist financing mostly resemble those relating to money laundering. While each individual indicator may not be sufficient to suggest that suspicious transaction is taking place, a combination of such situations may be indicative of a suspicious transaction. The list is intended as a guide and shall not be applied as a routine checklist in place of common sense.

E3. **Common Indicators**

(a) **General**

- Frequent address changes.
- Client does not want correspondence sent to home address.
- Client repeatedly uses an address but frequently changes the names involved.
- Client uses a post office box or general delivery address, or other type of mail drop address, instead of a street address when this is not the norm for that area.
- Client’s home or business telephone number has been disconnected or there is no such number when an attempt is made to contact client shortly after he/she has opened an account.
- Client is accompanied and watched.
- Client shows uncommon curiosity about internal systems, controls, policies and reporting; client has unusual knowledge of the law in relation to suspicious transaction reporting.
- Client has only vague knowledge of the amount of a deposit.
- Client gives unrealistic, confusing or inconsistent explanation for transaction or account activity.
- Defensive stance to questioning or over-justification of the transaction.
- Client is secretive and reluctant to meet in person.
- Unusual nervousness of the person conducting the transaction.
- Client is involved in transactions that are suspicious but seems blind to being involved in money laundering activities.
- Client insists on a transaction being done quickly.

- Client appears to have recently established a series of new relationships with different financial entities.
- Client attempts to develop close rapport with staff.
- Client offers money, gratuities or unusual favors for the provision of services that may appear unusual or suspicious.
- Client attempts to convince employee not to complete any documentation required for the transaction.
- Large contracts or transactions with apparently unrelated third parties, particularly from abroad.
- Large lump-sum payments to or from abroad, particularly with countries known or suspected to facilitate money laundering activities.
- Client is quick to volunteer that funds are “clean” or “not being laundered”.
- Client’s lack of business knowledge atypical of trade practitioners.
- Forming companies or trusts with no apparent business purpose.
- Unusual transference of negotiable instruments.
- Uncharacteristically premature redemption of investment vehicles, particularly with requests to remit proceeds to apparently unrelated third parties or with little regard to tax or other cancellation charges.
- Large or unusual currency settlements for investments or payment for investments made from an account that is not the client’s.
- Clients seeking investment management services where the source of funds is difficult to pinpoint or appears inconsistent with the client’s means or expected behavior.
- Purchase of large cash value investments, soon followed by heavy borrowing against them.
- Buying or selling investments for no apparent reason, or in circumstances that appear unusual, e.g. losing money without the principals seeming concerned.
- Forming overseas subsidiaries or branches that do not seem necessary to the business and manipulating transfer prices with them.
- Extensive and unnecessary foreign travel.
- Purchasing at prices significantly below or above market.
- Excessive or unusual sales commissions or agents fees; large payments for unspecified services or loans to consultants, related parties, employees or government employees.

(b) **Cash Transactions**

- Client frequently exchanges small bills for large ones.
- Deposit of bank notes with a suspect appearance (very old notes, notes covered in powder, etc).
- Use of unusually large amounts in traveler’s checks.
- Frequent domestic and international ATM activity.
- Client asks to hold or transmit large sums of money or other assets when this type of activity is unusual for the client.
- Purchase or sale of gold, diamonds or other precious metals or stones in cash.
- Shared address for individuals involved in cash transactions, particularly when the address is also for a business location, or does not seem to correspond to the stated occupation (for example, student, unemployed, self-employed, etc.).

(c) **Transactions Involving Accounts**

- Apparent use of personal account for business purposes.
- Opening accounts when the client’s address is outside the local service area.
- Opening accounts with names very similar to other established business entities.
- Opening an account that is credited exclusively with cash deposits in foreign currencies.
- Use of nominees who act as holders of, or who hold power of attorney over, bank accounts.

- Account with a large number of small cash deposits and a small number of large cash withdrawals.
- Funds being deposited into several accounts, consolidated into one and transferred outside the country.
- Use of wire transfers and the Internet to move funds to/from high-risk countries and geographic locations.
- Accounts receiving frequent deposits of bearer instruments (e.g. bearer cheques, money orders, bearer bonds) followed by wire transactions.
- Deposit at a variety of locations and times for no logical reason.
- Multiple transactions are carried out on the same day at the same branch but with an apparent attempt to use different tellers.
- Establishment of multiple accounts, some of which appear to remain dormant for extended periods.
- Account that was reactivated from inactive or dormant status suddenly sees significant activity.
- Cash advances from credit card accounts to purchase cashier's checks or to wire funds to foreign destinations.
- Large cash payments on small or zero-balance credit card accounts followed by "credit balance refund checks" sent to account holders.
- Attempting to open accounts for the sole purpose of obtaining online banking capabilities.

(d) **Transactions Related to Offshore Business Activity**

- Loans secured by obligations from offshore banks.
- Loans to or from offshore companies.
- Offers of multimillion-dollar deposits from a confidential source to be sent from an offshore bank or somehow guaranteed by an offshore bank.
- Transactions involving an offshore "shell" bank whose name may be very similar to the name of a major legitimate institution.

(e) **Accountants**

- Client receives unusual payments from unlikely sources which is inconsistent with sales.
- Use of many different firms of auditors and advisers for connected companies and businesses.
- Client has a history of changing bookkeepers or accountants yearly.
- Client is uncertain about location of company records.
- Company records consistently reflect sales at less than cost, thus putting the company into a loss position, but the company continues without reasonable explanation of the continued loss.
- Company shareholder loans are not consistent with business activity.
- Company makes large payments to subsidiaries or other entities within the group that do not appear within normal course of business.
- Company is invoiced by organizations located in a country that does not have adequate money laundering laws and is known as a highly secretive banking and corporate tax haven.

(f) **Tax Practitioners**

- Client appears to be living beyond his or her means.
- Client has no or low income compared to normal cost of living.
- Client has unusual rise in net worth arising from gambling and lottery gains.
- Client has unusual rise in net worth arising from inheritance from a criminal family member.
- Client owns assets located abroad, not declared in the tax return.
- Client obtains loan from unidentified parties.

- Client obtains mortgage on a relatively low income.

(g) **Factors arising from action by the entity or its directors**

Where an entity is actively involved in money laundering, the signs are likely to be similar to those where there is a risk of fraud, and include:

- Complex corporate structure where complexity does not seem to be warranted.
- Complex or unusual transactions, possibly with related parties.
- Transactions with little commercial logic taking place in the normal course of business.
- Transactions not in the normal course of business.
- Transactions where there is a lack of information or explanations, or where explanations are unsatisfactory.
- Transactions at an undervalue.
- Transactions with companies whose identity is difficult to establish as they are registered in countries known for their commercial secrecy.
- Extensive or unusual related party transactions.
- Many large cash transactions when not expected.
- Payments for unspecified services, or payments for services that appear excessive in relation to the services provided.
- The forming of companies or trusts with no apparent commercial or other purpose.
- Long delays in the production of company or trust accounts.
- Foreign travel which is apparently unnecessary and extensive.

APPENDIX F

Suspicious transactions shall be reported to the Suspicious Transaction Reporting Office, Commercial Affairs Department of the Singapore Police Force (STRO), by either submitting by post, via email or via STRO's electronic STR lodging system (STROLLS). Professional accountants should use the STR template set out below.

Suspicious Transaction Reporting Form – Generic

(1) Reporting of Suspicious Money Laundering Transactions pursuant to Section 39, Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act

(2) Reporting of Suspicious Terrorist Financing Activities pursuant to Section 8, Terrorism (Suppression of Financing) Act

*Items with asterix are mandatory fields

SECTION A: REPORTING COMPANY/BUSINESS	
Name*:	
Address*:	
Fax No:	
Report Reference No.:	
Reporting Officer	
Name*:	
Designation:	
Contact No*:	
Email address*:	
Contact Officer: (if different from reporting officer)	
Designation:	
Contact No.:	
Email address:	

SECTION B: PARTICULARS OF ENTITIES REPORTED ON (LEGAL PERSON) If you are reporting on Natural Person, please go to Section C	
Business Type*:	Corporation / Partnership / Sole Proprietor / Trustee or equivalent
Name*:	
Main Business Activity:	
Registration Number:	
Registration Date (dd/mm/yyyy):	
Country of Registration:	
Address:	
Foreign Address: (if any):	
Contact No.:	
Name(s) of CEO/ Partner/Sole-Proprietor/ Trustee or equivalent*:	
Date when particulars were last updated (where applicable):	
Business Relationship with subject (including account details if any)*:	

Authorised Signator(ies) Particulars	
Authorised Signatory for*:	
Name :	
Date of Birth (dd/mm/yyyy):	
Nationality:	
NRIC/Passport No./Other ID No.:	
Country of issue:	
Address:	
Foreign Address: (if any):	
Designation:	
Date of appointment as signatory (dd/mm/yyyy):	
Contact No.:	
Employment Details	
Occupation:	
Employer's Name:	

Address:	
Foreign Address: (if any):	
Contact No.:	

Beneficial Owner(s) Particulars	
Beneficial Owner for*:	
Name :	
Date of Birth (dd/mm/yyyy):	
Nationality:	
NRIC/Passport No./Other ID No.*:	
Country of Issue:	
Address:	
Foreign Address: (if any)	
Designation:	
Date of appointment as beneficial owner (dd/mm/yyyy):	
Contact No.:	
Employment Details	
Occupation:	
Employer's Name:	
Address:	
Foreign Address: (if any):	
Contact No.:	

SECTION C: PARTICULARS OF ENTITIES REPORTED ON (NATURAL PERSON)	
Name* :	
Other available information:	
NRIC/Passport No./ Other ID:	
Country of Issue:	
Date of Birth (dd/mm/yyyy):	
Nationality:	
Address:	
Foreign Address: (if any)	
Contact No.:	
Date when particulars were last updated (where applicable):	
Employment Details	
Occupation:	
Employer's Name:	
Main Business Activity:	
Address:	
Foreign Address (if any):	
Contact No.:	
Business Relationship with subject (including account details if any)*:	

SECTION D: SUSPICIOUS TRANSACTION(S)** ** Please provide details for at least one suspicious transaction		
Amount	**Date**	**Description of transaction**

Reason(s) for Suspicion*:

Other Relevant Information (including any other information which are linked to the transaction(s) and any actions taken by the reporting entity in response to the transaction):

A copy each of the following documents is attached:

☐ Customer Identification Documents

☐ Relevant Documents Supporting the Suspicious Transaction

_____
(Signature of Reporting Officer)

Date:

SUPPLEMENT A

SUPPLEMENTARY GUIDE FOR AUDITORS

This supplementary guide is intended to provide additional guidance to professional accountants when auditing and reporting on their client's financial statements (herein referred to as "auditor"). It is not stand alone guidance and shall be read in conjunction with the *Anti-Money Laundering and Countering the Financing of Terrorism – Requirements and Guidelines for Professional Accountants in Singapore* (Pronouncement), which provides general requirements and guidelines on AML and CFT compliance for all professional accountants.

Introduction

1. Whilst the AML and CFT legislations apply to auditors in the same way as they do to other individuals and organisations, they do not place obligations directly on auditors in their capacity as such. Nevertheless, the nature of the work undertaken by auditors may bring them into contact with terrorist financing activities or circumstances where proceeds of criminal activity is or may be laundered. Consequently, whilst in the normal course of auditing practice the matters referred to in this Supplement or in the Pronouncement may rarely become a matter of concern, the consequences of inaction or unwise action when terrorist financing or the laundering of criminal proceeds is or may be occurring could be serious. Auditors shall be aware of the appropriate actions to take.

2. The extent to which AML and CFT legislations affect the auditor's work differs between two broad categories of audit:

   (a) Audits of certain MAS regulated entities: certain entities in this category, such as banks, merchant banks and holders of Capital Markets Services licence, are required to comply with specific secondary legislations establishing additional obligations on them. These secondary legislations comprise Regulations, Notices and Guidelines issued by the MAS which set out certain prohibited businesses and require these institutions to implement and maintain certain procedures to forestall or prevent money laundering and terrorist financing. These entities are also normally expected by the regulators to adopt best practices guidelines issued by their respective industry associations, if any.

   In addition to reporting on their financial statements, their auditors are required to report to the MAS on matters of significance that come to their attention in the course of their work, including non-compliance with legislations, departures from its requirements and suspicions that the directors and management of such entities are implicated in money laundering or terrorist financing. Therefore, their auditors shall also be aware of key provisions contained in those secondary legislations and best practices guidelines issued by industry associations; and

   (b) Audits of other types of entity: in general, auditors of other types of entity are required only to take appropriate steps in response to factors encountered in the course of their work which lead them to suspect that money laundering or terrorist financing is taking place.

Responsibilities of Management

3. It is management's responsibility to ensure that the entity's operations are conducted in accordance with laws and regulations. The responsibility for the prevention and detection of money laundering and terrorist financing activities rests with management through the implementation and continued operation of adequate accounting and internal control systems. Such control systems reduce but do not eliminate the possibility of money laundering and terrorist financing activities.

4. The statutory audit process does not relieve management of these responsibilities.

General Responsibilities of Auditors

5. When reporting on financial statements, auditors perform their work in accordance with the Singapore Standards on Auditing (SSAs). The SSAs require that auditors:

   (a) Carry out procedures designed to obtain sufficient appropriate audit evidence, in accordance with the SSAs, to obtain reasonable assurance about whether the financial statements as a whole are free from material misstatement;

   (b) Evaluate the overall presentation of the financial statements, in accordance with relevant legislations and accounting standards; and

   (c) Issue a report containing a clear expression of their opinion on the financial statements.

   The SSAs also require auditors to consider the need to report to an appropriate authority in particular circumstances[14].

6. The auditor is not and cannot be held responsible for the prevention of, and failure to detect, money laundering and terrorist financing activities. External auditors performing financial statement audits are less likely than other professional accountants (such as forensic accountants and accountants in management positions) to encounter signs of possible money laundering and terrorist financing.

7. The fact that an annual audit is carried out may, however, act as a deterrent. As discussed in the auditing standards, audit work includes the consideration of only those systems and controls relevant to the preparation of the financial statements. Accordingly, an audit may not have identified all the internal control weaknesses that exist.

8. Furthermore, it is not the auditor's responsibility to detect suspicious activity in connection with a compliance or operational audit of an AML/CFT program or testing a Suspicious Transaction Reporting process.

9. Misstatements in financial statements may be caused by errors, fraud or breaches of law and regulations: money laundering (which may also be connected with fraudulent activity) and terrorist financing involve a breach of law.

10. Whilst auditors have no statutory responsibility to undertake work solely for the purpose of detecting money laundering and terrorist financing, they nevertheless shall take the possibility of money laundering and terrorist financing into account in the course of carrying out procedures relating to fraud and compliance with laws and regulations.

Customer Due Diligence

Know Your Client (KYC)

11. Reference shall be made to SSA 315 (Revised)[15], which requires the auditor to identify and assess the risks of material misstatement, whether due to fraud or error, at the financial statement and assertion levels, through understanding the entity and its environment, including the entity's internal control, thereby providing a basis for designing and implementing responses to the assessed risks of material misstatement.

12. Prior to acceptance of appointment, auditors consider the requirements and guidance of SSA 315 (Revised) to obtain a preliminary knowledge of the entity and its environment, including the structure of the entity, the nature of its business, the industry, ownership and any related parties, and perceived integrity of directors and management. Following appointment, auditors perform

[14] SSA 240, "*The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements*" and SSA 250, "*Consideration of Laws and Regulations in an Audit of Financial Statements*".
[15] SSA 315 (Revised), "*Identifying and Assessing the Risks of Material Misstatement through Understanding the Entity and Its Environment*".

procedures designed to identify significant changes to these matters. The requirements and guidance of SSA 315 (Revised) shall, in particular, be applied in conjunction with the requirements and guidance provided in SSA 240 and SSA 250.

13. Reference shall also be made to Singapore Standard on Quality Control (SSQC) 1[16]. SSQC 1 requires the professional firm to obtain reasonable assurance that it will only undertake or continue relationships and engagements where it has considered the integrity of the client and does not have information that would lead it to conclude that the client lacks integrity. With regard to the integrity of a client, matters that the professional firm considers include, for example:

    (a) The identity and business reputation of the client's principal owners, key management, related parties and those charged with its governance.

    (b) The nature of the client's operations, including its business practices.

    (c) Information concerning the attitude of the client's principal owners, key management and those charged with its governance towards such matters as aggressive interpretation of accounting standards and the internal control environment.

    (d) Whether the client is aggressively concerned with maintaining the professional firm's fees as low as possible.

    (e) Indications of an inappropriate limitation in the scope of work.

    (f) Indications that the client might be involved in money laundering or other criminal activities.

    (g) The reasons for the proposed appointment of the professional firm and non-reappointment of the previous firm.

    (h) The identity and business reputation of related parties.

Conduct of the Audit

Planning and Performing the Audit

14. When assessing the risks of material misstatement of the financial statements, auditors consider whether they may place reliance upon aspects of the internal control system. Where the auditors intend to place reliance upon the entity's internal control systems, sufficient evidence of the operating effectiveness of the internal control will be needed. However, an audit performed in order to express an opinion on the financial statements may not be regarded as providing assurance on the effectiveness of an entity's systems or on the actual incidence of fraud or breaches of law and regulations, including money laundering and terrorist financing. As directors are responsible for the prevention and detection of money laundering or terrorist financing activities, they may therefore wish to commission more detailed investigations in particular instances of concern. However, auditors shall take the possibility of money laundering and terrorist financing into account in the course of carrying out procedures relating to fraud and compliance with laws and regulations.

15. Specific requirements and guidance on detecting material misstatements caused by fraud and breaches of laws and regulations are set out in SSA 240 and SSA 250.

[16] SSQC 1, "*Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance and Related Services Engagements*".

Fraud

16. SSA 240 requires auditors to identify and assess the risks of material misstatement of the financial statements due to fraud; and for those assessed risks, to obtain sufficient appropriate audit evidence through designing and implementing appropriate responses and to respond appropriately to fraud or suspected fraud identified during the audit[17]. The auditors shall maintain an attitude of professional skepticism recognizing the possibility that a material misstatement due to fraud could exist, notwithstanding the auditor's past experience with the entity about the honesty and integrity of management and those charged with governance. Discussion on the susceptibility of the entity's financial statements to material misstatement due to fraud is also required to be carried out with appropriate members of the engagement team. Factors which may increase the risk of fraud occurring are noted in Appendix 1 to SSA 240.

17. A close connection exists between the indicators giving rise to an increased risk of fraud and those indicating money laundering: an illustrative list of indicators which may be indicative of suspicious transaction is given in Appendix E to the Pronouncement. Consequently, where the auditors identify such circumstances, they assess the possibility of a breach of law relating to money laundering as well as that of fraud.

Laws and Regulations

18. SSA 250 requires auditors to plan and perform the audit with an attitude of professional skepticism and requires auditors to carry out specified steps to help identify instances of non-compliance with laws and regulations that may have a material effect on financial statements. These steps consist of:

    (a) Obtaining a general understanding of the legal and regulatory framework applicable to the entity and the industry or sector and how the entity is complying with that framework;

    (b) Obtaining sufficient appropriate audit evidence regarding compliance with the provisions of laws and regulations generally recognised to have a direct effect on the determination of material amounts and disclosures in the financial statements;

    (c) Inquiring of management and, where appropriate, those charged with governance, as to whether the entity is in compliance with laws and regulations;

    (d) Inspecting correspondence, if any, with relevant licensing or regulatory authorities; and

    (e) Obtaining written representations that management has disclosed to the auditor all known instances of non-compliance or suspected non-compliance with laws and regulations whose effects shall be considered when preparing financial statements[18].

19. As explained in SSA 250, whether an act constitutes non-compliance with law or regulations is a legal determination that is ordinarily beyond the auditor's professional competence. However, auditors' training, experience and understanding of the entity and its industry may enable them to recognise that some acts coming to their attention may constitute money laundering or terrorist financing.

20. Auditors shall be alert for all breaches of laws and regulations which come to their attention in the course of their work and to take steps to determine the appropriate response[19]. Auditors of all entities shall therefore be sufficiently aware of the main provisions of the AML and CFT legislations in order to make a careful assessment of any factors encountered in the course of their work which lead them to suspect that crime is taking place, so as to obtain sufficient information to assess the effect on the financial statements and the implications for other aspects of their audit.

[17] SSA 240, paragraph 10.
[18] SSA 250, paragraphs 8, 12, 14 and 16.
[19] SSA 250, paragraph 15.

Additional Considerations for Audits of Financial Institutions

21. In general, AML and CFT laws and regulations are fundamental to financial institutions. Financial institutions are subject to regulation by the MAS and are required to comply with the requirements of the MAS.

22. When auditing the financial statements of such entities, auditors shall consider SSA 250 and carry out specified steps to help identify instances of non-compliance with requirements of the MAS that may have a material effect on financial statements. The auditor shall, if considered appropriate in accordance with SSA 580[20], also obtain a written representation from management on the steps taken, and procedures in place, to ensure compliance with the applicable requirements issued by the MAS. As set out in paragraph 2(a) of this Supplement, the auditors shall report to the MAS of any weakness in internal controls and non-compliance with legislations that come to their attention.

Reporting and Tipping-off

23. When auditing the financial statements of a regulated entity (for example, a bank), auditors have a statutory duty to report to the regulator matters of material significance to its function, or other specified matters, which come to the auditor's attention in the course of their work. Any knowledge or suspicions of involvement of the entity or the entity's management in money laundering or terrorist financing, or of failure to comply with an applicable requirement of the MAS, would normally be regarded as being of material significance to a regulator and so give rise to a statutory duty to report to the regulator. In normal circumstances, auditors can assume that reporting to a regulator does not open them to a charge of tipping-off.

Procedures When Possible Money Laundering or Terrorist Financing is Discovered or Suspected

24. SSA 250 requires auditors who become aware of a possible breach of law or regulations to obtain an understanding of the nature of the act and the circumstances in which it has occurred, and sufficient further information so as to evaluate the possible effect on the financial statements and its implications for other aspects of the audit[21].

25. SSQC 1, SSA 240 and SSA 250 set out requirements and guidance on withdrawal from the engagement, communication with client and responding to enquiry from the proposed in-coming auditor. Where such disclosure may amount to tipping-off, auditors shall consider obtaining legal advice.

The Auditor's Report on Financial Statements

26. Misstatements in financial statements may be caused by fraud or breaches of law and regulations: money laundering (which may also be connected with fraudulent activity) and terrorist financing involves a breach of law.

27. If it is known or suspected that money laundering or terrorist financing has occurred, the auditor shall consider the specific circumstances, including materiality, to assess whether the auditor's report shall be modified[22]. If auditors failed to pursue their suspicions or take other appropriate action, it might be argued that the issue of an opinion on the entity's financial statements, without the opinion being modified when the specific circumstances warrant this, enables it to present an appearance of legitimacy with the consequence that the criminal act can continue. This inference is more likely if the auditors knew that the person is or had been engaged in the crime. However, the auditor shall also consider the necessity of asking the STRO whether disclosure in the auditor's report on the financial statements, either through modifying the opinion or referring to fundamental uncertainty, could constitute tipping-off. If this is the case, auditors would be in a difficult position

[20] SSA 580, "*Written Representations".*
[21] SSA 250, paragraph 18.
[22] SSA 250, paragraphs 20, 25, 26 and 27.

and are likely to require legal advice as to how their responsibility to the shareholders of the entity may be discharged. Timing may be the crucial factor.

SUPPLEMENT B

SUPPLEMENTARY GUIDE FOR TAX PRACTITIONERS

This supplement is contributed by the Singapore Institute of Accredited Tax Professionals.www.siatp.org.sg

This supplementary guide is intended to provide additional guidance to professional accountants when providing tax services (herein referred to as "tax practitioners"). It is not stand alone guidance and shall be read in conjunction with the *Anti-Money Laundering and Countering the Financing of Terrorism – Requirements and Guidelines for Professional Accountants in Singapore* (Pronouncement), which provides general requirements and guidelines on AML and CFT compliance for all professional accountants.

General Responsibilities of a Tax Practitioner

1. Whilst the AML and CFT legislations apply to tax practitioners in the same way as they do to other individuals and organisations, they do not place obligations directly on tax practitioners in their capacity as such. Nevertheless, the nature of the work undertaken by tax practitioners may bring them into contact with terrorist financing activities or circumstances where proceeds of criminal activity is or may be laundered. Consequently, whilst in the normal course of providing tax services the matters referred to in this Supplement or in the Pronouncement may rarely become a matter of concern, the consequences of inaction or unwise action when terrorist financing or the laundering of criminal proceeds is or may be occurring could be serious. Tax practitioners need to be aware of the appropriate actions to take.

2. The work performed by tax practitioners covers routine compliance work to complex tax planning. Whilst tax practitioners are not legally obliged to undertake work solely for the purpose of detecting money laundering and terrorist financing, they nevertheless need to be alert to the risks from transactions or proceeds linked to money laundering and terrorist activities in the course of carrying out their work.

3. Routine tax compliance work encompasses activities such as the preparation of tax computations and submission of returns to the tax authorities. Tax planning work encompasses activities such as advising on structuring of tax affairs in a tax efficient manner.

4. Tax practitioners who have knowledge of or are suspicious of proceeds derived from any crime encountered during their course of work are required to report such knowledge, suspicion, or other related information to the STRO.

5. Tax practitioners should take proper care when assisting clients to ensure they do not become party to an arrangement which they know or suspect facilitates (by whatever means) the acquisition, retention, use or control of criminal property by or on behalf of another person.

Responsibilities of Management

6. It is management's responsibility to ensure that the entity's operations are conducted in accordance with laws and regulations. The responsibility for the prevention and detection of money laundering and terrorist financing activities rests with management through the implementation and continued operation of adequate accounting and internal control systems. Such control systems reduce but do not eliminate the possibility of money laundering and terrorist financing activities.

Money Laundering and Terrorist Financing Risks in the Tax Sector

7. The money laundering and terrorist financing risks areas that tax practitioners may encounter in practice include:

   (a) The client's wilful intent to evade tax, which can include the preparation and maintenance of false books of accounts or other records; and

   (b) Where during the course of dealing with the tax affairs of the client, it comes to their attention that the client is holding proceeds derived from illegal activities which may or may not be tax related.

Serious Tax Offences

8. Serious tax offences are designated as money laundering predicate offences in Singapore from 1 July 2013, in line with the FATF Recommendations. They are tax evasion and serious fraudulent tax evasion under Sections 96 and 96A of the Income Tax Act, Cap. 134, as well as fraud and improperly obtaining refund under Sections 62 and 63 of the Goods and Services Tax Act, Cap. 117A. See Annex for details.

9. Details of the criminal offences under the CDSA, TSFA and Penal Code are summarised in Appendices B, C and D respectively.

10. The common direct tax offences are:

   (a) Failing to declare all assessable income.

   (b) Claiming deductions for expenses which are fictitious or are not legally deductible.

   (c) Claiming personal relief on fictitious dependents.

11. The common indirect tax offences are:

   (a) Claiming input tax on fictitious purchases and other expenses.

   (b) Omitting output tax charged on local taxable supplies.

12. If the client is unwilling or refuses to disclose such offences or harbours a clear intention to evade taxes, tax practitioners are required to report the incident to the firm's MLRO and to the STRO as appropriate.

13. Tax practitioners should not continue to act on behalf of the client if they become aware that the client is deliberately committing serious tax offences and is unwilling to disclose such offences.

Risks Factors

14. Proceeds derived from criminal offences may become apparent to tax practitioners through the following:

   (a) Cash movements (e.g. transfers, deposits, expenditure, currency exchange etc);

   (b) Increase in income and/or capital gains; and

   (c) Unusual possession, unusual loan arrangements and increases in income which are not proportionate to legitimate business activities and investments.

15. Tax practitioners should be alert when they come across unusual transactions, particularly those which display the following characteristics:

   (a) Origin of funds is not clear;

(b) Identities of relevant parties are not clear;

(c) Transaction does not fit with knowledge of the client's background or legal sources of income; and

(d) There is no economical or logical explanation for the transaction.

16. The Inland Revenue Authority of Singapore (IRAS) has defined tax evasion as when someone has deliberately provided inaccurate or incomplete information about their activities to reduce his/her tax liability or obtain undue tax credits and refund.

17. Common characteristics that a client may be evading income tax are:

(a) Not wanting to issue a sales receipt.

(b) Maintaining two sets of accounts (excluding management accounts).

(c) Providing false invoices to claim fictitious expenses.

18. Common characteristics that a client may be evading GST are:

(a) Not wanting to issue a sales receipt or a tax invoice.

(b) Maintaining two sets of accounts (excluding management accounts).

(c) Providing false invoices to claim input tax on fictitious expenses or purchases.

(d) Providing false export documents to support zero-rated supplies of goods.

(e) Giving false information on customers and suppliers.

19. Tax practitioners should exercise caution as the above represent general guidance only. Clients may use a variety of other methods, both simple and complex, to evade their tax liabilities.

Client Due Diligence (CDD)

20. Tax practitioners may be called upon to advise another professional firm. There must be a clear agreement between the tax practitioner's firm and the other professional firm. The tax practitioner's firm is also required to conduct CDD on the professional firm.

21. In cases where the tax practitioner's firm is involved directly with the other professional firm's client, the tax practitioner's firm is required to conduct CDD on the other professional firm's client.

22. With the designation of serious tax offences as money laundering predicate offences, the professional firm's AML/CFT system should include policies, procedures and controls to effectively detect and deter the laundering of proceeds from wilful or fraudulent tax evasion. This includes supplementing the existing client acceptance and continuance process with tax-specific red flag indicators as well as critically reviewing existing clients to assess the tax legitimacy of assets booked. Professional firms should also establish proper escalation policies for managing high-risk clients, including appropriate senior management approval procedures.

Reporting

23. Unless the privilege reporting exemption applies, tax practitioners should report actual or suspected suspicious transactions to the firm's MLRO or directly to the STRO as appropriate. Tax practitioners would need to consider carefully whether they can continue providing the tax services and and should also consider obtaining legal advice and/or consulting with the STRO before undertaking further work.

ANNEX: TAX CRIMES DESIGNATED AS MONEY LAUNDERING PREDICATE OFFENCES

Direct tax offences under s.96 and s.96A Income Tax Act
s.96 Tax Evasion (1) Any person who wilfully with intent to evade or to assist any other person to evade tax: (a) omits from a return made under this Act any income which should be included; (b) makes any false statement or entry in any return made under this Act or in any notice made under s.76(8); (c) gives any false answer, whether verbally or in writing, to any question or request for information asked or made in accordance with the provisions of this Act; or (d) fails to comply with s.76(8)
s.96A Serious Fraudulent Tax Evasion (1) Any person who wilfully with intent to evade or to assist any other person to evade tax: (a) prepares or maintains or authorises the preparation or maintenance of any false books of account or other records or falsifies or authorises the falsification of any books of account or records; or (b) makes use of any fraud, art or contrivance or authorises the use of any such fraud, art or contrivance

Indirect tax offences under s.62 and s.63 Goods and Services Tax Act
s.62 Tax Evasion (1) Any person who wilfully with intent to evade or to assist any other person to evade tax: (a) omits or understates any output tax or overstates any input tax in any return made under this Act; (b) makes any false statement or entry in any return, claim or application made under this Act; (c) gives any false answer, whether verbally or in writing, to any question or request for information asked or made in accordance with the provisions of this Act; (d) prepares or maintains or authorises the preparation or maintenance of any false books of account or other records or falsifies or authorises the falsification of any books of account or records; or (e) makes use of any fraud, art or contrivance whatsoever or authorises the use of any such fraud, art or contrivance
s.63 Improperly Obtaining Refund Any person who knowingly: (a) causes; (b) attempts to cause; (c) does any act with intent to cause; or (d) makes default in performance of any duty imposed upon him by this Act with intent to cause, the refund to that person by the Comptroller of any amount in excess of the amount properly so refundable to him