KEMENTERIAN PERDAGANGAN DALAM NEGERI
DAN KOS SARA HIDUP

SURUHANJAYA SYARIKAT MALAYSIA
COMPANIES COMMISSION OF MALAYSIA

GUIDELINES RELATING TO THE OBLIGATIONS OF COMPANY SECRETARY AS A REPORTING INSTITUTION UNDER THE ANTI-MONEY LAUNDERING, ANTI-TERRORISM FINANCING AND PROCEEDS OF UNLAWFUL ACTIVITIES ACT 2001 (AMLA)

- This page is intentionally left blank -

TABLE OF CONTENT

- This page is intentionally left blank -

PART A
INTRODUCTION

1. BACKGROUND

1.1. Money laundering is a process of converting cash, funds or property derived from criminal activities to give it a legitimate appearance. It is a process to clean 'dirty' money in order to disguise its criminal origin.

1.2. Terrorism financing is the act of providing financial support to terrorists or terrorist organisations to enable them to carry out terrorist acts or to benefit any terrorist or terrorist organisation. While funds may come from criminal activities, they may also be derived from legitimate sources, for example, through salaries, revenue from legitimate business or donations including through non-profit organisations.

1.3. Proliferation financing is the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual use of goods used for non-legitimate purposes), in contravention of national law or, where applicable, international obligations.

1.4. In Malaysia like many other countries, money laundering, terrorism financing and proliferation financing poses a significant challenge to the financial system and the overall business sector.

1.5. Malaysia has taken steps to combat money laundering and enhance its anti-money laundering (AML), anti-terrorism financing and anti-proliferation financing regime, aligning with international standards and best practices.

The National Coordination Committee to Counter Money Laundering

1.6. The National Coordination Committee to Counter Money Laundering (NCC) is a high-level government body in Malaysia responsible for coordinating and overseeing efforts to combat money laundering, terrorism financing, and proliferation financing.

1.7. It comprises various government agencies, regulatory bodies, and stakeholders involved in AML, counter-financing of terrorism (CFT) and counter-financing of proliferation efforts.

1.8. NCC facilitates policy development, coordinates the National Money Laundering, Terrorism Financing, Proliferation Financing or other thematic risk assessments initiatives, formulates strategic planning based on National Risk Assessment (NRA) findings, fosters cooperation among ministries, law enforcement agencies, regulatory bodies, and reporting institutions, and oversees capacity building initiatives.

1.9. The NCC collaborates with international organizations like the Financial Action Task Force (FATF) to align Malaysia's AML/CFT efforts with global standards. It also monitors and evaluates the effectiveness of AML/CFT measures, recommends changes to existing laws, and publishes reports on threats, risks, and mitigation efforts.

The Companies Commission of Malaysia and Its Role as Supervisory Authority

1.10. The Companies Commission of Malaysia (SSM) is a member of NCC and responsible for regulating and overseeing companies and corporate entities.

1.11. SSM plays a crucial role in policy formulation, risk assessment, information sharing, capacity building, regulatory oversight, reporting and compliance, cooperation with other NCC members, and international cooperation.

1.12. SSM contributes to the NRA by providing input and data on corporate entities' risk of involvement in money laundering or terrorism financing activities. It also works with other NCC members to investigate and prosecute cases.

1.13. Being a member of NCC and a supervisory authority under the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLA), SSM is obliged to monitor and supervise company secretaries which are Reporting Institutions (RIs) under the AMLA.

Obligations of Company Secretary Relating to AML/CFT efforts

1.14. Company secretaries have obligations as RIs under Part IV of the AMLA.

1.15. Company secretaries are required to comply with Bank Negara Malaysia's (BNM) Anti-Money Laundering, Countering Financing of Terrorism and Targeted Financial Sanctions for Designated Non-Financial Businesses and Professions (DNFBPs) & Non-Bank Financial Institutions (NBFIs) (AML/CFT and TFS for DNFBPs and NBFIs) policy document (**BNM Policy Document**).

1.16. The reporting obligations under Part IV of the AMLA are expanded to be applicable not only on individuals but also at the firm level, when lawyers, accountants and company secretaries being such reporting institutions carry out the gazetted activities. This means, secretarial services firms are also required to report and comply with the anti-money laundering regulations when they are involved in such activities.

1.17. As clearly stated under the BNM Policy Document, RIs are required to take necessary steps to prevent money laundering and terrorism financing by having a system in place including ensuring compliance with laws, cooperation with law enforcement agencies and establishing internal controls that are consistent with the principles set out under the AMLA.

1.18. A company secretary must be able to appreciate his obligations under the Companies Act 2016 (CA2016) and the AMLA to ensure that he fully understands the requirements under these two distinct sets of regulations.

1.19. While the CA2016 primarily deals with governance and administration of a company, the AMLA focuses on anti-money laundering and counter-terrorism financing measures such as Know Your Customer (KYC), Due Diligence (DD) and continuous obligations. Company secretaries must navigate both sets of requirements to ensure that the company operates legally and ethically and at the same time complying with regulatory standards expected under the AMLA.

2. OBJECTIVE

2.1. These guidelines are intended to:

(a) set out the requirements and obligations imposed on company secretaries under the AMLA in preventing and combating money laundering and terrorism financing; and

(b) assist company secretaries in understanding the roles and responsibilities as RIs as set out in the BNM's Policy Document in implementing a comprehensive risk-based approach in managing ML/TF risks.

3. LEGAL PROVISIONS

3.1. These guidelines are issued pursuant to SSM's function as supervisory authority under subsection 21(1) of the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLA).

4. APPLICABILITY

4.1. These guidelines are applicable to all company secretaries, who are whether in person or through a firm or company prepares or carries out the following activities –

(a) act as a formation agent of legal entities;

(b) act as or arrange for another person to act as a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal entities;

(c) provide a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership, or any other legal entities or arrangement;

(d) act as or arrange for another person to act as a trustee of an express trust; or

(e) act as or arrange for another person to act as a nominee shareholder for another person.

4.2. These guidelines are made in addition to and not in derogation of any other guidelines issued by the SSM or any requirements as provided under the company laws and the AMLA.

4.3. A company secretary is required to comply with these Guidelines and the BNM Policy Document issued by BNM. Where there are differing requirements between the said guidelines, the more stringent requirements shall apply.

4.4. Non-compliance with any of the provisions in these Guidelines will subject the company secretary to actions under the AMLA, CA2016 or any other relevant provisions under the laws of which these Guidelines are subject to. Enforcement actions can be taken against the company secretary including its directors, officers, representatives, employees for any non-compliance with any requirements in these Guidelines.

4.5. Where the company secretary is unable to put in place the necessary mitigating measures as required under these guidelines or the BNM Policy Document, the company secretary is required to apply appropriate additional measures to mitigate the money laundering and terrorism financing (ML/TF) risks, and keep the necessary documents in relation to the additional measures implemented to manage the ML/TF risks arising from the identified gaps.

5. EFFECTIVE DATE

5.1. These guidelines shall have effect on immediate effect and remain effective and applicable unless amended or revoked.

6. DEFINITION

6.1. Unless otherwise defined, all words used in these Guidelines shall have the following and the same meaning as defined in the BNM Policy Document and other Acts administered by SSM.

"accurate"	Refers to information that has been verified for accuracy.
"beneficial owner"	In the context of legal person, beneficial owner refers to the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those natural persons who exercise ultimate effective control over a legal person. Reference to "ultimately owns or control" or "ultimate effective control" refers to situations in which ownership or control is exercised through a chain of ownership or by means of control other than direct control.
"beneficiary"	Depending on the context: In trust law, a beneficiary refers to the person or persons who are entitled to the benefit of any trust arrangement. A beneficiary can be a natural or legal person or arrangement. All trusts (other than charitable or statutory permitted non-charitable trusts) are required to have ascertainable beneficiaries. While trusts must always have some ultimately ascertainable beneficiary, trusts may have no defined existing beneficiaries but only objects of a power until some person becomes entitled as beneficiary to income or capital on the expiry of a defined period, known as the accumulation period. The period is normally co-extensive with the trust perpetuity period which is usually referred to in the trust deed as the trust period. In clubs, societies and charities, refers to the natural person(s), or groups of natural persons who receive

	charitable, humanitarian or other types of services of the clubs, societies and charities.
"board of a secretarial firm"	In relation to a company, refers to: (a) directors of the company who number not less than the required quorum acting as a board of directors; or (b) if the company has only one director, that director. In relation to: (a) a sole proprietorship, refers to the sole proprietor; or (b) a partnership, including limited liability partnership, refers to the senior or equity partners.
"close associate of PEP"	Refers to any individual closely connected to a politically exposed person (PEP), either socially or professionally. A close associate in this context includes: (a) extended family members, such as relatives (biological or non-biological relationship); (b) financially-dependent individuals (e.g. persons salaried by the PEP such as drivers, bodyguards, secretaries); (c) business partners or associates of the PEP; (d) prominent members of the same organisation as the PEP; (e) individuals working closely with the PEP (e.g. work colleagues or providing professional services); or (f) close friends.
"company secretary"	Refers to a person who is issued with a practising certificate under section 241 of the CA 2016. For the purpose of these Guidelines, company secretary includes any company secretary practising through a firm or a company.

"competent authority"	Refers to a person appointed by the Minister of Finance by order published in the *Gazette*, pursuant to section 7(1) of the AMLA. As of the date of issuance of these guidelines, this refers to Bank Negara Malaysia (BNM).
"customer"	Refers to a person for whom the company secretary/secretarial firm undertakes or intends to undertake business transaction. The term also refers to a client.
"customer due diligence (CDD)"	Refers to any measure undertaken pursuant to section 16 of the AMLA.
"director"	Refers to any person who occupies the position of director, however styled, of a body corporate and includes a person in accordance with whose directions or instructions the majority of directors or officers are accustomed to act and an alternate or substitute director. In relation to: (a) a sole proprietorship, refers to the sole proprietor; or (b) a partnership, including limited liability partnership, refers to the senior or equity partners.
"family members of PEP"	Refers to individuals who are related to a PEP either directly (consanguinity) or through marriage. A family member in this context includes: (a) parent; (b) sibling; (c) spouse; (d) child; or (e) spouse's parent; for both biological or non-biological relationships.

"higher risk"	Refers to circumstances where the company secretaries assesses the ML/TF risks as higher, taking into consideration, and not limited to the following factors: (a) Customer risk factors: • the business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic distance between the company secretary and the customer); • non-resident customers; • legal persons or arrangements that are personal asset holding vehicles; • companies that have nominee shareholders or shares in bearer form; • businesses that are cash-intensive; • the ownership structure of the company appears unusual or excessively complex given the nature of the company's business; • high net worth individuals; • persons from locations known for their high rates of crime (e.g. drug producing, trafficking, smuggling); • circumstances, businesses or activities identified by the FATF as having higher ML/TF risks; • legal arrangements that are complex (e.g. nominee relationships or layering with legal persons); and • persons who match the red flag criteria of the company secretaries. (b) Country or geographic risk factors: • countries identified by credible sources, such as mutual evaluation or published follow-up reports, as having inadequate AML/CFT systems;

	• countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations; • countries identified by the FATF, other FATF-style regional bodies or other international bodies as having higher ML/TF risks; • countries identified by credible sources as having significant levels of corruption or other criminal activities; and • countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country. (c) Product, service, transaction or delivery channel risk factors: • anonymous transactions (which may include cash); • non face-to-face business relationships or transactions; • payment received from multiple persons and/or countries that do not match the person's nature of business and risk profile; • payment received from unknown or unrelated third parties; and • nominee services.
"higher risk countries"	Refers to countries that are called by the FATF or the Government of Malaysia that pose a risk to the international financial system.
"international organisations"	Refers to entities established by formal political agreements between their member States that have the status of international treaties; their existence is recognised by law in their member countries; and they are not treated as residential institutional units of the countries in which they are

	located. Examples of international organisations include the following: (a) United Nations and its affiliate international organisations; (b) regional international organisations such as the Association of Southeast Asian Nations, the Council of Europe, institutions of the European Union, the Organisation for Security and Co-operation in Europe and the Organization of American States; (c) military international organisations such as the North Atlantic Treaty Organization; and (d) economic organisations such as the World Trade Organization
"legal arrangement"	Refers to express trusts or other similar legal arrangements.
"legal person"	Refers to any entity other than a natural person that can establish a permanent customer relationship with a company secretary or otherwise own property. This includes companies, bodies corporate, government-linked companies (GLCs), foundations, partnerships, or associations and other similar entities. GLC refers to an entity where the government is the majority shareholder or single largest shareholder and/or has the ability to exercise and influence major decisions such as appointment of board members and senior management.
"mobile channel"	Refers to conducting transactions through any electronic device using a mobile phone application provided by the company secretaries.
"online channel"	Refers to conducting transactions through any electronic device other than transactions conducted via the mobile channel.

"person"	Includes a body of persons, corporate or unincorporate.
"person conducting the transaction"	Refers to any natural person conducting the transaction or purporting to act on behalf of the customer, such as the person depositing into another customer's account or person undertaking a transaction on behalf of another person.
"politically exposed persons (PEPs)"	Refers to: (a) foreign PEPs – individuals who are or who have been entrusted with prominent public functions by a foreign country. For example, Heads of State or Government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations and important political party officials; (b) domestic PEPs – individuals who are or have been entrusted domestically with prominent public functions. For example, Heads of State or Government, senior politicians, senior government (includes federal, state and local government), judiciary or military officials, senior executives of state owned corporations and important political party officials; or (c) persons who are or have been entrusted with a prominent function by an international organisation which refers to members of senior management. For example, directors, deputy directors and members of the Board or equivalent functions. The definition of PEPs is not intended to cover middle ranking or more junior individuals in the foregoing categories.
"satisfied"	Where reference is made to a company secretary being "satisfied" as to a matter, the company secretary must be able to justify its assessment to the BNM or SSM in documentary form.

"secretarial firm"	Refers to an entity through which a company secretary offers secretarial services and is subject to reporting obligations under Part IV of the AMLA (Anti-Money Laundering Act) when a company secretary practising and the firm is engaged in activities that are designated as gazetted activities.
"Self-Regulatory Body (SRB)"	Refers to a body that represents a profession (e.g. lawyers, accountants or company secretaries), and which is made up of members from the profession, has a role in regulating the persons that are qualified to enter and who practice in the profession, and/or also performs certain supervisory or monitoring type functions. Such bodies should enforce rules to ensure that high ethical and moral standards are maintained by those practising the profession.
"senior management"	Refers to any person having authority and responsibility for planning, directing or controlling the activities of a company secretary or legal person including the management and administration of a secretarial firm or legal person.
"small-sized secretarial firm"	Refers to secretarial firm having 5 members and/or company secretaries who have been issued with Practising Certificate under section 241 of the Companies Act 2016 by SSM.
"supervisory authority"	Refers to ministries, agencies or SRBs which may exercise powers pursuant to section 21 of the AMLA. For the purpose of these guidelines, supervisory authority refers to SSM.
"targeted financial sanctions"	Refers to asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of persons designated or entities specified by the relevant United Nations Security Council Sanctions Committee or by the Minister of Home Affairs.
"third parties"	Refers to reporting institutions that are supervised by a relevant competent authority and that meet the requirements under paragraph 14 on Reliance on Third Parties, namely

	persons or businesses who are relied upon by the company secretaries to conduct the customer due diligence process. Reliance on third parties often occurs through introductions made by another reporting institution. This definition does not include outsourcing or agency relationships because the outsourced service provider or agent is regarded as synonymous with the reporting institution. Outsourced service providers or agents may include registered estate negotiators, marketing agents or outsourced telemarketers and others.

PART B
AML/CFT REQUIREMENTS

7. GENERAL PRINCIPLES AND POLICIES

7.1. A company secretary/secretarial firm is required to take the necessary steps to prevent ML/TF and have a system in place for reporting suspected ML/TF transactions to the Financial Intelligence and Enforcement Department (FIED).

7.2. In combating ML/TF, company secretary must ensure the following:

(a) Compliance with laws

A company secretary/secretarial firm must ensure compliance with all applicable laws and regulations. This includes conducting business activities in alignment with high ethical standards and refraining from providing services if there are reasonable suspicions that transactions are linked to ML/TF activities.

(b) Cooperation with law enforcement agencies

A company secretary/secretarial firm must engage in full cooperation with relevant law enforcement agencies. This entails taking necessary actions, such as promptly sharing information with the FIED, BNM and the relevant law enforcement agencies.

(c) Establishing Internal Control

A company secretary/secretarial firm is required to establish and adopt policies and procedures consistent with the principles outlined in the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLA) and these Guidelines. Additionally, he must conduct ongoing training programs to ensure that the board of directors, senior management, and employees remain informed about matters pertaining to the AMLA and these Guidelines.

(d) Risk-based approach

A company secretary/secretarial firm must ensure that the scope and depth of the policies and procedures for identifying, evaluating, monitoring, managing, and mitigating money laundering and terrorist financing risks correspond to the nature, scale, and complexity of its operations.

(e) Customer Due Diligence

A company secretary/secretarial firm must have an effective procedure for identifying its customers and obtaining satisfactory evidence to verify their identities.

8. APPLICATION OF RISK-BASED APPROACH

8.1. Risk-Based Approach (RBA)

(a) A company secretary/secretarial firm is required to take appropriate steps to identify, assess and understand their ML/TF risks at the institutional level, in relation to their customers, countries or geographical areas, products, services, transactions or delivery channels, and other relevant risk factors.

(b) In assessing ML/TF risks, company secretary/secretarial firm is required to have the following processes in place:

(i) documenting their risk assessments and findings;

(ii) considering all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied;

(iii) keeping the assessment up-to-date through a periodic review; and

(iv) having appropriate mechanism to provide risk assessment information to the BNM or SSM.

(c) A company secretary/secretarial firm is required to conduct additional assessment as and when required by the BNM or SSM.

(d) A company secretary/secretarial firm shall be guided by the results of the National Risk Assessment (NRA) issued by NCC in conducting their own risk assessments and shall take enhanced measures to manage and mitigate the risks identified in the NRA.

(e) **Appendix 7** provides the measures to be adopted in implementing RBA.

8.2. **Risk Control and Mitigation**

(a) A company secretary/secretarial firm is required to:

(i) have policies, procedures and controls to manage and mitigate ML/TF risks that have been identified;

(ii) monitor the implementation of those policies, procedures and controls and to enhance them if necessary; and

(iii) take enhanced measures to manage and mitigate the risks where higher risks are identified and where specified by the BNM or SSM.

9. AML/CFT INTERNAL COMPLIANCE PROGRAMME AND OBLIGATIONS OF THE BOARD OF DIRECTORS, SENIOR MANAGEMENT AND COMPLIANCE OFFICER

9.1. Policies, Procedures and Controls

(a) A company secretary/secretarial firm is required to develop and implement internal AML/CFT programmes which correspond to his ML/TF risks and the size, nature and complexity of his business operations.

(b) The programmes include the establishment of policies, procedures and controls to ensure high standards of integrity of its board of directors, senior management and employees as well as on-going training programmes.

(c) A company secretary/secretarial firm must ensure that policies and procedures are kept up-to-date with the regulatory requirements and are required to:

(i) document any changes to the policies, procedures and controls;

(ii) document the communication of the changes to employees; and

(iii) make (i) and (ii) available to the BNM or SSM upon request.

9.2. Board

General

(a) The Board must understand their roles and responsibilities in managing ML/TF risks.

(b) The Board must have knowledge and awareness of the ML/TF risks associated with business strategies, delivery channels and geographical coverage of its services.

(c) The Board must understand the AML/CFT measures required by the relevant laws, instruments issued under the AMLA, as well as the industry's standards and best practices in implementing AML/CFT measures.

Roles and Responsibilities

(d) The Board has the following roles and responsibilities:

(i) maintain accountability and oversight for establishing AML/CFT policies and minimum standards;

(ii) approve policies regarding AML/CFT measures within the secretarial firm, including those required for risk assessment, mitigation and profiling, customer due diligence (CDD), record keeping, on-going due diligence, suspicious transaction report and combating the financing of terrorism;

(iii) approve appropriate mechanisms to ensure the AML/CFT policies are periodically reviewed and assessed in line with changes and developments in the secretarial firm's services, technology as well as trends in ML/TF;

(iv) approve an effective internal control system for AML/CFT and maintain adequate oversight of the overall AML/CFT measures undertaken by the secretarial firm;

(v) define the lines of authority and responsibility for implementing AML/CFT measures and ensure that there is a separation of duty between those implementing the policies and procedures and those enforcing the controls;

(vi) ensure effective internal audit function in assessing and evaluating the robustness and adequacy of controls implemented to prevent ML/TF;

(vii) assess the implementation of the approved AML/CFT policies through regular reporting and updates by the Senior Management and Audit Committee; and

(viii) establish a Management Information System (MIS) that is reflective of the nature of the secretarial firm's operations, size of business, complexity of business operations and structure, risk profiles of services offered and geographical coverage.

9.3. **Senior Management**

(a) The senior management is accountable for implementing and managing AML/CFT compliance programmes in accordance with policies established by the Board, as well as the requirements of the applicable legislations, regulations, guidelines and the industry's standards and best practices.

Roles and Responsibilities

(b) The senior management has the following roles and responsibilities:

(i) be aware of and understand the ML/TF risks associated with business strategies, delivery channels and geographical coverage of its services offered and to be offered including new services, new delivery channels and new geographical coverage;

(ii) formulate AML/CFT policies to ensure that they are in line with the risks profiles, nature of business, complexity, volume of the transactions undertaken by the secretarial firm and its geographical coverage;

(iii) establish appropriate mechanisms and formulate procedures to effectively implement AML/CFT policies and internal controls approved by the Board, including the

mechanism and procedures to monitor and detect complex and unusual transactions or activities;

(iv) undertake review and propose to the Board the necessary enhancements to the AML/CFT policies to reflect changes in the secretarial firm's risk profiles, institutional and group business structure, delivery channels and geographical coverage;

(v) provide timely periodic reporting to the Board on the level of ML/TF risks facing the secretarial firm, strength and adequacy of risk management and internal controls implemented to manage the risks and the latest development on AML/CFT which may have an impact on the secretarial firm;

(vi) allocate adequate resources to effectively implement and administer AML/CFT compliance programmes that are reflective of the size, nature and complexity of the secretarial firm's operations and risk profiles;

(vii) appoint a Compliance Officer at management level at the parent company and designate a Compliance Officer at management level at each branch or subsidiary;

(viii) provide appropriate levels of AML/CFT training for its employees at all levels within the organisation, where relevant;

(ix) ensure that there is a proper channel of communication in place to effectively communicate the AML/CFT policies and procedures to all levels of employees;

(x) ensure that AML/CFT issues raised are addressed in a timely manner; and

(xi) ensure integrity of its employees by establishing appropriate employee assessment procedures.

9.4. **Compliance Management Arrangements**

(a) The Compliance Officer shall act as the reference point for AML/CFT matters within the secretarial firm.

(b) The Compliance Officer must have sufficient stature, authority and seniority within the secretarial firm to participate and be able to effectively influence decisions relating to AML/CFT matters.

(c) The Compliance Officer is required to be fit and proper to carry out his AML/CFT responsibilities effectively, which shall include minimum criteria relating to:

(i) probity, personal integrity and reputation;
(ii) competency and capability; and
(iii) financial integrity.

(d) With reference to requirements under paragraph 9.4(c)(i), the secretarial firm may take into consideration, the following factors or examples that may impair the effective discharging of the Compliance Officer's responsibilities, whether the person:

(i) is or has been the subject of any proceedings of a severe disciplinary or criminal nature;

(ii) has contravened any provision made by or under any written law designed to protect members of the public against financial loss due to dishonesty, incompetence or malpractice;

(iii) has contravened any of the requirements and standards in relation to fitness and propriety, of a regulatory body, government or its agencies or SRBs;

(iv) has engaged in any business practices which are deceitful, oppressive or otherwise improper (whether unlawful or

not), or which otherwise reflect discredit on his professional conduct;

(v) has been dismissed, asked to resign or has been resigned from employment or from a position of trust, fiduciary appointment or similar position because of questions about his honesty and integrity; and

(vi) has acted unfairly or dishonestly in the past, in his dealings with his customers, employer, auditors and regulatory authorities.

(e) With reference to requirements under paragraph 9.4(c)(ii), a company secretary may consider whether the person has satisfactory past performance or expertise, in consideration of the size, nature and complexity of their business operations.

(f) With reference to requirements under paragraph 9.4(c)(iii), a company secretary may consider the following factors:

(i) whether he has been and will be able to fulfil his financial obligations, whether in Malaysia or elsewhere, as and when they fall due; and

(ii) whether the person has been the subject of a judgment debt which is unsatisfied, either in whole or in part.

(g) The Compliance Officer must have the necessary knowledge and expertise to effectively discharge his roles and responsibilities, including keeping abreast with the latest developments in ML/TF techniques and the AML/CFT measures undertaken by the industry.

(h) The Compliance Officer is encouraged to attend certified AML/CFT courses conducted by SSM, BNM, SRBs and/or other relevant agencies.

(i) A secretarial firm is required to ensure that the roles and responsibilities of the Compliance Officer are clearly defined and documented.

(j) The Compliance Officer has a duty to ensure:

(i) compliance with the AML/CFT requirements;

(ii) proper implementation of appropriate AML/CFT policies and procedures, including CDD, record-keeping, on-going due diligence, suspicious transaction report and combating the financing of terrorism;

(iii) regular assessment of the AML/CFT mechanism such that it is effective and sufficient to address any change in ML/TF trends;

(iv) channels of communication from the respective employees to the branch or subsidiary Compliance Officer and subsequently to the Compliance Officer is secured and information is kept confidential;

(v) all employees are aware of the secretarial firm's AML/CFT measures, including policies, control mechanism and reporting channels;

(vi) establish and maintain relevant internal criteria (red-flags) to enable identification and detection of suspicious transactions;

(vii) appropriate evaluation of internally generated suspicious transaction reports by the branch or subsidiary Compliance Officers before being promptly reported to the FIED, BNM;

(viii) proper identification of ML/TF risks associated with new services or risks arising from the company secretarial firm's operational changes, including the introduction of new technology and processes; and

(ix) compliance with any other obligations that are imposed under Guidelines.

(k) A secretarial firm is required to inform the FIED, BNM, in writing or by completing the form provided in Appendix 3, within ten working days, on the appointment or change in the appointment of the Compliance Officer, including such details as the name, designation, office address, office telephone number, e-mail address and such other information as may be required.

(l) In the event where the Compliance Officer role is vacant, the senior management is deemed to be responsible for the duties of Compliance Officer pursuant to para 9.4(j).

9.5. **Employee Screening Procedures**

(a) A secretarial firm is required to establish an employee assessment procedure that are commensurate with the size, nature and complexity of the firm's operations and ML/TF risk exposure.

(b) The screening procedures under the employee assessment system or procedures shall apply upon hiring the employee and throughout the course of employment.

(c) The employee assessment system or procedures shall include:

(i) an evaluation of an employee's personal information, including employment and financial history; and

(ii) clear parameters or circumstances to trigger re-screening of employees during the course of their employment.

(d) In conducting financial history assessment, a secretarial firm may require employees to submit relevant credit reports or to complete self-declarations on the required information.

(e) The parameters to trigger re-screening may include change in job function or responsibility, promotion, or being in a position for a long period of time.

(f) A secretarial firm may determine that several functions may not be subject to screening requirements, provided that such functions do not have direct dealings with customers and/or are not involved in the monitoring of transactions, based on the size, nature, and complexity of his business operations and ML/TF risk profile.

9.6. Employee Training And Awareness Programmes

(a) A secretarial firm shall conduct awareness and training programmes on AML/CFT practices and measures for their employees. Refresher courses may be conducted at appropriate intervals depend on the firm's level of risk.

(b) The training conducted for employees must be appropriate to their level of responsibilities in detecting ML/TF activities and the risks of ML/TF identified by secretarial firm.

(c) The scope of training shall include, at a minimum:

(i) ML/TF risks;

(ii) CDD, enhanced CDD and on-going due diligence;

(iii) targeted financial sanctions screening;

(iv) risk profiling and risk assessment;

(v) suspicious transaction reporting mechanism and red flags; and

(vi) record keeping.

(d) A secretarial firm may consider distribution of circulars, guidance, publications and attendance of continuing education programs provided by the BNM, SRBs and/or other relevant agencies in developing, and as part of the internal training programmes.

(e) A secretarial firm shall document the provision of training to employees, including details on the date and nature of the training given.

(f) A secretarial firm must make available its AML/CFT policies and procedures for all employees and its documented AML/CFT measures must contain at least the following:

(i) the relevant documents on ML/CFT issued by the BNM or SSM;

(ii) the secretarial firm's internal AML/CFT policies and procedures.

(g) The employees must be made aware that they may be held personally liable for any failure to observe the AML/CFT requirements.

(h) A secretarial firm may determine that several functions may not be subject to the AML/CFT training requirements, provided that such functions do not have direct dealings with customers and/or are not involved in the monitoring of transactions, based on the size, nature and complexity of their business operations and ML/TF risk profile.

(i) In addition, training may be provided to specific categories of employees depending on the nature and scope of their functions:

(i) employees who deal directly with customers or establish business relationships may be trained to conduct CDD and ongoing due diligence, including circumstances where

enhanced CDD is required in higher risk situations. This includes detecting suspicious transactions and taking necessary measures upon determining a transaction to be suspicious;

(ii) employees who are supervisors and managers may be trained on the overall aspects of AML/CFT procedures and the appropriate risk-based approach to CDD. This includes consequences of non-compliance with requirements set out under the Guidelines; and

(iii) employees who deal directly with customers shall be trained on AML/CFT practices and measures prior to dealing with the customer.

9.7. **Independent Audit Function**

(a) The Board shall ensure regular independent audits of the internal AML/CFT measures to determine their effectiveness and compliance against:

(i) the AMLA and its subsidiary legislations and instruments issued under the AMLA; and

(ii) Guidelines and circulars on AML/CFT or other relevant requirements issued by SSM or BNM.

(b) Secretarial firm may appoint internal or external auditors to carry out the independent audit function.

(c) The independent audit function must be separated from the compliance function.

(d) The Board shall ensure that the roles and responsibilities of the auditor are clearly defined and documented. The roles and responsibilities of the auditor shall include, at a minimum:

(i) checking and testing the compliance with the AML/CFT policies, procedures and controls and effectiveness thereof; and

(ii) assessing whether current measures are in line with the latest developments and changes to the relevant AML/CFT requirements.

(e) The Board shall determine and ensure the frequency and scope of independent audits conducted commensurate with the ML/TF risks and vulnerabilities assessed by the firm. In addition, secretarial firm shall comply with any additional requirements on the frequency and scope of the independent audit as specified by the BNM.

(f) The scope of the independent audit shall include, at a minimum:

(i) compliance with the AMLA, its subsidiary legislation and instruments issued under the AMLA as well as guidelines and circulars on AML/CFT or other relevant requirements issued by SSM;

(ii) compliance with the secretarial firm's internal AML/CFT policies and procedures;

(iii) adequacy and effectiveness of the AML/CFT compliance programme; and

(iv) reliability, integrity and timeliness of the internal and regulatory reporting and management of information systems.

(g) In determining the frequency of the independent audit, the secretarial firm may be guided by the following circumstances:

(i) structural changes to the business of the secretarial firm such as mergers and acquisition;

(ii) changes to the number or volume of transactions reported to the FIED, BNM;

(iii) introduction of new services or new delivery channel; or

(iv) previous non-compliance under the AMLA which resulted in supervisory and/or enforcement action taken against the company secretary.

(h) The auditor must submit a written audit report to the Board to highlight the assessment on the effectiveness of established AML/CFT measures and inadequacies in internal controls and procedures including recommended corrective measures.

(i) Secretarial firm must ensure that such audit report including audit findings and the necessary corrective measures undertaken are made available to the BNM and SSM, upon request.

9.8. **Application for Small-sized Secretarial Firm**

(a) For **small-sized secretarial firm**, the following exemption or simplification applies:

(i) Paragraph 9.1 on Policies, Procedures and Controls requirements does not apply. However, such secretarial firms shall, at a minimum, adopt this policy document as their policies and procedures;

(ii) Paragraphs 9.2(d)(iii). and 9.2(d)(vi) of requirements on Board do not apply;

(iii) Paragraphs 9.3(b)(ii), 9.3(b)(iii) and 9.3(b)(viii) of requirements on Senior Management do not apply. However, the approval of overall Compliance Programme and enhanced due diligence is still within the accountability

of the individual with control on the overall operations of the secretarial firm;

(iv) Paragraph 9.5 on Employee Screening Procedures shall apply upon initial hiring only;

(v) Paragraph 9.6 on Employee Training and Awareness Programmes requirements shall be adopted in a simplified approach, such as via on-the-job training and third party training programme; and

(vi) Paragraph 9.7 on Independent Audit Functions requirements shall be exempted.

(b) Notwithstanding of the above, a small-sized secretarial firm is required to comply with the AML/CFT Compliance Programme requirements as and when specified by the BNM or SSM.

10. COMPANY SECRETARY'S DUTIES AS RI

10.1 In discharging his duties, a company secretary must comply with and put in place the following key and fundamental requirements under Part IV of the AMLA:

(a) Know Your Clients (Customer Due Diligence);

(b) Sanction Screening;

(c) Risk Profiling;

(d) Enhanced Due Diligence;

(e) Submit Suspicious Transaction Report;

(f) Record Keeping; and

(g) On-going Due Diligence.

* Note : Summary of AML/CFT Guidance is available in **Appendix 2**.

A. Know Your Clients (KYC) & Customer Due Diligence (CDD)

10.2 The major part of KYC process is to conduct Customer Due Diligence (CDD).

10.3 A company secretary is required to conduct CDD on customers and persons conducting the transaction, when:

(a) establishing business relations;

(b) carrying out any or occasional transaction involving the circumstances specified under paragraph 4.1 of these guidelines;

(c) have any suspicion of ML/TF, regardless of amount; or

(d) have any doubt about the veracity or adequacy of previously obtained information.

10.4 Company secretary is also required to comply with other specific CDD requirements as may be specified by the BNM and SSM from time to time.

10.5 When conducting CDD, a company secretary is required to:

(a) identify and verify that customer's identity using reliable, independent source documents, data or information;

(b) verify that any person acting on behalf of the customer is so authorised, and identify and verify the identity of that person;

(c) identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner, using the relevant information or data obtained from a reliable source, such that the company secretary is satisfied that he knows who the beneficial owner is; and

(d) understand, and where relevant, obtain information on, the purpose and intended nature of the business relationship.

10.6 Company secretary must verify and be satisfied with the identity of the customer or beneficial owner through reliable and independent documentation, electronic data or any other measures that company secretary deem necessary.

10.7 Company secretary shall determine the extent of verification method that commensurate with the identified ML/TF risks.

10.8 Company secretary must be satisfied with the veracity of the information referred to in paragraph 10.6 when verifying the identity of a customer or beneficial owner before or during the course of establishing a business relationship.

10.9 Company secretary must not engage in a business relation with a customer who fails to provide evidence of his identity.

10.10 **For an individual customer**, the company secretary is required to identify and verify the individual customer by obtaining at least the following information:

(a) full name;

(b) National Registration Identity Card (NRIC) number or passport number or reference number of any other official documents of the customer or beneficial owner;

(c) residential and mailing address;

(d) date of birth;

(e) nationality;

(f) occupation type;

(g) name of employer or nature of self-employment or nature of business;

(h) contact number (home, office or mobile);

(i) purpose of transaction, if any; and

(j) Beneficial owner, if any.

10.11 **For beneficial owner**, in conducting CDD a company secretary must adhere to the regulations, procedures, rules, practice notes, guidelines or any practice directives issued by SSM or jointly by BNM and SSM.

10.12 **For legal person (company)**[1], a company secretary is required to understand the nature of the customer's business, its ownership and control structure. A company secretary is required to identify and verify the following information:

(a) Company's name, company's registration number and proof of existence, such as Certificate of Incorporation/Constitution/

[1] For the purpose this paragraph, company includes company, business & Limited Liability Partnership (LLP).

Partnership Agreement (certified true copies/duly notarised copies, may be accepted), or any other reliable references to verify the identity of the customer;

(b) Business and registered address;

(c) Nature of business;

(d) Directors, shareholders' and senior management details;

(e) Particular of beneficial ownership in the register of beneficial ownership;

(f) Person transacting on behalf of the company (identify and verify the person authorised to represent the company either by means of a letter of authority or directors' resolution);

(g) The powers that regulate and bind the customer as well as the names of relevant persons having a Senior Management position; and

(h) Object of the company.

10.13 Where there is any doubt as to the identity of the company, beneficial owners or authorised persons during performing the CDD, the company secretary shall:

(a) conduct a basic search or enquiry on the background of such company to ensure that it has not been or is not in the process of being dissolved or liquidated, or is a bankrupt; and

(b) verify the authenticity of the information provided by such company with the SSM, LFSA or any other relevant authority.

10.14 A company secretary is exempted from obtaining a copy of the Certificate of Incorporation or Constitution and from verifying the identity of directors and shareholders of companies which fall under the following categories:

(a) public listed companies or corporations listed in Bursa Malaysia;

(b) foreign public listed companies:

(i) listed in recognised exchanges; and

(ii) not listed in higher risk countries.

(c) foreign financial institutions that are not from higher risk countries;

(d) an authorised company under the FSA and the Islamic Financial Services Act 2013 (i.e. any company that has been granted a licence or approval);

(e) company licensed or registered under the Capital Markets and Services Act 2007;

(f) licensed entities under the Labuan Financial Services and Securities Act 2010 and the Labuan Islamic Financial Services and Securities Act 2010;

(g) prescribed institutions under the Development Financial Institutions Act 2002; or

(h) licensed entities under the Money Services Businesses Act 2011.

10.15 Notwithstanding the above, company secretary is required to identify and maintain information relating to the identity of the directors and shareholders of the company referred to the above paragraph through a public register, other reliable sources or based on information provided by the customer.

10.16 A company secretary may refer to the Directives in relation to Recognised Stock Exchanges (R/R6 of 2012) issued by Bursa Malaysia in determining foreign exchanges that are recognised.

10.17 Company secretary is also required to comply with other specific CDD requirements as may be specified by the BNM from time to time.

CDD On Legal Arrangement

10.18 For customers that are legal arrangements company secretary is required to understand the nature of the customer's business, its ownership and control structure.

10.19 Company secretary is required to:

(a) identify the customer and verify its identity through the following information:

(i) name, legal form and proof of existence, such as Certificate of Incorporation/Constitution/Partnership Agreement (certified true copies/duly notarised copies, may be accepted), or any reliable references to verify the identity of the customer;

(ii) the powers that regulate and bind the customer as well as the names of relevant persons having a Senior Management position; and

(iii) the address of the trustee's registered office and if different, a principal place of business.

(b) identify and take reasonable measures to verify the identity of beneficial owners through the following information:

(i) for trusts, the identity of the settlor, the trustee(s), the protector (if any), the beneficiary or class of beneficiaries and any other natural person exercising ultimate effective control over the trust (including through the chain of control/ownership); or

(ii) for other types of legal arrangements, the identity of persons in equivalent or similar positions.

CDD on Clubs, Societies and Charities

10.20 For customers that are clubs, societies or charities, a company secretary shall conduct CDD on legal persons or on legal arrangements, where relevant, and require the customers to furnish the relevant identification including Certificate of Registration and other constituent documents. In addition, a company secretary is required to identify and verify the office bearer, or any person authorised to represent the club, society or charity, as the case may be.

10.21 A company secretary is also required to take reasonable measures to identify and verify the beneficial owners of the clubs, societies or charities.

10.22 Where there is any doubt as to the identity of persons referred to under paragraphs 10.21 and 10.22, the company secretary shall verify the authenticity of the information provided by such person with the Registrar of Societies, Labuan Financial Services Authority, SSM, Bahagian Hal Ehwal Undang-Undang, Jabatan Perdana Menteri or any other relevant authority.

B. Sanction Screening

10.23 A company secretary is required to conduct sanctions screening on the existing, potential or new clients against the Domestic List[2] and the United Nations Security Council Resolutions (UNSCR)[3] List[4].

10.24 In implementing this requirement, a company secretary is required to maintain a sanctions database which comprises at the minimum, the following:

(a) UNSCR List; and

(b) Domestic List.

10.25 A company secretary should have policies and procedures to ensure compliance with the obligation to maintain the list of entities in respect to the above list.

10.26 A company secretary is required to:

(a) keep abreast of the relevant UNSCR list relating to combating the financing of terrorism, which includes:

(i) UNSCR 1267(1999), 1373(2001), 1988(2011), 1989(2011) and 2253(2015) which require sanctions against individuals and entities belonging or related to Taliban, ISIL (Da'esh) and Al-Qaida; and

---

2 "**Domestic List**" refers to names and particulars of specified entities as declared by the Minister of Home Affairs under the relevant subsidiary legislation made under section 66B(1) of the AMLA.

3 The United Nations Security Council Resolutions (UNSCR) relating to terrorism financing are implemented pursuant to section 66B and section 66C of the AMLA by publication in the gazette by the Minister of Home Affairs. Malaysia as a member of the United Nations has an obligation to implement all the Resolutions passed in relation to targeted financial sanctions (TFS) on terrorism financing, proliferation financing and other UN sanctions.

4 "**UNSCR List**" refers to names and particulars of persons as designated by the United Nations Security Council (UNSC) or its relevant Sanctions Committee pursuant to the relevant United Nations Security Council Resolutions (UNSCR) and are deemed as specified entities by virtue of section 66C(2) of the AMLA or as designated persons under the relevant Strategic Trade Act 2010 (STA) subsidiary legislation.

(ii) new UNSCR list which is published by the UNSC or its relevant Sanctions Committee as published in the United Nations (UN) website;

(b) keep updated with the list of countries and persons designated as restricted end-users and prohibited end-users under the Strategic Trade Act 2010 (STA), in accordance with the relevant UNSCR relating to prevention of proliferation of weapons of mass destruction (WMD) as published in the UN website, as and when there are new decisions by the UNSC or its relevant Sanctions Committee; and

(c) keep updated with the list of designated countries and persons under the STA in accordance with the relevant UNSCRs relating to upholding of peace and security, through prevention of armed conflicts and human rights violations, as published on the UN website, as and when there are new decisions by the UNSC or its relevant Sanctions Committee.

10.27 A company secretary must ensure that:

(a) the UNSCR database is updated without delay and within a reasonable time upon publication of the UNSC or its relevant Sanctions Committee's designation in the United Nations (UN) website;

(b) the UNSCR list remain in the sanction database until the delisting of the specific entities by the relevant Sanctions Committee is published in the UN website:

https://www.un.org/securitycouncil

(c) the Domestic List database is updated without delay upon subsidiary legislation via Orders are published in the gazette by the Ministry of Home Affairs (MOHA):

http://www.moha.gov.my/index.php/en/maklumat-perkhidmatan/membanteras-pembiayaan-keganasan2/senarai-kementerian-dalam-negeri

(d) the information contained in the database made easily accessible to its employees at the head office, branch or subsidiary.

10.28 A company secretary may monitor and consolidate other countries' unilateral sanctions lists in their sanctions database.

10.29 A company secretary may also consider electronic subscription services in ensuring prompt updates to the sanctions database.

Related parties

10.30 A company secretary shall undertake due diligence on related parties.

10.31 In undertaking due diligence on the related parties, a company secretary is required to examine and analyse past transactions of the specified entities and related parties and maintain records on the analysis of these transactions.

10.32 In ascertaining whether an entity is owned or controlled by a specified entity, a company secretary may refer to the definition of "beneficial owner", and requirements in relation to CDD on beneficial owners.

Actions upon determination of positive name match

10.33 Upon determination and confirmation of a client's identity for any positive name match against the UNSCR or the domestic list, a company secretary is required to conduct the following without delay:

(a) Do not execute any transaction;

(b) Terminate such business relationship;

(c) Reject appointment (for potential client) and do not commence any business relation;

(d) Immediately report the actions undertaken with regards to determination and confirmation to the FIED, BNM and Inspector-General of Police.

10.34 Upon verification and confirmation that the client's identity does not match the UNSCR or the domestic list, the company secretary may continue the business as usual and conduct client risk profiling.

10.35 Company secretaries are required to ascertain potential matches with the Consolidated List to confirm whether they are true matches to eliminate "false positive". The company secretaries are required to make further inquiries from the customer or counter-party (where relevant) to assist in determining whether the match is a true match.

10.36 Company secretaries may also consolidate their database with the other recognized lists of designated persons or entities issued by other jurisdictions.

C. Risk Profiling

10.37 A company secretary is required to conduct risk profiling on their customers and assign an ML/TF a risk rating that is commensurate with their risk profile.

10.38 A risk profile must consider the following risk factors, where relevant:

(a) customer risk (e.g. resident or non-resident, type of clients, occasional or one-off, company structure, types of PEP, types of occupation);

(b) country or geographical risk (e.g. location of business, origin of customers);

(c) products, services, transactions or delivery channels (e.g. cash-based or noncash-based, face-to-face or non-face-to-face, domestic or cross-border); and

(d) any other information suggesting that the client is of higher risk.

10.39 A company secretary is expected to determine the appropriate risk parameters when considering the risk factors. These risk parameters will assist the company secretary in identifying the ML/TF risk factors for customers for the purpose of risk profiling.

10.40 Below are samples parameters that a company secretary may adopt for assessment of the ML/TF risk:

Risk Factor	**Parameters determined for risk profiling**		**Risk Rating**
Customer	Type	Individual	Low
		Company	Medium
		Legal Arrangement	High
	Social Status	Non-PEP	Low
		Local PEP	Medium
		Foreign PEP	High
	Nationality	Malaysia	Low
		Other Countries	Medium
		High-risk or sanctioned countries e.g. North Korea	High
	Country of Residence	Malaysia	Low
		Other Countries	Medium
		High-risk or sanctioned countries e.g. North Korea	High
Transaction or Distribution channel	Face-to-face		Low
	On behalf/Through intermediaries and/or agents		Medium
	Non-Face-to-face		High

Note 1: *The above is not meant to serve as exhaustive examples or prescriptions on specific risk factors or parameters which company secretary should apply for purpose of client risk profiling. Company secretary is expected to determine which risk factors and parameters are most appropriate in the context of the nature and complexity of clients served, product/services offered etc.*

Note 2: *In relation to 'Risk Profiling' while the examples above are based on a sample three-scale rating model (i.e Low, Medium, or High), this is not intended to restrict the client risk rating model adopted by company secretaries, which could be based on more granular approach i.e four-scale or five-scale or more rating model.*

10.41 The risk control and mitigation measures implemented by a company secretary shall be commensurate with the risk profile of the particular customer or type of customer. Where the ML/TF risks are assessed as higher risk, a company secretary must undertake enhanced CDD measures on the customer and, where applicable, the beneficial owner.

10.42 A company secretary is required to regularly review and update the customer's risk profile based on their level of ML/TF risks.

10.43 A company secretary shall provide timely reporting of the risk assessment, ML/TF risk profile and the effectiveness of risk control and mitigation measures to their Board and Senior Management. The frequency of reporting shall be commensurate with the level of risks involved and their operating environment.

Higher Risk Countries

10.44 A company secretary is required to conduct enhanced CDD proportionate to the risk, on business relationships and transactions with any person from higher risk countries for which this is called for by the FATF or by the Government of Malaysia.

10.45 Notwithstanding the generality of paragraph 10.44, the enhanced CDD shall include any specific CDD measure as may be imposed by the FATF or by the Government of Malaysia.

10.46 A company secretary is required to apply appropriate countermeasures, proportionate to the risks, when called upon to do so by the FATF or by the Government of Malaysia.

10.47 For the purpose of paragraph 10.46, the countermeasures may include the following:

(a) limiting business relationships or financial transactions with the identified country or persons located in the country concerned;

(b) maintaining a report with a summary of exposure to customers and beneficial owners from the country concerned and must be made available to the BNM, SSM or other relevant law enforcement agencies upon request; or

(c) conducting any other countermeasures as may be specified by the BNM.

10.48 In addition to the above, where ML/TF risks are assessed as higher risk, a company secretary is required to conduct enhanced CDD for business relationships and transactions with any person from other jurisdictions that have strategic AML/CFT deficiencies for which they have developed an action plan with the FATF.

10.49 For the purpose of requirements under paragraphs 10.44, 10.45, 10.46 and 10.48, company secretary shall refer to the FATF website: https://www.fatf-gafi.org/

D. Enhanced Customer Due Diligence (Enhanced CDD)

10.50 Company secretary is required to perform enhanced CDD where the ML/TF risks are assessed as higher risk. Where a company secretary provides nominee services, such business relations must be subjected to enhance CDD and enhanced on-going due diligence. Nominee services refer to nominee shareholding, directorship, or partnership services, where applicable. An enhanced CDD, shall include at least the following:

(a) obtaining basic CDD information (e.g. name, IC/Passport No., Address etc.;

(b) obtaining additional information on the customer and beneficial owner* (e.g. volume of assets and other information from commercial or public databases);

*(*For enhanced CDD on beneficial owner, please refer to the practice notes, guidelines or any practice directives issued by SSM)*

(c) enquiring on the source of wealth or source of funds. In the case of PEPs, both sources must be obtained; and

(d) obtaining approval from the Senior Management of the company secretary before establishing (or continuing, for existing customer) such business relationship with the customer. In the case of PEPs, Senior Management refers to Senior Management at the head office.

10.51 In addition, company secretary may also consider the following enhanced CDD measures in line with the ML/TF risks identified:

(a) obtaining additional information on the intended level and nature of the business relationship;

(b) where relevant, obtain additional information on the beneficial owner of the beneficiaries (for example, occupation, volume of assets, information available through commercial or public databases); and

(c) enquiring on the reasons for intended or performed transactions.

10.52 Where a company secretary forms a suspicion of ML/TF and has reasonable grounds to suspect that a transaction (including attempted or proposed) is connected to the unlawful activity, the company secretary is required to promptly lodge a suspicious transaction report (STR).

E. Suspicious Transaction Report (STR)

10.53 A secretarial firm must establish in place strong mechanisms for reporting suspicious transaction.

10.54 A compliance officer/company secretary is required to promptly submit STR to the FIED, BNM whenever he suspects or has reasonable grounds to suspect that the transaction (including attempted or proposed), regardless of the amount:

(a) appears unusual;
(b) has no clear economic purpose;
(c) appears illegal;
(d) involves proceeds from an unlawful activity or instrumentalities of an offence; or
(e) indicates that the customer is involved in ML/TF.

10.55 A compliance officer/company secretary must provide the required and relevant information that gave rise to doubt in the STR form, which includes but is not limited to the nature or circumstances surrounding the transaction and business background of the person conducting the transaction that is connected to the unlawful activity.

10.56 A secretarial firm must establish a reporting mechanism for the submission of suspicious transaction reports.

Filing Suspicious Transaction Report (STR) – Reporting Mechanism

10.57 A secretarial firm is required to ensure that the designated branch or subsidiary Compliance Officer is responsible for channelling all internal suspicious transaction reports received from the employees of the respective branch or subsidiary to the Compliance Officer at the parent company (the main firm). In the case of employees at the parent company, such internal suspicious transaction reports shall be channelled directly to the Compliance Officer.

10.58 A secretarial firm is required to have in place policies on the duration upon which internally generated suspicious transaction reports must be reviewed by the Compliance Officer, including the circumstances when the timeframe can be exceeded, where necessary.

10.59 Upon receiving any internal suspicious transaction report whether from the parent company, branch or subsidiary, the Compliance Officer must evaluate the grounds for suspicion. Once the suspicion is confirmed, the Compliance Officer must promptly submit the suspicious transaction report. In the case where the Compliance Officer decides that there are no reasonable grounds for suspicion, the Compliance Officer must document and file the decision, supported by the relevant documents.

10.60 A compliance officer/company secretary who has been granted access to the Financial Intelligence System (FINS) administered by the FIED, BNM must submit the suspicious transaction report through the following website:

https://fins.bnm.gov.my/

10.61 For a compliance officer/company secretary who have not been granted access to FINS, such compliance officer/company secretary must submit the suspicious transaction report, using the specified reporting form as provided in Bank Negara Malaysia's AML/CFT website at AML/CFT Policies - Anti Money Laundering / Countering Financing of Terrorism (AML/CFT) (amlcft.bnm.gov.my), or Appendix 5 of these guidelines, through any of the following channels:

(a) Mail : Director, Financial Intelligence and Enforcement Department, Bank Negara Malaysia, Jalan Dato' Onn, 50480 Kuala Lumpur.
(To be opened by addressee only)
(b) Email : str@bnm.gov.my

10.62 A compliance officer/company secretary must always observe any updates on the relevant template through the BNM-AML/CFT portal at https://amlcft.bnm.gov.my.

10.63 In the course of submitting the STR, a compliance officer/company secretary must ensure that:

(a) the suspicious transaction report is submitted within the next working day, from the date the Compliance Officer establishes the suspicion;

(b) ensure that utmost care must be undertaken to ensure that such reports are treated with the highest level of confidentiality. The company secretary has the sole discretion and independence to report suspicious transactions; and

(c) ensure that the suspicious transaction reporting mechanism is operated in a secured environment to maintain confidentiality and preserve secrecy.

10.64 A company secretary must provide additional information and documentation as may be requested by the FIED, BNM and must respond promptly to any further enquiries with regard to any report received under section 14 of the AMLA.

10.65 Where a suspicious transaction report has been lodged, a company secretary may update or make a fresh suspicious transaction report as and when a new suspicion arises.

Triggers for Submission *of STR*

10.66 A company secretary is required to establish internal criteria ("red flags") to detect suspicious transactions.

10.67 A company secretary must consider submitting a suspicious transaction report when any of its customer's transactions or attempted transactions fits the company secretary's description of "red flags". Examples of transactions that may constitute triggers to suspicious transaction are as per **Appendix 14**.

10.68 Company secretary may also refer to other examples that may be issued by the BNM, SSM, SRBs and international organisations for the purpose of reporting suspicious transactions.

Internally Generated Suspicious Transaction Reports

10.69 A secretarial firm must ensure that the compliance officer/company secretary maintains a complete file on all internally generated reports and any supporting documentary evidence regardless of whether such reports have been submitted. Where a compliance officer/company secretary decides that there are no reasonable grounds for suspicion, the compliance officer/company secretary must document and file the decision, supported by the relevant documents.

Disclosure of Suspicious Transaction Reports and Related Information

10.70 A company secretary is prohibited from disclosing any suspicious transaction report and any other information related to these reports, in accordance with section 14A of the AMLA. This includes any information on the subject or counterparties reported on, such as personal identification, account details, transaction details, the suspected offence or suspicious activities reported on, and any other information contained in the report.

10.71 The prohibition under Paragraph 10.65 does not apply where the exceptions under section 14A(3) of the AMLA apply.

10.72 Where the exceptions under section 14A(3) of the AMLA apply, company secretary must have the following measures in place:

(a) a set of parameters on:

(i) the circumstances where disclosure is required;
(ii) types of information that can be disclosed; and
(iii) to whom it can be disclosed;

(b) internal governance procedures to ensure that any disclosure is properly justified, duly authorised and managed in a controlled and secured environment;

(c) apprise all employees and intended recipients who are privy to the reports and related information to maintain confidentiality; and

(d) an effective audit trail is maintained in respect of the disclosure of such information.

10.73 For any disclosure of reports and related information pursuant to section 14A(3)(d) of the AMLA, a company secretary may make a written application to the Director, FIED, BNM for a written authorisation.

10.74 In making an application under paragraph 10.68, the company secretary shall provide the following:

(a) details and justification for the disclosure;

(b) details on the safeguards and measures in place to ensure confidentiality of information transmitted at all times;

(c) information on persons authorised by the company secretary to have access to the reports and related information;

(d) any other documents or information considered relevant by the company secretary; and

(e) any other documents or information requested or specified by Bank Negara Malaysia.

F. Record Keeping

10.75 A company secretary is required to keep the relevant records including any accounts, files, business correspondence and documents relating to transactions, in particular, those obtained during the CDD process. This includes documents used to verify the identity of customers and beneficial owners, and the results of any analysis undertaken. The records maintained must remain (either physical records or stored on electronic media) up-to-date and relevant and retrievable.

10.76 A company secretary must ensure that all relevant records relating to transactions which are kept are sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity.

10.77 A company secretary is required to keep the records for at least seven years following the completion of the transaction, the termination of the business relationship or after the date of the occasional transaction.

10.78 In situations where the records are subjected to on-going investigation or prosecution in court, they shall be retained beyond the stipulated retention period until such time a company secretary is informed by the relevant law enforcement agency that such records are no longer required.

10.79 A company secretary is required to retain the relevant records in a form that is admissible as evidence in court pursuant to the Evidence Act 1950 and make such records available to the BNM, SSM or other law enforcement agencies in a timely manner.

G. On-Going Due Diligence (ODD)

10.80 A company secretary is required to conduct on-going due diligence on the business relationship with its customers. Such measures shall include:

(a) scrutinising transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the company secretary's knowledge of the customer, their business and risk profile, including where necessary, the source of funds; and

(b) ensuring that documents, data or information collected under the CDD process is kept up-to-date and relevant, by undertaking reviews of existing records particularly for higher risk customers.

10.81 In conducting on-going due diligence, a company secretary may take into consideration the economic background and purpose of any transaction or business relationship which:

(a) appears unusual;

(b) is inconsistent with the expected type of activity and business model when compared to the volume of transaction;

(c) does not have any apparent economic purpose; or

(d) casts doubt on the legality of such transactions, especially with regard to complex and large transactions or involving higher risk customers.

10.82 The frequency in implementing paragraph 10.75 under on-going due diligence and enhanced on-going due diligence shall be commensurate with the level of ML/TF risks posed by the customer based on the risk profiles and nature of transactions.

10.83 In conducting enhanced on-going due diligence, a company secretary is required to:

(a) increase the number and timing of controls applied; and

(b) select patterns of transactions that need further examination.

Existing Customer – Materiality and Risk

10.84 Existing customers in this paragraph refer to those that are customers prior to the CDD obligations under section 16 of the AMLA becoming applicable to the company secretary.

10.85 Company secretary is required to apply CDD requirements to existing customers on the basis of materiality and risk. In assessing materiality and risk of the existing customer, a company secretary may consider the following circumstances:

(a) the nature and circumstances surrounding the transaction including the significance of the transaction;

(b) any material change in the way the account or business relationship is operated; or

(c) insufficient information held on the customer or change in customer's information.

10.86 Company secretary is required to conduct CDD 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.

11 OTHER MATTERS RELATING TO CDD

A. Delayed Verification

11.1. In certain circumstances where the ML/TF risks are assessed as low and verification is not possible at the point of establishing the business relationship, a company secretary may complete verification after the establishment of the business relationship to allow some flexibilities for his customer or beneficial owner to furnish the relevant documents.

11.2. Where delayed verification applies, the following conditions must be satisfied:

(a) this occurs as soon as reasonably practicable (shall not exceed ten working days or any other period as may be specified by the BNM) ;

(b) the delay is essential so as not to interrupt the company secretary's normal conduct of business;

(c) the ML/TF risks are effectively managed; and

(d) there is no suspicion of ML/TF.

11.3. A company secretary is required to adopt risk management procedures relating to the conditions under which the customer may utilise the business relationship prior to verification, and procedures to mitigate or address the risk of delayed verification.

11.4. The measures that company secretaries may take to manage such risks of delayed verification may include limiting the number, types and/or amount of transactions that can be performed.

B. Non Face-To-Face Business Relationship

11.5. A company secretary may establish non face-to-face (non-FTF) business relationships with its customers.

11.6. A company secretary shall obtain approval from their Board prior to the implementation of non-FTF business relationships.

11.7. A company secretary must comply with any additional measures imposed on the implementation of non-FTF as deemed necessary by the BNM.

11.8. A company secretary is required to be vigilant in establishing and conducting business relationships via electronic means, which includes mobile channel and online channel.

11.9. The Board shall set and ensure the effective implementation of appropriate policies and procedures to address any specific ML/TF risks associated with the implementation of non-FTF business relationships.

11.10. A company secretary must ensure and be able to demonstrate on a continuing basis that appropriate measures for identification and verification of the customer's identity are as effective as that of face-to-face customer and implement monitoring and reporting mechanisms to identify potential ML/TF activities.

11.11. In relation to paragraph 11.10, a company secretary shall take measures to identify and verify the customer's identity through any of the following:

(a) establishing independent contact with the customer;

(b) verifying the customer's information against reliable and independent sources to confirm the customer's identity and identifying any known or suspected ML/TF risks associated with the customer; or

(c) requesting, sighting and maintaining records of additional documents required to perform face-to-face customer verifications.

11.12. A company secretary must ensure the systems and technologies developed and used for the purpose of establishing business relationships using non-FTF channels (including verification of identification documents) have capabilities to support an effective AML/CFT Compliance Programme.

C. Failure To Satisfactorily Complete CDD

11.13. Where a company secretary is unable to comply with CDD requirements;

(a) the company secretary shall not commence business relations or perform any transaction in relation to a potential customer, or shall terminate business relations in the case of an existing customer; and

(b) the company secretary must consider lodging a suspicious transaction report under paragraph 10E.

D. CDD And Tipping-Off

11.14. In cases where the company secretary forms a suspicion of ML/TF and reasonably believes that performing the CDD process would tip-off the customer, the company secretary is permitted not to pursue the CDD process, document the basis of not completing the CDD and immediately file a suspicious transaction report under paragraph 10E.

11.15. Notwithstanding paragraph 11.14, the company secretary may consider proceeding with the transaction itself for purposes of furthering any inquiry or investigation of the ML/TF suspicion.

Notes: *Company secretary may refer to guidance and templates provided in parts C and D of this policy document in implementing the CDD and risk profiling requirements.*

12. NEW SERVICES AND BUSINESS PRACTICES

12.1. A company secretary is required to identify and assess the ML/TF risks that may arise in relation to the development of new products, services and business practices, including new delivery mechanisms, and the use of new or developing technologies whether for new or existing solutions.

12.2. A company secretary is required to:

(a) undertake the risk assessment prior to the launch or adoption of such new products, services, business practices and technologies;

(b) take appropriate measures to manage and mitigate the risks; and

(c) document the risk assessment in writing.

13. POLITICALLY EXPOSED PERSON

General

13.1. The requirements set out in this paragraph are applicable to all types of PEPs and family members or close associates of those PEPs.

13.2. In identifying individuals who fall within the definition of a close associate of a PEP, company secretary must take reasonable measures to determine the extent to which these individuals are directly engaged or involved in the activity of the PEP.

Foreign PEPs

13.3. Company secretary is required to put in place a risk management system to determine whether a customer or a beneficial owner is a foreign PEP.

13.4. Upon determination that a customer or a beneficial owner under paragraph 13.3 is a foreign PEP, the requirements of enhanced CDD specified in paragraph 10D and enhanced on-going due diligence as specified in paragraph 10.78 must be conducted.

Domestic PEPs or Person Entrusted With A Prominent Function By An International Organisation

13.5. A company secretary is required to take reasonable measures to determine whether a customer or beneficial owner is a domestic PEP or a person entrusted with a prominent function by an international organisation.

13.6. If the customer or beneficial owner is determined to be a domestic PEP or a person entrusted with a prominent function by an international organisation, company secretary is required to assess the level of ML/TF risks posed by the business relationship with the domestic PEP or person entrusted with a prominent function by an international organisation.

13.7. The assessment of the ML/TF risks as specified under paragraph 13.6, shall take into account the profile of the customer under paragraph 10.28 on Risk Profiling.

13.8. The requirements on enhanced CDD as specified under paragraph 10D and enhanced on-going due diligence as set out under paragraph 10.78 must be conducted in respect of domestic PEPs or persons entrusted with a prominent function by an international organisation who are assessed as higher risk.

13.9. Company secretary may apply CDD measures similar to other customers for domestic PEPs or persons entrusted with a prominent function by an international organisation if the company secretary is satisfied that the domestic PEPs or persons entrusted with a prominent function by an international organisation are not assessed as higher risk.

13.10. In assessing the ML/TF risk level of the customer, beneficial owner or beneficiary identified as a family member or close associate of a domestic PEP or a person entrusted with prominent public function by an international organisation, company secretary may consider the following factors:

(a) the family members or close associates have business interests related to the PEP's public functions (possible conflict of interest);

(b) the social standing or official capacity of the family members or close associates are such that it can be controlled, directed or influenced by the PEP;

(c) country from which the family members or close associates originate or reside; or

(d) the family members or close associates are known to be involved in businesses or activities that have a high probability of being abused as a vehicle for ML/TF by the PEP.

Sources of Information

13.11. A company secretary may refer to any of the following sources in identifying a PEP, a family member or a close associate of a PEP:

(a) in-house or commercial database;
(b) risk-information or guidance shared by the BNM, SSM or other regulatory authorities;
(c) public or open source information; or
(d) customer's self-declaration.

13.12. The examples of sources referred under paragraph 13.11 are not exhaustive and company secretaries are encouraged to develop internal references in identifying PEPs, family members or close associates of PEPs.

Cessation of PEP Status

13.13. A company secretary shall consider the following factors in determining whether the status of a PEP who no longer holds a prominent public function should cease:

(a) the level of informal influence that the PEP could still exercise, even though the PEP no longer holds a prominent public function; and

(b) whether the PEP's previous and current functions, in official capacity or otherwise, are linked to the same substantive matters.

14. RELIANCE ON THIRD PARTIES

Customer Due Diligence

14.1. A company secretary may rely on third parties to conduct CDD or to introduce business.

14.2. The ultimate responsibility and accountability for CDD measures shall remain with the company secretary relying on third parties.

14.3. A company secretary shall have internal policies and procedures in place to mitigate the risks when relying on third parties, including those from jurisdictions that have been identified as having strategic AML/CFT deficiencies that pose ML/TF risks to the international financial system.

14.4. A company secretary is prohibited from relying on third parties located in higher risk countries that have been identified in accordance with paragraph 10.44 to 10.49.

14.5. The relationship between a company secretary and the third parties relied upon by the company secretary to conduct CDD shall be governed by an arrangement that clearly specifies the rights, responsibilities and expectations of all parties. In placing reliance on the third party, the company secretary, at a minimum:

(a) must be able to obtain immediately the necessary information concerning CDD as required under paragraph 11; and

(b) must be reasonably satisfied that the third party:

(i) has an adequate CDD process;
(ii) has measures in place for record keeping requirements;
(iii) can provide the CDD information and provide copies of the relevant documentation immediately upon request; and
(iv) is properly regulated and subjected to AML/CFT supervision by relevant supervisory authority or competent authority.

14.6. A company secretary shall obtain an attestation from the third party to satisfy itself that the requirements in paragraph 14.5 have been met.

14.7. A company secretary may obtain written confirmation from the third party that it has conducted CDD on the customer or beneficial owner, as the case may be.

15. MANAGEMENT INFORMATION SYSTEM

15.1. A company secretary must have in place an adequate manual or electronic management information system (MIS) to complement its CDD process. The MIS is required to provide the company secretary with timely information on a regular basis to enable the company secretary to detect irregularities and/or any suspicious activity.

15.2. The MIS shall be commensurate with the size, nature and complexity of the company secretary's business operations and ML/TF risk profile.

15.3. The MIS shall include, at a minimum, information on multiple transactions over a certain period, large transactions, anomalies in transaction patterns, customer's risk profile and transactions exceeding any internally specified thresholds.

15.4. The MIS may be integrated with the company secretary's system that contains its customer's normal transactions or business profile, which is accurate, up-to-date and reliable.

16. OTHER REPORTING OBLIGATION

16.1. Company secretaries are required to submit the following reports to the FIED, BNM, as and when applicable:

(a) Data and Compliance Report issued by BNM and SSM; and

(b) any other report as may be specified by BNM and SSM.

Issued by:

SURUHANJAYA SYARIKAT MALAYSIA

28 December 2023

PART C
GLOSSARY, TEMPLATES AND FORMS

(Source of reference: BNM Policy Document)

APPENDIX 1 GLOSSARY

No	Abbreviation	Description
1.	AMLA	Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001
2.	AML/CFT	Anti-Money Laundering and Counter Financing of Terrorism
3.	CDD	Customer Due Diligence
4.	CO	Compliance Officer
5.	CRP	Customer Risk Profiling
6.	CSC	Club, Societies and Charities
7.	CTR	Cash Threshold Report
8.	Directive on TFSPF	Directive on Implementation of Targeted Financial Sanctions Relating to Proliferation Financing
9.	DNFBPs	Designated Non-Financial Businesses and Professions
10.	DPMS	Dealers in Precious Metals or Precious Stones
11.	EDD	Enhanced Customer Due Diligence
12.	FATF	Financial Action Task Force
13.	FATF Recommendations	FATF International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation
14.	FINS	Financial Intelligence System
15.	FSA	Financial Services Act 2013
16.	GLCs	Government-Linked Companies
17.	MIS	Management Information System
18.	ML/TF	Money Laundering and Terrorism Financing
19.	NCC	National Coordination Committee to Counter Money Laundering
20.	Non-FTF	Non Face-to-Face
21.	NRIC	National Registration Identity Card
22.	ODD	On-going Due Diligence
23.	PEPs	Politically Exposed Persons
24.	RBA	Risk-Based Approach
25.	SRB	Self-Regulatory Body
26.	STA	Strategic Trade Act 2010
27.	STR	Suspicious Transaction Report
28.	TFS	Targeted Financial Sanctions
29.	TFS-PF	Targeted Financial Sanctions Relating to Proliferation Financing
30.	UN	United Nations
31.	UNSC	United Nations Security Council
32.	UNSCR	United Nations Security Council Resolutions
33.	WMD	Weapons of Mass Destruction

BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

AML/CFT Guide

Bank Negara Malaysia (BNM) is the competent authority under the **Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLA).** Among others, BNM:

- Leads national efforts in AML/CFT
- Formulates effective AML/CFT regime/policies
- Receives and analyses Suspicious Transaction Reports (STRs)

Who is this guide for?

This guide is for reporting institutions that are Designated Non-Financial Businesses and Professions and Non-Bank Financial Institutions **("DNFBPs and NBFIs")** in Malaysia to comply with the requirements in the fight against money laundering and terrorism financing. It explains the MAIN* anti-money laundering & counter financing of terrorism (AML/CFT) requirements under the AMLA, the AML/CFT policy document issued for DNFBPs and NBFIs (AML/CFT and TFS for DNFBPs and NBFIs Policy Document) and other relevant documents issued by Bank Negara Malaysia.

The following businesses/professions are **"DNFBPs and NFBIs"** under the AML/CFT and TFS for DNFBPs and NBFIs Policy Document:

- Lawyers
- Accountants
- Trust companies
- Company secretaries
- Dealers in precious metals or precious stones (goldsmiths, jewellers, etc)
- Registered estate agents
- Licensed casino
- Licensed gaming outlets
- Moneylenders
- Pawnbrokers
- Leasing and factoring business

Please refer to the First Schedule of the AMLA for the full list and more details

Bank Negara Malaysia
Jalan Dato' Onn
50480, Kuala Lumpur
Tel: 1-300-88-5465 (1-300-88-LINK)
E-mail: fied@bnm.gov.my

***For the full list of requirements, please refer to:**

- Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLA)
- Anti-Money Laundering, Counter Financing of Terrorism and Targeted Financial Sanctions for Designated Non-Financial Businesses and Professions (DNFBPs)& Non-Bank Financial Institutions (NBFIs) (AML/CFT and TFS for DNFBPs and NBFIs Policy Document)

What do you need to do?

1 Know Your Clients

Do you have all these information?

For individuals:
- Name
- IC/Passport no.
- Address
- Date of birth
- Nationality
- Occupation type
- Name of employer/nature of self-employment/ nature of business
- Contact number (home, office or mobile)
- Purpose of transaction
- Beneficial owner, if any

For companies/businesses:
- Company/business name
- Business registration number
- Business address/registered address
- Nature of business
- Directors & shareholders/ beneficial owners' details

"Remember to verify the client's identity using reliable and independent source documents, information and data"

YES

NO

Follow up with your client

Client provides all information

If client refuses

Do not commence business and ...

2 Screening

Do you screen your clients' names against the **MOHA**[1] and **UNSCR Sanctions Lists for Terrorism**[2], **Proliferation**[3] **and Other UN-Sanctions Regimes**[4] ?

IF NO NAME MATCH

Continue business as usual and conduct ...

IF POSITIVE NAME MATCH

- Freeze the client's funds
- Block all transactions
- Reject the client, and ...

3 Risk Profiling

Do you conduct client risk Profiling based on the following risk factors:

1. Client
2. Product/service
3. Geographical location
4. Delivery channel

NO

For clients assessed as normal risk

For clients assessed as higher risk

Refer to AML/CFT and TFS for DNFBPs and NBFIs Policy Document for more information on how to comply.

4 Enhanced Due Diligence

Do you
i) ask for their source of funds/wealth?
ii) seek approval from your senior management prior to conduct business?

NO

YES

Throughout your business relationship, do you find the client suspicious?

YES

NO

Great! Continue business as usual. Remember to keep clients information up to date.

NO

Are there any changes to clients' information?

YES

5 Submit STR[6]

Fill up the Suspicious Transaction Report (STR) form and submit through
Email: str@bnm.gov.my or
Fax: +603-2693 3625

6 Record Keeping

Do you keep all KYC information, copies of ID documents, transaction details and any analysis of STRs filed/submitted?

YES

Do you keep all these for at least 6 years[5] **and ensure they are easily retrievable?**

NO

Well, you should start now!

YES

Keep it up!

NO

7 Repeat process

1 **MOHA: Ministry of Home Affairs**
http://www.moha.gov.my/index.php/en/maklumat-perkhidmatan/membanteras-pembiayaan-keganasan2/senarai-kementerian-dalam-negeri

2 **UNSCR: United Nations Security Council Resolutions (Terrorism)**
https://www.un.org/sc/suborg/en/sanctions/1267/aq_sanctions_list
https://www.un.org/sc/suborg/en/sanctions/1988/materials

3 **UNSCR: United Nations Security Council Resolutions (Proliferation of Weapons of Mass Destruction)**
https://www.un.org/sc/suborg/en/sanctions/1718/materials
https://www.un.org/en/sc/2231/list.shtml

4 **UNSCR: United Nations Security Council Resolutions (Other UN-Sanctions Regimes)**
htttps://www.un.org

5 **From the date of termination of the business relationship**

6 **Utmost care must be undertaken to ensure that STRs are treated with the highest level of confidentiality**

If you do NOT do any of these

Section in AMLA	Non compliance with	Maximum Penalty for Each Offence
13	Record keeping requirement	Fine up to RM1 million
14	Obligation to report suspicious transactions to BNM	
16	Obligation to conduct customer due diligence i.e. KYC	
17	Requirement to retain documents for at least 6 years	Fine up to RM 3 million or jail up to 5 years or both

For further details, please refer to the AML/CFT Microsite & STR form at http://amlcft.bnm.gov.my

(Source of reference: Bank Negara Malaysia)

APPENDIX 3 COMPLIANCE OFFICER NOMINATION NOTIFICATION FORM

Compliance Officer Nomination Notification Form
(Borang Pemberitahuan Pencalonan Pegawai Pematuhan)

IMPORTANT:
All reporting institutions under the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLA) are required to inform Bank Negara Malaysia (BNM) on the appointment or change in the appointment of the Compliance Officer pursuant to paragraph 11.5.13 of the Anti-Money Laundering, Countering Financing of Terrorism and Targeted Financial Sanctions for DNFBPs and NBFIs (AML/CFT and TFS for DNFBPs and NBFIs).

Please note that this notification of appointment under the Policy Document does not tantamount to registration or licensing by Bank Negara Malaysia.

Reporting institutions are highly encouraged to notify appointment of Compliance Officer via online nomination form accessible here: *http://amlcft.bnm.gov.my/co/* or any other way that may be specified by BNM.

PENTING:
Semua institusi pelapor di bawah Akta Pencegahan Pengubahan Wang Haram, Pencegahan Pembiayaan Keganasan dan Hasil daripada Aktiviti Haram 2001 perlu memaklumkan kepada Bank Negara Malaysia (BNM) berkaitan pelantikan atau penukaran Pegawai Pematuhan seperti yang tertakluk di bawah perenggan 11.5.13 Dokumen Dasar Pencegahan Pengubahan Wang Haram, Pencegahan Pembiayaan Keganasan dan Sekatan Kewangan Sasaran untuk DNFBPs dan NBFIs (AML/CFT dan TFS untuk DNFBPs dan NBFIs).

Harap maklum bahawa pemberitahuan pelantikan ini tidak bermaksud institusi pelapor didaftarkan atau dilesenkan oleh Bank Negara Malaysia.

Institusi pelapor sangat digalakkan untuk mengisi borang pemberitahuan pencalonan pegawai pematuhan atas talian yang boleh diakses di sini http://amlcft.bnm.gov.my/co/ atau cara lain yang boleh ditentukan oleh BNM.

<table>
<tr><th colspan="4">Type of Compliance Officer Nomination (Jenis Pencalonan Pegawai Pematuhan)</th></tr>
<tr><td rowspan="3">☐ New appointment
(Pelantikan baharu)</td><td colspan="3">☐ Change of appointment (Penukaran pelantikan)</td></tr>
<tr><td>Name of the previous Compliance Officer as per the NRIC/ Passport
(Nama Pegawai Pematuhan yang sebelumnya [mengikut NRIC/Pasport])</td><td colspan="2"></td></tr>
<tr><td>Please provide the Previous Compliance Officer No
(Sila berikan nombor Pegawai Pematuhan yang sebelumnya)</td><td colspan="2"></td></tr>
<tr><th colspan="4">Details of Compliance Officer (Maklumat Pegawai Pematuhan)</th></tr>
<tr><td>Name as per the NRIC/ Passport
(Nama mengikut NRIC/Pasport)</td><td colspan="3"></td></tr>
<tr><td>Identity Card No./Passport No.
(No. Kad Pengenalan/No. Pasport)</td><td></td><td>Email address
(Alamat e-mel)</td><td></td></tr>
<tr><td>Designation
(Jawatan)</td><td></td><td>Date of appointment
(Tarikh pelantikan)</td><td></td></tr>
<tr><th colspan="4">Company/Firm Information (Maklumat Syarikat/Firma)</th></tr>
<tr><td>Name as registered with selfregulatory body and/or Companies Commissions of Malaysia</td><td></td><td>CCM Business/ Limited Liability Partnership/ Company Registration Number
(No. pendaftaran perniagaan/syarikat)</td><td></td></tr>
</table>

(Nama seperti didaftar dengan badan kawal selia sendiri dan/atau Suruhanjaya Syarikat Malaysia)		***Licence/membership/ practicing certificate number*** *(No. lesen/keahlian/sijil amalan)*	
Type of company/firm *(Jenis syarikat/firma)*	☐ Headquarters *(Ibu Pejabat)* ☐ Branch *(Cawangan)*		
Sector *(Sektor)*	☐ Casino *(Kasino)*	☐ Licensed gaming outlets *(Institusi perjudian berlesen)*	
	☐ Lawyer *(Peguam)*	☐ Accountant *(Akauntan)*	
	☐ Company secretary *(Setiausaha syarikat)*	☐ Trust company *(Syarikat amanah)*	
	☐ Dealers in precious metals or stones *(Peniaga logam berharga atau batu berharga)*	☐ Registered estate agent (*Ejen harta tanah berdaftar)*	
	☐ Moneylender *(Pemberi pinjaman wang)*	☐ Pawnbroker (*Pemegang pajak gadai)*	
	☐ Leasing *(Pemajakan)*	☐ Factoring (*Pemfaktoran)*	
	☐ Other non-bank sectors *(Sektor bukan bank yang lain)* Please specify *(Sila nyatakan)*: _____		
Address *(Alamat)*			
City *(Bandar)*	**State** *(Negeri)*	**Postcode** *(Poskod)*	
Telephone No. *(No. Telefon)*		**Fax No.** *(No. Faks)*	
Company/firm email *(E-mel syarikat/firma)*			

Approved by *(Diluluskan oleh)*	
Signature of Senior Management *(Tandatangan Pengurusan Atasan)*	**Company/firm stamp** *(Cop syarikat/firma)*
Name of Senior Management *(Nama Pengurusan Atasan)*	enter text
Designation *(Jawatan)*	enter text

Please send the completed form to BNM using any of the following methods:
Sila hantar borang yang telah dilengkapkan kepada BNM melalui mana-mana cara berikut:

i. Online Form (*Borang atas talian* — http://amlcft.bnm.gov.my/co/
Or any other way that may be specified by BNM *(atau cara lain yang boleh ditentukan oleh BNM)*

ii. Email *(E-mel):* — fied@bnm.gov.my; or/*atau*

iii. Mail *(Pos)*: — Director
Financial Intelligence and Enforcement Department Bank Negara Malaysia Jalan Dato' Onn 50480 Kuala Lumpur

For BNM's use:

Compliance Officer Registration No:

Amendment date: 3 May 2021

APPENDIX 4 CUSTOMER DUE DILIGENCE FORM

Customer Due Diligence

Identification and verification of a customer as required under:

- Section 16 of the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLA); and
- Paragraph 14 of the Anti-Money Laundering, Countering Financing of Terrorism and Targeted Financial Sanctions for DNFBPs and NBFIs (AML/CFT and TFS for DNFBPs and NBFIs).

Disclaimer:

- *This document is intended for guidance on the implementation of CDD, TFS CRP and EDD in complying with the AML/CFT and TFS requirements under the AMLA only. Reporting institutions may develop their own forms or checklists in consideration of the size, nature and complexity of the business operations.*
- *This document does not contain exhaustive advice or information relating to the subject matter nor should it be used as substitute for legal advice. ☐ In the event that the information on Bank Negara Malaysia's official printed documents or any Acts differ from the information contained within this document, the information on such Act and official documents shall prevail and take precedence.*

Date:

1) INDIVIDUAL			
Full Name			
NRIC/Passport No.			
Date of Birth			
Residential Address			
Town			
State			
Postcode		**Country**	
Mailing Address *(if different from the above address)*			
Town			
State			
Postcode		**Country**	
Nationality			
Occupation Type			
Name of Employer/Nature of Business (if self-employed)			
Contact Number (home/office/mobile)			
Purpose of Transaction			

2) For LEGAL PERSON/LEGAL ARRANGEMENTS			
Company/Business Name			
Business Registration No.			
Business Type	☐ Sole Proprietorship ☐ Partnership ☐ Limited Liability Partnership ☐ Public Company ☐ Private Limited Company ☐ Trust ☐ Club/Society/Charity		
	☐ Other:_____		
Country of Incorporation/Registration			
Address of Registered Office (trustee for trust)			
Town			
State			
Postcode		**Country**	
Address of the Principal Place of Business *(If different from above)*			
Town			
State			
Postcode		**Country**	
Principle Business			
Contact No.			
Purpose of Transaction			
Name of Directors(s)/Partner(s)			
A) For Legal Person			
Name of Shareholder(s)/Beneficial Owner(s)	Name	Types of shares	Percentage
Name of Beneficial Owners through other means (e.g., Nominee shareholders etc.)	Name	Type of ownership/control/relationship	
Name of senior Management			
B) For Legal Arrangement			
Name		**ID**	**Address**
Settlor			
Trustee			
Protector (if any)			
Beneficiary/class of beneficiary			
Other BO information			
	Relationship with trust:		

PERSON TRANSACTING ON BEHALF OF INDIVIDUAL/LEGAL PERSON/LEGAL ARRANGEMENT

Full Name			
NRIC/Passport No.			
Date of Birth			
Address			
Town			
State			
Postcode		**Country**	
Nationality			
Occupation			
Name of Employer/Nature of Business			
Contact Number (home/office/mobile)			

VERIFICATION (For Office Use)	
Individual	Legal Persons/Legal Arrangement
• To verify and be satisfied with the identity of the customer or beneficial owner through reliable and independent documentation, electronic data or any other measures that the reporting institution deem necessary, for example: o Identity Card issued by Malaysian government o Employee Identity Card issued by ministries and statutory bodies o Foreign passport or identity card issued by the United Nations o Document issued by Malaysian government o Biometric identification o Organisation that maintains reliable and independent electronic data to verify customer's identity	• To verify the identity of the customer through the following information/documents, for example: o Constitution/Certificate of Incorporation/Partnership o Reliable references to verify the identity of customer; • To verify the identity of directors/shareholders with equity interest of more than twenty five percent/Partners through the following documents, for example, o Sections 58 and 78 Forms as prescribed by the Companies Commission of Malaysia or equivalent documents for Labuan companies or foreign incorporations o Other equivalent documents for other types of legal person o Authorisation for any person to represent the o Letter of authority or directors' resolution.

Targeted Financial Sanctions (TFS)

TFS as required under:

- Section 14(1)(c) of the AMLA;
- Paragraphs 23 and 24 of the AML/CFT and TFS for DNFBPs and NBFIs; and
- Directive on Implementation of Targeted Financial Sanctions Relating to Proliferation Financing (TFS-PF) under the Strategic Trade Act 2010, Strategic Trade (United Nations Security Council Resolutions) Regulations 2010 and Strategic Trade (Restricted End-Users and Prohibited End-Users) Order 2010.

Screen the name of customer against the MOHA and UNSCR Sanctions List for Terrorism and for Proliferation and Other UN-Sanctions Lists	☐ **Positive** name match	☐ **Negative** name match

If POSITIVE name match:

☐ freeze the customer's funds, other financial assets and economic resources OR block the transaction (where applicable), if existing customer;
☐ reject a potential customer, if the transaction has not commenced;
☐ submit a suspicious transaction report (STR) to Bank Negara Malaysia; and
☐ report to the Financial Intelligence and Enforcement Department, Bank Negara Malaysia and InspectorGeneral Police using the form attached in Appendix 6A, 6B, 7A or 7B where applicable.

Customer Risk Profiling (CRP)
CRP as required under paragraph 10 of the AML/CFT and TFS for DNFBPs and NBFIs.

In profiling the risk of its customers, reporting institutions must consider the following factors:

(a) Customer Risk, e.g.

Is the customer or the beneficial owner a foreign or domestic PEP?	☐ Foreign PEP **By default higher ML/TF risks & subject to EDD*
	☐ Domestic PEP
Nationality (resident or non-resident) of the customer/director/partner and shareholder/beneficial owner	☐ Malaysian
	☐ Foreigner
Is the customer/director/partner and shareholder/beneficial owner classified as High Net Worth individual?	☐ Yes
	☐ No
Type of customer	☐ New customer
	☐ Repeating customer
	☐ Occasional/One-Off
Size and structure customer's business?	☐ Large and complex structure
	☐ Small and simple structure
Type of occupation/business	☐ Lower risk occupation/business
	☐ Higher risk occupation/business i.e. cash intensive business/occupation
Is there any adverse remark on the customer/company' background from research via public or commercial database such as Google?	☐ Yes Please state:_____
	☐ No
Other consideration	

(b) Geographical Risk, e.g.

What is the country of origin of the customer, location of business, branches, beneficial owner, beneficiaries or related parties? List of higher risk countries is available at: - http://www.fatf-gafi.org	☐ Low risk countries
	☐ Countries having strategic AML/CFT deficiencies
	☐ Countries subject to a FATF call to apply countermeasures **By default higher ML/TF risk & subject to EDD and countermeasures*
Other consideration	

(c) Products/Service Risk, e.g.

Does the product/service offered provide anonymity to the customer?	☐ Yes
	☐ No
Does the product/service offered commensurate with the profile of the customer?	☐ Yes
	☐ No
Does the product/service offered involve complex and unusual transaction?	☐ Yes
	☐ No
Does the customer require nominee services?	☐ Yes
	☐ No
Does the company have nominee shareholder(s) or nominee director(s)? (for nominee service dispensed by lawyers, accountants and company secretaries)	☐ Yes
	☐ No

Does the product/service offered involve cross-border transactions?	☐ Yes
	☐ No
Other consideration	

(d) Transaction and Delivery Channel Risk, e.g.

Mode of payment	☐ Bank transfer or cheques
	☐ Physical cash
Delivery Channel	☐ Face-to-face
	☐ Through agent/intermediaries
	☐ Non face-to-face
Other consideration	

Other factors that affect the customer's ML/TF risk rating?

Overall risk assessment:	☐ Low	☐ Medium	☐ High

Enhanced Customer Due Diligence (EDD)

EDD as required under:

- Section 16 of the AMLA; and
- Paragraph 14 of the AML/CFT and TFS for DNFBPs and NBFIs.

Circumstances when EDD applies:

- Dealing with foreign PEPs
- Dealing with person from higher risk countries
- For gatekeepers (lawyers, accountants, company secretaries and trust companies), where nominee services are provided
- Customer assessed as having higher ML/TF risks based on customer risk profiling

Note:

For enhanced on-going due diligence, higher frequency of transaction monitoring is required to enable reporting institutions to identify any anomalies.

Individual name of higher risk customer/PEP	
Customer/PEP's role in Legal Person/Legal Arrangement, where relevant	

For higher ML/TF risk customers	
Source of Fund/ Source of Wealth	*In the case of PEPs, both sources must be obtained*
Additional Information on Customer and Beneficial Owner	*E.g. volume of assets and other information from public database, or customer declaration*
For customer subject to EDD – To be approved by Senior Management of the Firm	
Approval	☐ Approved ☐ Not approved Justification: _____ _____
Name of Senior Management	
Position/Designation	
Date	

APPENDIX 5 STR FORM FOR COMPANY SECRETARIES

RAHSIA

BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

Please send completed form to:

Financial Intelligence & Enforcement Department Bank Negara Malaysia
Jalan Dato' Onn, 50480 Kuala Lumpur

Fax:03 -2692 3625 Email:str@bnm.gov.my

Reference No:_____

CO Reg. No :_____

SUSPICIOUS TRANSACTION REPORT

FOR COMPANY SECRETARIES

a. This report is made pursuant to the requirement to report suspicious transaction under the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLA)

b. Under section 24 of the AMLA, no civil, criminal or disciplinary proceedings shall be brought against a person who makes a report unless it was made in bad faith

PART A: INFORMATION ON CUSTOMER

Account Holder

1)

Nationality			
Name			
Other/previous name (1)			
(2)			
(3)			
New NRIC no		Old NRIC no	
Other identification		Other identification type	
Gender			

Contact information

Residential/Business Address	Correspondence Address
Other Address	Previous Address

Email adddress					
Contact No.		-(off)		-(Res)	-(Mob)
Fax No.					

Employment information

Business/employment type	
Occupation	
Occupation Description	
Employer name	
Employer area	
Other known employment	

Marital Information

Marital status	
Spouse name	

Spouse identification

New NRIC No		Old NRIC No	
Other identification		Other Identification type	
Passport no		Place/country of issue	

PART B: TRANSACTIONS DETAILS

Attempted but not completed transaction	
Services rendered	Act as formation agent of legal entities
	Act as (or arrange for another person to act as) a director or secretary of a company, a partner of a partnership or a similar position in relation to other legal entities
	Provide a registered office, business address or accommodation, correspondence or administrative for a company, a partnership, or any other legal entities or arrangements
	Act as (or arrange for another person to act as) a trustee of an express trust
	Act as (or arrange for another person to act as) a nominee shareholder for another person
	Others (please specify)
Transaction date	
Transaction amount	

Foreign currency amount		Currency type	

PART C: DESCRIPTION OF SUSPICIOUS TRANSACTION

Ground for suspicion	Counterfeit/fraud/forgery
	Large/frequent/unusual cash or currency transaction
	Client identity is hard to obtain
	Formation of entities with no apparent business purpose
	Criminal breach of trust
	Activity inconsistent with customer profile
	Others (please specify)
Description of suspected criminal activity	
Details of the nature and circumstances surrounding it	
Date of report	

APPENDIX 6A TARGETED FINANCIAL SANCTIONS REPORTING (DNFBPs) – UPON DETERMINATION

REPORTING UPON DETERMINATION: ( ) TERRORISM FINANCING ( ) PROLIFERATION FINANCING ( ) OTHER SANCTIONED REGIMES

Please tick (☐) at the appropriate bracket

ALL Sanctions Regimes	**Terrorism Financing**
UNSCR No (If Available) : Date of UN Listing :	**Type of Lists : Domestic List ( ) UNSCR List ( )** **Circular/Gazette Reference No. :** **Circular/Gazette Reference Date :**
Match with Designated Person/Specified Individual & Entity : Yes ( ) No ( ) If YES, please fill-up the details in the form below	

No.	UNSCR Permanent Ref No/MOHA Reference No (e.g.) KPi.001/KDN .I.0 1-2014)	Customer Name	Address	NRIC/ Passport No.	Reporting Institution Name	Branch providing the product/ service/ facility (if applicable)	Product/service /facility offered, e.g. pawn, loan	Date of funds received by the reporting institution (DD/MM/YY)	Customer status (*before designation*) *e.g. existing/new on-boarding*	Status of product/service facility *(after designation) (e.g. frozen, terminated, etc.)*	Date product/ service /facility frozen/ terminated etc.) (DD/MM/YY)	Value of product/ service/facility	Please state the type and value of property for transactions relating to a property	Related Parties	Remarks
1.															
2.															
3.															
4.															

Reporting Institution Details

Reporting Institution Name :
Sector :
Contact Person :
Designation :
Tel & Fax No. :
E-mail :
Reporting Date :

Notes: Please submit the completed form to –

Reporting for ALL sanctions regimes	**In addition, reporting for TFS on Terrorism Financing**
Email	**Address**
Financial Intelligence and Enforcement Department, Bank Negara Malaysia • Address : amlsanctions@bnm.gov.my • Subject : Reporting upon Determination (CFT/CPF/OSR*) **to specify relevant sanctions regime*	**Ketua Polis Negara** (c) u/p: Pasukan Siasatan Jenayah Pengubahan Wang Haram dan Pembiayaan Keganasan Urusetia Pejabat Ketua Polis Negara, Tingkat 23, Menara 238, Jalan Tun Razak, 50400, Kuala Lumpur (d) u/p : Bahagian E8,Cawangan Khas Tingkat 24, Menara 2, Ibu Pejabat Polis, Bukit Aman, 50560, Kuala Lumpur

[Amendment date: 3 May 2021]

APPENDIX 6B TARGETED FINANCIAL SANCTIONS REPORTING (DNFBPS) - PERIODIC REPORTING ON POSITIVE NAME MATCH

PERIODIC REPORTING ON POSITIVE NAME MATCH: ( ) TERRORISM FINANCING ( ) PROLIFERATION FINANCING ( ) OTHER SANCTIONED REGIMES
Please tick (☐) at the appropriate bracket

Only for reporting on Terrorism Financing*	
Type of Lists	**: Domestic List ( ) UNSCR List ( )**

No.	UNSCR Permanent Ref Bo/MOHA Refreence No (e.g. KPi.001/KDN.I.01-	Customer Name	Address	NRIC/Passport No.	Reporting Institution Name	Branch providing the product/service/facility (if applicable)	Product/servuce/facility offered, e.g. pawn, loan	Date of funds received by the reporting institution (DD/MM/YY)	Account/Facility Status (before designation)	Status of product/servic e facility *(after designation) (e.g. frozen, terminated, etc.)*	Date of funds received by the reporting institution (DD/MM/YY)	Value of product/services/facility	Transaction Details (line by line transaction)					New Account Balance as at: (DD/MM/YY)			Related Parties	Remarks
													Transaction No.	Date (DD/MM/YY)	Type(CD/DR)	Amount (MYR)	Remarks	Banking (CR)	Banking (DR)	Please state the type and value of		
1.																						
													1.									
													2.									
2.																						
3.																						

Reporting Institution Details

Reporting Institution Name : (*please state all entities under the group if reporting done on group* basis)
Sector :
Contact Person :
Designation :
Tel & Fax No. :
E-mail :
Reporting Date :

Notes:

Please submit the completed form to	**Submission dates**	
Financial Intelligence and Enforcement Department, **Bank Negara Malaysia** • Email Address : amlsanctions@bnm.gov.my • Subject : Reporting upon Determination (CFT/CPF/OSR*) **to specify relevant sanctions regime*	**Terrorism Financing:**	UNSC List: Every 5th January and 5th July Domestic List: Every 15th May and 15th November
	Proliferation Financing & Other Sanctioned Regimes:	Only if there is any changes to the frozen funds (after first time reporting on positive name match) and latest by 15 January of the following calendar year

[Amendment date: 3 May 2021]

PART D
GUIDANCE

APPENDIX 7 Guidance on Application of Risk-Based Approach

1. Introduction

1.1 The risk-based approach (RBA) is central to the effective implementation of the anti-money laundering and countering financing of terrorism (AML/CFT) preventive requirements and the FATF Recommendations. The focus on risk is intended to ensure a company secretary is able to identify, assess and understand the money laundering and terrorism financing (ML/TF) risks to which it is exposed to and take the necessary AML/CFT control measures to mitigate them.

1.2 This Guidance seeks to:

(a) assist the company secretary to design and implement AML/CFT control measures by providing a common understanding of what the RBA encompasses; and

(b) clarify the policy expectations in relation to the assessment of business based and customer-based ML/TF risk in applying the RBA. In the event a company secretary has developed its own RBA, the company secretary is expected to ensure its RBA achieves the outcomes as specified in the BNM Policy Document as further clarified in this Guidance.

1.3 This Guidance is **not** intended to supersede or replace any of the existing mandatory requirements on RBA that are provided in Paragraph 10 of the AML/CFT and TFS for DNFBPs and NBFIs policy document.

1.4 The RBA–

(a) recognises that the ML/TF threats to a company secretary vary across customers, countries, products and services, transactions and distribution channels;

(b) allows the company secretary to apply appropriate policies, procedures, systems and controls to manage and mitigate the ML/TF risks identified based on the nature, scale and complexity of the company secretary's business and ML/TF risk profile; and

(c) facilitates more effective allocation of the company secretary's resources and internal structures to manage and mitigate the ML/TF risk identified.

1.5 The RBA provides an assessment of the threats and vulnerabilities of the company secretary from being used as a conduit for ML/TF. By regularly assessing the company secretary's ML/TF risks, it allows the company secretary to protect and maintain the integrity of its business and the financial system as a whole.

2. Institutional Risk Assessment and Customer Risk Profiling

2.1 The RBA entails two (2) assessments:

Institutional Risk Assessment (IRA)

A company secretary is expected to identify ML/TF risk factors that affect its business and address the impact on the company secretary's overall ML/TF risks.

- **Refer to requirements in paragraphs 10.2 and 10.3 in the AML/CFT and TFS for DNFBPs and NBFIs policy document**

I. ***Perform risk assessment -*** A company secretary is expected to perform an assessment on the degree of ML/TF risks that the company secretary's business is exposed to and determine its risk appetite level. To this end, a company secretary is

expected to formulate specific parameters of the ML/TF risk factors considered.

II. ***Formulate and implement business risk management and mitigation control measures*** **-** A company secretary is expected to establish and implement policies, controls and procedures to manage and mitigate the identified ML/TF risks. Such measures should be sufficiently adequate to manage and mitigate the ML/TF risks identified.

Customer Risk Profiling (CRP)

For CRP, a company secretary is expected to consider the inherent risks arising from the types of products, services, distribution channels, etc. that the customers are using and implement appropriate measures to manage and mitigate the ML/TF risks identified therein.

- ***Refer to requirements in paragraph 10.4 in the AML/CFT and TFS for DNFBPs and NBFIs policy document***

I. ***Determine the risk parameters for customer risk profiling*** - A company secretary is expected to identify specific ML/TF risk factors and parameters for customers' profiling. Where relevant, the company secretary may adopt similar parameters that have been used for the assessment of the ML/TF risk factors considered under the IRA.

II. ***Conduct risk profiling on customers*** – Based on the Customer Due Diligence (CDD) information obtained at point of on-boarding new customers, or ongoing CDD information obtained from existing

customers, as the case may be, a company secretary is expected to determine the ML/TF risk profile of each customer (e.g. high, medium or low) by applying the risk parameters determined above, in order to determine the appropriate level of CDD (i.e. standard or enhanced) that is applicable in respect of each customer. The resulting ML/TF risk profile may also have a bearing on the frequency and intensity of on-going CDD that is applicable throughout the duration of the business relationship with the customer.

III. ***Apply customer risk management and mitigation control measures*** – A company secretary is expected to apply the necessary risk management and mitigation policies, controls and procedures that are commensurate with the ML/TF risk profile of each customer, to effectively manage and mitigate the ML/TF risks identified. For example, customers assessed as having higher ML/TF risks should be subject to enhanced CDD procedures, senior management's approval should be obtained before offering or continuing to transact or provide professional services and the customer should be subject to more frequent and intense ongoing CDD procedures throughout the duration of the business relationship with the customer.

2.2 The RBA is expected to be tailored to the nature, scale and complexity of the company secretary's business, size, structure and activities.

2.3 A company secretary is expected to incorporate the RBA into its existing policies and procedures. All steps and

processes in relation to the RBA for purpose of IRA and CRP are expected to be documented and supported by appropriate rationale and be subject to approval by senior management and/or the Board of Directors, as appropriate.

2.4 Recognising that ML/TF risks evolve and are subject to change over time (arising from the emergence of new threats, introduction of new products/services, new technologies, expansion to new customer base etc.) a company secretary is expected to understand that assessing and mitigating ML/TF risks is not a static exercise. Therefore, a company secretary is expected to periodically review, evaluate and update the RBA accordingly.

2.5 The outcome of the IRA and CRP complement each other. Therefore, to effectively implement the RBA–

(a) a company secretary is expected to determine reasonable risk factors and parameters for the IRA and CRP; and

(b) over a period of time, data from the CRP may also be useful in updating the parameters of the IRA.

3. Institutional Risk Assessment (IRA)

A. Perform Risk Assessment

3.1 While there is no prescribed methodology, the IRA is expected to reflect material and foreseeable ML/TF threats and vulnerabilities which a company secretary is exposed to for the period under review. Hence, a company secretary may establish a manual or automated system to perform its risk assessment.

3.2 The company secretary is expected to evaluate the likelihood and extent of its ML/TF risks at a macro level. When assessing

the ML/TF risks, a company secretary is expected to consider all relevant risk factors that affect their business and operations, which may include the following:

(a) Specific risk factors or high risk crimes that the company secretary may consider for the purpose of identifying its ML/TF risks;

(b) Type of customers;

(c) Geographic location of the company secretary;

(d) Transactions and distribution channels offered by the company secretary;

(e) Products and services offered by the company secretary;

(f) Structure of the company secretary; and

(g) Findings of the National Risk Assessment (NRA).

3.3 The ML/TF risks may be measured based on a number of factors. The weight or materiality given to these factors (individually or in combination) when assessing the overall risks of potential ML/TF may vary from one company secretary to another, depending on their respective circumstances. Consequently, a company secretary is expected to make its own determination as to the risk weightage or materiality for each factor under consideration. These factors either individually or in combination, may increase or decrease potential ML/TF risks posed to the company secretary.

3.4 To assist a company secretary in assessing the extent of its ML/TF risks, the company secretary may consider the following examples of risk factors:

(a) ***Customers*** **–** in conducting business transactions, the company secretary is exposed to various types of customers that may pose varying degrees of ML/TF risks.

In analysing its customers' risk, a company secretary may consider the non-exhaustive examples below:

- *Exposure by type of customer, individuals and non-individuals (companies, businesses, legal arrangements, associations, etc.);*
- *Exposure by nationality i.e. local or foreign;*
- *Nature and type of business or occupation of the customers;*
- *Exposure to foreign PEP customers;*
- *Exposure to domestic PEP customers assessed as higher risk;*
- *Exposure to customers related to PEPs assessed as higher risk;*
- *Exposure to customers that are legal arrangements (e.g. trusts) and legal persons and the level of complexity of such legal structures;*
- *Exposure to customers that authorise a proxy/agent to represent on their behalf;*
- *Exposure to companies that have nominee shareholders or shares in bearer form;*
- *Exposure to legal persons or arrangements that are personal asset holding vehicles;*
- *Exposure to customers originating from or domiciled in, and/or transactions conducted in or through higher risk countries (called by FATF or Government of Malaysia) or tax haven jurisdictions.*

(b) ***Countries or geographic location*** – a company secretary should take into account such factors including the location of the company secretary's holding company, head office, branches and subsidiaries and agents (where applicable), and whether its holding company is located within a jurisdiction with full AML/CFT compliance as identified by a credible source. Further non-exhaustive examples are as below:

- *Location of its holding company, branches, subsidiaries, merchants and/or agents in:*
- *Tourist hotspots, crime hotspots, country's border and entry points;*
- *High risk countries called by the FATF or by the Government of Malaysia;*
- *Jurisdictions that have been identified by credible sources as having significant levels of corruption or other criminal activities e.g. reports by Transparency International, United Nations Office on Drugs and Crimes etc.;*
- *Jurisdictions that have been identified by credible sources as providing funding or support for money laundering, terrorism or proliferation of weapons of mass destruction.*

(c) ***Transactions and distribution channels*** – A company secretary has various modes of transaction and distribution of its products and services. Some of the modes of transaction and distribution channels may be more susceptible to ML/TF risks. For example, products sold via non-face-to-face channels are more susceptible to ML/TF as compared to products sold via face-to-face channels, and transactions conducted with third party agents of the company secretary may be more vulnerable to ML/TF in comparison to those conducted at the company secretary's own branches. In this regard, a company secretary is expected to consider the appropriate ML/TF risks attributed to all available modes of transactions and distribution that are offered to customers by the company secretary, including the following non-exhaustive examples:

- *Mode of distribution e.g. direct channel, or via agents, brokers, financial advisors, introducers, online or technology based transaction;*
- *Volume and frequency of non-face-to-face business relationships or transactions;*
- *Mode of payment e.g. cash-based transactions, e-payments;*
- *Cash intensive or other forms of anonymous transactions;*
- *Volume and frequency of transactions carried out in high risk areas or jurisdictions;*
- *Number of distribution channels located in high risk areas or jurisdictions; and/or*
- *Exposure to cross-border transactions and/or transactions in high risk jurisdictions.*

(d) ***Products and services*** – a company secretary is expected to identify the appropriate level of ML/TF risks attached to the types of products and services offered. Some of the non-exhaustive examples that the company secretary may take into account are as follows:

- *Nature of the products and services;*
- *Level of complexity of the products and services;*
- *Cash intensity related to the products and services;*
- *Market segments of the products and services;*
- *Products that are easily transferable to another party;*
- *Product's ownership not easily traceable to the owner;*
- *Product can be easily converted to cash or exchanged to another form;*
- *Customer can place deposit for a period of time for purchasing a product;*
- *Product can be easily transported or concealed;*

- *Product can be used as an alternative form of currency;*
- *Product that has high value in nature;*
- *Product can be purchased through non face-to-face channel;*
- *Allow use of virtual asset and other anonymous means of payment;*
- *Allow use of unusual means of payment e.g. high value items such as real estate, precious metals and precious stones;*
- *Services that enable clients to move funds anonymously; and/or*
- *Nominee services that may obscure ownership of legal person or legal arrangements.*

(e) ***Company secretary's structure*** – the ML/TF risk of a company secretary may differ according to its size, nature and complexity of the company secretary's business operations. Appropriate assessment of its business model and structure may assist a company secretary to identify the level of ML/TF risks that it is exposed to. In this regard, a company secretary may take into account the following non-exhaustive examples:

- *Number of branches, subsidiaries and/or agents;*
- *Size of the company secretary relative to industry/sector;*
- *Number and profile of employees;*
- *Degree of dependency on technology;*
- *Volume and value of cross border transactions;*
- *Volume and value of high-valued products;*
- *Cash intensity of the business; and/or*
- *Level of staff turnover, especially in key personnel positions.*

(f) ***Findings of the National Risk Assessment (NRA) or any other risk assessments issued by relevant authorities*** **–** in identifying, assessing and understanding the ML/TF risks, a company secretary is expected to fully consider the outcome of the NRA or any other equivalent risk assessments by relevant authorities:

Under the NRA, a company secretary is expected to take into account the following:

- *Sectors identified as highly vulnerable to ML/TF risks and the company secretary exposure to such sectors in relation to customer segments served;*
- *Crimes identified as high risk or susceptible to ML/TF and the adequacy of the company secretaries' mitigating measures to detect and deter such illegal proceeds or in preventing dealings with customers involved in such illicit activities; and/or*
- *Terrorism Financing and/or Proliferation Financing risks faced by the industry.*

(g) ***Other factors*** **–** a company secretary may also take into account other factors in determining its risk assessment such as:

- *Current trends and typologies for the sector in relation to ML/TF and other crimes;*
- *The company secretary's internal audit and regulatory findings;*
- *Current trends and typologies for other sectors with similar business model or product/service offerings in relation to ML/TF and other crimes;*
- *The number of suspicious transaction reports it has filed with Financial Intelligence and Enforcement Department, Bank Negara Malaysia; and/or*

- *Whether the company secretary has been subjected to service any freeze or seize order by any law enforcement agencies pursuant to AMLA, Dangerous Drugs (Forfeiture of Property) Act 1988, Malaysian Anti-Corruption Commission Act 2009, etc.*

3.5 In considering each risk factor mentioned above, a company secretary is expected to formulate parameters that indicate their risk appetite in relation to the potential ML/TF risks it may be exposed to. The company secretary is expected to set its own parameters according to the size, complexity of its business. Example 1 below is strictly for illustration purpose and is intended to facilitate better understanding on how the risk factors and parameters may be applied. It is **not** intended to serve as a prescription or recommendation on the parameters or specific thresholds to be adopted by the company secretary:

Example 1 for all sectors:

Risk Factor	Examples	Formulated Parameters
Customer	Higher risk customer	• Number of higher risk customers more than 20% of total customer base for a year • Number of politically exposed person (PEP) customers who are high risk is more than 5% of total customers
	Local and foreign customers	• Percentage of local and foreign customer for a year
	Companies with nominee shareholders or shares in bearer form	• Percentage of such companies against total non-individual customer base

Transactions and Distribution Channels	Cash intensive or other forms of anonymous transactions	• High volume of cash transactions above RM50,000 within a year • High volume of anonymous/proxy transactions exceeding RM50,000 per transaction within a year
	Percentage of non-face-to face transactions	• Non-face-to-face transactions exceeding 50% of total transactions
	Frequency and amount of cash payments	• Cash transactions above RM10,000
	Wide array of e-banking products and services	• More than 30% of new accounts are opened via internet, mail or telephone without prior relationship
Findings of NRA	Sectors identified as highly vulnerable to ML/TF risks	• Number of customers with occupation or nature of business from highly vulnerable sectors identified under the NRA
Note: *The above is not meant to serve as exhaustive examples or prescriptions on specific risk factors or parameters which company secretary should apply in assessing the ML/TF risks of the business. Company secretaries are expected to determine which risk factors and parameters are most appropriate in the context of the nature, scale and complexity of their respective businesses.*		

3.6 By applying all the risk factors and parameters in performing its risk assessment, a company secretary should be able to determine the extent of ML/TF risks that it is exposed to, on a quantitative and/or qualitative basis.

3.7 The outcome of the risk assessment would determine the level of ML/TF risks the company secretary is willing to accept (i.e. the company secretary's risk appetite) and its appropriate risk

rating. The risk appetite and risk rating will have a direct impact on the proposed risk management and mitigation policies, controls and procedures adopted by the company secretary.

3.8 Apart from ensuring that the risk assessment is reflected in its policies and procedures, a company secretary is also expected to justify the outcome of the risk assessment conducted. Company secretaries are reminded of the requirement under the AMLA and the AML/CFT and TFS for DNFBPs and NBFIs policy document to maintain proper records on any assessments and approvals by senior management and/or the Board of Directors on the ML/TF risk assessments conducted to enable reviews to be conducted as and when it is requested by the competent authority or supervisory authority.

B. Formulate and implement institutional risk management and mitigation control measures

3.9 Once a company secretary has identified and assessed the ML/TF risks it faces after performing its risk assessment under paragraph 3A above, a company secretary is expected to formulate and implement appropriate risk control measures in order to manage and mitigate those risks.

3.10 The intended outcome is that the mitigation measures and controls are commensurate with the ML/TF risks that have been identified.

3.11 The type and extent of the AML/CFT controls will depend on a number of factors, including:

(a) nature, scale and complexity of the company secretary's operating structure;

(b) diversity of the company secretary's operations, including geographical locations;

(c) types of customers;

(d) products or services offered;

(e) distribution channels used either directly, through third parties or agents or on non face-to-face basis;

(f) volume and size of transactions; and

(g) degree to which the company secretary has outsourced its operations to other entities or at group level, where relevant.

3.12 The following are non-exhaustive examples of the risk controls that a company secretary may adopt:

(a) restrict or limit financial transactions;

(b) require additional internal approvals for certain transactions and products or services;

(c) conduct regular training programmes for directors and employees or increase resources where applicable;

(d) employ technology-based screening or system-based monitoring of transactions; and

(e) employ biometric system for better customer verification.

4. Customer Risk Profiling (CRP)

A. *Determine the risk parameters for customer profiling*

4.1 A company secretary is expected to determine the appropriate risk parameters when considering the risk factors such as customer, country or geographic location, product or service and transaction or distribution channel. These risk parameters will assist the company secretary in identifying the ML/TF risk factors for customers for the purpose of risk profiling. Refer to the example below for illustration purposes:

4.2 Where relevant, a company secretary may adopt similar risk factors and parameters that have been used for the assessment of the ML/TF risks considered under the IRA.

Risk Factor	**Parameters determined for risk profiling**		**Risk Rating**
Customer	Type	Individual	Low
		Company	Medium
		Legal Arrangement	High
	Social Status	Non-PEP	Low
		Local PEP	Medium
		Foreign PEP	High
	Nationality	Malaysia	Low
		Other Countries	Medium
		High-risk or sanctioned countries e.g. North Korea	High
	Country of Residence	Malaysia	Low
		Other Countries	Medium
		High-risk or sanctioned countries e.g. North Korea	High
Transaction or Distribution channel	Face-to-face		Low
	On behalf/Through intermediaries and/or agents		Medium
	Non-Face-to-face		High

Note 1: *The above is not meant to serve as exhaustive examples or prescriptions on specific risk factors or parameters which company secretary should apply for purpose of client risk profiling. Company secretary is expected to determine which risk factors and parameters are most appropriate in the context of the nature and complexity of clients served, product/services offered etc.*

Note 2: *In relation to 'Risk Profiling' while the examples above are based on a sample three-scale rating model (i.e Low, Medium, or High), this is not intended to restrict the client risk rating model adopted by company secretaries, which could be based on more granular approach i.e four-scale or five-scale or more rating model.*

4.3 The different CRP parameters considered within the customer, country or geographic, product and transaction or distribution channel risk factors, may either individually or in combination impact the level of risk posed by each customer.

4.4 Identifying one high risk indicator for a customer does not necessarily mean that the customer is high risk. The CRP ultimately requires a company secretary to draw together all risk factors, parameters considered, including patterns of transaction and activity throughout the duration of the business relationship to determine how best to assess the risk of such customers on an on-going basis.

4.5 Therefore, a company secretary is expected to ensure that the CDD information obtained at the point of on-boarding and on-going due diligence is accurate and up to date.

B. ***Conduct risk profiling on customers***

4.6 Based on the processes under paragraph 4A above, a company secretary is expected to formulate its own risk scoring mechanism for the purpose of risk profiling its customers, e.g. high, medium or low. This will assist the company secretary to determine whether to apply standard or enhanced CDD measures in respect of each customer.

4.7 A company secretary is expected to document the reason and basis for each risk profiling and risk scoring assigned to its customers.

4.8 Accurate risk profiling of its customers is crucial for the purpose of applying effective control measures. Customers who are profiled as higher risk should be subject to more stringent control measures including more frequent monitoring compared to customers rated as low risk.

4.9 While CDD measures and risk profiling of customers are performed at the inception of the business relationship, the risk profile of a customer may change once the customer has commenced transactions. On-going monitoring would assist in determining whether the transactions are consistent with the customer's last known information.

C. Apply customer risk management and mitigation control measures

4.10 Based on the risk profiling conducted on customers, a company secretary is expected to apply the risk management and mitigation procedures, systems and control measures proportionate to the customers' risk profile to effectively manage and mitigate such ML/TF risks.

4.11 Non-exhaustive examples of risk management and mitigation control measures for CRP include:

(a) Develop and implement clear customer acceptance policies and procedures;

(b) Obtain, and where appropriate, verify additional information on the customer;

(c) Update regularly the identification of the customer and beneficial owners,

(d) Obtain additional information on the intended nature of the business relationship;

(e) Obtain information on the source of funds and/or source of wealth of the customer;

(f) Obtain information on the reasons for the intended or performed transactions;

(g) Obtain the approval of senior management to commence or continue business relationship;

(h) Conduct appropriate level and frequency of ongoing;

(i) monitoring commensurate with risks identified;

(j) Scrutinise transactions based on a reasonable monetary threshold and/or pre-determined transaction patterns; and

(k) Impose transaction limit or set a certain threshold.

5. Continuous application of RBA

5.1 The application of RBA is a continuous process to ensure that RBA processes for managing and mitigating ML/TF risks are kept under regular review.

5.2 A company secretary is expected to conduct periodic assessment of its ML/TF risks (preferably every two years or sooner if there are any changes to the company secretary's business model) taking into account the growth of the business, nature of new products/services and latest trends and typologies in the sector.

5.3 Through the periodic assessment, a company secretary may be required to update or review either its IRA or CRP.

5.4 A company secretary is expected to take appropriate measures to ensure that its policies and procedures are updated in light of the continuous risk assessments and ongoing monitoring of its customers.

6. Documentation of the RBA process

6.1 A company secretary is expected to ensure the RBA process is properly documented.

6.2 Documentation by the company secretary is expected to include:

(a) Process and procedures of the RBA;

(b) Information that demonstrates higher risk indicators have been considered, and where they have been considered and discarded, reasonable rationale for such decision;

(c) Analysis of the ML/TF risks and conclusions of the ML/TF threats and vulnerabilities to which the company secretary is exposed to; and

(d) Measures put in place for higher risk indicators and to ensure that these measures commensurate with the higher risks identified.

6.3 In addition, on a case-by-case basis, a company secretary is expected to document the rationale for any additional due

diligence measures it has undertaken compared to the standard CDD approach.

6.4 The documented risk assessment is expected to be presented, discussed and deliberated with the senior management (including the CEO) and the Board of Directors of the company secretary, where applicable.

APPENDIX 8 Institutional Risk Assessment Template

Risk Assessment Template

As required under:

- Section 19 of the AMLA; and
- Paragraphs 10.2 and 10.3 of the AML/CFT and TFS for DNFBPs and NBFIs.

Please also refer to Guidance on Application of Risk-Based Approach Application.

Disclaimer:

- *This document is intended for guidance on the implementation of institutional risk assessment to assist the reporting institution to comply with the requirements of the AMLA only. Company secretaries may develop their own template in consideration of the size, nature and complexity of the business operations.*
- *This document does not contain exhaustive advice or information relating to the subject matter nor should it be used as substitute for legal advice. ☐ In the event that the information on Bank Negara Malaysia's official printed documents or any Acts differ from the information contained within this document, the information on such Act and official documents shall prevail and take precedence.*

In conducting risk assessment i.e. to identify, assess and understand their ML/TF risks at the institutional level, the reporting institution may consider the following examples of risk factors:

a) Overall Business Risk

Identifying higher risk business activities:

No	Main Business Activities	ML Risk	TF Risk	% Contribution to Total Business
1	*E.g. Selling of gold jewelleries including precious stones e.g. diamonds*	*E.g. High*	*E.g High*	*E.g. 90%*

Firm's structure:

No of Branches	
No of Agents	
No of Employees	

Mapping of AMLA requirements to respective division/department/job-scope:

No	AMLA Requirements	Responsible/Related Division/Department/Job Scope	Policies and Procedures?	Awareness Level & Training
1	*E.g. Customer Due Diligence*	*E.g. Front Counter Staff*	*E.g. High*	*E.g. Weak/Inadequate*

a) Product and Services Risk

i. Product

For each product, reporting institution may consider the following risk factors:

No	Risk Factor	
1	Product can be easily transferable to another party	☐ Yes
		☐ No
2	Product's ownership not easily traceable to customer	☐ Yes
		☐ No
3	Product can be easily converted to cash or exchange to another form	☐ Yes
		☐ No
4	Customer can place deposit for a period of time for product purchase	☐ Yes
		☐ No
5	Product can easily be transported or concealed	☐ Yes
		☐ No
6	Product can be used as an alternative form of currency	☐ Yes
		☐ No
7	Product is high value in nature	☐ Yes
		☐ No
8	Customer can purchase product through non-face-to-face channel	☐ Yes
		☐ No
9	Allow use of virtual asset and other anonymous means of payment.	☐ Yes
		☒ No
10	Allow use of unusual mean of payment e.g. high value items such as real estate, precious metals and stones.	☐ Yes
		☐ No
11	Others (Please specify):	

Product risk assessment:	☐ Low	☐ Medium	☐ High

ii. Services

For each service, reporting institution may consider the following risk factors:

No	Risk Factor	
1	Services that allow deposit/payment from third-party/unknown parties	☐ Yes
		☐ No
2	Services that allow transfer of fund to third-party/unknown parties	☐ Yes
		☐ No
3	Services that allow cross-border fund transfer	☐ Yes
		☐ No
4	Services allow customer to deposit/transfer fund through the firm's client account	☐ Yes
		☐ No
5	Services include creation/setting up of complex legal arrangements	☐ Yes
		☐ No

6	Services that are capable of concealing beneficial ownership from competent authorities	☐ Yes ☐ No
7	Services that provide nominee director/shareholders	☐ Yes ☐ No
8	Services that provide anonymity in relation to the client's identity	☐ Yes ☐ No
9	Services are offered through use of agent or intermediary	☐ Yes ☐ No
10	Services that allow the use of shell companies or companies with ownership through nominee shares or bearer shares or control through nominee and corporate directors	☐ Yes ☐ No
11	Customer can acquire services through non face-to-face channel	☐ Yes ☐ No
12	Services allow use of virtual asset and other anonymous means of payment	☐ Yes ☐ No
13	Services allow use of unusual mean of payment e.g. high value items such as real estate, precious metals and stones	☐ Yes ☐ No
14	Others (please specify):	

Services risk assessment:	☐ Low	☐ Medium	☐ High

Overall product and services risk assessment:	☐ Low	☐ Medium	☐ High

b) Customer Risk

No	Risk Factors		Total	Percentage (%)
1	Type of customers	Individual customers		
		Legal persons		
		Legal arrangements		
		Clubs, Societies and Charities		
		Others (Please specify):		
2	Type of occupation for individual customers	Salaried		
		Self-employed – Trading		
		Services		
		Others		
3		Trading		

	Nature and type of business of legal persons	Services			
		Cash intensive business (e.g. retail)			
		Others			
4	Risk Level (based on RI's own customer risk profiling)	Low risk			
		Medium risk			
		High risk			
5	Characteristics of customers	High net worth			
		Domestic PEPs			
		Foreign PEPs			
6	Structure/nature of customer	Legal persons which has complex structure or multiple layer of ownership			
		Legal persons which has nominee relationship			
		Customers that are cash intensive businesses			
		Others (please specify):			
7	Geographical location of customer	Domestic	All local customers		
			From within business area		
			Outstation customers		
		Foreign	All foreign customers		
			Customer from higher risk countries*		
8	Other factors (please specify):				

Overall customer risk assessment:	☐ Low	☐ Medium	☐ High

(c) Geographical Location Risk

		Total	Percentage (%)
Local Headquarters and Branch Location	No of branches including headquarters located at/near tourist hotspots		
	No of branches including headquarters located at/near crime hotspots		
	No of branches including headquarters located at/near country's border		
	No of branches including headquarters located at/near country's entry points		
Foreign Branch Location	No of branches located in higher risk countries		

Geographical location risk assessment:	☐ Low	☐ Medium	☐ High

(d) Transactions and Delivery Channel Risk

No	Risk Factors			Total	Percentage (%)
1	Mode of delivery		Volume of non-face-to-face transactions e.g. online, agents		
			Value of non-face-to-face transactions (RM) e.g. online, agents		
2	Mode of payment	Cash	Volume of cash transaction (no. of cash transaction/total no. of all transaction)		
			Value of cash transaction (total value of cash transaction/total value of all transaction)		
			Average cash transaction (Total value of cash transaction/total no. of cash transaction)		
		Electronic payment	Volume of e-payment (no. of epayment transaction/total no. of all transaction)		

			Value of e-payment transaction (total value of e-payment transaction/total value of all transaction)		
			Average e-payment transaction (Total value of e-payment transaction/total no. of e-payment transaction)		
3	Transaction location	Local	Fund received from outside your business area		
			Fund transferred to outside your business area		
		Foreign	Fund received from outside Malaysia		
			Fund transferred to outside Malaysia		
			Volume of transactions from/to higher risk countries		
			Value of transactions from/to higher risk countries		

Transaction and delivery channel risk assessment:	☐ Low	☐ Medium	☐ High

(e) Total Institutional ML/TF Risk Level

Total Institutional ML/TF Risk Level	☐ Low	☐ Medium	☐ High

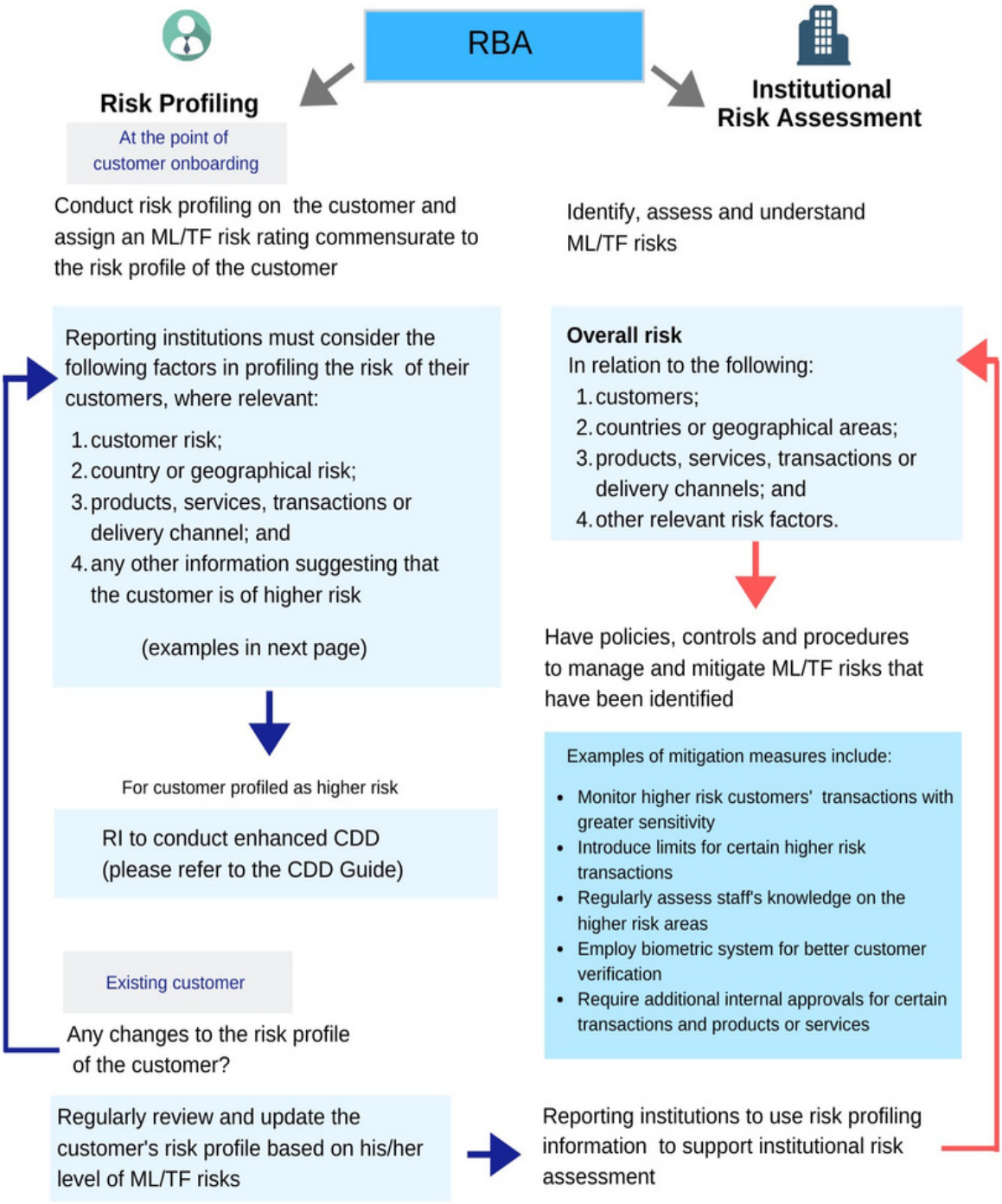
(f) Risk Control and Mitigation

No.	Identified High Risk ML/TF Areas: Product/Services/Locations/Work-Process/Division/Customer or Group of Customers/Transaction Type/Delivery Channel	Proposed Control Measures – Policies, procedures and controls to manage and mitigate ML/TF risks that have been identified
1	*E.g. High exposure to higher risk customers*	*E.g. monitor higher risk customer's transactions with greater sensitivity*
2	*E.g. High exposure to politically exposed persons*	*E.g. employ technology-based screening for effective enhanced due diligence*
3	*E.g. Identified higher risk transactions*	*E.g. introduce limit for identified higher risk transactions*

APPENDIX 9 INFOGRAPHIC ON RISK BASED APPROACH

Risk Based Approach (RBA) Guide

RBA is the process of identifying, assessing and understanding your firm's exposure to the money laundering/ terrorism financing (ML/TF) risks and taking reasonable and appropriate anti-money laundering and counter financing of terrorism (AML/CFT) measures effectively and efficiently to mitigate and manage the risks.



Note: Please refer to Paragraph 10 of the Anti-Money Laundering, Countering Financing of Terrorism and Targeted Financial Sanctions for Designated Non-Financial Businesses and Professions (DNFBPs) & Non-Bank Financial Institutions (NBFIs) (AML/CFT and TFS for DNFBPs & NBFIs)

Risk Factors for Risk Profiling and Institutional Risk Assessment

The risk factors to be considered for risk profiling and institutional risk assessment are generally similar. The difference lies wherein that risk profiling looks at the individual customer, while institutional risk assessment looks at the risks of the firm/ business as a whole.

EXAMPLES OF RISK FACTORS

RISK PROFILING	INSTITUTIONAL RISK ASSESSMENT
Customer risk • Politically exposed person (PEPs) • High net worth customer e.g. customer with assets worth RM3 million and above • Nationality • Customer with large and complex business structure • Involvement of nominee shareholder/ director • Any adverse news on the customer e.g. involvement in investigations or having criminal records	**Customer risk** • What is the **overall** exposure of your firm to higher risk customers?
Product/ service risk • Product/ service provides anonymity • Value/ volume/ type of product/ service not commensurate with the customer profile • Involves nominee services • Involves complex and unusual transactions	**Product/ service risk** • What is the **overall** exposure of your firm to higher risk products/ services?
Geographical risk • Customer connected to or originates from higher risk countries (called by the Financial Action Task Force or Government of Malaysia) • Location of business	**Geographical risk** • What is the **overall** exposure of your firm to geographical risk?
Transaction/ delivery channel risk • Non face-to-face • Cross border transaction • Involves complex and unusual payment methods • Involvement of unknown third parties for payments	**Transaction/ delivery channel risk** • What is the **overall** exposure of your firm to transaction/ delivery channel risk?
	Examples of Additional risk factors: • **Size of business**: Larger size and structurally complex firms are exposed to higher ML/TF risks • **Risks identified in NRA**: Exposure to customers from highly vulnerable sectors pose higher ML/TF risks

(Source of reference: Bank Negara Malaysia)

APPENDIX 10 **INFOGRAPHIC ON COMPLIANCE OFFICER'S ROLE AND RESPONSIBILITIES**

Compliance Officer (CO) Guide

What is the role of CO?

A CO is the **reference point** for anti-money laundering and counter financing of terrorism (AML/CFT) matters within the reporting institution (RI).

A CO is legally required to submit suspicious transaction reports (STRs) on behalf of the RI.

Criteria of CO

- Have sufficient stature, authority and seniority within the RI to participate and be able to effectively influence decisions relating to AML/CFT
- Be fit and proper to carry out AML/CFT responsibilities effectively
- Have necessary knowledge and expertise to effectively discharge roles and responsibilities

What are CO's duties?

1. Ensure RI puts in place **adequate AML/CFT policies and procedures**
2. Ensure **RI's compliance** with the AML/CFT requirements and any other obligations that are imposed under the AMLA, subsidiary legislation and relevant instruments
3. Establish and maintain relevant internal criteria **(red flags)** to enable identification and detection of suspicious transactions
4. Ensure **secure** channel of communication from employees to the CO and information is kept **confidential**
5. Ensure all employees are **aware** of the RI's AML/CFT measures, including policies, control mechanism and reporting channels
6. **Evaluate internal STR appropriately** before promptly submitting to Financial Intelligence and Enforcement Department, Bank Negara Malaysia
7. Regularly **assess** the AML/CFT mechanism i.e control measures and procedures
8. Identify ML/TF risks associated with **new products/ services/ or arising from the RI's operational changes**
9. Ensure **effective implementation** of appropriate AML/CFT policies and procedures

Appointment of CO

Reporting institutions are required to notify Bank Negara Malaysia on the appointment of CO in **writing*** or by completing the **Compliance Officer Nomination Form** which can be found at the relevant appendix of Anti-Money Laundering, Countering Financing of Terrorism and Targeted Financial Sanctions for Designated Non-Financial Businesses and Professions (DNFBPs) & Non-Bank Financial Institutions (NBFIs) (AML/CFT and TFS for DNFBPs & NBFIs Policy Document) within 10 working days on the appointment or change in the appointment of CO via any of the following methods:

E-mail: fied@bnm.gov.my
Mail: Director
Financial Intelligence and Enforcement Department
Bank Negara Malaysia
Jalan Dato' Onn
50480 Kuala Lumpur
Fax: 03-26910368

* Please include details such as name, designation, office address, office telephone number, fax number, e-mail address

Note: Please refer to Section 19 of the Anti-Money Laundering, Countering Financing of Terrorism and Targeted Financial Sanctions for Designated Non-Financial Businesses and Professions (DNFBPs) & Non-Bank Financial Institutions (NBFIs) (AML/CFT and TFS for DNFBPs & NBFIs Policy Document)

(Source of reference: Bank Negara Malaysia)

APPENDIX 11 INFOGRAPHIC ON CUSTOMER DUE DILIGENCE

Customer Due Diligence (CDD) Guide

When to conduct CDD?

1. Establishing Business Relations

You are required to conduct CDD at the point of establishing a business relationship with your customer.

2. Carrying Out Any or Occasional Transaction involving the Circumstances or Amount as Specified under Paragraphs 14A to 14H of the Policy Document

LICENSED CASINO

Any transaction equivalent to **RM10,000** and above. This includes circumstances where the transaction is carried out in a single transaction or several transactions in a day that appear to be linked

LICENSED GAMING OUTLETS

Customer's winning equivalent to **RM50,000** and above, including in situations where the transaction is carried out in a single transaction or through several transactions that appear to be linked

MONEYLENDERS

When giving out financing equivalent to **RM3,000** and above, including in situations where the transaction is carried out in a single transaction or through several transactions, in a day that appear to be linked

PAWNBROKERS

Pledge amount equivalent to **RM3,000** and above, including in situations where the transaction is carried out in a single transaction or through several transactions, in a day that appear to be linked

DEALERS IN PRECIOUS METALS OR PRECIOUS STONES

Any cash transaction equivalent to **RM50,000** and above with the customer, or any other amount as may be specified by the competent authority. This includes:

- Transaction conducted in a single transaction or through several transactions in a day that appear to be linked and across all branches of the reporting institution; and
- Aggregate payments over a period of time for a single purchase

GATEKEEPERS (lawyers, accountants, company secretaries and trust companies)

When preparing or carrying out any of the Gazetted Activities for their clients
(Please refer to the Policy Document for further details)

REGISTERED ESTATE AGENTS

To conduct CDD on both purchaser and seller, or landlord and tenant of the property

3. Suspicion of money laundering or terrorism financing (ML/TF)

When you have any suspicion of (ML/TF) regardless of the amount or thresholds

4. Doubt

When you have any doubt about the accuracy or adequacy of previously obtained information on a particular customer

Note: Please refer to Section 16 of the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLA) and Paragraph 14 of the Anti-Money Laundering, Countering Financing of Terrorism and Targeted Financial Sanctions for Designated Non-Financial Businesses and Professions (DNFBPs) & Non-Bank Financial Institutions (NBFIs) (AML/CFT and TFS for DNFBPs & NBFIs Policy Document)

What are specific information needed based on the customer type?

To comply with the CDD requirements, you are required to identity the customer and verify the customer's identity using reliable and independent documentation, electronic data or any other measures that you deem necessary.

1 INDIVIDUAL CUSTOMER AND BENEFICIAL OWNER

- Name
- NRIC / Passport number
- Residential and mailing address
- Date of birth
- Nationality
- Occupation type
- Name of employer or nature of self-employment / nature of business
- Contact number
- Purpose of transaction

2 LEGAL PERSON (LP), LEGAL ARRANGEMENT (LA) AND CLUB, SOCIETY AND CHARITY (CSC)

Step 1 Understand the nature of the customer's business, its ownership and control

Step 2 Identify the customer and verify its identity through the following information:

Legal Person
e.g. company/ business

- Name, legal form and proof of existence;
- Company/ business registration number;
- Powers that regulate and bind the customer, as well as persons having senior management position;
- Business and registered address;
- Any persons authorised to represent the company/ business; and
- Nature of business

Legal Arrangement
e.g. trust

- Name, legal form and proof of existence;
- Powers that regulate and bind the customer, as well as persons having senior management position; and
- Business address and address of the trustee's registered office

Club, Society and Charity
e.g. *persatuan, yayasan*

- Pursuant to CDD undertaken on LP or LA, where relevant; and
- Office bearer or any person authorised to represent the CSC

Examples of verification documents

- Certificate of Incorporation
- Constitution
- Directors' Resolution
- Partnership Agreement
- Trust Deed
- Certificate of Registration
- Identification Documents of Office Bearers

Step 3 **Identify and take reasonable measures to verify the identity of beneficial owners through the following information:**

Who is a Beneficial Owner (BO)?

- Refers to any **natural person(s) who ultimately OWNS or CONTROLS a customer and/or the natural person on whose behalf a transaction is being conducted**
- Also includes those **natural persons who exercise ULTIMATE EFFECTIVE CONTROL** over a legal person or arrangement

'Ultimately owns or controls' or 'ultimate effective control' refers to situations in which ownership or control is exercised through a chain of ownership or by means of control other than direct control

Legal Person

A. Identity of the **natural person(s)** who ultimately has a controlling ownership interest in a legal person. At a minimum, this includes:

>25% Identification of directors/ shareholders with **equity interest of more than 25%;**

B. If there is doubt on the controlling ownership interest - the identity of the **natural person** exercising control through other means; **AND**

C. When there is no **natural person** identified under **A** or **B** above, the identity of the **natural person** who holds the senior management position

Legal Arrangement

A. Identity of:

- Settlor;
- Trustee(s);
- Protector (if any);
- Beneficiary or class of beneficiaries; and
- Any other **natural person exercising ultimate effective control over the trust** (including through chain of control / ownership)

B. For other types of LA, the identity of persons in equivalent or similar positions

Club, Society and Charity

A. Pursuant to CDD undertaken on LP or LA, where relevant;

B. Identity of other members with effective control of the CSC

Examples of Other Means by which Natural Persons Exercise Control on LP, LA or CSC

Contractual associatons or personal connections with management or directors

Recipient of loan or other benefit (e.g. tenancy of property / licence to property) having conditions granting control rights

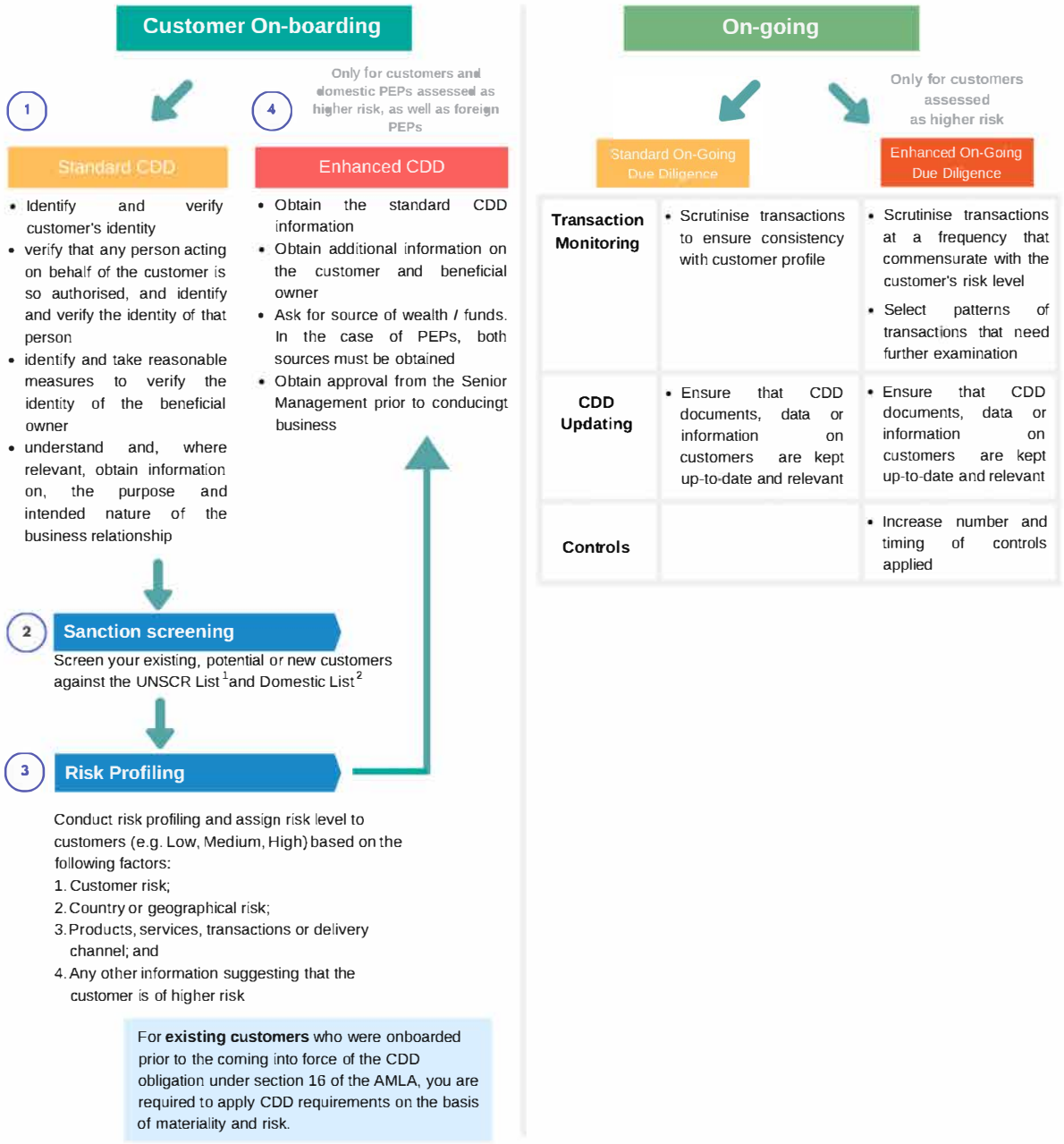
Other ability to exert significant influence on corporate activity (e.g. veto rights, decision rights, right to profit, etc)

Other ownership arrangements (e.g. nominees, joint ownership arrangements)

Management control (the right to appoint or remove majority of directors)

Ownership of voting rights

Customer Due Diligence (CDD) Process Flow



1 **Consolidated UNSCR List:** https://www.un.org/securitycouncil/content/unsc-consolidated-list
2 **Domestic List:** http://www.federalgazette.agc.gov.my

Note: Please refer to Section 16 of the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLA) and Paragraph 14 of the Anti-Money Laundering, Countering Financing of Terrorism and Targeted Financial Sanctions for Designated Non-Financial Businesses and Professions (DNFBPs) & Non-Bank Financial Institutions (NBFIs) (AML/CFT and TFS for DNFBPs & NBFIs Policy Document)

(Source of reference: Bank Negara Malaysia)

Suspicious Transaction Report (STR) Guide

What is an STR?

STRs are documents that reporting institutions are required to submit when having suspicion that a customer is involved in **money laundering (ML), terrorism financing (TF) or other serious crimes**

Why submit STRs?

STRs provide law enforcement agencies valuable information/ intelligence of potential crime activities

When to submit STRs?

Regardless of the amount being transacted, you are required to promptly submit an STR, whenever you suspect or have reasons to suspect that the transaction (including attempted transactions):

- appears unusual
- has no clear economic purpose
- appears illegal
- involves proceeds from an unlawful activity or instrumentalities of an offence
- indicates that the customer is involved in ML/TF

How do you recognise suspicious transactions?

1. **Screen** customer account
2. **Ask** customer appropriate questions
3. **Find** out customer's record/ review known information
4. **Evaluate** information gathered and consider to submit an STR

You are also required to establish **red flags** relevant to your business or service to facilitate the detection of suspicious transactions.
Examples of red flags are provided in the Policy Document.

DO

- Ensure that STRs are submitted within the next working day, from the date the Compliance Officer establishes the suspicion
- Establish reporting mechanism for submission of STR
- Establish policies on the duration for Compliance Officer to review internal STRs
- Ensure that STR is treated with utmost confidentiality

DON'T

- Disclose submission of STRs to anyone else, except under certain circumstances (refer to Section 14A of Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLA) and Paragraph 20 of the Policy Document)
- Tip off the person(s) being reported - do treat them as normal clients so they do not suspect that STRs have been filed on them

How to submit STRs?

1. Fill up the STR form, which can be found at www.amlcft.bnm.gov.my or the relevant appendix of the Anti-Money Laundering, Countering Financing of Terrorism and Targeted Financial Sanctions for Designated Non-Financial Businesses and Professions (DNFBPs) & Non-Bank Financial Institutions (NBFIs) (AML/CFT and TFS for DNFBPs & NBFIs Policy Document)

2. The Compliance Officer of the reporting institution to submit the STR via any of the following methods:

a) **Mail**: Director
Financial Intelligence and
Enforcement Department
Bank Negara Malaysia
Jalan Dato' Onn
50480 Kuala Lumpur
(To be opened by addressee only)

b) **Fax**: +603-26933625

c) **Email**: str@bnm.gov.my

d) **FINS platform** (where applicable):
https://bnmapp.bnm.gov.my/fins2

Note: Please refer to Section 14 of the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 and Paragraph 19 of the Anti-Money Laundering, Countering Financing of Terrorism and Targeted Financial Sanctions for Designated Non-Financial Businesses and Professions (DNFBPs) & Non-Bank Financial Institutions (NBFIs) (AML/CFT and TFS for DNFBPs & NBFIs Policy Document)

(Source of reference: Bank Negara Malaysia)

APPENDIX 13 INFOGRAPHIC ON TARGETED FINANCIAL SANCTIONS

Targeted Financial Sanctions on Terrorism Financing, Proliferation Financing and Other UN-Sanctions Regimes Guide

Targeted financial sanctions are measures for asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of specified entities/ designated persons who are being sanctioned.

Terrorism financing is the act of providing financing for terrorist acts, and for terrorists and terrorist organisations, through legitimate or illegitimate sources.

Proliferation financing is the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.

Other UN-Sanctions Regimes refer to any other United Nations Sanctions Committee (UNSC) sanctions regimes in relation to upholding of peace and security, and prevention of armed conflicts and human right violations.

WHAT DO YOU NEED TO DO?

1 MAINTAIN & UPDATE SANCTIONS LISTS

You are required to maintain a sanctions database on the United Nations Security Council Resolutions (UNSCR) List and Domestic List.

The UNSCR List and Domestic List contain names and particulars of persons designated as specified entities/ designated persons by the UNSC and the Minister of Home Affairs (MOHA), respectively.

You may refer to the lists from the following websites:

- **Consolidated UNSCR List:** https://www.un.org
- **Domestic List**: http://www.federalgazette.agc.gov.my

You are required to update the database upon publication of designation or specification by the UNSC or MOHA

2 NAME SCREENING & DUE DILIGENCE

You are required to conduct sanctions screening on **existing, potential or new customers** (including beneficial owners and beneficiary) against the sanctions lists.

- Ensure that potential matches are true matches and not false positives

Conduct due diligence on **related parties** (refer FAQ)

3 FREEZE/ REJECT

In the event of positive name match, you are required to, immediately and without delay:

- Reject transactions for **new/ potential** customers
- Freeze funds/ properties for **existing** customers
- Block transactions (where applicable)

4 REPORT

In the event of positive name match, you are required to immediately:

- Report to the Financial Intelligence and Enforcement Department (FIED), Bank Negara Malaysia and Inspector-General of Police (where relevant)
- Submit Suspicious Transaction Report (STR) to FIED

You should also submit STRs when suspecting that an account or transaction (including attempted transaction) is linked to a specified entity / designated person / related party

WHAT TO DO WITH FUNDS/ PROPERTIES BELONGING TO SANCTIONED INDIVIDUALS?

The funds and properties may continue receiving deposits, dividends, interests, bonuses or other benefits. However, such funds and benefits must remain frozen as long as the specified entities / designated persons continue to be listed under the UNSCR List and Domestic List.

Where the freezing is made in relation to **terrorism financing**,

- Any dealings with the frozen funds or properties, whether by the specified entity, related parties or any interested party, requires prior written authorisation from the Minister of Home Affairs.
- You may advise the customer, a related party or any interested party of the frozen funds or properties to make an application to the Minister of Home Affairs to allow exemption for basic and extraordinary expenditures e.g. rent, medicine, etc.
- You shall only proceed with the payments upon receiving written authorisation from the Minister of Home Affairs.

Where the freezing is made in relation to **proliferation financing and other UN-sanctions**,

- Any dealings with frozen funds, other financial assets, or economic resources, whether by the designated country, person, identified related parties or interested parties, require prior written authorisation from the Strategic Trade Controller (STC) under the Strategic Trade Act (STA)
- You may advise the customer, a related party or any interested party of the frozen funds, other financial assets or economic resources, or to the blocked or rejected transaction, to make an application to the STC under the STA to allow exemptions on basic and extraordinary expenditures and to allow payments due under contracts entered into prior to the designation.
- You shall only proceed with the payment only upon receiving the prior written authorisation and confirmation of the STC under the STA.

WHO SHOULD YOU REPORT TO AND HOW?

Terrorism Financing

(Upon determination of name match against **Domestic List, UNSCR 1988 and 1267 lists**)

	1 Upon Determination	2 Periodic Reporting
Frequency	Immediately after determination of a positive name match	For positive name match against: • ***UNSCR Lists*** Every 5 January and 5 July • ***Domestic List*** Every 15 May and 15 Nov Not required for customers who conduct one-off transactions and where the customers do not maintain an account with the reporting institution
Recipient	FIED, Bank Negara Malaysia & Inspector-General of Police	FIED, Bank Negara Malaysia
Form	Appendix 6A or 6B, where applicable	Appendix 7A or 7B, where applicable

Proliferation Financing and Other UN-Sanctions Regimes

(Upon determination of name match against **UNSCR 1718 and 2231 lists**)

	1 Upon Determination	2 Periodic Reporting
Frequency	Immediately after determination of a positive name match	Only if there is any changes to the frozen funds (after first time reporting on positive name match) and latest by 15 January of the following calendar year Not required for customers who conduct one-off transactions and where the customers do not maintain an account with the reporting institution
Recipient	FIED, Bank Negara Malaysia	FIED, Bank Negara Malaysia
Form	Appendix 6A or 6B, where applicable	Appendix 7A or 7B, where applicable

FREQUENTLY ASKED QUESTIONS (FAQ)

1 Who are "related parties"?

- Persons related to the properties and funds that are wholly or jointly owned or controlled, directly or indirectly, by specified entities/ designated persons; and
- Persons acting on behalf or at the direction of specified entities/ designated persons

2 Can the RI accept loan repayments from specified entities/ designated persons?

If the loan agreement was made prior to the listing of the specified entity/ designated person on the sanction lists, you may continue to receive the loan repayments on the agreement

Note: Please refer to paragraphs 23 and 24 of the Anti-Money Laundering, Countering Financing of Terrorism and Targeted Financial Sanctions for Designated Non-Financial Businesses and Professions (DNFBPs) & Non-Bank Financial Institutions (NBFIs) (AML/CFT and TFS for DNFBPs & NBFIs Policy Document)

(Source of reference: Bank Negara Malaysia)

PART E
RED FLAGS

APPENDIX 14 EXAMPLES OF RED FLAGS

Examples of Red Flags/Triggers for suspicion

Disclaimer:
These examples of red flags are intended as guidance in complying to the AMLA only. Company secretaries are required to establish internal red flags to detect suspicious transactions.

Generic red flags

A. *Red Flags involving Customers who are Individuals*

1. Customer refuses to provide information required by the company secretary, attempts to minimise the level of information provided or provides information that is misleading or difficult to verify

2. Client who avoids personal contact without logical explanation

3. Financial activities and transactions of the customer are inconsistent with the customer profile

4. Unexplained inconsistencies arising from the process of identifying or verifying the customer

5. Customer insists on the use of an intermediary (either professional or informal) without logical justification

6. Customer who has previously been convicted for any serious crime

7. Customer who is under investigation or has known connections with criminals

8. Customer uses multiple bank accounts (from domestic or foreign jurisdiction) to complete a transaction without logical explanation

9. Customer provides falsified records or counterfeit documentation

10. Customer conducts large or frequent transactions using foreign currency without any economic rationale

11. Customer is unusually concerned and/or makes inquiries about the AML/CFT requirements and internal compliance policies, procedures or controls

B. Red Flags involving Customers who are Legal Persons or Legal Arrangements

1. Legal person which demonstrated a long period of inactivity following incorporation, followed by a sudden and unexplained increase in activities

2. Legal person which is registered under a name that indicates that the company performs activities or services that it does not provide without good reason

3. Legal person or legal arrangement which is registered under a name that appears to mimic the name of other companies, particularly high-profile multinational corporations without good reason

4. Legal person or legal arrangement which is registered at an address that does not match the profile of the company without good reason

5. Legal person or legal arrangement which is registered at an address that is also listed for numerous other companies or legal arrangements, indicating the use of a mailbox service without good reason

6. Where the director or controlling shareholder(s) cannot be located or contacted

7. Where the director or controlling shareholder(s) do not appear to have an active role in the company without logical explanation

8. Where the director, controlling shareholder(s) and/or beneficial owner(s) are listed against the accounts of other legal persons or arrangements, indicating the use of professional nominees

9. Legal arrangement or trust which declared an unusually large number of beneficiaries or controlling interests

10. Legal person, legal arrangement or trust which authorised numerous signatories without logical explanation or business justification

11. Legal person or legal arrangement which is incorporated/formed in a jurisdiction that is considered to pose high ML/TF risk

12. Legal person which conducts financial activities and transactions inconsistent with its corporate profile

13. Legal person which involves multiple shareholders who each hold an ownership interest just below the identification of beneficial ownership threshold

14. Legal person which has indication of being used as a shell company e.g. use of informal nominees, no real business activities undertaken, does not have physical presence

15. Media or other reliable sources suggest that the customer may be linked to criminal activity

C. Red Flags involving Transactions

1. Transactions conducted are questionable, or generate doubts that cannot be sufficiently explained by the client
2. Transaction involves the use of multiple large cash payments without logical explanation
3. Customer regularly conducts transactions with international companies without sufficient corporate or trade justification
4. Frequent and cumulatively large transactions without any apparent or visible economic or lawful purpose
5. Payments received for products/services from a third party who is not the owner of the funds, without any apparent reasons
6. Transactions that require the use of complex and opaque legal entities or legal arrangements without logical explanation
7. Transactions or instructions involve unnecessary complexity or which do not constitute the most logical, convenient and secure way to do business
8. High volume of transactions within short period of time without economic purpose or commercial justification
9. Unnecessary routing of funds or payments from/to/through third party account without logical explanation
10. Transactions conducted via multiple payments from the same or different accounts/mode of payment which are broken down into smaller amounts without logical explanation
11. Transactions which are conducted hastily or without due consideration a person would normally give to such transactions

D. Red Flags involving Geographical Location

1. Large numbers of incoming or outgoing fund transfers take place for no logical business or other economic purpose, to or from locations of ML/TF concern
2. Legal persons or legal arrangements are incorporated/formed in a jurisdiction that has ML/TF concern
3. Customer has unexplained geographic distance from the company secretary

E. Red Flags involving Delivery Channel

1. Use of a third party to avoid personal contact without logical explanation

Sector Specific Red Flags

Company Secretaries

1. A significant increase in capital for a recently incorporated company or successive contributions over a short period of time to the same company
2. Receipt by the company of an injection of capital or assets that is high in comparison with the business, size or market value of the company
3. A large financial transaction, especially if requested by a recently created company, where it is not justified by the corporate purpose, the activity of the client or its group companies
4. Provision of nominee director or shareholder services without a clear and legitimate commercial purpose or some reasonable justification

5. Use of shell companies where foreign ownership is spread across multiple jurisdictions
6. Family members with no role or involvement in the running of the business are identified as beneficial owners of legal persons
7. Client receives large sums of capital funding quickly following incorporation/formation, which is spent or transferred elsewhere in a short period of time without commercial justification
8. Client has multiple shareholders who each hold an ownership interest just below the identification of beneficial ownership threshold
9. Client makes frequent payments to foreign professional intermediaries without any logical reasons or without commercial justification
10. Clients are interested in foreign company formation, particularly in jurisdictions known to offer low-tax or secrecy incentives, without commercial explanation
11. Company with complex structures or multiple layers of shareholders, i.e. intertwining with multiple legal persons or legal arrangements without logical explanation
12. Transactions occurring between two or more parties that are connected without an apparent business rationale
13. Business transaction that involves family members of one or more of the parties without a business rationale
14. Large or repeat transaction, and the executing customer is a signatory to the account, but is not identified as having a controlling interest in the company or assets

15. Transactions executed from a business account but appears to fund personal purchases, including the purchase of assets or recreational activities that are inconsistent with the company's profile

16. Transaction executed from a business account and involves a large sum of cash, either as a deposit or withdrawal, which is inconsistent with the company's profile

17. Clients are interested in foreign company formation, particularly in jurisdictions known to offer low-tax or secrecy incentives, without commercial explanation