



Cambodia Financial Intelligence Unit

Unofficial Translation

N° B12.022.008.S.K.N.N

Directive
On
Internal Controls for Reporting Entity

Pursuant to the Law on Anti-Money Laundering and Combating the Financing of Terrorism promulgated by the Royal Kram No. NS/RKM/0620/021 dated 27 June 2020 the Cambodia Financial Intelligence Unit (CAFIU) issues Directive on Internal Controls for Reporting Entity.

1. Scope

This Directive shall apply to reporting entity referred to in Article 4 of the Law on Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT). This Directive should also applicable to reporting entity that are part of a financial group or reporting entity that have foreign branches or majority owned subsidiaries.

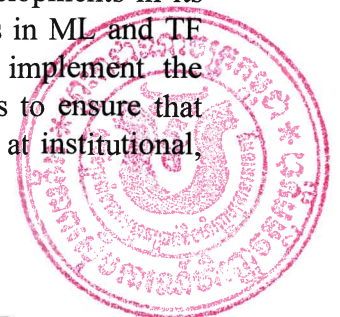
2. Risks and Internal Controls

2.1. The reporting entity shall be aware of and understand the ML/TF risks that are required to be assessed in accordance with Article 8 of the Law on AML/CFT and relevant regulations. The reporting entity shall ensure that the result of risk assessment is disseminated, for information and training purposes, to all staffs and senior managements.

2.2. The reporting entity shall ensure that internal policies, procedures and system and controls for AML/CFT are in place and effectively implemented. The internal policies, procedures and system and controls shall detail customer due diligence (CDD) procedures, risk management practices, record keeping requirements, on-going CDD requirements, procedures for reporting transactions and other relevant requirements as required by the Law on AML/CFT in compliance with legal requirements and commensurate with the nature and size of the reporting entity, complexity of operations and the assessed levels of ML/TF risk.

2.3. The reporting entity shall oversee and review internal policies, procedures and system and controls of the overall AML/CFT policies, procedures and controls.

2.4. The reporting entity shall review and assess regularly and keep up to date the internal policies, procedures and system and controls in line with the changes and developments in its products, services, delivery channels and technology systems, as well as trends in ML and TF techniques at both sectoral and national levels. The reporting entity shall implement the necessary changes to the internal policies, procedures and system and controls to ensure that they are sound and appropriate and commensurate with currently assessed risk at institutional, sectoral and national levels.



2.5. The reporting entity shall ensure that an independent internal and external audit is regularly undertaken that reviews the adequacy of the internal policies, procedures and system and controls having regard to the requirements of laws and regulations related to AML/CFT and the effectiveness of their implementation.

2.6. The reporting entity shall ensure that the roles and responsibilities of the independent internal auditor are clearly defined and documented and at least include:

- a) testing the effectiveness of the internal policies, procedures and system and controls;
- b) reporting on the adequacy of AML/CFT control mechanisms including the appointment of compliance officer, training and awareness programs for staff, where relevant, its agents and distributors, employee screening mechanisms and AML/CFT internal audit manual; and
- c) reporting on whether measures put in place are in line with current developments and changes of the relevant AML/CFT requirements.

2.7. The reporting entity shall ensure that audit findings are reported on a regular basis. The audit report shall highlight inadequacies of any AML/CFT measures and control systems within the reporting entity. The reporting entity shall ensure that necessary steps are taken to rectify the situation.

2.8. The reporting entity shall put in place an adequate management information system for identifying, detecting and scrutinizing business relationships and occasional transactions, that they suspect or have reasonable grounds to suspect that such relationship is related to proceeds from an unlawful activity or the customer involving ML or TF. The management information system shall provide reporting entity timely information on a regular basis to enable them to detect and report suspicious activities.

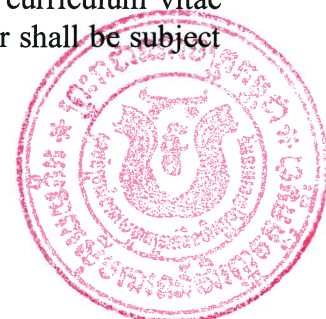
2.9. Reporting entity shall ensure that the reporting system put in place for the detection and submission of suspicious transaction reports and/or relevant documents to CAFIU is operated in a secured and confidential manner.

3. Employee Integrity

Reporting entity shall ensure that an employee assessment system is established to adequately screen and assess its employees, both existing and new, to ensure that the competency and the integrity of its employees are not compromised. The employee assessment system shall at least examine and record personal information including criminal records, employment and financial history as well as regulatory and supervisory actions against, of its employees as part of the recruitment process and existing employees.

4. Anti-Money Laundering and Combating the Financing of Terrorism Compliance Officer

4.1. Reporting entity shall appoint a compliance officer and attach his/her curriculum vitae pursuant to Article 17 of Law on AML/CFT. The appointed compliance officer shall be subject to an approval from CAFIU. *spM*



4.2. Reporting entity shall inform the CAFIU upon the change in the appointment or resignation of the compliance officer and designate a senior officer to be temporary contact point with CAFIU in order to ensure continuity of the AML/CFT obligations. The reporting entity shall submit the appointment of new compliance officer for approval from CAFIU within 1 (one) month after the change in the appointment or resignation of the compliance officer.

4.3. Reporting entity shall ensure that the roles and responsibilities of the compliance officer are clearly defined and documented. The roles and responsibilities of the AML/CFT compliance officer should include at least ensuring:

- a) implementation of the AML/CFT policies;
- b) the establishment, development and effective implementation of appropriate AML/CFT procedures including customer acceptance policy, CDD, risk management practice, record keeping, on-going monitoring, reporting of transactions and other relevant requirements of the Law on AML/CFT;
- c) regular monitoring and assessment of AML/CFT methods to ensure that AML/CFT internal policies, procedures and system and controls are sufficient to address the changing methods and trends of predicate offence and money laundering and financing of terrorism;
- d) the channel of communication between the compliance officer and employees and/or other relevant employees is secured and that any information is kept confidential;
- e) all employees are aware of AML/CFT measures including policies, procedures, control mechanisms and channels of reporting to ensure the effectiveness of such measures;
- f) the identification of money laundering and financing of terrorism risks associated with new products or services, delivery channel or arising from the reporting entity's operational changes, such as the introduction of new technology and processes.
- g) submission of transaction reports as set in Article 12 of the Law on AML/CFT to CAFIU;
- h) management of the ongoing ML/TF risk assessment process; and
- i) employee performance of pursuant to the requirements of policy, procedure, law and regulation related to AML/CFT and CAFIU recommendations.

4.4. Compliance officer shall have necessary knowledge, expertise and experiences to responsibly and effectively discharge his/her roles and responsibilities that shall not be interfered by any person. The compliance officer should have access and rights to have all documents and information from units, subsidiaries, and branches related to customer account and transactions.

4.5. The AML/CFT policies and procedures of reporting entity shall permit the compliance officer to directly obtain reports of unusual activities from relevant employees even if he/she



does not know precisely what the underlying unlawful activity is or whether such activities have occurred. Once this report is satisfied with the requirement in Article 12 and Article 13 of the Law on AML/CFT, the compliance officer shall submit the suspicious transaction report to CAFIU.

5. Staff Training and Awareness Programs

5.1. Reporting entity shall have an adequate ongoing awareness and training programs on AML/CFT for its employees, where relevant, its agents and distributors, that are commensurate with the size of the reporting entity's business and its level of ML and TF risk. The training and awareness programs must be extended to all new and existing employees.

5.2. The AML/CFT training programs shall ensure the effective implementation of AML/CFT policies and procedures and the understanding of ML/TF risks associated with the reporting entity.

5.3. Reporting entity shall ensure that proper channels of communication are in place to inform all levels of employees in reporting entity, agents and distributors of the applicable AML/CFT policies and procedures.

5.4. Reporting entity shall ensure that employees are aware of AML/CFT policies, internal controls and manual in place and the requirements as specified in laws and regulations related to AML/CFT.

5.5. The reporting entity shall develop and update internal AML/CFT manual which at least contains:

- a) the laws and regulations related to AML/CFT;
- b) the FATF Recommendations and Interpretive Notes; and
- c) Other guidelines or procedures issued by CAFIU

5.6. The reporting entity shall adapt at least the following training packages for the various sectors of employees within their institutions:


a) New Employees

A general background to laws and regulations on AML/CFT and ML/TF theories.

b) Front-Line Employees

Employees who deal directly with the customers shall be trained at least in identifying transactions, the measures to be taken once a transaction is deemed to be suspicious, factors that may give rise to suspicions, large volume transaction reporting and enhanced customer due diligence.

c) Employees - Account Opening/New Customers

Employees, who are responsible for account opening or the acceptance of new customers, shall receive the equivalent training given to front-line employees and shall at least be trained in customer identification and verification, opening of accounts and establishing business relationship with customers. 



d) Supervisors and Managers

Supervisors and managers shall receive a higher level of instruction covering all aspects of AML/CFT including law, regulations, policies, and procedures of which include the penalties for non-compliance to the AML/CFT requirements.

5.7. These training and awareness programs shall be regularly conducted and kept up to date with refresher courses provided for employees. New employees shall be trained within 3 (three) months after the commencement of employment and front-line employees, supervisors and managers shall have at least refresher training annually.

6. Targeted Financial Sanctions Against the Financing of Terrorism

6.1 Reporting entity shall take the necessary measures to ensure compliance with the United Nations Security Council (UNSC) Resolutions and relevant regulations and legislation on targeted financial sanctions against the financing of terrorism.

6.2 Reporting entity shall extend the suspicious transaction report mechanism to cover the financing of terrorism or property or funds or other services that is suspected to be subject to targeted financial sanctions.


6.3 Reporting entity shall maintain a record of names and particulars of terrorists in the United Nations list and any terrorists designated by the authorities of Cambodia and they shall consolidate records with the other recognized lists of designated persons. Information contained in the records shall be updated and relevant and made easily accessible to employees for the purpose of identifying suspicious transactions and freezing accounts, funds or other services.

6.4 Reporting entity shall conduct checks of the names of new and existing customers against the names in the United Nations and domestic lists of designated terrorists. If there is a name match, the reporting entity shall verify and confirm the identity of its customer. If the customer and the person listed in the records are the same person, the reporting entity shall, without delay and without prior notice, freeze the customer's property, funds or other services pursuant to the law and regulation and relevant court orders and promptly inform the CAFIU. Where reporting entity suspect that a transaction is terrorist or terrorism financing related, it shall make a suspicious transaction report to the CAFIU.

7. Foreign Branches and Subsidiaries

7.1 Reporting entity that are or are part of a financial group or reporting entity that have foreign branches or majority owned subsidiaries shall implement the group wide programs.

7.2 A group wide program shall incorporate:

- a) all requirements set from point 2 to point 6 of this Directive;
- b) policies and procedures for sharing information between members of the group for the purposes of undertaking CDD and ML/TF risk management;
- c) provision of customer information at group level of audit, compliance and ML/TF risk management and mitigation. This provision shall be conducted for the purpose of AML/CFT; and 



- d) policies and procedures to maintain the confidentiality, appropriate use of the information exchanged between group members and to prevent tipping-off.

7.3 Reporting entity that have foreign branches and majority owned subsidiaries must require such branches and subsidiaries to implement AML/CFT measures that are consistent with the requirements imposed by the Law on AML/CFT and this Directive:

- a) where the laws of the countries in which a foreign branches or majority owned subsidiaries of a reporting entity located are more stringent than the Law on AML/CFT and this Directive, the reporting entity shall implement the AML/CFT requirements in foreign countries when it was permitted by CAFIU.
- b) where the AML/CFT requirements of the countries in which the foreign branches or majority owned subsidiaries located are less stringent than those imposed in Cambodia, reporting entity shall require the foreign branches or majority owned subsidiaries implement the AML/CFT requirements in Cambodia unless it was permitted by the laws of the countries in which their foreign branches and majority owned subsidiaries operate.
- c) In the event that the laws of the countries in which a foreign branches or majority owned subsidiaries of a reporting entity do not permit the foreign branches or majority owned subsidiaries to comply with AML/CFT requirements in Cambodia, financial groups shall:
 - i. devise appropriate additional measures to manage and mitigate the ML/TF risks, and
 - ii. notify CAFIU.

7.4 The requirements of Article 15 of the Law on AML/CFT do not prevent confidential communications between reporting entity that are part of the same group that may be required for the implementation of point 7.2 (b) and (c) of this Directive. Reporting entity shall put in place mechanisms for sharing and using information in the same group to ensure security and confidentiality protection of information.

8. Supervisory Powers

To ensure CAFIU to perform their role and responsibilities pursuant to Article 23.2 of the Law on AML/CFT, the reporting entity shall respect the power of CAFIU as follow:

- a) enter the premises of a reporting entity for the purpose of inspecting, copying or gaining possession any document or records or other information or things;
- b) request a reporting entity to produce any necessary document, reports, records or others; and
- c) requires management, officer or employee of a reporting entity to provide any indispensable information or assistance. *Sy M*



9. Sanction

Any reporting entity which do not comply with this Directive shall be penalized as stated in Article 36 and Article 37 of the Law on AML/CFT.

Up on receiving this directive, all reporting entities shall effectively implement this Directive from the date of the signature. *sp*

Phnom Penh, 11 January 2022

Cambodia Financial Intelligence Unit

Head *sp*

(Signed and Sealed)

SAY SAM ATH

Attention to:

- Office of the Council of Ministers
- National Coordination Committee on Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Proliferation
- Cambodia Financial Intelligence Unit's Board of Directors
- Documentations-Archives

