RULE

Effective Compliance Programme for the Prevention and Detection of Money Laundering, Terrorist Financing and Proliferation Financing for Financial Services Providers

xxxx 2026

Table of Contents

List of Acronyms

AML	Anti-Money Laundering
AMLCO	Anti-Money Laundering Compliance Officer
AMLR	Anti-Money Laundering Regulations
CDD	Customer Due Diligence
CFT	Countering the Financing of Terrorism
CIMA	Cayman Islands Monetary Authority
CPF	Counter Proliferation Financing
CRF	Compliance Reporting Form
DMLRO	Deputy Money Laundering Reporting Officer
EDD	Enhanced Due Diligence
e-KYC	Electronic Know Your Customer
FRA	Financial Reporting Authority
FSP	Financial Service Providers
KYC	Know Your Customer
MAA	Monetary Authority Act
ML/TF/PF	Money Laundering, Terrorist Financing and Proliferation Financing
MLRO	Money Laundering Reporting Officer
NRA	National Risk Assessment
PEP	Politically Exposed Person
POCA	Proceeds of Crime Act
PFPA	Proliferation Financing (Prohibition) Act
RBA	Risk-Based Approach
SAR	Suspicious Activity Report
SDD	Simplified Due Diligence
TFS	Targeted Financial Sanctions

Rule on Effective Compliance Programme for the Prevention and Detection of Money Laundering, Terrorist Financing and Proliferation Financing for Financial Services Providers

1. Introduction

1.1. This document establishes the Cayman Islands Monetary Authority's (the "Authority" or "CIMA") Rules on Effective Compliance Programme for the Prevention and Detection of Money Laundering, Terrorist Financing and Proliferation Financing for Financial Service Providers ("FSPs") in the Cayman Islands (the "Rule").

1.2. This Rule should be read in conjunction with the following:

(a) the Proceeds of Crime Act ("POCA");
(b) Anti-Money Laundering Regulations ("AMLRs");
(c) the Beneficial Ownership Transparency Act ("BOTA");
(d) the Terrorism Act ("TA");
(e) the Proliferation Financing (Prohibition) Act ("PFPA");
(f) Authority's Rule on Sanctions Compliance and Targeted Financial Sanctions;
(g) Guidance Notes on the Prevention and Detection of Money Laundering and Terrorist Financing in the Cayman Islands;
(h) Rule and Statement of Guidance on Internal Controls for Regulated Entities;
(i) Rule on Corporate Governance for Regulated Entities;
(j) Statement of Guidance on Outsourcing for Regulated Entities;
(k) any other relevant legislation issued by the Cayman Islands Government ("CIG") and regulatory instruments issued by the Authority from time to time (the "AML/CFT/CPF Framework").

1.3. FSPs should be aware of the enforcement powers of the Supervisory Authorities under the AMLRs.

2. Background

2.1. The Authority's legislative mandates include the regulation and supervision of a broad spectrum of financial services operating in and from within the Cayman Islands. In performing its regulatory, advisory and co-operative functions, CIMA shall endeavour to reduce the possibility of financial services business or relevant financial business being used for the purpose of money laundering or other financial crimes.

2.2. CIMA implements a well-defined and proportionate, Risk-Based Approach ("RBA") to supervision, while conforming to internationally applied standards and best practices insofar as they are relevant and appropriate to the circumstances of the Islands. This ensures that the necessary systems and processes are in place to identify, assess, monitor, manage, and mitigate risks related to Money Laundering, Financing of Terrorism and Proliferation Financing ("ML/TF/PF").

2.3. The Rule aligns with CIMA's Mission to protect and enhance the integrity of the financial services industry of the Cayman Islands and supports CIMA's strategic objectives to improve the effectiveness in combating financial crime and to establish a proactive, sustainable, and effective financial services regulation to promote new products/models and enable the existing business products/models to thrive.

3. Statement of Objectives

3.1. The Rule sets out the minimum requirements of an effective compliance programme for the prevention and detection of ML/TF/PF by FSPs.[1]

4. Statutory Authority

4.1. The Rule is consistent with the Authority's principal functions under section 6(1)(b) of the MAA, which provides that:

"(1) *The principal functions of the Authority are —*

(b) regulatory functions, namely —

(i) to regulate and supervise financial services business carried on in or from within the Islands in accordance with this Act and the regulatory acts;

(ii) to monitor compliance with the anti-money laundering regulations; and

(iii) to perform any other regulatory or supervisory duties that may be imposed on the Authority by any other act;".

4.2. The Rule is also consistent with section 34(1) of the MAA, which provides that:

"(1) After private sector consultation and consultation with the Minister charged with responsibility for Financial Services, the Authority may —

(a) issue or amend rules or statements of principle or guidance concerning the conduct of licensees and their officers and employees, and any other persons to whom and to the extent that the regulatory acts may apply;

(b) issue or amend statements of guidance concerning the requirements of the anti-money laundering regulations or the provisions of the regulatory acts; and

(c) issue or amend rules or statements of principle or guidance to reduce the risk of financial services business being used for money laundering or other criminal purposes."

[1] For requirements relating to compliance with sanctions and targeted financial sanctions, FSPs must refer to the *Rule on Sanctions Compliance and Targeted Financial Sanctions*.

4.3. This Rule supplements the AMLRs, including Regulations 3, 4, 5, 6 and 8, by establishing the minimum requirements applicable to FSPs:

(a) Regulation 3 of the AMLRs mandates entities engaged in relevant financial business to implement appropriate compliance programmes, systems, and training;
(b) Regulation 4 outlines the responsibilities of the Anti-Money Laundering Compliance Officer ("AMLCO");
(c) Regulation 5 requires the creation of systems and training to combat ML/TF/PF;
(d) Regulation 6 sets out the requirements for group-wide programmes; and
(e) Regulation 8 and 8A mandate that entities involved in relevant financial business conduct enterprise-wide and country or geographic ML/TF/PF risk assessments, taking into account credible sources and applying enhanced measures where higher risks are identified.

5. Scope of Application

5.1. This Rule applies to all FSPs that are regulated and supervised by CIMA under the Regulatory Acts, inclusive of branches, subsidiaries, affiliates and any other members of a CIMA-regulated financial group.

5.2. All FSPs who are conducting relevant financial business must comply with the requirements set out in the AMLRs.

5.3. Each FSP must implement a compliance programme that is commensurate with its size, complexity, structure, nature of business, and the risk profile of its operations.

5.4. References to any act or regulation shall be construed as references to those provisions as commenced, amended, modified, re-enacted or repealed and replaced from time to time.

6. Definitions

6.1. The following definitions are provided for the purposes of this Rule:

(a) **"Anti-Money Laundering Compliance Officer"** has the same meaning as defined in the AMLRs.

(b) "**Business Relationship"** has the same meaning as defined in the AMLRs.

(c) "**Competent Authority"** has the same meaning as defined in the AMLRs.

(d) **"Compliance Programme"** means a documented framework of policies, procedures, controls, and oversight mechanisms designed to ensure ongoing compliance with the AML/CFT/CPF Framework.

(e) **"Customer"** has the same meaning as defined in the AMLRs.

(f) **"Governing Body"** of a Regulated Entity is the Board of Directors where the entity is a corporation, the General Partner where the entity is a partnership, the manager where the entity is a Limited Liability Company, and the Board of Trustees where the entity is a trust business, or any equivalent governing structure as appropriate, taking into account the nature, size, and legal form of the Regulated Entity**.**

(g) **"electronic-Know Your Customer" or "e-KYC"** means the conducting of a customer's identification process through digital technology verification mechanisms.

(h) **"family members"** has the same meaning as defined in the AMLRs.

(i) **"financial group"** has the same meaning as defined in the AMLRs.

(j) **"Financial Reporting Authority" or "FRA"** has the same meaning as defined in POCA.

(k) **"Financial Service Providers" or "FSPs"** means all persons carrying on relevant financial business specified in POCA.

(l) **"Money Laundering"** has the meaning given by section 144(10) of POCA.

(m) **"Money Laundering Reporting Officer" and "Deputy Money Laundering Reporting Officer"** have the same meaning as defined in the AMLRs.

(n) **"Proliferation"** has the same meaning as defined in Proliferation Financing (Prohibition) Act;

(o) **"Regulatory Acts"** means any one or more of the Acts as prescribed in Section 2 of the MAA and any Regulations made under them or the POCA, and any other Act that may be prescribed by the Cabinet by regulations made under Section 46 of the MAA.

(p) **"Relevant Financial Business"** has the same meaning as defined in POCA.

(q) **"Supervisory Authorities"** has the same meaning as defined in the AMLRs.

(r) **"Targeted Financial Sanction" or "TFS"** is a specific type of financial sanction with stated objectives, one of which is the prevention of terrorist financing and proliferation financing. TFS includes both asset freezing and prohibitions, as well as directions, to prevent funds or other assets, including virtual assets, from being made available, directly or indirectly, for the benefit of designated persons and entities.

(s) **"Terrorist Financing" or "TF"** means doing any act which constitutes an offence under sections 19 to 22 of the Terrorism Act or under POCA, or in the case of an act done otherwise than in the Islands, would constitute such an offence if done in the Islands.

7. Governance and Overview of the Compliance Programme

7.1 The Governing Body of the FSP shall establish and maintain a clear governance framework for the Compliance Programme, which at a minimum must:

(a) document, define, assign, and communicate the roles and responsibilities of all persons involved in the implementation and oversight of the programme;

(b) appropriately assign responsibilities to promote accountability and effectiveness;

(c) designate an Anti-Money Laundering and Compliance Officer ("AMLCO"), who is a natural person operating no lower than a management level, to be responsible for the compliance programme; and

(d) appoint a Money Laundering Reporting Officer.

7.2 FSPs must establish, implement, and maintain a comprehensive and effective Compliance Programme that is designed to detect, prevent, and report on ML/TF/PF/TFS as required under the AML/CFT/CPF Framework.

7.3 The Compliance Programme, at a minimum, must include the following core components:

(a) Designation of an AMLCO who is responsible for implementing and overseeing the compliance programme;

(b) Documentation of detailed written policies and procedures for Know Your Customer, reporting, etc., approved by the Governing Body;

(c) Development, documentation and implementation of a risk management framework including a periodic risk assessment programme to evaluate risks from clients, services, locations and technology to effectively apply a risk-based approach and mitigate the risks of ML/TF/PF occurring in the course of business;

(d) Delivery of ongoing compliance training programme and plan for all staff, including the governance body and relevant parties on AML, CFT, CFP and TFS obligations; and

(e) the development, maintenance, and ongoing evaluation of a compliance programme that reflects the nature, type, and scope of activities conducted, and ensures its effectiveness.

8 Designation of the AMLCO

8.1 FSPs must ensure, at the time of designation and on an ongoing basis, that the AMLCOs are of good repute, possess integrity, are suitably qualified and experienced to perform their functions, and are financially sound, and shall provide to the Authority, upon request, such information and evidence as the Authority may require in this regard.

8.2 The designated AMLCO must:

(a) possess the authority to oversee the effectiveness of the FSP's AML/CFT/CPF systems and ensure compliance with applicable AML/CFT obligations, including the AMLRs and this Rule.

(b) have direct access to senior management and the Governing Body.

(c) operates independently of the business and operational functions that they oversee to ensure an objective and unbiased assessment of the compliance programme.

(d) have access to sufficient resources to carry out their duties effectively.

(e) have a sound understanding of the FSP's business model, activities, products, services, functions, and structure.

(f) possess the knowledge of AML/CFT/CPF and sanctions-evasion risks relevant to the FSP's business sector, as well as emerging issues, trends and typologies.

8.3 The designation of an AMLCO does not absolve an FSP of its obligations; therefore, an FSP must remain ultimately responsible for the design, implementation and functioning of the FSP's compliance programme to ensure compliance with the AML/CFT/CPF Framework.

8.4 The AMLCO must develop and maintain the FSP's compliance systems and controls, including the documentation of the policies and procedures. This documentation must clearly demonstrate apportioned roles for countering ML/TF/PF.

8.5 The AMLCO must ensure that the FSP's Compliance Programme includes the maintenance of records, including those for declined business, register of Politically Exposed Persons ("PEPs") (including family members and Close Associates), Competent Authority requests, Suspicious Activity Reports ("SARs"), transaction alerts, and sanctions monitoring.

8.6 The AMLCO may delegate specific duties to other employees or third parties, for example, to staff in other locations or branches; however, the AMLCO must retain the overall responsibility for the proper implementation and functioning of the compliance programme.

8.7 The AMLCO must ensure that the FSP's employees are trained on the provisions of the AMLRs and the process for escalating suspicious transactions to the Money Laundering Reporting Officer ("MLRO") (or alternate Deputy Money Laundering Reporting Officer ("DMLRO")) for further review.

8.8 The AMLCO must ensure that the Governing Body is kept informed of the operations of the Compliance Programme, which includes escalating any ML/TF/PF or sanctions issues as appropriate.

9 Development and Documentation of a Risk Assessment Program

9.1 FSP must perform and document a risk assessment of its business to establish, implement and document an RBA to AML/CFT/CPF risk present in its business that is commensurate with the nature, size, complexity, structure, and risk profile of its operations.

9.2 In implementing and applying the RBA, the FSP must:

(a) identify and assess ML/TF/PF risks in relation to their applicants/customer types, geographic area in which the applicants/customers reside or operate, and where the FSP operates, the products and services that the FSP offers and their delivery channels;

(b) review and incorporate the findings and conclusions of the Cayman Islands National Risk Assessment ("NRA") and any subsequent updates of such assessment into their internal risk assessment process;

(c) design and implement policies, controls and procedures that are approved by the Governing Body to manage and mitigate the ML/TF/PF risks that they identified from its risk assessment, commensurate with the respective risks identified;

(d) monitor the effectiveness of the implementation of the policies, controls and procedures and enhance or revise them as necessary to address identified weaknesses or emerging risks;

(e) document and keep their risk assessments current through ongoing reviews and updates as necessary;

(f) document the RBA, including its implementation and monitoring procedures, and its updates; and

(g) have effective mechanisms to report to the relevant competent authorities as required under the relevant acts or regulations.

9.3 FSPs must assess all the other relevant ML/TF/PF risk factors for which reliable information is available before determining the overall risk level and the appropriate level and type of mitigation to be applied. This would include, but is not limited to, the ML/TF/PF risks identified at the national level through the

NRA (or similar assessment) or risk assessment conducted by the relevant Supervisory Authority, whichever is most recently issued.

9.4 Where there are higher ML/TF/PF risks, FSPs must implement enhanced due diligence measures to manage and mitigate those risks; and correspondingly, where the ML/TF/PF risks are lower, simplified due diligence measures are permitted. However, simplified due diligence measures shall not be permitted whenever there is a suspicion of ML/TF/PF.

9.5 When identifying and assessing risk, FSPs must adopt risk assessment policies and procedures approved by the Governing Body that are commensurate with their size, complexity, structure, nature of business and risk profile of their operations.

9.6 FSPs must document their risk assessments, including documentation of inherent and residual risks, to demonstrate the basis for their response to the identified risks, including the level of risk assigned and the type of mitigation measures applied, and how the risks are aggregated to arrive at the overall risk rating.

9.7 FSPs must keep these assessments up-to-date and maintain mechanisms to provide risk assessment information to the relevant Supervisory Authority (including Competent Authorities and Self-Regulatory Bodies, if required).

9.8 FSPs must document their RBA. Documentation of relevant policies, procedures, review results and responses should enable the FSP to demonstrate the following to the relevant Supervisory Authority, competent authorities and/or to a court:

(a) risk assessment systems, including how the FSP assesses ML/TF/PF risks in relation to their applicants/customer types, geographic area in which the applicants/customers reside or operate, and where the FSP operates, the products and services that the FSP offers and their delivery channels;

(b) details of the implementation of appropriate systems and procedures, including due diligence requirements, in light of its risk assessment;

(c) how it monitors and, as necessary, improves the effectiveness of its systems and procedures; and

(d) the arrangements for reporting to senior management and the Governing Body on the results of ML/TF/PF risk assessments and the implementation of its ML/TF/PF risk management systems and control processes.

10 Detailed Policies and Procedures

10.1 FSPs must document their compliance policies, procedures and control mechanisms and make them accessible to all relevant parties, inclusive of parties executing relevant outsourced functions.

10.2 The Governing Body must approve the compliance policies and procedures established and implemented by the FSP and ensure they are reviewed periodically (at a minimum once per year) and updated to reflect changes in risk, business activities, or regulatory requirements in a timely manner.

10.3 FSPs must ensure that the policies and procedures in their Compliance Programme are proportionate to the size, complexity, structure, scale, and exposure of their activities to ML/TF/PF/TFS risks. At a minimum, such policies and procedures shall address:

(a) assessment of risk and application of a risk-based approach;

(b) customer Due Diligence ("CDD") and ongoing monitoring, including enhanced measures for higher-risk customers such as Politically Exposed Persons ("PEPs");

(c) record-keeping and retention in accordance with applicable Acts and regulations;

(d) outsourcing of the compliance programme or components of the compliance programme, ensuring that any outsourced functions do not impede regulatory access and that the FSP remains ultimately responsible for compliance with relevant obligations;

(e) notifying the Authority in writing, within a reasonable timeframe, of any material outsourced compliance function(s);

(f) procedures for suspicious activity detection, transaction monitoring, investigation, escalation, and reporting, including travel rule requirements; and

(g) sanctions compliance, including screening against UN, UK, Cayman Islands regimes, TFS, and PF risk mitigation[2].

10.4 Customer Due Diligence ("CDD")

10.4.1 FSPs must establish and maintain procedures to identify and verify the identity of all customers, beneficial owners and persons purporting to act on behalf of customers, before establishing a business relationship or carrying out a one-off transaction.

10.4.2 When conducting CDD measures on applicants that are legal persons or legal arrangements, FSPs must identify and verify the applicant's identity and clearly understand the nature of its business, ownership, and control structure.

10.4.3 FSPs must ensure that customer identification and verification are based on reliable, independent source documents, data, or information in

[2] As stipulated within the Authority's *Rule on Sanctions Compliance and Targeted Financial Sanctions.*

accordance with the AMLRs, and that the methods applied align with the results of the FSP's risk assessment of the customer.

10.4.4 FSPs must ensure that any decision to onboard a customer remotely, using electronic Know Your Client ("e-KYC") methods and digital ID technologies, is dependent on the risks presented and assessed, and, where applicable, considers the application of tiered CDD.

10.4.5 Where the customer, product, service, or jurisdiction is identified as higher risk for ML/TF/PF, the FSP must conduct additional verification measures to ensure the accuracy of e-KYC procedures.

10.4.6 FSPs must not open or maintain anonymous accounts, accounts in fictitious names or numbered accounts.

10.4.7 FSPs must monitor transactions to determine whether they are linked to mitigate the risk of one-off transactions being deliberately restructured into two or more transactions of smaller values to circumvent the applicable threshold (KYD 10,000).

10.4.8 FSPs must conduct CDD when:

(a) establishing a business relationship;

(b) carrying out a one-off transaction valued in excess of ten thousand dollars (KYD 10,000), or equivalent, which comprises a single transaction or several transactions of smaller values that appear to be linked;

(c) carrying out one-off transactions that are wire transfers;

(d) there is a suspicion of ML/TF/PF; or

(e) there are doubts as to the veracity or adequacy of the previously obtained customer identification information.

10.4.9 FSPs must assess and ensure that the nature and purpose of the proposed business relationship or transaction are in line with their expectations and use CDD information as a basis for ongoing monitoring.

10.4.10 FSPs must obtain, verify and retain a copy of the certified document granting a person the authority to act on behalf of the applicant or customer.

10.4.11 FSPs must assess the ML/TF/PF risks associated with a person who has been granted permission to act on behalf of the customer or applicant as part of their CDD.

10.4.12 FSPs must conduct CDD measures on a person who has been granted permission to act on behalf of the applicant or customer equivalent to

those required of an applicant. This includes identification, verification and risk assessment.

10.4.13 FSPs conducting long-term insurance business must, in addition to the CDD measures required for the applicant/s and beneficial owner/s, apply CDD measures to the beneficiary(ies) of insurance policies as soon as they are identified or designated and must do so before the time of the pay-out of the policy. For:

(a) beneficiary(ies) that are specifically named as natural persons, legal persons or legal arrangements, the FSP must record and verify the name of the beneficiary using reliable and independent source documents, data, or information; and

(b) beneficiary(ies) designated by characteristics or by class (e.g. spouse or children), or by other means (e.g. under a will), the FSP must obtain sufficient information to be satisfied that it will be able to establish the identity of the beneficiary before the time of the pay-out.

10.4.14 When conducting CDD on applicants who are legal arrangements, FSPs must identify the beneficial owners of the applicant and take measures, based on the level of ML/TF/PF risk, to verify the identity of such persons, using reliable and independent source documents, data, or information.

10.4.15 For trust companies, the FSPs must identify and verify the identity of the settlor, the trustee(s), the protector (if any), the enforcer (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust (including through a chain of control/ownership).

10.4.16 For other legal arrangements aside from trust companies, the FSP must identify and verify the identity of persons holding equivalent or similar positions of ownership or control.

10.4.17 FSPs must periodically review their records on applicants or customers and update those records as necessary whenever material changes occur to the arrangement or its control structure.

10.4.18 Where a FSP is unable to satisfactorily complete and comply with CDD requirements specified in the AMLRs and this Rule, the FSP must:

(a) not open the account; commence or continue a business relationship; or perform any transaction for or with the customer; and

(b) terminate the business relationship promptly and consider whether the circumstances warrant filing a SAR.

10.4.19 An FSP shall perform Enhanced Due Diligence ("EDD") where it determines that a customer or the business relationship is high-risk in

accordance with AMLRs or results of its risk assessment, and shall not open an account, or establish or continue a business relationship, where it is unable to perform EDD as required.

10.4.20 In determining whether a customer or applicant qualifies for Simplified Due Diligence ("SDD"), the FSP must ensure that:

(a) its assessment of the customer or applicant's risk is complete, and it has considered all relevant risk factors before determining that the customer or applicant is low risk;

(b) the identified low risks are consistent with the findings of the Cayman Islands' NRA or any relevant guidance issued by the Authority or other relevant Supervisory Authority; and

(c) there are no circumstances giving rise to suspicion of ML/TF/PF or doubt the veracity of customer identification information or any other higher-risk scenarios.

10.4.21 Where a FSP decides to apply SDD measures to an applicant or customer, it must:

(a) document the basis for applying SDD, including the risk assessment and risk factors considered and the justification for application of SDD measures;

(b) review such documentation periodically to assess whether the customer or applicant still qualifies for SDD measures and update this documentation where there are changes in the customer's risk profile; and

(c) make the documentation available to the relevant Supervisory Authority on request.

10.4.22 Where the FSP applies SDD to a customer or applicant, it must continue to conduct sanctions screening in accordance with the requirements of the AMLRs and the Cayman Islands sanctions regime.

10.5 Record Keeping Requirements

10.5.1 FSPs must maintain all necessary transaction records, including identification data obtained through the CDD process, account files, business correspondence, and transaction records, for at least five (5) years after the end of a business relationship or the completion of a one-off transaction. Such records must be retained in a manner that ensures they are readily available to the Authority or other Supervisory Authorities upon request.

10.5.2 FSPs must ensure that records of identification data and verification documents obtained through digital ID systems and e-KYC procedures

are easily accessible, maintained, and can be made available without delay to Competent Authorities upon request.

10.5.3 FSPs must obtain, maintain and keep accurate, adequate and up-to-date beneficial ownership information for all customers that are legal persons or legal arrangements.

10.5.4 FSP must retain all beneficial ownership records at least five (5) years after the date on which:

(a) the customer (a legal entity) is dissolved or otherwise ceases to exist; or
(b) the customer ceases to be a customer of the FSP.

10.6 Outsourcing Requirements

10.6.1 Regarding the outsourcing of the Compliance Programme, or any part thereof, the FSP must:

(a) assess the associated risks, including the country risk of the associated outsourcing arrangement; and

(b) ensure that any outsourcing arrangement does not impair its ability to meet AML/CFT/CPF obligations or manage its risks effectively.

10.6.2 Before entering into any outsourcing arrangement, an FSP must conduct appropriate due diligence on the proposed service provider to assess its fitness and propriety, competence and capability to perform the outsourced activity.

10.6.3 Where the associated risks of an outsourcing arrangement cannot be effectively identified, managed, or mitigated, the FSPs must not enter into or continue with the outsourcing arrangement.

10.6.4 Where an FSP enters into an outsourcing arrangement, the FSP must ensure that the outsourcing agreement clearly sets out the respective rights and obligations of both parties.

10.6.5 FSP must not enter into or continue an outsourcing arrangement where access to data, information or systems relating to the outsourced activity by the Authority or any other Supervisory Authority may be impeded by confidentiality, secrecy, privacy, or data protection restrictions. The FSP remains ultimately responsible for compliance with the AMLRs and this Rule, irrespective of any outsourcing arrangement.

10.6.6 FSP must notify the Authority of any material outsourcing agreement that relates to the functions of its compliance programme.

11 Delivery of Ongoing Compliance Training Programme and Employee Screening

11.1 FSPs must establish, document, and implement an effective training programme and plan that ensures all relevant personnel understand and comply with the requirements of POCA, the AMLRs, the TA, the PFPA, and all associated regulations, rules and guidance.

11.2 The FSP must deliver such training at a frequency and level commensurate with the entity's risk exposure, business activities, and staff responsibilities.

11.3 FSPs must ensure that all their employees, including senior management and employees with AML/CFT/CPF responsibilities, are competent, fit and proper to discharge their assigned responsibilities.

11.4 FSPs must establish and implement recruitment and selection procedures and controls, which include screening prospective employees through fit and proper checks, integrity screening, due diligence, and background checks, to ensure staff competence, integrity and prevent ML/TF/PF.

11.5 FSPs must establish and implement ongoing monitoring and updating of screening records periodically, which include fit and proper checks, integrity screening, due diligence, and background checks, to ensure staff competence, integrity and prevent ML/TF/PF.

11.6 Where the FSP has employees, agents, or other persons authorised to act on their behalf, they must develop and maintain a written, ongoing compliance training programme, and ensure that all appropriate staff, in accordance with Regulation 5 of the AMLRs, receive training on ML/TF/PF prevention on a regular basis.

11.7 FSPs must provide employees on an ongoing basis with training in the recognition and treatment of transactions carried out by, or on behalf of, any person who is, or appears to be, engaged in ML/TF/PF, or whose assets are subject to targeted financial sanctions applicable in the Cayman Islands.

11.8 The FSP's training programmes must, at a minimum, cover the following:

(a) the requirements under POCA, AMLRs, PFPA, TA and associated Regulations;

(b) background information on ML/TF/PF, including related technical jargon, interpretations, definitions, methods, and activities;

(c) the business or professional vulnerability to ML/TF/PF risks (providing indicators and examples);

(d) the compliance policies and procedures developed to meet the requirements under the relevant acts and associated regulations for preventing and detecting ML/TF/PF risks, including the reporting, record keeping and KYC requirements; and

(e) the internal systems, roles and responsibilities for detecting and deterring ML/TF/PF activities and dealing with suspicious activities or transactions.

11.9 FSPs must document the training plan and the schedule for delivering and implementing their ongoing compliance training programmes.

11.10 FSPs must document and implement the steps they will take to ensure their employees, agents, or other persons authorised to act on their behalf receive an appropriate level of training relevant to their duties and position, on an ongoing basis.

11.11 An FSP's training plan must include descriptions about:

(a) training recipients;

(b) training topics and materials and sources;

(c) training methods for delivery (e.g., self-directed learning, information sessions, face-to-face meetings, classrooms, conferences and on-the-job training where instruction is provided); and

(d) training frequency.

11.12 The recipients of an FSP's training must include those who:

(a) have contact with clients, such as front-line staff or agents;

(b) are involved in client transaction activities;

(c) handle cash, funds, or virtual currency for the FSP, in any way; and

(d) are responsible for implementing or overseeing the compliance program, including the compliance officer, senior management, information technology staff, members of the Governing Body or internal auditors.

11.13 While FSPs may employ instructors from among in-house personnel or an external service provider, they are not absolved from ultimate responsibility. FSPs must ensure that such persons have knowledge of the relevant acts, associated regulations and compliance obligations.

11.14 While the FSP may use an external service provider to manage its training programme, the FSP must assess and determine whether the external service provider's services and training content are suitable for its business.

11.15 While an FSP may use one or more training methods, the method(s) must be appropriate to the size, complexity, structure, nature of business and risk profile of its operations.

11.16 The frequency of an FSP's training programme, which must be delivered at regular intervals (for example, monthly, semi-annually, annually), when certain events occur (for example, before a new employee deals with clients, after a procedure or regulation is changed), or by using a combination of both.

11.17 FSP's training programme and plan should be tailored appropriately to the size, complexity, structure, nature of business and risk profile. For example, a larger FSP may decide to provide different types of training to its employees, agents, or other persons authorised to act on its behalf based on their specific roles and duties. Circumstances of this nature must be explained in an FSP's training plan.

11.18 An FSP must maintain a record of the training that has been delivered, which must include at a minimum the date when the training took place, a list of the attendees who received the training, and the topics and content that were covered and make this available to the Authority or any other Supervisory Authority upon request.

12 Demonstration of the Effectiveness Review

12.1 As part of the AML/CFT/CPF systems and controls, an FSP must establish and maintain an independent audit function to review and test the Compliance Programme, ensuring its adequacy, effectiveness and alignment with the applicable legislative and regulatory obligations, including AMLRs and any regulatory requirements issued by the Authority, including prescribed returns.

12.2 The audit function must be carried out by persons independent of the FSP's operations and compliance functions, and the audit report filed with the Authority no later than 15 September of each year, or as otherwise prescribed by the Authority.

12.3 Regardless of whether the audit function of the Compliance Programme is outsourced, the FSP must remain ultimately responsible for ensuring that the Compliance Programme is adequate and operates effectively.

12.4 Any independent audit to assess the adequacy, effectiveness, and implementation of the FSP's Compliance Programme may be conducted internally but must not be undertaken internally for more than two consecutive years. For example, if the audit is conducted internally for two consecutive years, then the next audit must be conducted by an external service provider.

Money Laundering Reporting Officer and Reporting of Suspicious Activity or Transactions

12.5 Each FSP must appoint a Money Laundering Reporting Officer ("MLRO") at the management level, who is responsible for receiving and assessing SARs from staff and, where appropriate, making external SARs to the Financial Reporting Authority ("FRA").

12.6 FSPs must designate a DMLRO, who shall act and discharge the functions of the MLRO in the absence of the MLRO.

12.7 FSPs must ensure, at the time of appointment or designation and on an ongoing basis, that the MLRO and DMLRO are of good repute, possess integrity, are suitably qualified and experienced to perform their functions, and are financially sound, and shall provide to the Authority, upon request, such information and evidence as the Authority may require in this regard.

12.8 An FSP must ensure that all suspicious activities or transactions identified are reported to the MLRO or DMLRO and that appropriate arrangements are in place to safeguard the confidentiality and restricted use of such information. An FSP must not disclose, directly or indirectly, to any customer or third party that a SAR has been, or will be, made, or that an investigation is being, or may be, carried out.

12.9 An FSP must, without delay, file a SAR with the FRA where it knows, suspects, or has reasonable grounds to suspect that a transaction, attempted transaction or activity may involve MF/TF/PF.

13 Enforcement

13.1 Whenever there has been a breach of any Rule herein, the Authority's policies and procedures, as contained in its Enforcement Manual, will apply, in addition to any other powers provided in the Regulatory Acts, the AMLRs and the MAA.

13.2 This Rule is issued pursuant to the Authority's statutory powers and shall have the force of law. In the event of any inconsistency or conflict between the Rule and any prior or existing guidance notes, policy statements, or interpretative materials issued by the Authority, the obligations within this Rule shall take precedence.

14 Effective Date

14.1 This Rule will come into effect on the date that it is published in the Gazette.

Pavilion East, Cricket Square
PO Box 10052
Grand Cayman KY1-1001
Cayman Islands

Tel: +1 (345) 949-7089
www.cima.ky