RULE

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

July 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
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) Regulatory Policy on Fitness and Propriety;
(k) Statement of Guidance on Outsourcing for Regulated Entities; and
(l) any other relevant legislation issued by the Cayman Islands Government ("CIG") and regulatory instruments issued by the Authority from time to time (altogether referred to as "AML/CFT/CPF Regime").

1.3. FSPs should be aware of the enforcement powers granted to the Competent Authorities under the AMLRs, including the Authority in its capacity as the Supervisory Authority for the financial services sector.

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 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."

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");

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

(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 conducting relevant financial business perform 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.

4.4. In the event of any conflict or inconsistency between the provisions of these Rules and the AMLRs, the AMLRs shall take precedence and shall prevail.

5. Scope of Application

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

5.2. 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.

5.3. Where an FSP relies on a third party or a member of its financial group to perform AML/CFT/CPF functions, it shall, notwithstanding such reliance, remain satisfied that such functions comply with this Rule and the Anti-Money Laundering Regulations of the Cayman Islands, and shall retain ultimate responsibility for such compliance.

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) **"Beneficial Owner"** has the same meaning as defined in the AMLRs.

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

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

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

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

(g) **"Governing Body"** of a Financial Service Provider 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 Financial Service Provider**.**

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

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

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

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

(l) **"Financial Service Providers" or "FSPs"** means all persons conducting relevant financial business.

(m) **"Money Laundering"** has the meaning as defined in POCA.

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

(o) **"Proliferation"** has the same meaning as defined in the Proliferation Financing (Prohibition) Act.

(p) **"Regulatory Acts"** has the same meaning as "Regulatory Laws", as defined in Section 2 of the Monetary Authority Act (MAA).

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

(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. The governance framework, at a minimum, must:

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

(b) assign responsibilities in a manner that promotes accountability and effectiveness of the Compliance Programme;

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

(d) designate a Money Laundering Reporting Officer ("MLRO") and a Deputy Money Laundering Reporting Officer ("DMLRO") who are natural persons operating at no lower than a management level.

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 and comply with TFS, as required under the AML/CFT/CPF Regime.

7.3 An FSP's Compliance Programme, at a minimum, must include the following core components:

(a) designation of an AMLCO who is responsible for the implementation and oversight of the Compliance Programme;

(b) documentation of detailed written policies and procedures of the Compliance Programme;

(c) development, documentation and implementation of a risk management framework including a periodic risk assessment programme to evaluate ML/TF/PF risks presented by customers, products/services, transactions, country or geographic area, and delivery channels, to effectively apply a risk-based approach and mitigate the risks occurring in the course of business;

(d) delivery of ongoing compliance training programme and training plan for all staff, the Governing Body, and any other relevant parties, to ensure awareness of and compliance with applicable AML, CFT, CPF, and TFS obligations; and

(e) development, maintenance, and conducting of ongoing evaluations of the effectiveness of the Compliance Programme in a manner proportionate to the nature, type, and scope of the activities conducted by the FSP[2].

8. Designation of the AMLCO, MLRO and DMLRO

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 with sufficient skills and experience to perform their functions, and shall provide to the Authority, upon request, such information and evidence as the Authority may require in this regard.

[2] For further details on obligations for Demonstration of Effectiveness, please see Section 12.

8.2 The designated AMLCO of an FSP must:

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

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

(c) perform the compliance function independently and objectively from the business and operational functions subject to their oversight, and, where full separation is not practicable, ensure conflicts of interest are effectively managed;

(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; and

(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 development, implementation and effectiveness of the FSP's Compliance Programme to ensure compliance with its obligations under the AML/CFT/CPF Regime.

8.4 The AMLCO must ensure the development and maintenance of the FSP's compliance systems and controls, including the documentation of the policies and procedures. This documentation must clearly demonstrate allocation of roles and responsibilities for countering ML/TF/PF across the FSP's governance and internal control framework.

8.5 The AMLCO must ensure that the FSP's Compliance Programme includes appropriate systems, controls and procedures to ensure effective 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 effectiveness 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 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, including escalating any ML/TF/PF or sanctions issues as appropriate, and providing periodic reports, at least annually.

Appointment of the MLRO and Designation of the DMLRO

8.9 The appointed MLRO in accordance with Rule 7.1 (d) must be responsible for receiving and assessing SARs from staff and, where appropriate, making external SARs to the Financial Reporting Authority ("FRA").

8.10 FSPs must designate a DMLRO, also at a managerial level, who shall act and discharge the functions of the MLRO in the absence of the MLRO.

8.11 FSPs must ensure, at the time of appointment or designation and on an ongoing basis, that the MLRO and DMLRO are suitably qualified with sufficient skills and experience to perform their functions, and shall provide to the Authority, upon request, such information and evidence as the Authority may require in this regard.

9. Development and Documentation of a Risk-Based Approach

9.1 An FSP shall establish, implement, and apply a Risk-Based Approach ("RBA") designed to identify, assess, manage, and mitigate ML/TF/PF risks to which it is exposed. The RBA must be proportionate to the nature, size, complexity, structure, and risk profile of its operations and in line with applicable acts and regulatory requirements.

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

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

(b) review and must, at a minimum, consider the findings and conclusions of the most recent Cayman Islands National Risk Assessment (NRA), together with any other relevant internal and external risk factors, as part of its internal risk assessment process;

(c) develop and implement policies, controls and procedures that are approved in line with Rule 10.2, to manage and mitigate the ML/TF/PF risks 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 its risk assessments current through ongoing reviews and updates as necessary;

(f) document and update its risk assessments without delay upon the occurrence of any material trigger event that may impact the effectiveness, adequacy, or relevance of the risk assessment, including, but not limited to:

i. New products or business lines;
ii. Expansion into higher risk geographical areas;

iii. Mergers, acquisitions or significant corporate restructuring; and
iv. Economic or geopolitical developments affecting risk exposure.

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

(h) have effective mechanisms to report to the Authority as required under the relevant acts or regulations.

9.3 FSPs must assess all 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 assessments conducted by the relevant Competent 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 may be applied at the customer level, in accordance with applicable Customer Due Diligence requirements. 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, controls and procedures that are proportionate to 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 the risk assessment information to the Authority.

9.8 FSPs must document their RBA. Documentation of relevant policies, procedures, review results, and responses must enable the FSP to demonstrate the following to the Authority:

(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, considering the results of the risk assessments;

(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, Procedures and Controls

10.1 FSPs must document the Compliance Programme's policies, procedures and control mechanisms and make them accessible to all relevant parties, inclusive of parties executing relevant outsourced functions.

10.2 The policies of an FSP must be approved by the Governing Body, while related procedures and controls must be approved by either senior management or the Governing Body (or both). Further, the Governing Body must ensure that such policies and procedures are reviewed and updated in a timely manner, proportionate to the size, complexity, structure, nature of business, and risk profile of its operations, and to reflect changes in risk, business activities, or regulatory requirements.

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 an RBA;

(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 the travel rule requirements as applicable; and

(g) financial sanctions compliance, including screening against official sanctions lists[3].

10.4 Where a Financial Service Provider (FSP) relies on a third party or a member of its financial group to perform AML/CFT/CPF functions, the FSP shall, upon request by the Authority, provide timely and sufficient evidence demonstrating how it remains satisfied that such relied-upon functions comply with the requirements under this Rule and the AMLRs.

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

10.5 Customer Due Diligence ("CDD")

10.5.1 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 when establishing a business relationship or carrying out a one-off transaction.

10.5.2 Where an FSP is unable to complete verification of a customer, beneficial owner, or any person acting on behalf of the customer prior to establishing a business relationship or conducting a one-off transaction, the FSP shall take all reasonable measures to complete such verification as soon as practicable thereafter.

10.5.3 Where an FSP establishes a business relationship or conducts a transaction prior to completing customer due diligence, the FSP shall apply heightened monitoring and scrutiny to the business relationship and any transactions undertaken until such time as the required verification is completed.

10.5.4 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.

10.5.5 FSPs must ensure that customer identification and verification are based on reliable, independent source documents, data, or information in accordance with the AMLRs, and that the methods applied align with the results of the FSP's risk assessment of the customer.

10.5.6 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, as applicable, considers the application of simplified, standard, or enhanced customer due diligence measures.

10.5.7 Where the FSP has identified a higher risk for ML/TF/PF in relation to customers, products, services, or jurisdictions, the FSP must apply enhanced due diligence measures proportionate to the risks.

10.5.8 FSPs must implement controls to prevent the opening or maintenance of anonymous or fictitious accounts and ensure that all customers are appropriately identified, verified and subject to ongoing monitoring.

10.5.9 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 as outlined in Rule 10.5.10 below.

10.5.10 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.

10.5.11 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.

10.5.12 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.

10.5.13 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.

10.5.14 FSPs must conduct CDD on a person who has been granted permission to act on behalf of the applicant or customer to the same standard as that applied to the applicant or customer. This includes identification, verification and risk assessment.

10.5.15 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, where verification is required, must do so before or at 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, or by other means, 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.

10.5.16 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.

10.5.17 For legal arrangements such as trusts, 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 natural person exercising ultimate effective control over the trust (including through a chain of control/ownership).

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

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

10.5.20 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.

10.5.21 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 Competent Authority, whichever is most recently issued; and

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

10.5.22 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) periodically reassess the customer or applicant's risk profile to determine whether the customer or applicant still qualifies for SDD measures and document this reassessment and update the customer's level of risk where there are changes in the customer's or applicant's risk profile; and

(c) make the documentation supporting the application of SDD measures available to the Authority on request.

10.5.23 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 applicable financial sanctions legislation of the Cayman Islands.

10.6 Record Keeping Requirements

10.6.1 FSPs must maintain all 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 available to the Authority upon request without delay.

10.6.2 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 the Authority upon request.

10.6.3 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 and keep such information under periodic review.

10.6.4 FSPs 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.

10.7 Outsourcing Requirements

10.7.1 Regarding the outsourcing of the Compliance Programme[4], or any parts thereof, the FSP must:

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

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

(c) conduct and keep records of the CDD conducted on the service provider prior to the outsourcing arrangement.

10.7.2 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.

10.7.3 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.

[4] For the avoidance of doubt, the procurement of third-party AML/CFT/CPF training services does not constitute outsourcing of the Compliance Programme for the purposes of this Rule, provided that the FSP retains full responsibility for determining training requirements, assessing the suitability of the provider and content pursuant to Rules 11.13 and 11.14, and overseeing the adequacy of training delivered.

10.7.4 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.

10.7.5 FSPs must not enter into or continue an outsourcing arrangement where access to data, information or systems relating to the outsourced activity by the 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.

10.7.6 FSPs must notify the Authority of any outsourcing agreement that relates to material functions[5] 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 employees, agents, and other persons authorised to act on their behalf understand and comply with the requirements of POCA, the AMLRs, the TA, the PFPA, and all applicable legislation.

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

11.3 FSPs must establish and implement recruitment and selection procedures and controls, including screening prospective employees through fitness and propriety checks, integrity screening, due diligence, and background checks, to ensure staff competence and integrity, and to prevent ML/TF/PF.

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

11.5 The FSP's training programmes must be administered on an ongoing basis and delivered at least annually. The training should, at a minimum, cover the following:

(a) the requirements under POCA, AMLRs, PFPA, TA and applicable legislation;

(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) 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 financial sanctions and TFS applicable in the Cayman Islands;

[5] As defined within the Authority's Statement of Guidance on Outsourcing for Regulated Entities.

(e) the 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

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

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

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

(a) training recipients;

(b) training topics and materials;

(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.

11.8 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 and internal auditors.

11.9 While FSPs may use in-house personnel or external service providers to deliver compliance training, the FSP retains ultimate responsibility for that delivery. FSPs must ensure that the persons delivering the compliance training programme have sufficient knowledge of the relevant legislation and compliance obligations applicable to the FSP.

11.10 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 appropriate to the size, complexity, structure, nature of business and risk profile of its operations.

11.11 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.

11.12 The FSP's training programme must be delivered at regular intervals (for example, monthly, semi-annually, annually), when certain events occur[6], or by using a combination of both.

11.13 FSP's training programme must 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.

11.14 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 upon request.

12. Demonstration of the Effectiveness

12.1 As part of the AML/CFT/CPF systems and controls, an FSP must establish and maintain independent audit procedures (hereafter referred to as the "audit") 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 FSP must ensure that:

(a) the audit is carried out at a frequency commensurate with its size, complexity, structure, nature of business, and the risk profile, as determined by the FSP's risk assessment or as otherwise required by the Authority;

(b) the audit is carried out by suitably qualified persons who are independent and separate from those involved in the design, implementation, or operation of the policies, procedures, systems, and controls under audit, and who are free from any conflict of interest that could impair their objective judgment;

(c) the FSP must, upon request, provide the Authority with the documentation of the independence of any person who performed the audit of the Compliance Programme, including the basis on which such independence was determined; and

(d) the audit report is filed with the Authority as soon as practically possible after the completion of the audit, or as otherwise prescribed by the Authority.

12.3 The audit may be conducted internally[7] but must not be undertaken internally for more than two (2) consecutive audit cycles. For example, if the audit is conducted internally for two consecutive cycles, then the next audit must be conducted by an external service provider.

[6] for example, before a new employee deals with clients or after a procedure or regulation is changed
[7] Internally refers to any individual or unit that is employed by, engaged under contract by, or otherwise forms part of the FSP's organisational structure, and that is subject to the direction, control, or oversight of the FSP.

12.4 FSPs must establish and implement effective remediation measures to address any deficiencies, breaches, or weaknesses identified through the audit within appropriate timeframes commensurate with their nature, materiality, and associated risk.

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

Reporting of Suspicious Activity or Transactions

12.6 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.

12.7 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.

12.8 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, shall 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 This Rule will come into effect on **18 September 2026**, which is sixty (60) days after it was 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