



New AML & Sanctions Rules Webinar Summary Highlights

30 September 2026

The Cayman Islands Monetary Authority ("CIMA") hosted a webinar providing an overview of the new Rule on Effective Compliance Programme for the Prevention and Detection of Money Laundering, Terrorist Financing and Proliferation Financing for Financial Services Providers (the "AML Rule") and the Rule on Compliance with Financial Sanctions and Targeted Financial Sanctions (the "Sanctions Rule"). Both Rules were issued in July 2026 and came into effect on 18 September 2026.

1. Purpose of the New Rules

The Rules strengthen and clarify CIMA's expectations for financial crime compliance and support Cayman's focus on demonstrating effectiveness under the Financial Action Task Force's Fifth Round Mutual Evaluation. They are not intended to create an entirely new AML/CFT/CPF framework; rather, they build on existing legislative and regulatory requirements and provide clearer, enforceable expectations for how those requirements should be implemented and demonstrated in practice.

A central message throughout the webinar was that effective compliance is about more than having policies and procedures on paper. Regulated entities should be able to demonstrate that their frameworks operate effectively, are proportionate to their risks, and are supported by appropriate governance, controls, resources and oversight.

2. Scope and Application

The AML Rule applies to Financial Service Providers ("FSPs") conducting relevant financial business and regulated and supervised by CIMA under the Regulatory Acts, including applicable branches, subsidiaries, affiliates and members of a CIMA-regulated financial group.



The Sanctions Rule applies to Regulated Persons that are supervised and regulated by CIMA under the Regulatory Acts, irrespective of the type of financial business conducted in and from within the Cayman Islands.

Therefore, the Sanctions Rule applies across all of CIMA's regulated sectors, including insurance and reinsurance business.

Where AML/CFT/CPF functions are outsourced or performed by another group entity or service provider, the regulated entity retains ultimate responsibility for compliance.

3. A Risk-Based and Proportionate Compliance Programme

The AML Rule does not prescribe a one-size-fits-all Compliance Programme. The nature and extent of the programme should reflect the entity's size, complexity, structure, business activities and risk profile.

Risk assessments should identify and assess relevant money laundering, terrorist financing and proliferation financing risks across customers, products and services, transactions, geographic exposure and delivery channels.

Controls such as policies and procedures, due diligence, training, governance, reporting and other compliance measures should be proportionate to the risks identified.

The Governing Body remains ultimately accountable for the effectiveness of the Compliance Programme and should retain effective oversight of the programme.

The AMLCO, MLRO and DMLRO functions remain important components of the framework and should have appropriate competence, independence, resources and access to relevant information.

Training and employee screening should be tailored to the nature and risks of the business.

4. Demonstrating Effectiveness

CIMA emphasised that supervisory expectations increasingly focus on whether compliance arrangements work in practice. Entities should be able to demonstrate effective governance, current and meaningful risk assessments, appropriately designed controls, ongoing monitoring and timely remediation of identified weaknesses.



The existence of a policy or procedure alone is not sufficient; entities should retain evidence of implementation and effectiveness.

Independent testing should provide meaningful assurance that the Compliance Programme is operating effectively and is proportionate to the entity's risk profile.

CIMA will use a risk-based supervisory approach, including onsite inspections for higher risk FSPs and desk-based reviews for FSPs with lesser risk, to assess compliance and effectiveness.

5. Independent AML Audit: Key Clarifications

A significant portion of the discussion addressed questions about independent AML audits. CIMA clarified that the requirement to maintain an independent AML audit function is not new, as this exists under Regulation 5 of the Anti-Money Laundering Regulations ("AMLRs"); the new Rule introduces an important reporting requirement.

There is no universal annual audit cycle or single first-audit date for all FSPs. Audit frequency should be determined by the entity's own risk assessment and risk profile, taking into account factors such as size, complexity, customer profile, products, geographic exposure, outsourcing arrangements and ML/TF/PF and sanctions risks.

The Rule does not reset the audit clock. An entity that has already completed an audit in accordance with its existing obligations does not automatically need to conduct another audit solely because the Rule came into effect.

The resulting independent audit report must be submitted to CIMA as soon as practicable after completion.

The auditor must be appropriately qualified and genuinely independent of the activities being reviewed. Entities should retain evidence supporting the auditor's independence and qualifications.

A review of a service provider may provide useful assurance, but it does not automatically replace an independent review of the FSP's own Compliance Programme. The FSP should be able to demonstrate sufficient coverage of its entity-specific risks, governance and oversight of delegated functions.



6. Financial Sanctions Compliance, Screening and Monitoring Requirements

The Sanctions Rule establishes specific requirements for Financial Sanctions and Targeted Financial Sanctions compliance and requires sanctions compliance to be integrated into the overall AML/CFT/CPF Compliance Programme.

Regulated Persons should maintain appropriate policies, procedures, systems and controls for compliance with Financial Sanctions and Targeted Financial Sanctions.

Sanctions exposure must be considered as part of the risk assessment process. Specifically, Rule 7.2 requires Regulated Persons to consider any sanctions that may apply to applicants, Customers or countries, when conducting risk assessments.

Regulated Persons must screen applicants, Customers, beneficial owners, transactions, service providers and other relevant parties (including Connected Persons).

Systems must enable the re-screening of existing Customers and Connected Persons without delay once a Sanctions List has been updated.

Regulated Persons must have policies, procedures, systems and controls in place for the ongoing monitoring of business relationships or one-off transactions for the purposes of preventing, countering and reporting Terrorist Financing and Proliferation Financing.

Regulated Persons must implement appropriate policies, systems and controls to comply with the statutory reporting framework for sanctions reporting requirements, as administered by the Financial Reporting Authority.

Simplified due diligence does not reduce or waive sanctions screening obligations. A Regulated Person must re-screen all Customers when a Sanctions List has been updated, regardless of the Customer's due diligence risk classification. Compliance with Financial Sanctions and Targeted Financial Sanctions is an absolute legal obligation.



7. CIMA's Enhanced Risk-Based Supervisory Approach

The webinar outlined enhancements to CIMA's AML/CFT/CPF supervision designed to increase the Authority's ability to assess effectiveness across all sectors. Supervisory intensity will be aligned with the risk profile of the regulated entity.

Desk-based reviews will be used for lower-risk entities and, where appropriate, between onsite inspection intervals for higher-risk entities.

Initial desk-based reviews will include an evaluation of Business Risk Assessments and independent AML internal audit reports, with further focus on terrorist financing and proliferation financing preventative compliance measures to follow. The expansion of the Authority's desk-based supervisory tools will start with the Business Risk Assessment, as this will drive the scope and frequency of the AML audit.

Entities may be asked to provide requested documentation within approximately five business days through CIMA's designated secure process.

Where deficiencies are identified, entities will be given an appropriate remediation period based on the nature, scale and complexity of the findings. Repeat findings may carry greater supervisory weight, and enforcement action may be considered where warranted.



8. Key Questions and Practical Reminders

Question	Key Message
Does the Rule require a new AML audit immediately?	No. Audit timing remains risk-based. The new requirement is the submission of the completed audit report to CIMA as soon as practicable.
Can an FSP rely entirely on a service-provider audit?	Not automatically. The FSP must be able to demonstrate that its own Compliance Programme, including entity-specific risks and oversight of outsourced arrangements, has been independently reviewed and tested.
Is sanctions screening risk-based?	Sanctions compliance is an absolute legal obligation in the Cayman Islands. Therefore, a Regulated Person must re-screen all Customers when a Sanctions List has been updated, regardless of the Customer's due diligence risk classification. Further, simplified due diligence does not waive screening requirements. With respect to the risk-based approach, reference is made to obligations under Regulation 8 of the AMLRs.
Does outsourcing transfer responsibility?	No. Delegating activities does not transfer the regulated entity's regulatory responsibility or accountability.
Does every FSP need the same audit scope?	No. Scope and depth should be driven by the FSP's size, nature, complexity, activities and risk profile.



9. Key Takeaways for Regulated Entities

- Review the AML/CFT/CPF Compliance Programme against the new Rules and confirm that it remains appropriate to the entity's current risk profile.
- Ensure the Business Risk Assessment is current, comprehensive and reflective of ML/TF/PF risks and the entity's business activities including the number of Customers and volume of transactions with corresponding geographic risk exposures.
- Confirm that governance arrangements clearly establish accountability and effective oversight by the Governing Body and senior management.
- Review the independence, scope and frequency of AML internal audit arrangements and ensure the rationale is supported by the entity's risk assessment.
- Ensure independent audit reports are submitted to CIMA as soon as practicable following completion.
- Integrate sanctions compliance into the overall AML/CFT/CPF Compliance Programme and ensure that screening, monitoring, record-keeping and reporting are in line with the Sanctions Rule.
- Review outsourced arrangements to ensure the regulated entity maintains effective oversight and does not rely solely on a service provider's controls or review.
- Maintain clear evidence of implementation, testing, training, monitoring, Board oversight and remediation. Demonstrating effectiveness is as important as having the framework in place.

CIMA extends its sincere thanks to our staff presenters and participants for contributing to the success of this webinar.

Resources:

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

[Rule on Compliance with Financial Sanctions and Targeted Financial Sanctions](#)