



AML SUPERVISION DEPARTMENT E-NEWSLETTER

FROM POLICY TO PRACTICE: GETTING AML PROGRAMS RIGHT



Introduction:



The AML Supervision Department (AMLSD) continues to strengthen engagement with registrants and licensees to promote the effective implementation of Anti-Money Laundering, Countering the Financing of Terrorism, and Countering Proliferation Financing (AML/CFT/CPF) obligations.



The 2024 - 2025 sectoral reviews have shown that, although AML/CFT policies and procedures are documented, there is still a significant gap between what is written and what is carried out in practice. In many cases, controls exist in theory but not consistently implemented in daily operations. This gap weakens governance, oversight, internal controls, risk management, and the effective use of a risk-based approach.



International standards underscore that effective AML/CFT compliance is not measured solely by the presence of documented policies and procedures, but by the extent to which these measures are consistently implemented, fully understood by those responsible for their application, and operating effectively in practice to achieve the intended risk mitigation outcomes. An AML/CFT framework should enable an entity to identify, assess, understand, and mitigate money laundering, terrorist financing, and proliferation financing risks relevant to its business.



This newsletter aims to help registrants and licensees bridge the gap between policy and practice by highlighting supervisory expectations, common deficiencies, and practical measures that support effective compliance.

What Does a Complete AML/CFT Framework Look Like?

A robust AML/CFT framework is a system of governance, controls, processes, and people working together to identify, manage, and mitigate financial crime risks.

Importantly, an effective AML/CFT framework is not a one-size-fits-all model. Rather, it should be tailored to the size, nature, complexity, and risk profile of each business to ensure that risk mitigation measures are appropriate and effective.

Higher-risk sectors may require more robust controls, enhanced due diligence measures, and strengthened oversight arrangements. While businesses assessed as lower risk remain responsible for demonstrating that they have identified, assessed, and understood their ML/TF/PF risks, and have implemented proportionate controls and mitigation measures that are appropriate to their risk profile and effective in managing those risks.



An Effective Framework Requires Active:

1 GOVERNANCE AND ACCOUNTABILITY

An effective AML/CFT framework begins with strong governance. Directors and senior management are responsible for ensuring that AML/CFT obligations are understood, adequately resourced, and effectively implemented throughout the business. Governance arrangements should clearly define roles, responsibilities, reporting lines, and accountability for AML/CFT compliance.

2 THE ASSESSMENT, IDENTIFICATION & MITIGATION OF RISK:

A risk-informed approach is fundamental to developing and maintaining an effective AML/CFT framework. The Business Risk Assessment (BRA) forms the foundation of this understanding, enabling entities to identify their vulnerabilities and apply controls that are commensurate with their level of exposure. The findings of the BRA should influence every aspect of the AML/CFT programme—from customer due diligence and transaction monitoring to staff training, governance arrangements, and resource allocation—ensuring that compliance efforts are focused where risks are greatest.



3 IMPLEMENTATION

Policies and procedures should be translated into standard operational practices. All relevant employees are expected to understand their responsibilities and consistently apply customer due diligence measures, ongoing monitoring requirements, record-keeping obligations, sanctions screening procedures, and suspicious activity reporting processes.

Entities must be able to demonstrate that their AML/CFT framework is operating effectively in practice and not merely documented on paper.



Examples of Evidence

Entities may demonstrate effective implementation through:

 Completed customer due diligence files.	 Independent review reports.
 Monitoring reports.	 Risk assessment updates.
 Board and management reports.	 Remediation tracking logs.
 Compliance testing records.	 Suspicious activity escalation records.
 Training records.	

This includes evidencing that policies, procedures, systems, and controls are implemented, understood, and consistently applied across the organisation. Effective implementation enables institutions to identify, assess, manage, and mitigate ML/TF risks, while supporting sound governance and risk-based decision-making.

Beyond documented policies and procedures, effective AML/CFT frameworks demonstrate measurable risk management outcomes. Entities should be able to demonstrate not only that controls exist, but that those controls are successfully identifying, managing, and mitigating ML/TF/PF risks. The effectiveness of controls should be assessed periodically to ensure they continue to achieve their intended objectives and remain proportionate to the entity's risk profile.

A framework that is not effectively implemented creates significant vulnerabilities and may undermine an entity's ability to detect and prevent financial crime. Businesses that fail to operationalise their AML/CFT controls remain susceptible to exploitation by criminals seeking to launder funds or finance terrorist activities.



4 MONITORING AND OVERSIGHT

AML/CFT controls should be regularly monitored to determine whether they remain effective and fit for purpose. Monitoring helps to identify weaknesses, emerging risks, and areas requiring corrective action.

Monitoring should include periodic testing of customer files, transaction monitoring processes, sanctions screening controls, and suspicious activity reporting procedures to assess whether AML/CFT controls are operating effectively in practice. Such testing can help identify control weaknesses, validate the effectiveness of existing measures, and support the timely implementation of corrective actions.

The form of monitoring may vary depending on the risk level of the business. Higher risk entities may conduct formal compliance reviews, testing programmes, and management reporting, while low risk entities may rely on periodic self-assessments and management reviews. Regardless of approach, entities should be able to demonstrate that controls are regularly assessed and that identified deficiencies are addressed in a timely manner.

Effective oversight helps ensure that AML/CFT obligations remain a priority and that compliance measures continue to operate as intended.

5 CONTINUOUS IMPROVEMENT

Financial crime risks continue to evolve, and AML/CFT frameworks must evolve with them.

Entities should regularly review and update their risk assessments, policies, procedures, and controls to reflect changes in their business activities, customer profiles, products and services, delivery channels, regulatory requirements, and emerging money laundering, terrorist financing, and proliferation financing risks.

Continuous improvement should also take account of lessons learned from internal reviews, supervisory findings, industry guidance, and emerging typologies.

Entities should maintain documented remediation plans to address weaknesses identified through internal reviews, independent testing, supervisory examinations, outreach engagements, and regulatory feedback. Remediation efforts should be tracked to completion and periodically reviewed to ensure corrective actions are effective.

A framework that is regularly reviewed and strengthened is more likely to remain effective over time.

6 TRAINING, DEVELOPMENT, AND CAPACITY BUILDING

People are one of the most valuable components of an effective AML/CFT programme. Directors, senior management, compliance officers, and employees should receive ongoing training that is relevant to their roles and responsibilities.

Training programmes should be tailored to the role and risk exposure of employees. Staff involved in customer onboarding, transaction monitoring, sanctions compliance, and suspicious activity reporting may require more frequent and specialised training to support the effective performance of their AML/CFT responsibilities.

Training should go beyond understanding legal and regulatory requirements. It should also help individuals develop a deeper understanding of the products and services offered by the business, customer risk indicators, sector-specific threats, emerging typologies, sanctions obligations, and suspicious activity reporting requirements.

Building internal knowledge and expertise enables staff to identify unusual activity, apply appropriate controls, and make informed risk-based decisions.

Capacity building for low risk entities may include self-directed learning, participation in AMLSD outreach initiatives, industry training programmes, and staying informed about emerging risks and regulatory developments. Regardless of size, ongoing learning is essential to maintaining an effective AML/CFT framework.

In Conclusion

An AML/CFT framework is not judged solely by the quality of its written policies, but by how effectively those policies are implemented, monitored, and embedded within the day-to-day operations of the business.

Strong governance, effective oversight, capable personnel, and a commitment to continuous improvement help ensure that AML/CFT controls remain effective and proportionate to the risks faced by the entity.

AMLSD expects registrants and licensees to maintain sufficient documentation and records to demonstrate that AML/CFT measures are not only established but operating effectively in practice. The ability to evidence implementation and effectiveness remains a key component of AML/CFT compliance.

Looking Ahead

In the next edition, we will examine the core components of an effective AML/CFT framework, aligned with the FATF Standards, and the documentation and evidence that supervisors expect registrants and licensees to maintain to demonstrate compliance.



FOR FURTHER GUIDANCE,

Please visit:

www.tcifsc.tc or

Email us at:

amloutreachunit@tcifsc.tc