S/ SDS DATA SYSTEMS

EAST AFRICA AML/CFT BRIEF / ISSUE 01

EAST AFRICA'S AML/CFT TEST IS NOW EXECUTION.

Grey-list remediation, virtual-asset exposure and the intelligence value of reporting.

Richard Kabiru SDS ANALYSIS

REPORTING DATE
13 JULY 2026

GEOGRAPHIC SCOPE
EAST AFRICA AND THE HORN

CORE AUDIENCE
FINANCIAL INSTITUTIONS, DNFBPS AND PUBLIC AUTHORITIES

EXECUTIVE PERSPECTIVE

The formal position is largely unchanged. The burden of execution is not.

Kenya and South Sudan remain under FATF increased monitoring. Kenya's virtual-asset framework is still moving from legislation to supervision. On 8 July, the United Nations amended one entry on the ISIL and Al-Qaida sanctions list. Taken together, these developments point to a common regional problem: the rules are becoming clearer, but the quality of implementation remains uneven.

For financial institutions, the immediate task is to convert policy into reliable data, working controls and useful intelligence. Virtual-asset exposure may appear through personal accounts, mobile-money collections, processors and offshore providers. Sanctions screening depends on accurate list ingestion and rescreening. STR performance depends on identifiers, transaction detail and a clear explanation of suspicion.

DNFBPs face the same problem from a different position. They may see fewer transactions than banks, but often hold better information on ownership, authority, source of funds and commercial purpose.

The practical question extends beyond what changed in law. Institutions need to show how the change affected customer behaviour, payment routes, report quality and the ability to act.

SDS ASSESSMENT

The next phase of AML/CFT reform will be judged less by the number of rules adopted and more by the quality of supervision, intelligence and enforcement they produce.

A NOTE FOR DNFBPS

DNFBPs include designated non-financial businesses and professions such as lawyers, accountants, real-estate actors, dealers in precious metals and stones, casinos and trust or company service providers, subject to national law.

FINDING 01

Implementation is now the test

Kenya's reform agenda links supervision, reporting, ownership data, financial intelligence and enforcement. Weak performance at one stage reduces the value of progress elsewhere.

FINDING 02

Virtual-asset exposure is indirect

Most institutions will encounter the risk through ordinary payment rails and customer relationships, not through transactions labelled as virtual assets.

FINDING 03

Reporting volume is a weak proxy

An increase in STRs may reflect supervisory pressure. It does not show that reports can be linked, disseminated or used in an investigation.

QUESTIONS FOR MANAGEMENT

For compliance, risk and board reporting.

Q1 **Can we evidence the latest sanctions update?**
The record should cover the source file, ingestion time, field mapping, screening run and any required rescreening.

Q2 **Can we identify indirect VASP exposure?**
Test counterparties, devices, transaction velocity, common beneficiaries and links to known providers.

Q3 **Can an external analyst follow the suspicion?**
The STR should explain the expected activity, the observed deviation, the parties involved and the movement of value.

Q4 **Are we measuring activity or effect?**
Submission counts show work completed. Linkage, dissemination, investigation and intervention show value.

01 / INCREASED MONITORING

Grey-list remediation will be judged by the connection between supervision, intelligence and enforcement.

FATF's statement of 19 June 2026 retained Kenya and South Sudan among jurisdictions under increased monitoring. This is not a direction to reject every customer, payment or business relationship linked to either jurisdiction. A risk-based approach requires institutions to distinguish jurisdictional weakness from the risk presented by a specific customer or transaction.

Kenya's remaining action areas form a single operating chain: risk-based supervision, STR quality, beneficial ownership, use of financial intelligence, money-laundering investigations, targeted financial sanctions and oversight of non-profit organisations. Progress becomes meaningful when these parts reinforce one another. Better reporting has limited value where ownership data cannot identify the natural person who controls the customer or asset.

South Sudan requires a different analytical response. Institutional constraints, overdue action items and exposure to cash, procurement and politically connected networks support greater use of relationship and network analysis. Oil-sector intermediaries, public contracts, PEPs, NGOs, cash movement and regional property should be examined as connected activity.

A grey list identifies a jurisdictional weakness. It does not determine the risk of every customer.

7

Kenya's remaining reform areas need to operate as one control chain rather than as separate compliance projects.

3

The practical tests are clear: stronger supervision, better use of financial intelligence and credible enforcement outcomes.

JURISDICTION	PRIMARY EXECUTION GAP	IMPLICATION FOR INSTITUTIONS
Kenya	Converting reform into better reporting, ownership resolution and case outcomes.	Track report quality, linkage, ownership enrichment, dissemination and investigative use.
South Sudan	Capacity constraints and high exposure to cash, procurement and politically connected networks.	Prioritise common controllers, repeated counterparties, oil intermediaries, NGO contractors and regional property.
Regional institutions	Pressure to use broad de-risking instead of customer-level analysis.	Document the risk drivers and apply proportionate enhanced measures.

THE POLICY ERROR

Broad de-risking is administratively simple but analytically weak. It can move activity into smaller institutions, informal channels and less transparent payment routes while leaving the underlying risk intact.

A PRACTICAL EFFECTIVENESS DASHBOARD

Trend by sector and reporting institution.

INDICATOR	WHAT IT SHOWS	WEAK PERFORMANCE
Identifier completeness	The ability to match subjects, accounts and counterparties without manual reconstruction.	High report volume with missing, inconsistent or unreliable identifiers.
Ownership resolution	The ability to identify the natural person who owns or controls the customer, company or asset.	Legal persons reported repeatedly without controller-level information.
Network linkage	The share of reports connected to prior subjects, beneficiaries, devices, addresses or transactions.	Reports remain isolated despite recurring names and counterparties.
Analytical conversion	The share of reporting that supports enrichment, dissemination, investigation or another documented risk action.	Submission counts increase while downstream use remains flat.

02 / REGULATORY TRANSITION

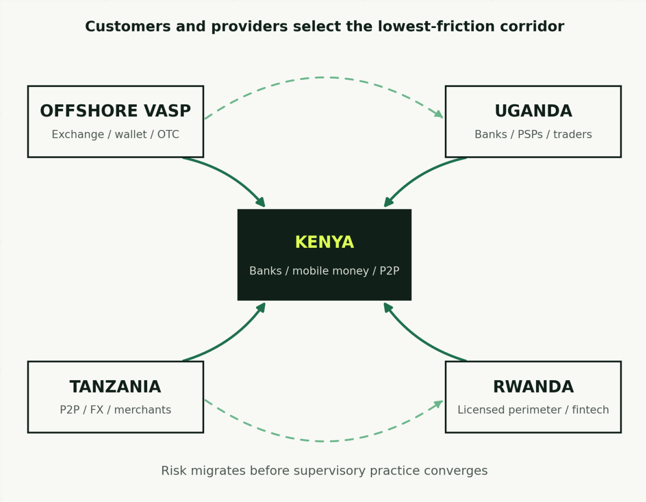
Virtual-asset exposure is becoming an ordinary-payments problem.

Kenya's draft Virtual Asset Service Providers Regulations signal the direction of travel. They do not, by themselves, give reporting institutions a complete view of exposure during the transition to licensing and supervision.

Most customers will not present as virtual-asset users. Exposure may be routed through personal bank accounts, mobile-money collections, informal peer-to-peer traders, payment processors, offshore exchanges and merchants that use stablecoins for settlement.

Differences in regulatory timing across Kenya, Uganda, Rwanda and Tanzania create scope for substitution. Customers and providers can shift to the jurisdiction, platform or payment corridor that presents the least friction, while the underlying economic activity remains regional.

Transaction monitoring should therefore begin with behaviour and relationships, not product labels. Relevant features include repeated small collections, rapid consolidation, common beneficiaries, device links, pass-through activity and payment purposes that do not match the customer's profile or supporting documents.



PATTERN

Retail collection accounts

Numerous incoming payments are consolidated and transferred to a provider, trader or common beneficiary soon after receipt.

PATTERN

Misstated payment purpose

Payments are described as imports, gaming, consulting or online services, but invoices, counterparties and account behaviour do not support the explanation.

PATTERN

Fiat on- and off-ramps

Value moves outside the visible banking chain, while cash, bank or mobile-money conversion occurs at the entry and exit points.

MINIMUM DATA VIEW FOR VASP EXPOSURE

Start with a usable view before adding complex models.

01
Customer and account
KYC profile, occupation, expected activity, source of funds and linked accounts.

02
Counterparty
Known exchanges, traders, processors, repeated payees and common beneficiaries.

03
Channel and device
Bank, mobile money, card, IP address, device, agent and access location.

04
Flow behaviour
Collection, consolidation, pass-through, cash-out and rapid cross-border movement.

05
Economic purpose
Invoice, goods, service, trade route and explanation consistent with the value moved.

03 / INTELLIGENCE YIELD

STR growth matters only when the reports can be converted into intelligence.

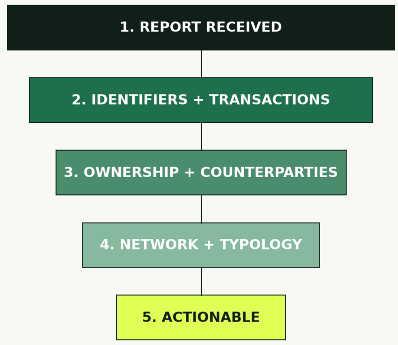
Grey-list remediation often increases filing volumes. Institutions become more cautious, supervisors ask for evidence of compliance and borderline cases are escalated. This may be a rational short-term response, but it can also increase the number of reports without improving their analytical value.

A useful STR does three things. It identifies the parties with enough precision to support matching. It explains how the activity differs from the customer's known profile or stated purpose. It provides enough transaction and ownership detail for the FIU to test links, reconstruct the movement of value and assess the wider network.

This standard applies across sectors, but the source material differs. Banks and payment firms can contribute transaction depth. DNFBPs can contribute context on ownership, legal authority, property, source of funds and the commercial purpose of a transaction.

The relevant performance question is therefore not how many reports were filed. It is how many could be enriched, linked, disseminated and used.

THE INTELLIGENCE VALUE CHAIN



Each missing field reduces the probability that a report survives the path from filing to investigative use.

FIVE QUESTIONS BEFORE FILING

01 What activity would be expected from this customer, business or transaction?

02 What changed, and why is the deviation material rather than merely unusual?

03 Who owns, controls, instructs or benefits from the parties involved?

04 How did value move across accounts, products, channels and jurisdictions?

05 What evidence supports the suspicion, and which links should the FIU test first?

A concise report can still be complete. A vague report cannot.

MEASURE

Data sufficiency

Names, identification numbers, accounts, contacts, addresses and ownership links that can be matched reliably.

MEASURE

Linkage potential

The extent to which a report can be connected to other subjects, transactions, locations, devices or prior intelligence.

MEASURE

Downstream utility

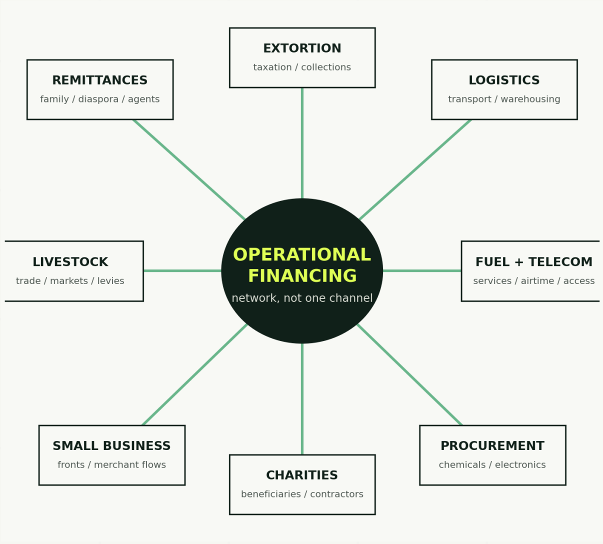
Dissemination, investigative uptake, restraint, recovery, prosecution or another documented risk intervention.

ANALYTICAL JUDGEMENT

Defensive filing moves uncertainty from the reporting institution to the FIU. It does not improve the quality of the underlying information.

04 / NETWORK ANALYSIS

Terrorist-financing analysis should follow the commercial network, not the payment product.



INDICATOR STACKING: FROM ALERT TO ASSESSMENT

Transaction behaviour
Splitting, rapid pass-through, unusual cash conversion, repeated merchant collections or unexplained cross-border settlement.

Network and control
Common controllers, repeated beneficiaries, shared devices, linked merchants, border locations or circular flows.

Commercial contradiction
Activity inconsistent with the stated business, trade route, procurement need, customer profile or known source of funds.

No single indicator establishes terrorist financing. Confidence increases when independent sources point to the same explanation.

Al-Shabaab-related risk is regional because revenue collection, movement, procurement and commercial support extend beyond Somalia. Kenya, Ethiopia, Djibouti, Uganda and Tanzania can appear within the same financial or supply chain.

Remittances remain relevant, but they are neither unusual nor distinctive on their own. The wider picture may include taxation and extortion, transport, livestock and agricultural trade, fuel, telecommunications, small-business fronts and the procurement of chemicals or electronic components.

This changes the unit of analysis. A single sender or transfer is rarely sufficient. Greater weight should be placed on repeated beneficiaries, linked merchants, common controllers, border locations, procurement patterns and activity that conflicts with the stated business.

A network-based approach can also reduce false positives. Legitimate remittance activity is extensive. Analytical confidence increases when transaction behaviour is supported by network, geographic, ownership and commercial indicators.

SANCTIONS CONTROL

The UN amended entry QDi.439 on 8 July 2026. Institutions should update machine-readable list data, validate field mapping, test aliases and transliterations, and rescreen affected activity. Vendor confirmation should not replace internal evidence that the update was applied correctly.

05 / CONTROL AGENDA

Institutions should focus the response on control weaknesses they can measure.

FINANCIAL INSTITUTIONS + PSPS

Build an indirect exposure view

Virtual-asset and sanctions risk should be visible through linked customers, counterparties, channels and transaction behaviour.

- Validate sanctions-list ingestion and field mapping.
- Identify known exchanges, traders and processors.
- Detect rapid collection, consolidation and pass-through.
- Link customers across devices, accounts and beneficiaries.

DNFBPS

Improve ownership and funds evidence

Professional intermediaries often hold information that cannot be inferred from a payment record.

- Identify the natural person who owns or controls the client.
- Record the source of authority and source of funds.
- Explain third-party payments and unusual urgency.
- Retain documents that support the stated commercial purpose.

ALL REPORTING INSTITUTIONS

Raise the analytical standard of STRs

The report should make the suspicion clear without requiring the FIU to recreate the institution's internal review.

- State the expected activity and the material deviation.
- Identify counterparties, controllers and beneficiaries.
- Describe the movement of value across the full period.
- Distinguish transactional suspicion from general risk.

FIUS + SUPERVISORS

Measure conversion, not submission alone

Sector feedback should show which reporting practices produce usable intelligence and which create volume without value.

- Track identifiers, ownership links and narrative quality.
- Measure linkage, dissemination and investigative uptake.
- Compare conversion rates across sectors and institutions.
- Target supervisory action at recurring data weaknesses.

THE TEST

A control should be judged by what it enables: better identification of risk, a clearer explanation of activity or a timely intervention. Controls that add paperwork without improving any of these outcomes deserve review.

WHAT TO WATCH NEXT

The next signal is likely to appear in implementation data before it appears in another headline.

01

Kenyan VASP regulations

Final rules, licensing mechanics, supervisory allocation and the treatment of customers and providers during the transition period.

02

FATF remediation evidence

Changes in STR quality, beneficial-ownership access, sanctions implementation, investigations, prosecutions and asset outcomes.

03

Regional enforcement patterns

Cases involving virtual assets, mobile money, trade, property, professional intermediaries and cross-border payment corridors.

East Africa's AML/CFT frameworks are becoming denser. The remaining gap is execution.

The relevant evidence will be found in the quality of customer data, the identification of indirect exposure, the usefulness of STRs and the connection between financial intelligence and enforcement.

For management, the question is no longer simply if a policy exists. The question is if the institution can show, from its own data, that the policy is changing what it detects and how it responds.

SELECTED PUBLIC SOURCES

1. Financial Action Task Force, *Jurisdictions under Increased Monitoring*, 19 June 2026.
2. Central Bank of Kenya, *Invitation for Comments on the Draft Virtual Asset Service Providers Regulations, 2026*, 18 March 2026.
3. United Nations Security Council, *List of updates to the UNSC Consolidated List*, entry QDi.439 amended 8 July 2026.
4. Financial Action Task Force, *An Effective System to Combat Money Laundering and Terrorist Financing*.
5. Financial Action Task Force, *Guidance on AML/CFT-related Data and Statistics*.
6. Public regulatory and sanctions material reviewed for the reporting period ending 13 July 2026.

ABOUT THE AUTHOR

Richard Kabiru

Richard works across financial intelligence, AML/CFT, data analytics and systems design.

METHOD + DISCLAIMER

This publication separates confirmed public developments from the author's analytical judgement. It does not represent the position of any public institution and is not legal or regulatory advice.