AFRICAN ASSOCIATION OF ACCOUNTANTS - GENERAL

AAAG FRAMEWORK FOR DETECTION OF ILLICIT FINANCIAL

A STRATEGIC AND OPERATIONAL GUIDE FOR OFFICES OF ACCOUNTANTS GENERAL IN AFRICA

AFRICAN ASSOCIATION OF ACCOUNTANTS - GENERAL

AAAG FRAMEWORK FOR DETECTION OF ILLICIT FINANCIAL FLOWS

A STRATEGIC AND OPERATIONAL GUIDE FOR OFFICES OF ACCOUNTANTS GENERAL IN AFRICA

APRIL 2026

1.0 Strategic Context

Illicit Financial Flows (IFFs) continue to undermine domestic resource mobilisation, distort public financial management systems, and weaken fiscal sovereignty across Africa. Offices of Accountants General, by virtue of their control over financial reporting, treasury operations, and government accounting systems, are uniquely positioned to act as first-line detectors of suspicious financial transactions.

This framework is, thus, aims to strengthen the capacity of Offices of Accountants General to systematically identify, analyse, and respond to illicit financial flows through structured processes, data-driven analytical tools, and effective institutional coordination. In doing so, the framework seeks to position OAGs not merely as custodians of public accounts but as strategic actors in safeguarding public resources, enhancing fiscal transparency, and supporting the broader fight against financial leakages and economic crime.

2.0 Scope and Purpose

The framework applies across key areas of public financial management where the risk of illicit financial flows is most pronounced. This includes government financial transactions throughout the expenditure and revenue cycle, particularly in relation to budget execution, procurement, payments, and revenue administration. It also extends to the financial activities of State-Owned Enterprises, which often manage substantial public assets and commercial transactions that may present heightened vulnerability to opacity, leakages, and weak oversight. Further, the framework covers cross-border transactions linked to public funds, recognising that illicit financial flows frequently involve the movement of value across jurisdictions through trade misinvoicing, offshore structures, or external contracting arrangements. In addition, it encompasses donor-funded and project-based expenditures, where fragmented reporting arrangements, multiple implementing entities, and complex funding channels may create opportunities for misapplication or concealment of funds. Together, this scope ensures a comprehensive and risk-informed basis for OAG engagement in the detection and analysis of illicit financial flows.

This framework is designed to:

a) Strengthen early detection mechanisms within government financial systems
b) Provide a risk-based approach to identifying suspicious transactions
c) Guide the selection and application of analytical tools
d) Enable institutional coordination with anti-corruption and financial intelligence bodies
e) Support data-driven oversight and accountability

3.0 Conceptual Definition of IFFs in a PFM Context

Within the OAG environment, IFFs manifest as:

a) Unrecorded or misclassified public transactions
b) Deliberate manipulation of financial records
c) Leakages through procurement, payroll, or revenue systems

d) Cross-border financial misreporting
e) Fraudulent or non-compliant financial activities

4.0 Framework Architecture

The framework is structured around five interlinked pillars:

a) Pillar 1: Risk Identification and Mapping
b) Pillar 2: Transaction Monitoring and Red Flag Detection
c) Pillar 3: Data Analytics and Tools Application
d) Pillar 4: Institutional Coordination and Escalation
e) Pillar 5: Capacity Building and Continuous Improvement

Taken together, the Pillars provide an operational system by linking risk identification, transaction monitoring, data analytics, institutional escalation, and sustained capacity development. In this way, the framework positions Offices of Accountants General not merely as custodians of financial records but as strategic guardians of public resources, capable of using data, systems, and coordinated oversight to detect, deter, and respond to illicit financial flows.

4.1 Pillar 1: Risk Identification and Mapping

The objective of this pillar is to enable the Office of the Accountant General to systematically identify the areas, transactions, entities, and processes within the public financial management system where illicit financial flows are most likely to arise. This requires moving beyond general awareness of risk to a more deliberate process of pinpointing where vulnerabilities exist, how they manifest, who is involved, and which systems or control weaknesses may be exploited to conceal or facilitate suspicious financial activity.

In practice, risk identification and mapping is the foundation of the entire framework. An OAG cannot effectively detect suspicious transactions unless it first understands which parts of the public finance architecture are most exposed to abuse. This pillar, therefore, calls for a structured assessment of transaction flows, institutional processes, approval chains, data sources, and control gaps across government operations.

4.1.1 Key Risk Domains in OAG Systems

a) Procurement

Typical IFF Exposure: Overpricing, ghost suppliers, bid rigging, collusion, contract splitting, duplicate payments.

Procurement remains one of the highest-risk areas because it involves large volumes of public expenditure, multiple actors, and significant discretion in supplier selection, contract management, and payment approval. Illicit financial flows may arise where contracts are deliberately overpriced, payments are made to non-existent or related-party suppliers, or procurement processes are manipulated to favour particular firms. Risk is especially high where there is a weak linkage between procurement systems, contract registers, and payment systems.

Practical relevance for OAGs:

The OAG should monitor whether payments correspond to valid contracts, approved procurement plans, delivery confirmations, and registered suppliers. Particular attention should be paid to repeated awards to the same vendors, payments just below approval thresholds, unusually high unit costs, and multiple invoices for similar goods or services.

b) Payroll

Typical IFF Exposure: Ghost workers, duplicate salaries, unauthorised allowances, payments to separated staff, payroll manipulation.

Payroll systems may be exploited through the creation of fictitious employees, retention of employees who have retired or resigned, duplication of employee records, or inflation of allowances and benefits. These leakages may not always appear dramatic individually, but over time they can result in substantial diversion of public funds.

Practical relevance for OAGs:

The OAG should ensure regular reconciliation between payroll records, human resource databases, establishment registers, and bank payment files. Red flags include multiple employees using the same bank account, salary payments to persons without valid national identification or staff numbers, abrupt spikes in payroll costs, and continued payments after termination or transfer.

c) Revenue

Typical IFF Exposure: Under-collection, diversion of receipts, tax evasion, suppression of collections, and delayed banking.

Revenue-related IFF risks arise where public revenues are collected but not fully declared, recorded, or remitted. This may occur in tax administration, non-tax revenue collection, customs, licensing, service fees, or other government income streams. In some instances, funds may be collected outside official channels or diverted before they enter the treasury systems.

Practical relevance for OAGs:

The OAG should compare expected revenue against actual collections, reconcile source system records with bank deposits and treasury ledgers, and investigate unusual variances, persistent arrears, or unexplained shortfalls. High-risk areas include cash-based collections, decentralised revenue points, and entities with weak digital controls.

d) Public Debt

Typical IFF Exposure: Hidden liabilities, misreporting of obligations, irregular borrowing, unrecorded guarantees, and inflated debt servicing transactions.

Public debt presents IFF risks where obligations are contracted outside approved processes, where liabilities are deliberately omitted from records, or where debt servicing arrangements conceal excessive fees, irregular commissions, or undisclosed contractual commitments.

The risk is heightened in environments with fragmented debt management systems or weak disclosure practices.

Practical relevance for OAGs:

The OAG should reconcile debt records with loan agreements, disbursement statements, debt servicing schedules, and treasury payment data. Particular scrutiny should be given to off-budget borrowing, contingent liabilities, government guarantees, and debt-related payments to intermediaries whose roles are unclear or insufficiently documented.

e) Grants and Transfers

Typical IFF Exposure: Misallocation, leakage, diversion of earmarked funds, duplicate disbursements, and weak beneficiary verification.

This area includes intergovernmental transfers, donor disbursements, subsidies, social grants, and project financing. Risks arise when funds are transferred to entities or beneficiaries without adequate verification, when funds intended for specific purposes are used for unrelated expenditures, or when reporting and accountability arrangements are too weak to trace end use.

Practical relevance for OAGs:

The OAG should verify whether disbursements align with approved budgets, financing agreements, and beneficiary records. Red flags include unsupported transfer requests, significant delays in acquittal, repeated transfers without expenditure reports, and discrepancies between funds released and activities delivered.

f) Public Assets

Typical IFF Exposure: Undervalued disposals, theft, unrecorded assets, irregular transfers, misuse of government property.

Public assets, including land, buildings, vehicles, equipment, inventories, and strategic reserves, can be a major source of illicit value extraction where disposal processes are opaque, asset registers are incomplete, or assets are transferred without proper authorisation and valuation. Weak asset management systems can conceal theft, underpricing, or private appropriation of public resources.

Practical relevance for OAGs:

The OAG should maintain or support reliable asset registers, reconcile disposals against approvals and valuations, and examine whether sale proceeds are fully recorded and remitted. Areas of concern include assets sold below market value, missing inventory, unexplained write-offs, and inconsistencies between physical verification results and accounting records.

g) Cross-Border Financial Flows

Typical IFF Exposure: Trade misinvoicing, capital flight through offshore accounts, transfer pricing manipulation (particularly within State-Owned Enterprises), illicit profit shifting, and concealed external payments.

Cross-border transactions represent a critical and often complex channel through which illicit financial flows occur. These flows typically involve the movement of value across jurisdictions in ways that obscure the true nature, origin, or destination of funds. Trade misinvoicing, through over-invoicing imports or under-invoicing exports, is one of the most prevalent mechanisms used to shift value out of a country. Similarly, public funds may be diverted into offshore accounts through inflated contracts, external service payments, or undisclosed financial arrangements. In the case of State-Owned Enterprises, transfer pricing abuses may arise where transactions between related entities are deliberately mispriced to shift profits to low-tax or opaque jurisdictions.

Practical relevance for OAGs:

The OAG should monitor cross-border payments linked to procurement contracts, debt servicing, consultancy fees, and SOE transactions. This includes verifying whether payments align with contractual terms, benchmarking pricing against international standards, and examining whether the counterparties are legitimate and appropriately registered. Particular attention should be paid to payments routed through intermediary jurisdictions, transactions involving tax havens, large foreign currency transfers with limited supporting documentation, and discrepancies between customs data and financial records. Collaboration with customs authorities, central banks, and financial intelligence units is essential in this domain.

h) Systemic and Control Environment Risks

Typical IFF Exposure: Weak or bypassed internal controls, manual overrides in IFMIS, absence of audit trails, unauthorised system access, data manipulation, and fragmented financial systems.

Systemic risks arise not from a single transaction type, but from weaknesses in the overall control environment that allow illicit financial flows to occur undetected or unchallenged. These include inadequate segregation of duties, excessive reliance on manual processes, weak system controls, and poor system integration. Manual overrides in IFMIS or other financial systems can allow transactions to bypass established approval workflows, while the absence of reliable audit trails makes it difficult to trace who initiated, approved, or altered transactions. In such environments, even well-designed policies may be rendered ineffective due to weak enforcement and system vulnerabilities

Practical relevance for OAGs

The OAG should assess the integrity of financial systems and the robustness of embedded controls. This includes monitoring the frequency and justification of manual overrides, reviewing user access rights to ensure appropriate segregation of duties, and verifying that all transactions are logged with complete audit trails. Red flags include frequent system overrides without documented justification, users with excessive privileges, missing or altered transaction histories, and inconsistencies between system-generated reports and underlying data. Strengthening system controls, enforcing access governance, and ensuring end-to-end integration between financial systems are critical to mitigating these risks.

Key Actions Under Pillar 1

a) Develop an IFF Risk Register

The OAG should establish a formal IFF Risk Register as a working tool to document, assess, and monitor potential sources of illicit financial flows across government systems. This register should not be a generic compliance document; rather, it should serve as a living instrument that identifies:

i. the specific risk area;
ii. the nature of the suspected IFF vulnerability;
iii. the likely methods or schemes through which the risk may materialise;
iv. the systems, entities, and transaction types affected;
v. the control weaknesses enabling the risk;
vi. the likelihood and impact of occurrence; and
vii. the responsible office for monitoring and mitigation.

Practical value:

A well-designed risk register helps the OAG prioritise limited analytical and investigative resources. It also creates a consistent basis for engagement with internal audit, anti-corruption agencies, supreme audit institutions, procurement authorities, and financial intelligence units.

b) Conduct Risk Scoring

Once risks are identified, the OAG should conduct risk scoring to assess which areas require the highest degree of attention. A simple High / Medium / Low rating may be used initially, but over time this can evolve into a more detailed scoring methodology based on factors such as:

i. value of transactions involved;
ii. frequency of occurrence;
iii. complexity of the transaction chain;
iv. degree of manual intervention;
v. historical incidence of fraud or irregularity;
vi. quality of internal controls; and
vii. ease with which the risk can be concealed.

Practical value:

Risk scoring ensures that the OAG does not treat all risks equally. For example, a low-value but frequent payroll anomaly may require a different response from a high-value, complex procurement transaction involving external parties and cross-border payments. This approach supports targeted monitoring and more efficient deployment of analytical tools.

c) Map Risks to Financial Systems and Data Sources

The OAG should clearly map identified risks to the systems, platforms, and datasets through which they can be detected. This includes IFMIS, payroll systems, HR databases, e-

procurement platforms, revenue management systems, debt management systems, banking records, asset registers, customs systems, donor project platforms, and beneficial ownership or company registry data where available.

This step is critical because a risk can only be monitored effectively if the OAG knows where the relevant evidence sits, which datasets need to be reconciled, and which system-generated indicators can reveal suspicious patterns.

Practical value

For example:

i. Procurement risks may require matching supplier data, contract awards, invoice records, and payment files;
ii. Payroll risks may require comparing HR records, personnel lists, and bank account data;
iii. Donor fund risks may require linking project budgets, withdrawal applications, expenditure returns, and treasury releases.

Mapping risks to data sources also helps the OAG determine what analytical tools are most appropriate for each risk domain.

d) Operational Interpretation of Pillar 1

In practical terms, Pillar 1 requires the OAG to ask four core questions:

i. Where in the public finance system are leakages most likely to occur?
ii. What forms are those leakages likely to take?
iii. Which systems, records, and transactions can reveal them?
iv. Which risks should be prioritised for immediate monitoring and analysis?

By answering these questions, the OAG creates a clear risk intelligence base from which transaction monitoring, anomaly detection, and institutional response can proceed in a focused and evidence-based manner. Pillar 1 is therefore not merely a preliminary diagnostic step; it is the strategic entry point for effective IFF detection. It enables the Office of the Accountant General to shift from broad concern about financial leakages to a disciplined and intelligence-led understanding of where the greatest threats lie, how they operate, and what data and systems must be interrogated to uncover them. By establishing this foundation, the OAG is better positioned to deploy analytical tools more effectively, strengthen preventive controls, and support timely escalation of suspicious transactions for further action.

4.2 Pillar 2: Transaction Monitoring and Red Flag Detection

The objective of this pillar is to enable OAG to systematically monitor financial transactions and identify suspicious patterns using predefined indicators (red flags). This pillar translates risk awareness (from Pillar 1) into active surveillance, ensuring that high-risk transactions are not only known but continuously interrogated.

In practice, this requires embedding rules-based and data-driven monitoring mechanisms within financial systems to detect anomalies in real time or through periodic review. Transaction monitoring is the frontline detection function of the

framework. It involves scanning large volumes of financial data across IFMIS, payroll, procurement, and revenue systems to identify transactions that deviate from expected norms. Rather than attempting to review every transaction manually, OAGs should rely on structured red flag indicators that automatically highlight transactions requiring further scrutiny.

4.2.1 Core Red Flag Categories

a) Transactional Red Flags

Typical Indicators include:

i. Unusual transaction sizes or frequency
ii. Round-number transactions
iii. Transactions just below approval thresholds

Practical interpretation

These indicators point to potential manipulation of transaction values to bypass controls or conceal irregularities. For example, repeated transactions just below approval thresholds may suggest deliberate structuring to avoid higher-level authorisation. Similarly, round-number payments (e.g., exact multiples) may indicate fabricated or estimated figures rather than actual costs.

Application in OAG systems

The OAG should configure automated queries or dashboards to flag such transactions across payment systems, procurement records, and treasury disbursements.

b) Behavioural Red Flags

Typical Indicators include:

i. Repeated use of the same vendors
ii. Rapid contract awards
iii. Unusual timing (weekends, after-hours)

Practical interpretation

Behavioural red flags highlight patterns that suggest potential collusion, preferential treatment, or circumvention of due process. For instance, repeated awards to a single vendor may indicate restricted competition, while transactions processed outside normal working hours may signal attempts to avoid scrutiny.

Application in OAG systems

The OAG should analyse vendor concentration, procurement timelines, and transaction timestamps to detect irregular behavioural patterns.

c) System-Based Red Flags

Typical Indicators include:

i. Manual overrides in IFMIS
ii. Backdated entries
iii. Missing audit trails

Practical interpretation

These indicators reflect weaknesses or deliberate manipulation within financial systems. Manual overrides may bypass established controls, while backdated entries can be used to conceal timing discrepancies or unauthorised transactions. Missing audit trails undermine traceability and accountability.

Application in OAG systems

The OAG should regularly review system logs, override reports, and audit trail completeness to ensure system integrity is maintained.

d) Cross-System Inconsistencies

Typical Indicators include:

i. Payroll vs HR database mismatches
ii. Procurement vs payment discrepancies

Practical interpretation

Illicit financial flows often exploit gaps between systems that are not fully integrated. For example, payments may be made to individuals not reflected in HR records, or procurement payments may not correspond to valid contracts.

Application in OAG systems

The OAG should perform periodic reconciliations across systems to ensure consistency and completeness of records.

4.2.2 Operational Output of Pillar 2

At the end of this pillar, the OAG should have:

i. A catalogue of red flag indicators tailored to national systems
ii. Automated or semi-automated transaction monitoring routines
iii. A flagged transactions log for further analysis
iv. Defined thresholds for escalation to investigation

4.3 Pillar 3: Data Analytics and Tools Application

This Pillar aims to equip OAG with the analytical capability to interrogate financial data, identify hidden patterns, and transform raw transactional information into actionable intelligence. While Pillar 2 identifies suspicious transactions, Pillar 3 provides the analytical depth required to understand and validate those suspicions. It shifts the

focus from detection to evidence-based analysis, enabling OAGs to distinguish between anomalies and genuine irregularities.

4.3.1 Operational Context

a) Analytical Techniques

Each technique serves a distinct investigative purpose:

i. **Trend Analysis:** Detects unusual fluctuations over time (e.g., sudden spikes in procurement spending) by examining how values change over time to identify unusual increases, decreases, or patterns that do not align with normal operations. For example, if monthly procurement spending is usually around $2 million but suddenly jumps to $8 million in one month without a clear reason, this spike may indicate irregular or inflated transactions.

ii. **Outlier Detection:** Flags transactions that significantly deviate from norms by identifying transactions that are significantly higher or lower than typical values within a dataset. For example, if most supplier payments range from $5,000 to $20,000 but one payment is $250,000, that transaction is an outlier and should be investigated.

iii. **Network Analysis:** Reveals relationships between entities by mapping connections (such as suppliers, employees, and bank account relationships) to uncover hidden connections or collusion. For example, if two different suppliers share the same bank account or contact details, network analysis may reveal a link between them, suggesting possible bid rigging or fraud.

iv. **Duplicate Detection:** Identifies repeated transactions that may indicate duplicate payments or fraud. For example, if the same invoice number, amount, and supplier appear twice in the system and both were paid, this may indicate a duplicate or fraudulent payment.

v. **Ratio Analysis:** Highlights inconsistencies in financial relationships (e.g., cost per unit anomalies) by comparing relationships between financial values to identify inconsistencies or inefficiencies. For example, if the cost per kilometre of road construction is significantly higher in one project compared to similar projects, this may indicate overpricing or misallocation of funds.

vi. **Benford's Law Analysis:** Identifies unnatural number distributions indicative of fabricated data by checking whether the distribution of numbers (especially leading digits) follows a natural pattern; deviations may suggest manipulated or fabricated data. For example, in naturally occurring financial data, numbers starting with "1" appear more frequently than "9". If a dataset shows an unusually high number of transactions starting with "7" or "9", it may indicate artificial manipulation.

Practical application

These techniques should be applied to datasets extracted from IFMIS, payroll, procurement, and revenue systems, particularly in high-risk areas identified under Pillar 1.

b) Tool Selection Framework
Different tools serve different levels of analytical maturity:

i. Basic tools (Excel, Power BI): Suitable for initial analysis and dashboards
ii. Audit tools (Audit Command Language, IDEA): Enable deep forensic interrogation
iii. Visualisation tools (Tableau, Power BI): Support interpretation and reporting
iv. AI/ML tools (Python, R): Enable predictive and advanced anomaly detection
v. Database tools (SQL): Allow interrogation of large datasets

Practical application

OAGs should adopt a tiered approach, starting with accessible tools and progressively building toward advanced analytics as capacity improves.

c) Tool Selection Criteria
Tool selection should be guided by:

i. Data volume and complexity
ii. Existing ICT infrastructure (including IFMIS integration)
iii. Availability of skilled personnel
iv. Cost and long-term sustainability
v. Need for real-time vs periodic analysis

Practical interpretation

A country with limited resources may prioritise Excel and Power BI, while more advanced environments may adopt AI-driven tools integrated directly into IFMIS.

4.3.2 Operational Output of Pillar 3
a) Standardised analytical procedures and scripts
b) A defined tool stack aligned to national capacity
c) Analytical dashboards and reports
d) Documented evidence trails for flagged transactions

4.4 Pillar 4: Institutional Coordination and Escalation
This Pillar aims to ensure that suspicious transactions identified through monitoring and analysis are properly investigated, acted upon, and resolved through coordinated institutional response.

4.4.1 Operational Context
The OAG is not an investigative or prosecutorial body in isolation. An effective response to illicit financial flows requires structured collaboration among institutions responsible for financial intelligence, audit, enforcement, and regulation. Therefore, this pillar ensures that detection efforts translate into meaningful action and accountability.

a) Key Stakeholders
Depending on the country context, the following represents the key stakeholders in the IFFs within the OAG environment:

i. Financial Intelligence Units (FIUs)
ii. Revenue Authorities
iii. Anti-Corruption Agencies
iv. Supreme Audit Institutions (SAIs)
v. Central Banks
vi. Law Enforcement Agencies

b) Escalation Protocol

i. Detection of Suspicious Transaction - Triggered through red flag monitoring or analytical review.
ii. Internal Validation within OAG - The OAG confirms whether the anomaly is legitimate or requires escalation by reviewing supporting documentation and system records.
iii. Documentation and Evidence Consolidation - All relevant data, transaction records, system logs, and analysis outputs are compiled into a structured case file.
iv. Referral to Appropriate Authority - Depending on the nature of the issue, the case is referred to FIUs, anti-corruption bodies, or law enforcement.
v. Monitoring of Case Progress - The OAG tracks the status of referred cases to ensure follow-through and closure.

c) Practical Considerations

i. Establish formal MoUs or protocols with partner institutions
ii. Define clear thresholds for escalation
iii. Ensure secure data sharing mechanisms
iv. Maintain a case tracking system

4.4.2 Operational Output of Pillar 4

v. A formal IFF escalation and referral framework
vi. Standardised case documentation templates
vii. A case tracking and reporting system
viii. Strengthened inter-agency collaboration

4.5 Pillar 5: Capacity Building and Continuous Improvement

This Pillar aims to build and sustain the institutional, technical, and human capacity required for effective detection and response to illicit financial flows. IFF detection is not a one-time intervention but a continuous capability that must evolve alongside emerging risks, technologies, and financial practices. This pillar ensures that OAGs remain adaptive, skilled, and forward-looking.

4.5.1 Key Interventions

i. Develop IFF Detection Training Programs - Structured training covering risk identification, data analytics, forensic techniques, and system interrogation.
ii. Integrate IFF Modules into Capacity Building - Embedding IFF awareness into broader public financial management reforms ensures alignment with accounting, reporting, and audit processes.
iii. Establish Centres of Excellence within OAGs - Dedicated units specialising in data analytics, forensic accounting, and financial intelligence.

iv. Promote Peer Learning Across AAAG Member States - Facilitate knowledge exchange, case studies, and benchmarking across countries.
v. Conduct Regular Simulation Exercises - Test detection systems and institutional response through scenario-based exercises.

4.5.2 Practical Interpretation

Capacity building should not be limited to training workshops but should include:

i. Hands-on use of analytical tools
ii. Real-case analysis
iii. Continuous professional development
iv. Institutional knowledge retention

4.5.3 Operational Output of Pillar 5

i. A structured capacity development roadmap
ii. Skilled personnel in analytics and forensic review
iii. Institutionalised learning mechanisms
iv. Continuous improvement of detection systems

5.0 Closing Strategic Insight

The detection of illicit financial flows must move beyond post-fact audit reviews to a model of real-time financial intelligence embedded within government systems. Given their central role in financial control, reporting, and systems oversight, Offices of Accountants General are uniquely positioned to serve as the first line of defence against IFFs, provided they are supported by the appropriate frameworks, analytical tools, and institutional mandate.

THE AFRICAN ASSOCIATION OF ACCOUNTANTS GENERAL (AAAG)

Plot 488a, Lake Road | Kabulonga – Lusaka, Zambia | +260 958120115

info@aaag.africa | www.aaag.africa

Follow us on Social Media

AFRICAN ASSOCIATION OF ACCOUNTANTS GENERAL

WWW.AAAG.AFRICA