SPECIAL ISSUE

THE KENYA GAZETTE

Published by Authority of the Republic of Kenya

(Registered as a Newspaper at the G.P.O.)

Vol. CXXVIII—No. 127 **NAIROBI, 27th July, 2026** **Price Sh. 60**

GAZETTE NOTICE NO. 11488

THE CONSTITUTION OF KENYA

THE COMMISSION ON REVENUE ALLOCATION

STANDARDS AND GUIDELINES ON THE AUTOMATION OF COUNTY OWN SOURCE REVENUE

IN EXERCISE of the powers conferred by Article 216 (1) *(c)* and (2) of the Constitution of Kenya, the Commission on Revenue Allocation, in consultation with the National Treasury, the Council of Governors, the Office of the Auditor-General, the Office of the Controller of Budget, the Information and Communication Technology Authority and the County Governments, issues the following Standards and Guidelines—

ISSUED: MAY, 2026

Preface

The Commission on Revenue Allocation (hereinafter "the Commission") issues these Standards and Guidelines on the Automation of County Own Source Revenue (hereinafter "the Guidelines") pursuant to Article 216 (1) *(c)* of the Constitution of Kenya, which mandates the Commission to make recommendations concerning the financing of, and financial management by, County Governments.

In discharging that mandate, and in accordance with Article 216 (2), the Commission seeks to—

(a) promote and give effect to the criteria set out in Article 203 (1) *(e)* and *(i);*

(b) define and enhance the revenue sources of both the National and County Governments; and

(c) encourage fiscal responsibility in the management of public resources.

The Guidelines establish a uniform, secure, interoperable and accountable framework for the design, procurement, deployment, operation and oversight of County Revenue Management Systems (CRMS) across all County Governments. They respond to systemic challenges in Own Source Revenue (OSR) mobilisation, including fragmented systems, weak integration, poor auditability and the absence of common standards.

These Guidelines supersede any previous guidelines issued by the Commission in relation to the automation of County Own Source Revenue and shall serve as the reference framework for the National Government, the County Governments and service providers.

PART I—PRELIMINARY

1. Citation and commencement

(1) These Guidelines may be cited as the Commission on Revenue Allocation Standards and Guidelines on the Automation of County Own Source Revenue, 2026.

(2) These Guidelines shall come into force on the date of their publication in the Kenya Gazette.

2. Interpretation

In these Guidelines, unless the context otherwise requires—

"Commission" means the Commission on Revenue Allocation established under Article 215 of the Constitution;

"County Government" has the meaning assigned to it under Article 176 of the Constitution;

"County Revenue Management System" or "CRMS" means an integrated information and communication technology platform deployed by a County Government for the registration, assessment, billing, collection, accounting, reporting and audit of Own Source Revenue;

"IFMIS" means the Integrated Financial Management Information System operated by the National Treasury;

"Own Source Revenue" or "OSR" means revenue raised by a County Government pursuant to Article 209 (3) of the Constitution;

"SCOA" means the Standard Chart of Accounts issued by the National Treasury;

"service provider" means any person or entity contracted to design, supply, customise, host, support or otherwise provide services in respect of a CRMS; and

such other terms as are defined in Annex 12 (Glossary and Acronyms), which shall apply to these Guidelines as if reproduced in this paragraph.

3. Object and purpose

(1) The general object of these Guidelines is to establish a standardised, secure and interoperable revenue management framework that enhances Own Source Revenue mobilisation, ensures prudent public financial management, and upholds the principles of equity, transparency and accountability.

(2) The specific objects of these Guidelines are to—

(a) standardise the functional and technical specifications of CRMS deployments across all County Governments;

(b) improve OSR performance through automation, reconciliation and enforcement;

(c) ensure compliance with the Constitution, the Public Finance Management Act, 2012, the Public Procurement and Asset Disposal Act, 2015, and the Data Protection Act, 2019;

(d) enable seamless integration with IFMIS, SCOA, IPRS, KRA, BRS, NTSA and GIS systems;

(e) safeguard the integrity, confidentiality and availability of revenue data;

(f) strengthen transparency and auditability through digital logs and reporting;

(g) build institutional capacity for sustainable system management;

(h) promote shared services and joint procurement in order to reduce costs;

(i) preserve County autonomy in system administration and revenue decision-making; and

(j) promote fiscal prudence, reduce revenue leakages and support equitable development.

4. Scope and application

(1) These Guidelines apply to—

(a) all County Governments;

(b) the National Government;

(c) private sector vendors, contractors and service providers; and

(d) development partners supporting digital revenue reforms.

(2) These Guidelines cover the full lifecycle of a CRMS, including—

(a) planning, budgeting and needs assessment;

(b) procurement and contracting;

(c) system development, acquisition or customisation;

(d) deployment, data migration and integration;

(e) operation, maintenance and user management; and

(f) audit, reporting and continuous improvement.

PART II—PROBLEM CONTEXT AND GUIDING PRINCIPLES

5. Problem statement and rationale

(1) Notwithstanding the constitutional empowerment of County Governments under Article 209 (3) of the Constitution to impose property rates, entertainment taxes and charges for services they provide, many counties continue to underperform in OSR collection on account of—

(a) fragmented and manual revenue systems within County Governments;

(b) limited automation and narrow functional coverage of existing systems;

(c) poor integration with national databases, including IPRS, BRS and IFMIS;

(d) non-standard procurement practices that lead to vendor lock-in;

(e) inadequate audit trails and weak data security;

(f) resistance to digital adoption;

(g) weak institutional capacity in information and communication technology and in revenue automation; and

(h) inadequate assurance of data migration during vendor transitions.

(2) The challenges set out in sub-paragraph (1) have resulted in—

(a) revenue leakages and reduced fiscal sustainability;

(b) inconsistent reporting standards that limit the comparability and reliability of financial data across counties and over time;

(c) compromised service delivery, as unpredictable or declining revenues constrain budget execution and public investment;

(d) weakened oversight by public finance management institutions due to fragmented or unreliable revenue data;

(e) increased exposure to fraud, abuse and system manipulation, particularly where audit trails, access controls and transaction logs are inadequate; and

(f) ineffective transitions between administrations, where incoming County leadership is unable to access or rely upon inherited digital systems, records or service contracts.

(3) A unified standards framework is therefore necessary to ensure consistency, interoperability, compliance and the long-term sustainability of CRMS.

6. Guiding principles

Every CRMS implementation shall adhere to the following principles—

(a) constitutionalism and the rule of law, requiring compliance with the Constitution and all applicable laws;

(b) accessibility, ensuring equal access to revenue services for all ratepayers, including marginalised groups;

(c) accountability and transparency, ensuring full traceability of transactions and decisions;

(d) data integrity and protection, in compliance with the Data Protection Act, 2019;

(e) interoperability and standardisation, through the use of open application programming interfaces and national standards;

(f) County autonomy, with each County retaining administrative control over local system functions;

(g) collaboration, through the encouragement of shared infrastructure and joint initiatives;

(h) multi-channel accessibility, requiring systems to be accessible by web, mobile and Unstructured Supplementary Service Data (USSD), and to comply with disability access standards; and

(i) efficiency, requiring systems to minimise operational cost and maximise revenue collection.

PART III—LEGAL AND INSTITUTIONAL FRAMEWORK

7. Constitutional basis

These Guidelines are issued under, and shall be read in conjunction with, the following provisions of the Constitution—

(a) Article 6 (2), which recognises the County Governments as distinct but interdependent units of governance that shall conduct their mutual relations on the basis of consultation and cooperation;

(b) Article 201, which requires that revenue raising and expenditure be guided by openness, accountability, equity and the prudent use of public resources;

(c) Article 203 (1) (e) and (i), which require, in the determination of the equitable share of national revenue, that consideration be given to the need to provide incentives for each County Government to optimise its capacity to raise revenue, and to provide for fiscal responsibility;

(d) Article 209 (3), which authorises County Governments to impose property rates, entertainment taxes and charges for services they provide, subject to national legislation; and

(e) Article 216 (1) (c), (2) (b) and (c), which empower the Commission to make recommendations concerning the financing of, and financial management by, County Governments, to define and enhance the revenue sources of both the National and County Governments, and to encourage fiscal responsibility.

8. Statutory framework

These Guidelines shall be implemented in accordance with—

(a) the Public Finance Management Act, 2012, in particular sections 12 (e), 125 and 133, and Parts VI and VII thereof relating to financial systems, revenue collection and oversight;

(b) the County Governments Act, 2012, in particular sections 104 and 115 relating to transparent financial management and public participation;

(c) the Public Procurement and Asset Disposal Act, 2015, which ensures competitive and transparent procurement of information and communication technology systems;

(d) the Data Protection Act, 2019, which governs the lawful processing, storage and protection of personal and financial data; and

(e) the Intergovernmental Relations Act, 2012, which facilitates coordination between the National and County Governments.

PART IV—STANDARDS, OBJECTIVES AND SPECIFICATIONS

9. Objectives

The deployment of a CRMS under these Guidelines shall aim to—

(a) enhance OSR mobilisation and support the financial autonomy of counties;

(b) standardise OSR collection and management across all County Governments;

(c) promote transparency, accountability and efficiency in revenue collection and reporting;

(d) ensure interoperability with national financial and regulatory systems;

(e) standardise functional and technical capabilities across counties; and

(f) strengthen data governance, auditability and compliance.

10. Functional standards

(1) Every CRMS shall meet the minimum functional requirements set out in Annex 1, covering—

(a) revenue source registration and identity management;

(b) tariff configuration, assessment and billing;

(c) payment processing and receipting;

(d) debt management and enforcement;

(e) self-service and access channels;

(f) configuration, period close and reporting; and

(g) audit trails and notifications.

(2) Annex 1 is binding and forms an integral part of these Guidelines.

11. Technical standards

(1) Every CRMS shall meet the minimum technical requirements set out in Annex 2, covering system architecture, hosting, infrastructure, software and development practices, integration and interoperability, security and privacy, performance and resilience, e-enforcement, disaster recovery and business continuity, reporting and analytics, configuration and extensibility, data management, and documentation and handover.

(2) Annex 2 is binding and forms an integral part of these Guidelines.

PART V—GOVERNANCE, OWNERSHIP AND ADMINISTRATION

The CRMS shall operate as a unified platform, developed and maintained by County Governments in accordance with this Part.

12. System ownership and administrative rights

(1) Ownership of the CRMS platform, including the core infrastructure and all vendor contracts entered into in respect of the platform, shall vest in the respective County Government.

(2) Each County Government shall retain exclusive operational and administrative rights over its CRMS, including user management, system configuration, data access and revenue reporting.

13. Compliance with the Guidelines

(1) Each CRMS platform shall comply with the functional requirements set out in Annex 1, the technical requirements set out in Annex 2, and the service-level provisions set out in Annex 6.

(2) No deviation from the standards prescribed in these Guidelines shall be permitted save where formally reviewed and approved through the governance structure established in paragraph 14.

14. Joint governance and oversight

(1) Each County Government shall establish a Joint Technical Committee under the chairmanship of the County Treasury and comprising representatives of all departments generating Own Source Revenue.

(2) The Joint Technical Committee shall—

(a) oversee policy decisions and system upgrades affecting the CRMS;

(b) monitor vendor performance against the Service Level Agreement; and

(c) provide strategic guidance on the ongoing development of the CRMS.

15. Data sovereignty and security

(1) Each County Government shall retain full ownership of, and custodial rights over, its revenue data; and no other party shall access such data save with the prior written approval of the County Government concerned.

(2) The CRMS platform shall comply with the Data Protection Act, 2019, and with all applicable national cybersecurity standards.

16. Local user administration and support

(1) Each County Government shall establish internal administrative structures to manage user roles, provide frontline support and escalate system issues.

(2) The County ICT Directorate shall operate a help desk and shall coordinate change management, capacity building and periodic training for County users.

PART VI—PROCUREMENT, DEVELOPMENT AND DEPLOYMENT

17. Lead implementing agency

The County Treasury shall be the lead implementing agency, and shall undertake the procurement, design, customisation and deployment of the CRMS in accordance with the Public Procurement and Asset Disposal Act, 2015, the Public Finance Management Act, 2012, and the applicable ICT standards.

18. Acquisition and modular configuration

The CRMS shall be acquired or developed as a shared system with modular capabilities that allow County-level configuration, operational autonomy and independent access to reporting and user management tools.

19. Procurement of third-party components

The procurement of third-party components, hosting services and core infrastructure shall be managed centrally by the County ICT Directorate, including vendor contracting, software licensing, support services and integration with national systems such as IFMIS, SCOA, BRS and IPRS.

20. County deployment responsibilities

Each County Government shall be responsible for financing and executing its respective local deployment activities, including hardware provisioning, staff training, onboarding, change management and the establishment of localised support infrastructure.

21. Conformity to specifications

All components of the system, including development, configuration and rollout, shall conform to the functional specifications in Annex 1, the technical standards in Annex 2 and the service-level requirements in Annex 6. No customisation or divergence from the approved architecture shall be permitted save in accordance with the governance framework established under Part V.

22. Contractual safeguards

All contracts and implementation arrangements relating to the CRMS shall include express provisions for data protection, source code escrow, knowledge transfer and system sustainability, so as to ensure long-term performance and institutional ownership.

23. Change management

Each County Government shall develop and approve a Change Management Plan in the form set out in Annex 9 prior to go-live, addressing stakeholder engagement, process redesign and the mitigation of resistance.

24. Open standards

All development under these Guidelines shall follow open standards and shall avoid arrangements that result in vendor lock-in.

PART VII—IMPLEMENTATION FRAMEWORK

The implementation of a CRMS shall comprise preparation by a County multi-sectoral committee, the acquisition of the system, its commissioning and its operational implementation, in accordance with this Part.

25. Co-ordination mechanisms

Effective co-ordination of the CRMS platform shall be ensured through structured multi-level committees and technical units that promote inter-county collaboration, operational oversight and accountability.

26. County CRMS Committees

(1) Each County Government shall establish a County CRMS Committee chaired by the County Executive Committee Member for Finance and comprising representatives from the ICT, Internal Audit, Legal, Revenue and Planning departments.

(2) The County CRMS Committee shall—

(a) oversee local deployment of the CRMS;

(b) ensure cross-departmental coordination;

(c) approve system customisations within the framework of these Guidelines; and

(d) escalate policy issues to the national level.

27. Project Implementation Units

(1) Each County Government shall establish a Project Implementation Unit.

(2) Each County Project Implementation Unit shall coordinate local infrastructure setup, user training, change management and day-to-day liaison during rollout and support phases.

28. Risk management

(1) Each County Government shall adopt the Risk Management Framework set out in Annex 5 to identify, assess, mitigate and monitor risks relating to the CRMS.

(2) Key risks to be addressed under sub-paragraph (1) include—

prolonged system breakdown;

(a) data loss;

(b) vendor lock-in;

(c) user resistance; and

(d) privacy breaches.

29. Data migration

All data migration relating to the CRMS shall be undertaken in accordance with the Data Migration and Cutover Plan set out in Annex 8, so as to ensure accuracy, integrity and minimal disruption to service.

PART VIII—MONITORING, EVALUATION AND COMPLIANCE

30. Purpose of monitoring and evaluation

The monitoring and evaluation arrangements under this Part are intended to ensure accountability, continuous improvement and compliance with these Guidelines.

31. Monitoring and evaluation principles

Monitoring and evaluation under these Guidelines shall be guided by the following principles—

(a) accuracy, requiring that data be factual and verifiable;

(b) timeliness, requiring that reports be submitted on schedule;

(c) transparency, requiring that findings be accessible to authorised stakeholders;

(d) consistency, through the use of standardised formats across counties; and

(e) actionability, requiring that findings be used to inform corrective action.

32. Monitoring framework

(1) Each County Government shall conduct daily system checks to verify, in real time, the integrity of the system, the accuracy of its data, its uptime and the management of incidents.

(2) Each County Government shall submit quarterly compliance reports, in the form set out in Annex 5, to the Commission, the National Treasury and other oversight agencies.

(3) The Office of the Auditor-General, in conjunction with County Internal Audit departments, shall conduct an annual audit of the CRMS to evaluate system controls, financial accuracy, legal compliance and data governance.

(4) The Commission, in alignment with its constitutional mandate under Article 216 (2), shall periodically assess the efficacy and efficiency of CRMS deployment and use across counties.

(5) Periodic compliance audits shall be conducted using the Compliance Audit Tool set out in Annex 4 to evaluate alignment with the functional requirements, technical standards, data governance arrangements and service-level commitments under these Guidelines.

33. Key Performance Indicators

(1) The performance of each CRMS shall be monitored and evaluated against the following minimum Key Performance Indicators, which shall guide service level agreements, compliance audits and overall system performance assessments—

(a) system uptime of not less than 99.5 per cent on a monthly basis, excluding scheduled maintenance windows;

(b) compliance with all mandatory integration requirements, including seamless interoperability with IFMIS, SCOA, BRS, IPRS and other designated national platforms;

(c) automatic posting of all transactions to the customer and transaction ledgers, without manual intervention, so as to ensure reconciliation accuracy and auditability;

(d) a user satisfaction index of not less than 80 per cent across system usability, responsiveness and support services, measured through structured surveys;

(e) zero tolerance for unresolved critical security incidents, with all reported incidents addressed within defined service level timelines and continuous monitoring for vulnerabilities;

(f) the capability to generate all mandatory statutory, financial, audit and management reports in real time or near real time, in the formats prescribed by these Guidelines; and

(g) a peak transaction processing capacity of not less than 1,200 transactions per second across all channels, ensuring scalability to handle peak demand without degradation of performance.

(2) Where additional indicators are agreed between a County Government and the Commission, the same shall be reduced to writing and incorporated into the Service Level Agreement.

34. Compliance enforcement

(1) Where a County Government or the National Treasury is in material non-compliance with these Guidelines—

(a) the Commission and the Council of Governors shall jointly issue a formal Compliance Notice, specifying the breach and a mandatory ninety-day remediation period; and

(b) the entity in breach shall submit a written Remedial Plan, the implementation of which shall be monitored by the Commission, with a view to restoring compliance within the period specified.

(2) Where a breach persists or recurs, the Commission shall escalate the matter to the Intergovernmental Budget and Economic Council in accordance with the Intergovernmental Relations Act, 2012.

(3) All compliance actions, resolutions and outcomes under this paragraph shall be documented and shared with relevant oversight bodies, and the Commission may publish anonymised compliance summaries to promote transparency and peer accountability.

35. Dispute resolution

Any dispute arising in the implementation of these Guidelines shall be resolved in accordance with the Intergovernmental Relations Act, 2012.

PART IX—REVIEW AND EFFECTIVE DATE

36. Review and amendment

(1) These Guidelines shall be reviewed every three years by the Commission in consultation with the relevant stakeholders.

(2) An early review of these Guidelines may be triggered by—

(a) any major legal or constitutional change relevant to public finance or revenue administration;

(b) any significant technological advancement that materially affects the matters governed by these Guidelines; or

(c) persistent non-compliance or systemic failure.

(3) Any review under this paragraph shall include stakeholder consultations and technical validation.

(4) Any revised Guidelines shall be gazetted as a statutory notice.

37. Effective date

These Guidelines shall take effect immediately upon their publication in the Kenya Gazette.

Note: All Annexes referred to in these Guidelines are binding and form an integral part hereof.

ANNEX 1—MINIMUM FUNCTIONAL REQUIREMENTS

CHECKLIST FOR THE CRMS

Section 1—Purpose

This Annex specifies the minimum functional requirements for the CRMS to ensure that deployments are compliant, interoperable and capable of supporting the full revenue lifecycle, from source registration through to reporting and audit.

Section 2—Scope

These requirements apply to all CRMS deployments, whether County-specific or part of a centralised national platform, and shall be observed in the procurement, development, implementation, commissioning and operation of every CRMS.

Section 3—Priority Codes

In the table that follows, the priority code "M" denotes a mandatory requirement and the priority code "S" denotes a "should-have" requirement that is desirable for optimal performance.

Section 4—Functional Requirements

Ref.	*Functional Area*	*Requirement*	*Priority*	*Test Procedure*	*Evidence*
FR.1	Registry & Identity Management	Maintain a central register of taxpayers, ratepayers and businesses linked to National ID, KRA PIN and BRS number; support many-to-many relationships between entities and revenue streams, parcels and accounts; scale to not less than one million records.	M	Create, update and search sample records; merge duplicates; execute API query.	Screenshots; search logs; API specification.
FR.2	Registry & Identity Management	Link a single entity to multiple revenue streams including land rates, single business permits, parking, market fees and similar revenue streams.	M	Link not less than three streams to one taxpayer and generate a consolidated account.	Consolidated account report.
FR.3	Registry & Identity Management	Store and retrieve supporting documents such as identity cards, licences and plans against each profile.	M	Upload and retrieve documents for sample record.	Document logs.
FR.4	Registry & Identity Management	Detect and flag duplicate accounts for review and merge with audit trail.	M	Create duplicate entries; verify that the system flags and merges them.	Duplicate detection report.
FR.5	Registry & Identity Management	Maintain a full history of all interactions, including applications, inspections, bills, payments and licences.	M	Open sample record and review history.	History log export.

Ref.	*Functional Area*	*Requirement*	*Priority*	*Test Procedure*	*Evidence*
FR.6	Registry & Identity Management	Maintain individual customer or ratepayer ledgers showing all transactions, running balances and aging, in addition to system journals.	M	View sample ledger and verify accuracy against transactions.	Ledger report.
FR.7	Registry & Identity Management	Maintain full transaction ledgers for each revenue stream with SCOA coding.	M	Generate stream ledger report and verify SCOA mapping.	Transaction ledger export.
FR.8	Registry & Identity Management	Search registry by multiple criteria including name, identity number, KRA PIN, location and status.	M	Run multi-criteria search and verify results.	Search results screenshot.
FR.9	Registry & Identity Management	Bulk import and export of registry data in CSV or Excel format, with validation.	M	Import test file and review validation logs.	Import and export logs.
FR.10	Revenue Source & Tariff Management	Configure revenue streams in accordance with the County Finance Act, the Tariff and Pricing Policy or applicable schedules.	M	Load tariff schedule and check application.	Tariff configuration logs.
FR.11	Revenue Source & Tariff Management	Add new revenue streams without vendor intervention, including setting of tariffs, SCOA codes and parameters.	M	Create a new stream and generate a bill.	Stream creation log.
FR.12	Revenue Source & Tariff Management	Rule-based engine to compute fees, penalties and interest, with version history showing effective and expiry dates, reason codes and an audit trail of changes.	M	Configure not less than ten tariffs; simulate bulk changes; show version history.	Configuration guide; change log.
FR.13	Revenue Source & Tariff Management	Bulk upload of tariffs from the Finance Bill or Tariff Policy, including zone-based rates.	M	Import bulk tariff file and verify in system.	Import log; tariff list.
FR.14	Revenue Source & Tariff Management	Map all revenue items to the Standard Chart of Accounts codes and enforce mapping before billing.	M	Attempt unmapped billing and verify that the system blocks the action.	SCOA mapping report.
FR.15	Revenue Source & Tariff Management	Maintain a register of county-owned assets tied to revenue streams, including markets, buildings and equipment.	M	Add asset and link to a revenue stream.	Asset register export.
FR.16	Revenue Source & Tariff Management	Geo-reference revenue sources for spatial planning and enforcement, with support for shapefile and GeoJSON import, layer-based queries and spatial analytics.	S	Map sample sources and view on GIS layer.	GIS map screenshot; integration document.
FR.17	Revenue Source & Tariff Management	Configure billing frequencies per stream, including daily, monthly, annual and seasonal.	M	Change billing cycle and generate bills.	Billing configuration logs.
FR.18	Revenue Source & Tariff Management	Automatic application of penalties and interest; approval of waivers and exemptions with thresholds, reason codes and document	M	Process penalty and waiver and check audit trail.	Waiver workflow log.

Ref.	*Functional Area*	*Requirement*	*Priority*	*Test Procedure*	*Evidence*
		attachments; maker-checker controls enforced.			
FR.19	Revenue Source & Tariff Management	Categorise streams by ward, market or category, and set revenue targets.	S	Assign targets and run performance report.	Target allocation file.
FR.20	Applications, Billing, Payments, Receipting	End-to-end workflow from application to inspection, billing, payment and issuance of licence or permit.	M	Apply for service and follow through to licence issue.	Workflow screenshots.
FR.21	Applications, Billing, Payments, Receipting	Customisable checklists for each service, enforced before billing.	M	Configure checklist and submit application.	Checklist configuration export.
FR.22	Applications, Billing, Payments, Receipting	Automatic flagging of accounts due for renewal, with reminders sent by SMS, email or USSD.	M	Simulate renewal period and send reminder.	Reminder logs.
FR.23	Applications, Billing, Payments, Receipting	Acceptance of payments through mobile money, electronic funds transfer, cards, USSD and agency banking, with support for offline queueing and synchronisation, and for reversals and chargebacks.	M	Process payments through each channel and simulate offline synchronisation.	Payment logs.
FR.24	Applications, Billing, Payments, Receipting	Instant issuance of receipts and confirmation to the payer.	M	Complete payment and check confirmation.	Receipt copy; SMS or email log.
FR.25	Applications, Billing, Payments, Receipting	Match daily collections with bank and wallet statements on a T+1 basis, with exception worklists and closure SLAs requiring not more than 1 per cent unresolved after T+3.	M	Import bank file, auto-match and review exceptions.	Reconciliation report.
FR.26	Applications, Billing, Payments, Receipting	Processing of refunds and reversals through an approval workflow with full audit trail.	M	Initiate reversal and check logs.	Reversal log.
FR.27	Applications, Billing, Payments, Receipting	Support for partial payments, overpayments through credit wallets, and split payments.	S	Test each case and verify balances.	Payment allocation report.
FR.28	Applications, Billing, Payments, Receipting	Generation of invoices in PDF and e-bill formats with unique payment references; mass billing and re-billing with traceability; batch capability of not less than 100,000 invoices in under thirty minutes.	M	Run batch test and verify lineage.	Batch report; runbook.
FR.29	Debt Management & Enforcement	Generation of aging reports for 30, 60, 90 and 180+ days, by stream and by ward.	M	Produce report for sample data.	Aging report.
FR.30	Debt Management & Enforcement	Creation of instalment payment plans and monitoring of compliance.	M	Set plan and test missed-payment alert.	Payment plan report.
FR.31	Debt Management & Enforcement	Automated reminders by SMS, email or application, with a dunning workflow including escalation.	M	Trigger reminders and check logs.	Reminder logs.
FR.32	Debt Management & Enforcement	Case management with field assignment, GPS and time-stamped actions,	S	Issue e-ticket and inspect GPS logs.	Enforcement logs; field application demonstration.

Ref.	*Functional Area*	*Requirement*	*Priority*	*Test Procedure*	*Evidence*
		outcome tracking, and not less than 90 per cent of cases geo-stamped.			
FR.33	Debt Management & Enforcement	Restriction of repeat offenders, with policy-based exemptions permitted.	S	Add to and remove from list and verify block.	Blacklist log.
FR.34	User, Collector & Agent Management	Registration of revenue staff and assignment of roles per the County organogram.	M	Add staff and assign role.	Staff registry export.
FR.35	User, Collector & Agent Management	Assignment of collectors to sources or targets and monitoring of performance.	M	Allocate targets and review report.	Target assignment log.
FR.36	User, Collector & Agent Management	Registration and management of external collection agents, with assignment of roles and targets.	S	Add agent, set target and check report.	Agent assignment log.
FR.37	User, Collector & Agent Management	Real-time staff and agent performance metrics.	S	Display live dashboard.	Dashboard screenshot.
FR.38	Self-Service & Access Channels	Permit taxpayers to access accounts, bills, payments, receipts, applications and support tickets, with one-time-password login and compliance with Web Content Accessibility Guidelines.	M	Log in, complete payment and verify accessibility.	Portal transaction log; test scripts.
FR.39	Self-Service & Access Channels	Enable low-bandwidth access by USSD for key services.	S	Dial USSD and complete task.	USSD session log.
FR.40	Self-Service & Access Channels	Provide an officer application (for assessment, inspection and enforcement) and a taxpayer application (for payment, viewing and renewal), with an offline-first design and conflict handling on synchronisation.	S	Demonstrate applications and test offline synchronisation.	Application demonstration; device policy.
FR.41	Self-Service & Access Channels	Compliance with accessibility standards and multilingual support in English and Kiswahili.	S	Switch language and view accessibility tools.	Accessibility settings log.
FR.42	Configuration, Period Close & Reporting	Update of rates, cycles and penalties without code changes; support for multi-language and geographic parameters such as wards, streams and holidays.	M	Change rate and apply in bill.	Configuration change log.
FR.43	Configuration, Period Close & Reporting	Daily ledger posting, reconciliation and reporting with system lock, with authorised re-opens permitted.	M	Run end-of-day and attempt back-dated entry.	End-of-day report; lock log.
FR.44	Configuration, Period Close & Reporting	Period lock, roll forward of balances, aging of debt and generation of monthly reports.	M	Run end-of-month and check ledgers and reports.	End-of-month reports.
FR.45	Configuration, Period Close & Reporting	Closure of fiscal year, carry forward of arrears and balances, and archiving of year-specific	M	Run end-of-year and verify opening balances.	End-of-year close report.

Ref.	*Functional Area*	*Requirement*	*Priority*	*Test Procedure*	*Evidence*
		parameters and tariffs.			
FR.46	Configuration, Period Close & Reporting	Generation of statutory, management and ad hoc reports (not less than 30 standard reports), an ad hoc builder and export in CSV, XLSX or JSON formats.	M	Run sample reports and export.	Report catalogue; samples.
FR.47	Configuration, Period Close & Reporting	Production of SCOA-coded exports compatible with IFMIS.	M	Export sample and import to IFMIS test environment.	Export file; IFMIS log.
FR.48	Configuration, Period Close & Reporting	Generation of maps and spatial reports for mapped revenue sources.	S	Run GIS query.	GIS map screenshot.
FR.49	Configuration, Period Close & Reporting	Production of logs of all sensitive actions and configuration changes; tamper-evident hash; role-based retrieval; retention for not less than seven years.	M	Generate audit report and verify hash.	Audit log export.
FR.50	Configuration, Period Close & Reporting	Provision of REST or JSON APIs using OAuth 2.0 or OpenID, webhooks, API throttling and versioning; API uptime of not less than 99 per cent and 95th percentile latency of not more than two seconds.	M	Review API documentation and run test calls.	API documentation; monitoring screenshots.

ANNEX 2—MINIMUM TECHNICAL REQUIREMENTS

CHECKLIST FOR THE CRMS

Section 1—Purpose

This Annex sets out the minimum technical specifications and compliance requirements for the CRMS, so as to ensure security, scalability, interoperability and operational performance across County Governments.

Section 2—Scope

This Annex applies to all CRMS implementations, whether developed in-house, procured commercially or provided as part of a centralised national platform, and shall be observed during procurement, implementation, commissioning and operation.

Section 3—Priority Codes

In the table that follows, the priority code "M" denotes a mandatory requirement and the priority code "S" denotes a "should-have" requirement that is desirable for optimal performance.

Section 4—Technical Requirements

Ref.	*Technical Area*	*Requirement*	*Priority*	*Test Procedure*	*Evidence*
TR.1	System Architecture & Hosting	Adopt a modular, service-oriented or microservices architecture; include stateless APIs and a message queue for asynchronous jobs; support independent upgrades; scale to not less than 200 per cent of projected volumes over five years; define auto-scaling thresholds.	M	Review architecture diagrams and simulate load test.	Architecture document; load test results.
TR.2	System Architecture & Hosting	Support deployment on-premises, in a Government-approved data centre, in a compliant local cloud or in a hybrid configuration; conduct a security and total cost of ownership assessment for the chosen deployment.	M	Inspect hosting setup and review assessment.	Hosting certificate; TCO and security report.

Ref.	*Technical Area*	*Requirement*	*Priority*	*Test Procedure*	*Evidence*
TR.3	System Architecture & Hosting	For centralised deployments, provide logical data segregation, per-County encryption keys and per-tenant administrative roles.	M	Inspect multi-tenancy configuration and run segregation tests.	Multi-tenancy configuration report.
TR.4	System Architecture & Hosting	Achieve uptime of not less than 99.5 per cent per quarter, with failover mechanisms and load balancing.	M	Review monitoring logs and conduct failover test.	Uptime report; failover log.
TR.5	System Architecture & Hosting	Provide separate development, test, training and production environments, with controlled promotion of configurations between them.	M	Inspect environment structure.	Environment configuration report.
TR.6	Infrastructure	Use enterprise-grade redundant infrastructure; NVMe or SAN storage for the database; TLS termination at the load balancer.	M	Inspect hardware specifications and test TLS.	Infrastructure inventory; TLS configuration log.
TR.7	Infrastructure	Where on-premises hosting is used, ensure uninterruptible power supply, generator backup, controlled physical access, closed-circuit television and environmental monitoring.	M	Inspect facilities and review monitoring.	Facility inspection report.
TR.8	Infrastructure	Automated, encrypted backups, comprising daily full backups and hourly incremental backups, with quarterly restore tests.	M	Review backup configuration and perform restore.	Backup log; restore report.
TR.9	Software Stack & Development Practices	Use supported long-term-support operating systems and a relational database with ACID compliance; implement read replicas for analytics workloads.	M	Review operating system and database versions and verify replica configuration.	OS and database version list; replica status report.
TR.10	Software Stack & Development Practices	Implement a continuous integration and continuous deployment pipeline; perform static and dynamic application security testing; maintain an artefact repository; adopt infrastructure-as-code.	M	Review DevSecOps configuration and inspect automated test reports.	CI/CD configuration documents; SAST and DAST reports.
TR.11	Software Stack & Development Practices	Maintain centralised logging using ELK or an equivalent, performance metrics and application performance monitoring traces; define and configure alert thresholds.	M	Inspect logging setup and trigger alerts to validate thresholds.	Logging configuration; sample alert records.
TR.12	Software Stack & Development Practices	Ensure compliance with the Government Enterprise Architecture, the Government Interoperability Framework and the OWASP Application Security Verification Standard.	M	Review compliance checklist and test results.	Compliance certification or signed checklist.
TR.13	Integration &	Provide secure APIs or	M	Generate SCOA-	SCOA export file;

Ref.	*Technical Area*	*Requirement*	*Priority*	*Test Procedure*	*Evidence*
	Interoperability	files for two-way integration with IFMIS, and enforce SCOA mapping on all transactions.		coded export and perform IFMIS import in test environment.	IFMIS import log; mapping validation.
TR.14	Integration & Interoperability	Integrate with IPRS, BRS, NTSA, HMIS and GIS platforms using REST or JSON APIs with OAuth 2.0 or OpenID, and apply mutual TLS for sensitive transactions.	M	Conduct API test calls and inspect secure connection configurations.	API test logs; API documentation; connection configurations.
TR.15	Integration & Interoperability	Support integration with bank host-to-host services, ISO 20022 and ISO 8583 messaging where applicable, and mobile money APIs; ensure automated reconciliation.	M	Process test transactions across all financial rails and validate reconciliation outputs.	Payment logs; reconciliation reports; integration certificates.
TR.16	Integration & Interoperability	Provide documented, version-controlled APIs; enforce versioning (for example /v1); apply rate limits; achieve API uptime of not less than 99 per cent and 95th percentile latency of not more than two seconds.	M	Inspect API documentation and run uptime and latency tests.	API monitoring reports; API portal screenshots.
TR.17	Integration & Interoperability	Provide sandbox credentials, Swagger or OpenAPI documents, sample payloads, an error catalogue and integration test cases for all mandatory integrations.	M	Review artefact package and run sample integration tests.	Artefact inventory; integration test logs.
TR.18	Security & Privacy	Implement role-based access control and attribute-based access control to enforce least privilege, segregation of duties and maker-checker controls.	M	Review role and attribute matrix; simulate access; verify maker-checker.	Role and attribute configuration; access logs.
TR.19	Security & Privacy	Require multi-factor authentication for privileged and administrative accounts, and support single sign-on using SAML and OpenID Connect.	M	Attempt administrative login to verify MFA and test single sign-on.	MFA screenshots; SSO setup logs.
TR.20	Security & Privacy	Encrypt data in transit using TLS 1.2 or higher and at rest using AES-256, and rotate keys at regular intervals.	M	Inspect encryption configuration and review key rotation logs.	Security configuration; key rotation schedule.
TR.21	Security & Privacy	Conduct quarterly vulnerability scans and annual penetration tests; remediate critical vulnerabilities within thirty days and high-severity vulnerabilities within sixty days.	M	Review scan results and penetration test reports and confirm remediation timelines.	Scan reports; penetration test report; remediation logs.
TR.22	Security & Privacy	Conduct a Data Protection Impact Assessment for every module; implement consent and notice mechanisms; embed privacy by design.	M	Inspect DPIA documents and test consent capture in workflows.	DPIA reports; consent logs.

Ref.	*Technical Area*	*Requirement*	*Priority*	*Test Procedure*	*Evidence*
TR.23	Security & Privacy	Maintain a registry of authorised devices; enforce session timeouts and concurrent login limits; provide remote wipe.	M	Simulate lost device and perform remote wipe; review session logs.	Device registry; remote wipe report.
TR.24	Security & Privacy	Enable anti-tamper protections; log and alert on suspicious activities and configuration changes.	M	Attempt unauthorised alteration and review tamper logs.	Tamper protection configuration; tamper log export.
TR.25	Performance & Resilience	Process not less than 1,200 transactions per second across all channels during peak periods.	S	Perform load testing with simulated peak volumes.	Load test results; benchmark report.
TR.26	Performance & Resilience	Complete key transactions (billing, payment posting, receipting) within two seconds under normal load.	M	Time transactions during testing and verify thresholds.	Transaction timing logs.
TR.27	Performance & Resilience	Provide offline operation for core functions (billing, receipting, enforcement) with secure store-and-forward synchronisation.	M	Simulate offline activity and synchronisation; confirm data integrity.	Offline transaction logs; synchronisation report.
TR.28	Performance & Resilience	Make GIS layers accessible offline on enforcement devices, and synchronise updates when online.	S	Load and navigate offline GIS map and synchronise updates.	Offline GIS logs; synchronisation confirmation.
TR.29	E-Enforcement & Field Operations	Integrate with mobile or point-of-sale devices for issuing enforcement notices, tickets and penalties with GPS and time-stamping.	M	Issue test e-ticket via device and verify GPS and time stamp.	Enforcement case log; GPS data report.
TR.30	E-Enforcement & Field Operations	Capture photographic, video and documentary evidence linked to case records.	M	Upload test evidence to a case file and confirm linkage.	Case file with media.
TR.31	E-Enforcement & Field Operations	Provide configurable workflows for enforcement actions, assignment, escalation and SLA tracking.	M	Execute sample workflow and verify SLA alerts.	Workflow configuration; SLA log.
TR.32	E-Enforcement & Field Operations	Enable export or API integration with external judicial systems for escalation to court or recovery agencies.	S	Export sample enforcement case and verify data receipt.	Export log; receiving system confirmation.
TR.33	Disaster Recovery & Business Continuity	Maintain an in-country disaster recovery site with a recovery point objective of not more than fifteen minutes and a recovery time objective of not more than two hours.	M	Review DR architecture and conduct failover test.	DR documentation; failover logs.
TR.34	Disaster Recovery & Business Continuity	Conduct bi-annual disaster recovery drills, and document failover and fallback against defined success criteria.	M	Execute DR drill and review results.	DR drill report; recovery metrics.
TR.35	Disaster Recovery & Business Continuity	Maintain a Business Continuity Plan that includes manual fallback procedures, a	M	Review BCP and simulate communication process.	Approved BCP; simulation report.

Ref.	*Technical Area*	*Requirement*	*Priority*	*Test Procedure*	*Evidence*
		communication tree and stakeholder notification templates.			
TR.36	Disaster Recovery & Business Continuity	Automated daily full backups and hourly incremental backups, with quarterly restore tests.	M	Inspect backup logs and perform test restoration.	Backup logs; restore verification.
TR.37	Disaster Recovery & Business Continuity	Automatic failover for critical services, with quarterly failover tests.	M	Simulate outage, trigger failover and measure downtime.	Failover test results; monitoring logs.
TR.38	Reporting & Analytics	Reporting engine with not less than thirty standard reports and an ad hoc builder; export to PDF, CSV, XLSX and JSON.	M	Generate sample reports and test exports.	Report catalogue; files.
TR.39	Reporting & Analytics	Configurable real-time dashboards showing revenue performance, targets, arrears and trends; data must match underlying reports.	M	Compare dashboard metrics to reports.	Dashboard screenshots; comparison logs.
TR.40	Reporting & Analytics	Forecasting tools to project revenue trends and arrears recovery on the basis of historical data.	S	Run forecast analysis on test data and verify model accuracy.	Forecast report; analytics configuration.
TR.41	Configuration & Extensibility	Permit changes to rates, penalties, waivers, workflows and forms via parameters, with full audit of configuration changes.	M	Update parameters and verify change logs.	Configuration change log; settings.
TR.42	Configuration & Extensibility	Support English and Kiswahili interfaces and multiple currency formats.	S	Switch language and test currency display.	Language and currency settings logs.
TR.43	Configuration & Extensibility	Add new revenue streams with tariffs, SCOA codes, workflows and reporting templates without vendor intervention.	M	Add new stream in test and verify.	Stream creation log; billing test.
TR.44	Data Management	Implement validation rules to prevent incomplete or invalid data, and enforce mandatory fields.	M	Attempt to save invalid data and review errors.	Validation error log; configuration.
TR.45	Data Management	Provide migration tools, including mapping, cleansing, trial loads and reconciliation.	M	Perform trial migration and reconcile data.	Migration plan; reconciliation report.
TR.46	Data Management	Archive inactive records in accordance with the retention schedule, and purge only after multi-level authorisation with audit logging.	M	Archive and purge samples in test.	Archive and purge logs; authorisations.
TR.47	Documentation & Handover	Deliver a system design dossier, data model and dictionary, API documentation, configuration runbooks, standard operating procedures, administrator and user manuals, test reports, training materials and an escrow package containing source code and build scripts.	M	Review documentation set for completeness and compliance.	Documentation inventory; escrow confirmation.

ANNEX 3—PROCUREMENT AND COMPLIANCE EVALUATION MATRIX

Section 1—Purpose

This Annex provides a standard evaluation matrix for the uniform, transparent and objective assessment of CRMS proposals during procurement, commissioning and compliance review.

Section 2—Scope

This Annex applies to Procurement Evaluation Committees, Commissioning Teams, and Oversight and Audit Teams.

Section 3—Evaluation Matrix

Evaluation Area	*Criteria*	*Linked FR/TR*	*Weight (%)*	*Scoring Method*
Preliminary Evaluation	Submission of mandatory documents, including bid security, tax compliance certificate, signed forms and eligibility requirements.	Not applicable	Pass / Fail	All documents must be provided for a bid to proceed.
Functional Requirements Compliance (Mandatory)	Meets all mandatory functional requirement items in Annex 1.	FR.1 to FR.50	25	Pass or fail in respect of mandatory items; optional items scored proportionally between 0 and 1.
Functional Requirements Compliance (Optional)	Meets the "should-have" functional requirement items.	FR.16, FR.19, FR.27, FR.30 to FR.31, FR.33, FR.35, FR.39 to FR.40, FR.42, FR.48	5	Weighted score by number of optional items implemented.
Technical Requirements Compliance (Mandatory)	Meets all mandatory technical requirement items in Annex 2.	TR.1 to TR.47 (Mandatory)	25	Pass or fail in respect of mandatory items; points awarded for exceeding minimum specifications.
Technical Requirements Compliance (Optional)	Meets the "should-have" technical requirement items.	TR.25, TR.28, TR.32, TR.40, TR.42	5	Weighted score by number of optional items implemented.
Integration & Interoperability	Successful integration with IFMIS, SCOA, IPRS, BRS, GIS, HMIS, NTSA and payment channels.	FR.14, FR.47, TR.13 to TR.17	5	Live or sandbox test evidence demonstrating error-free transactions.
Security & Compliance	Meets security, privacy and data protection requirements and passes vulnerability and penetration testing.	TR.18 to TR.24	5	Review of audit logs, security reports and test results.
Performance & Resilience	Meets throughput, uptime, offline capability, and disaster recovery and business continuity benchmarks.	TR.1, TR.4, TR.25 to TR.28, TR.33 to TR.37	5	Load tests, disaster recovery drill reports and offline simulation.
Implementation Approach & Plan	Methodology, migration plan, training, change management and post-go-live support.	TR.45, TR.47, FR.42 to FR.45	10	Review of project plan, timelines and resource allocation.
Vendor Experience & Capacity	CRMS deployments in not less than three counties, with verifiable references and a local technical team.	Not applicable	5	Reference checks; review of team curricula vitae.
Total Cost of Ownership	Five-year total cost of ownership, including licences, hosting, maintenance, upgrades and training.	Not applicable	5	Evaluation of detailed cost breakdown.
Risk & Exit Strategy	Data portability, source code escrow, exit and migration plan, and SLA commitments.	TR.47, FR.11, FR.49	5	Review of SLA, escrow agreement and exit plan.

ANNEX 4—COMPLIANCE AUDIT TOOL FOR THE CRMS

Section 1—Purpose

This Annex provides a structured compliance checklist for commissioning, post-implementation review, annual audit and spot-check exercises.

Section 2—Scope

This Annex applies to all County Governments and National implementing agencies operating a CRMS, and is intended for use by Internal Audit, the Commission, the National Treasury, the Auditor-General and quality-assurance consultants.

Section 3—Compliance Audit Checklist

In the "Rating" column, an auditor shall record one of the following ratings: "Compliant", "Partially Compliant" or "Non-Compliant".

Ref.	Audit Area	Compliance Standard	Linked FR/TR	Test Procedure	Evidence	Rating	Remediation
A4.1	Registry & Identity Management	Central registry linked to National ID, KRA PIN and BRS; many-to-many relationships supported; capacity of not less than one million records.	FR.1	Inspect registry; search and link records; run API query.	Screenshots; API logs.		
A4.2	Registry & Identity Management	Customer and transaction ledgers with SCOA coding in place.	FR.6, FR.7	View ledgers and verify SCOA mapping.	Ledger reports; SCOA export.		
A4.3	Revenue Source & Tariff Management	All streams configured per the Finance Act or Tariff Policy, with version history maintained.	FR.10, FR.12	Compare system tariffs to legal schedule; review change logs.	Tariff configuration logs.		
A4.4	Revenue Source & Tariff Management	SCOA mapping enforced for all billable items.	FR.14, TR.13	Attempt unmapped billing and confirm system block.	SCOA mapping report.		
A4.5	Applications, Billing & Payments	Batch billing capacity of not less than 100,000 invoices in under thirty minutes met; re-billing maintains lineage.	FR.28	Run batch and review logs.	Batch run logs.		
A4.6	Applications, Billing & Payments	All mandatory payment channels active; offline queue and synchronisation functional; reversals tracked.	FR.23, TR.27	Process payments and simulate offline mode.	Payment logs.		
A4.7	Applications, Billing & Payments	Receipts issued instantly and confirmation sent to payer.	FR.24	Complete payment and verify receipt and SMS.	Receipt copy; SMS log.		
A4.8	Applications, Billing & Payments	Daily T+1 reconciliation; not more than 1 per cent unresolved after T+3.	FR.25	Inspect reconciliation reports and check closure rates.	Reconciliation logs.		
A4.9	Debt Management & Enforcement	Aging reports generated and dunning workflow active.	FR.29, FR.31	Run arrears report and check reminders.	Aging report; reminder log.		
A4.10	Debt Management & Enforcement	GPS and time-stamped enforcement actions logged; not less than 90 per cent geo-stamped.	FR.32, TR.29	Issue e-ticket and verify GPS logs.	Enforcement logs.		
A4.11	Debt Management & Enforcement	Evidence capture linked to case files.	TR.30	Upload sample evidence to case and confirm linkage.	Case file with media.		
A4.12	Security & Privacy	Roles and attributes correctly configured; maker-checker in place.	TR.18	Review role matrix and simulate access.	Role configuration report.		
A4.13	Security & Privacy	Multi-factor authentication	TR.19, TR.20	Test MFA and inspect encryption	MFA logs; encryption		

Ref.	Audit Area	Compliance Standard	Linked FR/TR	Test Procedure	Evidence	Rating	Remediation
		enforced for privileged accounts; TLS 1.2 or higher and AES-256 encryption active.		setup.	configuration.		
A4.14	Security & Privacy	Quarterly scans and annual penetration test conducted; critical vulnerabilities remediated within thirty days.	TR.21	Review reports and confirm remediation dates.	Security reports.		
A4.15	Security & Privacy	DPIAs completed and consent capture mechanisms functional.	TR.22	Inspect DPIA and test consent prompts.	DPIA documents; consent logs.		
A4.16	Performance & Resilience	Not less than 1,200 transactions per second at peak and response time of not more than two seconds.	TR.25, TR.26	Run performance test and measure response.	Load test reports.		
A4.17	Performance & Resilience	Offline billing, receipting and enforcement operational, with synchronisation working.	TR.27	Simulate offline operations and synchronise data.	Offline logs.		
A4.18	Disaster Recovery & BCP	DR site operational with recovery point objective of not more than fifteen minutes, recovery time objective of not more than two hours, and two drills per year.	TR.33, TR.34	Inspect DR site and review drill reports.	DR drill report.		
A4.19	Disaster Recovery & BCP	Daily full and hourly incremental backups, with quarterly restores successful.	TR.36	Check backup jobs and perform restore.	Backup and restore logs.		
A4.20	Disaster Recovery & BCP	Automatic failover tested quarterly and uptime SLA met.	TR.37	Simulate outage and verify failover.	Failover logs.		
A4.21	Reporting & Analytics	Not less than thirty standard reports, an ad hoc builder, and all export formats functional.	FR.46, TR.38	Generate reports and test exports.	Report catalogue.		
A4.22	Reporting & Analytics	Real-time dashboards match report data.	TR.39	Compare dashboard against reports.	Dashboard screenshot; comparison log.		
A4.23	Configuration & Extensibility	Rates, penalties, waivers and workflows updated via parameters, with changes logged.	TR.41	Update configuration and review change logs.	Configuration logs.		
A4.24	Configuration & Extensibility	New streams added without vendor intervention, fully functional.	TR.43	Create new stream and test billing and reporting.	Stream creation log.		
A4.25	Documentation & Handover	All required documentation and escrow package delivered.	TR.47	Inspect documentation inventory.	Documentation list; escrow confirmation.		

ANNEX 5—RISK MANAGEMENT FRAMEWORK FOR THE CRMS

Section 1—Purpose

This Annex establishes a standard approach for identifying, assessing, mitigating and monitoring risks during the lifecycle of a CRMS.

Section 2—Scope

This Annex applies to County CRMS operations, to centralised national deployments and to third-party service providers.

Section 3—Risk Register and Management Matrix

ID	*Category*	*Description*	*Impact*	*Likelihood*	*Severity*	*Owner*	*Mitigation*	*Contingency*	*Key Risk Indicator*
R1	Technical—Infrastructure	System downtime due to hardware failure or hosting outage.	Revenue loss and public dissatisfaction.	Medium	High	ICT Unit and Vendor	Redundant infrastructure; high-availability design; monitoring.	Activate DR site; failover within RTO of two hours.	Uptime percentage; mean time to recover.
R2	Technical—Application	Bugs or defects disrupt billing, payments and reconciliation.	Delayed collections and inaccurate data.	Medium	High	ICT Unit and Vendor	QA and UAT before updates; DevSecOps pipeline with rollback.	Revert to last stable version; patch within SLA.	Defect density; time to patch.
R3	Security	Data breach or unauthorised access to taxpayer data.	Legal penalties and reputational damage.	Medium	High	ICT and Security Officer	RBAC and ABAC; MFA; encryption; security audits.	Activate incident response; notify regulators and affected parties.	Number of security incidents; failed login attempts.
R4	Integration	Failure of integration with IFMIS, SCOA, payment channels or registries.	Delayed reporting and revenue posting errors.	Medium	High	ICT, Finance and Vendor	Integration testing; API monitoring; SLAs.	Manual upload; escalate to partner.	API success rate; reconciliation variance.
R5	Data Management	Loss or corruption of financial records.	Loss of accountability and breach of compliance.	Low	High	ICT and Vendor	Encrypted backups; quarterly restore tests.	Restore from backup; conduct forensic analysis.	Backup success rate; restore success rate.
R6	Operational—Collection	Fraudulent collection or diversion by staff or agents.	Revenue leakage and legal action.	Medium	High	Revenue Department and Internal Audit	Cashless collections; reconciliation controls; monitoring.	Suspend accounts and initiate audit.	Collector performance variance.
R7	Operational—Enforcement	Delay or failure in enforcement due to technical or logistical issues.	Drop in compliance and revenue shortfall.	Medium	Medium	Enforcement and ICT	E-enforcement devices; SLA monitoring.	Escalate cases; maintain manual logs.	Enforcement completion rate.
R8	Change Management	User resistance to system or process changes.	Low adoption and parallel manual processes.	Medium	Medium	HR and Change Lead	Training; sensitisation; support channels.	Coaching; leadership escalation.	Adoption rate; help desk tickets.
R9	Regulatory	Non-compliance with the Data Protection, Public Finance Management or procurement	Fines, legal sanctions and halted operations.	Low	High	Legal and Compliance	Compliance reviews; legal vetting.	Suspend risky processes; remediate.	Number of audit findings.

ID	*Category*	*Description*	*Impact*	*Likelihood*	*Severity*	*Owner*	*Mitigation*	*Contingency*	*Key Risk Indicator*
		laws.							
R10	Business Continuity	Disaster, such as fire, flood or cyber-attack, disrupts operations.	Extended downtime and loss of revenue.	Low	High	ICT and DR Lead	DR site; BCP drills; environmental controls.	Activate BCP; failover to DR.	BCP drill success; recovery time.
R11	Vendor Management	Vendor insolvency, dispute or poor performance.	Delays and loss of support.	Medium	Medium	Procurement, ICT and Legal	SLAs; escrow for source code; alternate vendor readiness.	Activate escrow; engage alternate vendor.	SLA breach rate.
R12	GIS & Field Operations	Inaccurate GIS mapping or field data capture failures.	Poor targeting and incomplete asset register.	Medium	Medium	GIS and ICT	GPS audits; offline GIS maps; training.	Manual validation; re-map.	Percentage of verified GIS assets.

ANNEX 6—SAMPLE SERVICE LEVEL AGREEMENT FOR THE CRMS

Section 1—Purpose

This Annex sets out a template defining the performance standards, responsibilities and remedies applicable to the provision, operation and support of a CRMS by a Vendor to a Client.

Section 2—Scope of Services

The services governed by this template Service Level Agreement ("SLA") shall include hosting and infrastructure (where applicable), application maintenance, integration maintenance, security management, disaster recovery and business continuity, help desk and incident management, and training and the updating of documentation.

Section 3—Performance Metrics

Service Area	*Metric*	*Target*	*Linked FR/TR*
System Availability	Uptime per quarter	Not less than 99.5%	TR.4
Incident Response	Acknowledgement of Priority 1 (Critical) incidents	Not more than 15 minutes	TR.18, TR.19
Incident Resolution	Restoration of service (Critical)	Workaround within 2 hours; full fix within 8 hours	TR.18, TR.19
Reconciliation Accuracy	Daily reconciliation completion	100% at T+1; not more than 1% unresolved after T+3	FR.25
Integration Availability	Success rate for mandatory integrations	Not less than 99%	TR.13 to TR.17
Security Compliance	Vulnerability remediation	Critical within 30 days; high within 60 days	TR.21
Backup and Restore	Quarterly restore test success rate	100%	TR.36
DR Drill Success	Meeting of RPO and RTO targets	RPO not more than 15 minutes; RTO not more than 2 hours	TR.33, TR.34
Training Delivery	Completion of agreed training plan	100% attendance and evaluation	TR.47
Documentation Updates	Update window following any change	Within 5 working days	TR.47

Section 4—Priority Levels and Resolution Targets

Priority	*Definition*	*Response Time*	*Resolution Target*
P1 — Critical	Complete outage; core revenue functions unavailable.	Within 15 minutes	Workaround within 2 hours; full fix within 8 hours
P2 — High	Major function degraded; workaround available.	Within 30 minutes	Full fix within 24 hours
P3 — Medium	Minor function affected; low business impact.	Within 2 hours	Full fix within 5 days
P4 — Low	Cosmetic or user interface issue; no business impact.	Within 4 hours	Fix in next planned release

Section 5—Reporting and Review

The Vendor shall submit monthly service performance reports to the Client, and the parties shall hold quarterly review meetings to assess SLA performance and identify opportunities for continuous improvement.

Section 6—Penalties and Service Credits

Breach	*Penalty / Service Credit*
Uptime falling below 99.5%	5% of the monthly service fee for every 0.5% of shortfall.
Missed Critical issue resolution time	10% of the monthly service fee per incident.
Missed DR recovery point or recovery time objectives	15% of the monthly service fee per failed test.
Failure to remediate a critical vulnerability within the prescribed time	10% of the monthly service fee per breach.

Cumulative penalties in any one quarter shall not exceed 25 per cent of the quarterly service fee. Persistent non-compliance may trigger termination of the contract.

Section 7—Escalation Path

(a) Service Desk or Help Desk Officer;

(b) Vendor Support Manager;

(c) Vendor Chief Technology Officer or senior management; and

(d) Client steering committee.

Section 8—Change Management

All system changes shall be approved by the Client and tested in a staging environment before deployment to production.

Section 9—Termination and Exit Management

Upon termination of the SLA, the Vendor shall provide to the Client the latest system backup in an open format, updated documentation, transfer of source code and configurations as provided under the contract, and a knowledge transfer to the Client or to a replacement vendor.

ANNEX 7—STAKEHOLDER CONSULTATION RECORD

Section 1—Purpose

This Annex documents the stakeholder engagement process undertaken in the formulation of these Guidelines, in compliance with Article 10 and Article 232 of the Constitution and with applicable public participation laws.

Section 2—Scope

The consultation record covers the identification of relevant stakeholders, the engagement methods used, the key issues raised, and the manner in which those issues have been addressed in these Guidelines.

Section 3—Stakeholder Groups Consulted

(a) County Governments, including County Executive Committees for Finance and ICT, County Treasuries, County Assemblies' Finance Committees, and County Revenue Boards and Directorates;

(b) intergovernmental bodies, including the Council of Governors and the Intergovernmental Budget and Economic Council;

(c) development partners and civil society, including the World Bank, the United Nations Development Programme, GIZ, USAID and civil society organisations advocating for transparency and good governance;

(d) the private sector, including CRMS solution providers and integrators, banks and payment service providers, and telecommunications companies; and

(e) the general public, including taxpayers, business associations, resident associations and traders.

Section 4—Consultation Record

Date	*Stakeholder Group*	*Organisation / Representative*	*Mode*	*Key Issues Raised*	*How Addressed*	*Evidence*

Section 5—Supporting Evidence Checklist

(a) stakeholder notices and invitations issued;

(b) draft guidelines circulated for comment;

(c) attendance registers for all meetings;

(d) minutes and recordings of consultations;

(e) written submissions from stakeholders; and

(f) feedback matrix linking comments to changes in these Guidelines.

ANNEX 8—DATA MIGRATION AND CUTOVER PLAN

Section 1—Purpose

This Annex provides a structured framework to ensure the safe, accurate and efficient migration of data from legacy revenue management systems or manual records into the CRMS, with minimal disruption to service delivery and no loss of data integrity.

Section 2—Scope

This Annex applies to all County Governments and National implementing agencies deploying a CRMS, including migration from legacy systems such as LAIFOMS and earlier revenue management systems, the transition from manual registers, and the consolidation of multiple systems into a single CRMS.

Section 3—Migration Principles

(a) accuracy, requiring that migrated data match verified source data exactly;

(b) completeness, requiring that all relevant historical and current records be migrated;

(c) integrity, requiring that relationships between records, such as those between customers, ledgers and transactions, be preserved;

(d) compliance, requiring that data comply with SCOA coding, the Data Protection Act, 2019, and statutory retention rules;

(e) auditability, requiring that every migration step be logged and documented; and

(f) minimal downtime, requiring that cutover be planned to avoid prolonged service interruption.

Section 4—Migration Phases and Activities

Phase	*Activity*	*Description*	*Linked FR/TR*	*Deliverable*
Pre-Migration Assessment	Data Inventory	Identify all existing data sources and repositories.	TR.45	Data inventory report.
Pre-Migration Assessment	Data Mapping	Map each data element from source to CRMS target field, ensuring SCOA mapping.	FR.14; TR.13	Data mapping matrix.
Pre-Migration Assessment	Data Cleansing	Remove duplicates, correct inconsistencies and complete missing data.	FR.4; TR.44	Cleansed dataset.
Pre-Migration Assessment	Migration Tool Setup	Configure vendor-supplied migration utilities and scripts.	TR.45	Tool setup log.
Pre-Migration Assessment	Migration Plan Approval	Secure sign-off for migration scope, schedule and responsibilities.	TR.47	Approved migration plan.
Trial Migration	Trial Load	Perform migration in a test or staging environment.	TR.45	Trial migration logs.
Trial Migration	Reconciliation	Compare trial migrated data to source records and verify ledgers and balances.	FR.6; FR.7	Reconciliation report.
Trial Migration	User Verification	Departmental review and sign-off of trial data.	FR.1 to FR.3	User sign-off forms.
Cutover Preparation	Freeze Changes	Halt non-critical changes to source data during the migration window.	TR.5	Change freeze notice.
Cutover Preparation	Final Backup	Take a full backup of source systems before migration.	TR.36	Backup confirmation log.
Cutover Preparation	Communication	Notify stakeholders of the cutover date, downtime and contingency plan.	TR.35	Communication plan.
Final Migration & Go-Live	Final Load	Load the final dataset into the production CRMS.	TR.45	Final migration log.
Final Migration & Go-Live	Validation	Run validation checks and sample reports post-load.	FR.43 to FR.47	Validation checklist.
Final Migration & Go-Live	Cutover Execution	Switch operations to the CRMS and decommission legacy entry points.	TR.35	Cutover report.
Post-Go-Live Support	Hypercare Period	Provide dedicated vendor and on-site support for a defined period.	TR.47	Support logs.
Post-Go-Live Support	Parallel Reconciliation	Compare CRMS data against legacy data for a defined period.	FR.25	Reconciliation reports.
Post-Go-Live Support	Final Sign-off	Formal acceptance of migrated data.	TR.47	Acceptance certificate.

Section 5—Roles and Responsibilities

Role	*Responsibility*
County ICT Unit	Coordinate migration; validate technical tools; manage backups and environments.

Role	*Responsibility*
County Finance and Revenue Department	Validate SCOA mappings; verify ledger and transaction accuracy.
Vendor Migration Team	Provide migration tools; execute migration and cutover; resolve issues.
Data Protection Officer	Ensure compliance with privacy laws during migration.
Project Manager	Oversee migration timeline, scope and resources.
Audit and Quality Assurance Team	Independently verify migration quality and compliance.
Commission on Revenue Allocation	Offer technical capacity assistance.

Section 6—Key Risks and Mitigation

Risk	*Potential Impact*	*Mitigation*
Data loss during migration	Missing or incomplete records.	Multiple backups; trial runs; reconciliation checks.
Incomplete SCOA mapping	Reporting and IFMIS errors.	Pre-validation of mappings; enforcement of SCOA codes.
Extended downtime	Service disruption.	Plan migration window; define fallback plan.
User resistance	Continued use of old processes.	Early training; user participation in migration.
Privacy breach	Legal penalties.	Secure handling; role-based access; encryption.

ANNEX 9—CHANGE MANAGEMENT AND TRAINING PLAN

Section 1—Purpose

This Annex sets out the structured approach for managing organisational change, stakeholder adoption and capacity building during the transition to a CRMS.

Section 2—Change Management Phases

Phase	*Key Activities*	*Deliverables*	*Linked FR/TR*
Readiness Assessment	Assess current processes, systems, skills and stakeholder perceptions.	Readiness report; stakeholder mapping.	TR.47
Communication Planning	Develop strategy, key messages, channels and timeline.	Communication plan; briefing materials.	TR.35
Stakeholder Engagement	Hold meetings with user groups, management and oversight bodies.	Engagement logs; feedback matrix.	FR.1; FR.38
Impact Analysis	Identify process and role changes and the key performance indicators affected.	Change impact report.	TR.47
Resistance Management	Identify potential resistance and plan mitigation.	Resistance plan.	TR.47
Change Champion Network	Appoint departmental champions to support adoption.	Champion roster; role descriptions.	TR.47

Section 3—Training Plan Structure

Training Type	*Target Audience*	*Objectives*	*Responsibility*	*Delivery Method*	*Duration*	*Linked FR/TR*
System Overview	Executive leadership and managers.	Understand system purpose, benefits and governance.	County ICT and Vendor	Workshop or briefing	0.5 day	FR.1 to FR.3; TR.47
Functional User Training	Revenue and finance officers and enforcement staff.	Operate modules for billing, receipting, reconciliation and enforcement.	County ICT and Vendor	Hands-on workshops	2 to 3 days	FR.20 to FR.32
Technical and Administrative Training	ICT and system administrators.	Manage users, roles, configurations, integrations, backups and security.	County ICT and Vendor	Laboratory sessions	3 to 5 days	TR.9 to TR.24; TR.36
Integration Training	ICT and finance integration staff.	Manage IFMIS, SCOA, payment and registry integrations.	County ICT and Vendor	Practical configuration sessions	2 days	FR.14; TR.13 to TR.17
Security and Compliance Training	All users.	Understand data security, privacy laws and role-based controls.	County ICT and Vendor	E-learning or interactive	1 day	TR.18 to TR.22

Training Type	*Target Audience*	*Objectives*	*Responsibility*	*Delivery Method*	*Duration*	*Linked FR/TR*
Reporting and Analytics Training	Management, M&E and finance teams.	Generate statutory and management reports, dashboards and analytics.	County ICT and Vendor	Workshop	1 day	FR.43 to FR.48; TR.38 to TR.40
DR and BCP Training	ICT and operations staff.	Conduct DR drills, backup restores and continuity processes.	County ICT and Vendor	Simulation	0.5 to 1 day	TR.33 to TR.37
Change Champion Coaching	Change champions.	Support peer adoption and escalate feedback.	County ICT and Vendor	Peer coaching	Ongoing	TR.47

Section 4—Communication Guidelines

(a) pre-go-live: weekly updates, frequently-asked-question documents and early demonstrations;

(b) go-live: daily updates, escalation contacts and public notices; and

(c) post-go-live: success stories, usage statistics and surveys.

Section 5—Adoption Monitoring and Success Criteria

(a) user login frequency and transaction volumes;

(b) help desk ticket trends and resolution times;

(c) compliance with new processes, and decommissioning of manual systems within three months of go-live;

(d) not less than 90 per cent of targeted users trained, and competency scores of not less than 80 per cent after training; and

(e) stakeholder satisfaction of not less than 80 per cent in user surveys, with adoption metrics meeting projections.

ANNEX 10—STANDARD REPORTS CATALOGUE

Section 1—Purpose

This Annex defines the minimum set of reports that the CRMS shall produce in order to meet statutory, operational, management, analytical and transparency requirements.

Section 2—Report Categories

Category	*Description*	*Frequency*	Linked FR/TR
Statutory and Financial Reports	Legally required reports, SCOA-coded and IFMIS-compatible.	Monthly, quarterly or annually	FR.44; TR.13
Management and Operational Reports	Reports that support internal decision-making.	Daily, weekly or monthly	FR.43; TR.38
Debt and Enforcement Reports	Reports tracking arrears, payment plans and enforcement actions.	Weekly or monthly	FR.29 to FR.33; TR.29 to TR.31
GIS and Asset Reports	Spatial insights relating to revenue assets.	Monthly or quarterly	FR.16; FR.48; TR.28
Analytical and Forecasting Reports	Predictive insights for planning.	Quarterly or annually	TR.39; TR.40

Section 3—Minimum Standard Reports

Ref.	*Report Name*	*Description and Purpose*	*Frequency*	*Format*	*Linked FR/TR*
SR.1	County Revenue Summary	Consolidated revenue by stream, ward and SCOA code; IFMIS-ready.	Monthly	PDF; XLSX; SCOA CSV	FR.44; TR.13
SR.2	Daily Collections Report	Daily revenue by stream, collector and payment channel.	Daily	PDF; XLSX	FR.43; FR.25
SR.3	Bank and Channel Reconciliation Report	Matches transactions to bank or mobile money records; flags exceptions.	Daily	PDF; XLSX	FR.25; TR.15
SR.4	SCOA Export File	SCOA-coded export for posting to IFMIS.	Monthly	SCOA CSV	FR.44; TR.13
SR.5	Arrears Aging Report	Outstanding balances by age buckets.	Monthly	PDF; XLSX	FR.29; TR.39
SR.6	Payment Plan Compliance Report	List of payment plans, instalments and defaults.	Weekly	PDF; XLSX	FR.30
SR.7	Enforcement Action	All enforcement cases, GPS-stamped actions and	Monthly	PDF; XLSX	FR.32; TR.29

Ref.	*Report Name*	*Description and Purpose*	*Frequency*	*Format*	*Linked FR/TR*
	Register	outcomes.			
SR.8	Waivers and Exemptions Report	Approved waivers and exemptions with full details.	Monthly	PDF; XLSX	FR.18
SR.9	Top Revenue Sources	Ranked streams and accounts with trend analysis.	Monthly	PDF; XLSX	FR.19; TR.39
SR.10	Revenue versus Target Performance	Actual collections compared with targets by stream and ward.	Monthly	PDF; XLSX	FR.19; TR.39
SR.11	Licence and Permit Register	All licences and permits showing active, expired and pending status.	Monthly	PDF; XLSX	FR.20 to FR.22
SR.12	Asset Revenue Report	Revenue derived from county-owned assets.	Quarterly	PDF; XLSX	FR.15
SR.13	GIS Asset Map and Revenue Overlay	Map of assets and revenue sources with collection data.	Quarterly	PDF; GIS Shapefile	FR.16; FR.48
SR.14	Transaction Audit Report	All transactions with user, timestamp and action.	Monthly	PDF; XLSX	FR.49; TR.15
SR.15	Configuration Change Audit	All configuration changes affecting tariffs, SCOA and roles.	Monthly	PDF; XLSX	FR.42; TR.41
SR.16	Security Incident Report	Failed logins, access violations and resolved vulnerabilities.	Quarterly	PDF	TR.18 to TR.21
SR.17	Revenue Forecast Report	Predictive revenue by stream and ward.	Quarterly	PDF; XLSX	TR.40
SR.18	DR and BCP Test Report	Results of disaster recovery and business continuity tests.	Bi-annually	PDF	TR.33 to TR.35
SR.19	Public Transparency Report	Non-confidential summary for public release.	Quarterly	PDF; Web	FR.38; TR.39
SR.20	Collector Performance Report	Collections per collector or agent with efficiency metrics.	Monthly	PDF; XLSX	FR.35

ANNEX 11—DATA AND RECORDS GOVERNANCE

Section 1—Purpose

This Annex establishes the rules, responsibilities and standards for the secure, accurate and compliant management of all data and records within a CRMS, so as to ensure transparency, accountability and long-term integrity.

Section 2—Scope

This Annex applies to all data captured, processed, stored or transmitted by the CRMS, including taxpayer and revenue records, SCOA-coded transactions, audit logs and configuration changes, backups, archives and purged records.

Section 3—Data Ownership and Stewardship

Role	*Responsibility*
County Government (Data Owner)	Holds legal ownership of CRMS data within its jurisdiction.
National implementing agency (in respect of centralised data)	Holds ownership of the central repository and of inter-county integration data.
ICT Unit	Serves as technical custodian of databases, backups and recovery operations.
Revenue Department	Acts as custodian of taxpayer and transaction records and enforces SCOA compliance.
Data Protection Officer	Ensures compliance with data protection laws and privacy policies.
Internal Audit	Verifies governance controls and the accuracy of data.

Section 4—Data Classification

Classification	Description	Examples
Public	Accessible without restriction.	Aggregated revenue reports.
Internal	For internal staff use only.	Operational dashboards.
Confidential	Restricted to authorised roles.	Taxpayer profiles; SCOA codes.
Restricted	Highest level of sensitivity.	Encryption keys; investigation records.

Section 5—Data Quality Standards

Standard	*Requirement*	*Linked FR/TR*
Accuracy	Records must match source documents.	FR.6; FR.7; TR.44
Completeness	Mandatory fields enforced, with no null values where not permitted.	TR.44
Consistency	Standard formats for dates, SCOA codes and identifiers.	FR.14; TR.13
Timeliness	Updates posted in real time or near real time.	TR.26
Integrity	Referential integrity maintained across related datasets.	FR.1; FR.2

*Section 6—Retention, Archiving and Disposa*l

(a) retention: financial, transactional and audit data shall be retained for not less than seven years;

(b) archiving: inactive records shall be archived after two years, but shall remain retrievable for audit;

(c) purging: purging shall be permitted only after the retention period and only with multi-level authorisation and audit logging; and

(d) backup: daily full backups and hourly incremental backups shall be maintained, and quarterly restore tests shall be conducted.

Section 7—Records Management Controls

Control Area	*Requirement*	*Linked FR/TR*
Audit Trails	Immutable logs maintained for all create, update and delete actions.	FR.49; TR.15
SCOA Compliance	All transactions SCOA-coded.	FR.14; TR.13
Source Documentation	All records linked to scanned or uploaded supporting documents.	FR.3
Version Control	History maintained of tariffs, SCOA updates and configuration changes.	FR.12; TR.41
Retrieval and Search	Multi-criteria search functionality available for any record.	FR.8

Section 8—Access and Security Auditing

(a) user access rights shall be reviewed quarterly, with immediate revocation upon role change or exit;

(b) annual penetration testing and quarterly vulnerability scans shall be conducted; and

(c) logs shall be reviewed for suspicious activity and anomalies investigated.

Section 9—Compliance Monitoring and Indicators

(1) An annual Data and Records Governance audit shall be conducted by Internal Audit, with oversight inspections by the Commission and the National Treasury.

(2) Key Governance Indicators shall include—

(a) the percentage of records with complete SCOA mapping;

(b) the percentage of records meeting accuracy benchmarks;

(c) the number of unauthorised access incidents; and

(d) the backup and restore success rates.

ANNEX 12—GLOSSARY AND ACRONYMS

Section 1—Purpose

This Annex standardises the definitions and abbreviations used throughout these Guidelines, in order to ensure clarity, accuracy and uniformity of interpretation.

Section 2—Glossary of Key Terms

Term	*Definition*
Access Control	The process of granting or denying requests to obtain and use information and system services, managed through Role-Based Access Control and Attribute-Based Access Control.
Ad hoc Report	A report created on demand to meet a specific information need outside scheduled reporting.
API (Application Programming Interface)	A set of protocols and tools that enable communication between systems.
Audit Trail	A secure, chronological record of all system activities showing the user, action and time.
Business Continuity Plan (BCP)	Documented procedures to ensure continued operations during and after a disruption.
Cutover	The planned process of switching operations from a legacy system to a new system.
Customer Ledger	A detailed account record showing all transactions, charges, payments and balances for a taxpayer.
Data Cleansing	The detection and correction or removal of corrupt, inaccurate or incomplete data.

Term	*Definition*
Data Protection Impact Assessment (DPIA)	An assessment to identify and minimise data protection risks.
Disaster Recovery (DR)	The strategies and procedures used to restore IT systems, applications and data after a disruption.
End-of-Day (EoD) Process	The daily procedure of closing financial transactions, reconciling and locking entries.
End-of-Month (EoM) Process	The monthly closing procedure used to roll forward balances, age debt and lock the period.
End-of-Year (EoY) Process	The annual closing procedure for the fiscal year, including carrying forward balances and archiving.
Failover	Automatic switching to a standby system when the primary system fails.
Finance Act	Legislation outlining the revenue streams, rates and penalties for a fiscal year.
Geographic Information System (GIS)	A system for capturing, storing, analysing and displaying spatial or geographic data.
Hypercare Period	The intensive vendor and project team support provided immediately after go-live.
Immutable Log	A log file that cannot be altered or deleted, ensuring audit integrity.
Integration Test	Verification that separate system components work together as intended.
Maker-Checker Control	A control under which one user initiates a process and another approves it.
Multi-Factor Authentication (MFA)	A security measure requiring more than one verification method for login.
Multi-Tenancy	An architecture in which one system instance serves multiple clients with data segregation.
Parametric Configuration	The configuration of system behaviour through parameters, without changes to code.
Payment Channel	The method used to process payments, such as mobile money, electronic funds transfer, USSD or point of sale.
Reconciliation	The matching of system records to bank or payment provider records to ensure accuracy.
Recovery Point Objective (RPO)	The maximum acceptable amount of data loss, measured in time.
Recovery Time Objective (RTO)	The maximum acceptable time to restore services after a disruption.
Standard Chart of Accounts (SCOA)	The uniform coding framework used for government accounting.
Tamper-Evident	A feature that shows when an attempt has been made to alter data or logs.
Transaction Ledger	A record of all transactions for a specific revenue stream, with SCOA coding.
Version Control	A system that records changes to files or configurations and allows rollback.

Section 3—Acronyms

Acronym	*Full Form*
ABAC	Attribute-Based Access Control
API	Application Programming Interface
BCP	Business Continuity Plan
BRS	Business Registration Service
CEC	County Executive Committee
CoG	Council of Governors
CRA	Commission on Revenue Allocation
CRMS	County Revenue Management System
CSV	Comma-Separated Values
DPIA	Data Protection Impact Assessment
DR	Disaster Recovery
EoD	End-of-Day
EoM	End-of-Month
EoY	End-of-Year
ELK	Elasticsearch, Logstash, Kibana
FR	Functional Requirement
GEA	Government Enterprise Architecture
GIF	Government Interoperability Framework
GIS	Geographic Information System

Acronym	*Full Form*
HMIS	Health Management Information System
IBEC	Intergovernmental Budget and Economic Council
ICT	Information and Communication Technology
ID	Identification
IFMIS	Integrated Financial Management Information System
IPRS	Integrated Population Registration System
JSON	JavaScript Object Notation
KPI	Key Performance Indicator
KRA	Kenya Revenue Authority
LTS	Long-Term Support
MFA	Multi-Factor Authentication
NTSA	National Transport and Safety Authority
OAG	Office of the Auditor-General
OCOB	Office of the Controller of Budget
OSR	Own Source Revenue
OTP	One-Time Password
PDF	Portable Document Format
PFM	Public Finance Management
POS	Point of Sale
RBAC	Role-Based Access Control
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SAML	Security Assertion Markup Language
SAST	Static Application Security Testing
SCOA	Standard Chart of Accounts
SLA	Service Level Agreement
SSO	Single Sign-On
TCO	Total Cost of Ownership
TLS	Transport Layer Security
TR	Technical Requirement
UAT	User Acceptance Testing
UPS	Uninterruptible Power Supply
USSD	Unstructured Supplementary Service Data
UUID	Universal Unique Identifier
VAT	Value Added Tax
XML	Extensible Markup Language

CERTIFICATION

These Annexes to the Standards and Guidelines have been reviewed and approved for publication and implementation by the Commission on Revenue Allocation in accordance with its constitutional mandate under Article 216 of the Constitution of Kenya, the Public Finance Management Act, 2012, and all other relevant statutory provisions. In issuing these Guidelines, the Commission seeks to promote prudent use of public resources, to ensure value for money, and to enhance revenue generation and management across all County Governments and National Government implementing entities.

Dated the 28th May, 2026.

MARY WANYONYI CHEBUKATI,
Chairperson, Commission on Revenue Allocation.

ROBLE NUNO,
Commission Secretary/Chief Executive Officer,
Commission on Revenue Allocation.

PRINTED AND PUBLISHED BY THE GOVERNMENT PRINTER, NAIROBI