AFRICA GOVERNANCE AND CIVIC INNOVATION HUB

www.agcih. africa

WORKING PAPER NO. 003

Version 1.0 | March 2026 | Under Active Development

Procurement as the Gateway of Digital State Power

Governance Implications for AI and Digital Systems in African Public Administration

Danai Hazel Kudya
Founder, Africa Governance and Civic Innovation Hub (AGCIH)
Dana.kudya@agcih.africa

Suggested Citation

Kudya, D.H. (2026). Procurement as the Gateway of Digital State Power: Governance Implications for AI and Digital Systems in African Public Administration. AGCIH Working Paper No. 003, Version 1.0. Africa Governance and Civic Innovation Hub. www.agcih.africa

Doctrines advanced in this paper: Procurement Entry Doctrine | Continuous Administration | Administrative Hosting Capacity | Sovereign Administrative Authority | Governance Readiness

Executive Summary

Africa's governments are procuring digital systems at speed. Revenue authorities are replacing legacy platforms with AI-enabled tax systems. Ministries of Home Affairs are building integrated population registries linked to biometrics and surveillance infrastructure. Local authorities are adopting ERP systems across service functions. Courts, hospitals, customs authorities, and social protection bodies are acquiring platforms that restructure their internal operations. This is real, it is accelerating, and it is consequential.

And yet: the governance frameworks surrounding this transformation continue to start too late. Most attention goes to deployment, regulation, ethics review, or public controversy. By that stage, however, the most consequential decisions have already been made. The architecture of state power in the digital era is shaped earlier, and more quietly, through procurement.

This paper advances a direct proposition: procurement is not an administrative process for acquiring goods and services. In the digital era, it is the gateway through which digital systems, algorithmic logics, vendor dependencies, and data infrastructures enter the state. Through procurement, governments do not simply purchase software. They often determine the operational conditions under which public authority will later be exercised, supervised, challenged, or lost.

For this reason, procurement must be understood as a governance event.

The paper is grounded in three interlocking doctrines that together form the AGCIH framework for digital public authority:

The AGCIH Doctrinal Chain

Continuous Administration - the foundational obligation: the state must keep governing, across time, across systems, across vendor relationships. This principle is newly urgent in an era when the instruments of governance are procured from external actors and hosted outside institutional boundaries.

Administrative Hosting Capacity - the institutional mechanism: the practical ability of a public institution to contain a digital system within its administrative authority. Hosting is not technical server location. It is institutional command.

Procurement Entry Doctrine - the gateway moment: the principle that digital and AI systems enter public administration through procurement decisions that determine whether the state retains the administrative continuity, hosting capacity, and sovereign authority it is legally and constitutionally obligated to preserve.

The paper draws on documented African procurement experiences including Uganda's Electronic Passenger System, the Ugandan and Zimbabwean facial recognition programmes, the DRC's biometric identity procurement, and Zimbabwe's own digital transformation trajectory to ground the argument in institutional reality rather than theory.

The paper concludes with the AGCIH Procurement Governance Matrix: a practical scored assessment tool that public institutions can apply before any AI or digital system procurement. It replaces abstract principles with operational criteria that procurement officers, legal advisers, policy units, and oversight bodies can use.

The case is not against digital transformation. It is for digital transformation conducted under conditions that preserve public authority, institutional continuity, and accountable governance. Procurement is where that work must begin.

PREFACE

How This Paper Positions Itself Within the Existing Field

The argument that procurement matters for AI governance is not new, and this paper does not claim otherwise. The OECD's Governing with Artificial Intelligence report (2025) dedicates substantial analysis to AI in procurement contexts. The World Economic Forum's AI Procurement in a Box toolkit (2020), co-designed with government partners, produced practical guidelines for responsible AI purchasing decisions. The GovLab at New York University published a focused analysis of AI procurement challenges in 2023, documenting structural gaps between technical and governance requirements in government contracting. The AI Now Institute has argued that procurement is a lever for addressing market concentration in digital infrastructure. The United States Office of Management and Budget issued AI procurement memoranda in 2024 and 2025 requiring agencies to conduct rights and safety impact assessments before acquiring high-impact AI systems. In Europe, the EU AI Act and related procurement directives increasingly require transparency and fundamental rights compliance to be addressed at the point of acquisition. These are serious contributions, and this paper builds on them.

Where this paper departs from the existing field and where its originality resides is in three specific respects that are stated plainly here so that readers can assess them.

First, the existing literature treats procurement primarily as a risk management exercise. It asks how governments can buy AI responsibly. It produces checklists, guidelines, and impact assessment frameworks oriented towards mitigating harm during or after deployment. It does not ask the prior and more foundational question: what does the act of procurement do to the institutional authority and administrative continuity of the state? The OECD's 2025 guidance focuses substantially on using AI to improve procurement processes and on ensuring ethical use. It does not develop a doctrinal account of what procurement transfers, embeds, or surrenders within the administrative structure of the state. This paper argues that the foundational question is not responsible acquisition but institutional governance and that distinction changes the entire analytical frame.

Second, the existing literature is almost entirely produced from OECD, EU, and US institutional contexts. It reflects administrative realities and legal infrastructures of countries with mature procurement regulation, integrated legal-technical institutional capacity, and established oversight bodies. Scholarship on responsible AI in Africa has acknowledged that AI is entering public administration through procurement arrangements often conducted under confidential terms, in the absence of mature regulatory safeguards, increasing the risk of regulatory capture and vendor lock-in. But this recognition has not produced a governance doctrine or an operational tool designed specifically for African institutional conditions where donor-driven procurement timelines compress governance diligence, where legal-technical capacity is unevenly distributed across ministries and tiers of government, where exit from vendor dependency carries different fiscal and operational costs, and where control over critical digital infrastructure has direct implications for administrative sovereignty. This paper is written from within the African institutional context, not as an adaptation of frameworks developed elsewhere.

Third, the doctrinal architecture advanced in this paper does not exist in the existing literature. The three named doctrines; Continuous Administration, Administrative Hosting Capacity, and the Procurement Entry Doctrine arranged as an interlocking governance chain applied to digital procurement are original contributions of this paper. The question of how AI implementation can be embedded in rights-based frameworks and legal safeguards, including public procurement and data protection regulation, is identified in the academic literature as critical for the legitimate and sustainable adoption of AI in Africa. But identifying the question is not the same as answering it. No existing work has named Administrative Hosting Capacity as

a doctrine, defined it operationally, and linked it to a procurement governance obligation. No existing work has built a scored governance matrix structured around these doctrinal criteria for African public institutions.

The administrative law principles invoked in this paper, institutional competence, non-delegable functions, traceability, and procedural fairness, are established doctrines. The procurement risks documented in Section 12, vendor lock-in, data dependency, workflow capture, and governance dilution appear in OECD and GovLab literature. This paper does not claim to have discovered them. It claims to have given them an institutional home: a named doctrinal architecture grounded in African administrative realities, with a practical governance tool that public institutions can apply before the next contract is signed.

One further positioning note is necessary. The African Union's Continental AI Strategy, endorsed by the AU Executive Council in July 2024, represents a significant continental commitment to AI governance. Its Phase 1 implementation (2025–2026) focuses on establishing governance frameworks and national AI strategies. This paper's contribution is complementary but distinct: where the AU Strategy sets continental direction and ethical principles, this paper provides an operational governance doctrine for the procurement decisions that will determine whether those principles are operationally realisable within state institutions. Strategic commitment and institutional architecture are not the same thing. Both are necessary. AGCIH's work addresses the second.

That is a precise and defensible claim to originality. It is the claim on which this paper stands.

1. Introduction: Africa's Digital Transformation Is Real, and Procurement Is Its Gateway

Across Africa, governments are acquiring digital systems for functions that sit at the heart of state authority. Revenue authorities are replacing legacy platforms with integrated tax management systems incorporating AI-driven risk assessment and case selection. Ministries of Home Affairs are building population registries integrated with biometric passports, facial recognition infrastructure, and surveillance systems. Social protection bodies are digitising beneficiary verification and disbursement. Courts are implementing case management platforms. Local authorities are adopting enterprise resource planning systems. In almost every sector, digital transformation has moved from aspiration to active implementation.

Zimbabwe is not an exception. The Zimbabwe Revenue Authority commissioned TaRMS, its Tax Administration and Revenue Management System, in August 2025, following a phased rollout that began in December 2023. Zimbabwe's population register is now the operational backbone for civil servants' audit, vehicle registration, mobile phone user registration, social welfare payments, and the planned integrated digital identity system. The national government published the 2026–2030 Digital Roadmap (National AI Strategy, officially launched 13 March 2026) and, through the policy, is establishing ZAIRA (Zimbabwe Artificial Intelligence Regulatory Authority) as a dedicated oversight body. Digital transformation is a stated national priority.

What is less clear and what most governance frameworks have not yet resolved is how digital systems are acquired, what conditions govern their entry into state institutions, and whether the public bodies adopting them retain the authority, visibility, and institutional control that responsible digital administration requires. This is where procurement becomes decisive.

Public institutions do not adopt digital systems in the abstract. They acquire them through contracts, tenders, pilot arrangements, donor-supported procurements, managed services, software subscriptions, and vendor partnerships. In practice, digital transformation enters government through procurement. And procurement decisions about what to buy, from whom, on what terms, under what hosting arrangements, with what contractual safeguards often determine the future conditions of administrative control before governance debates have fully begun.

This paper argues that procurement must be reconceived as a governance event: a moment at which the state either secures or surrenders the conditions for Continuous Administration of the digital systems through which it governs. It introduces three interlocking doctrines; Continuous Administration, Administrative Hosting Capacity, and the Procurement Entry Doctrine as the analytical and operational foundation for a more mature approach to digital public procurement in Africa.

The argument is not against digital adoption. Africa's governance needs are real, and digital systems offer genuine capacity gains. The argument is that adoption without adequate governance architecture is not modernisation. It is exposure.

2. Procurement Is Not Neutral: The Case for Procurement as Governance

Procurement is conventionally understood as an administrative function for securing goods and services competitively, transparently, and at fair value. These remain essential principles. But in the digital era, they are no longer sufficient.

Digital systems are not ordinary commodities. They do not add capacity to an unchanged institution. They reorganise institutional practice. A tax management platform changes how assessments are generated, how compliance is scored, and how enforcement cases are selected. A population registry changes how identity, access, and benefit eligibility are determined. A judicial case management system changes how files are tracked, how cases are prioritised, and how the state maintains records of its own decisions. A social protection database changes how exclusion and verification operate at scale. Procurement of such systems is therefore an act of institutional configuration, not simply acquisition.

When a ministry procures a digital platform, it may be determining how decisions are initiated and authorised; where operational visibility lies; whether the institution can inspect or contest system outputs; whether data can be extracted, transferred, or locally governed; whether the system supports or displaces existing legal mandates; and whether future modifications remain under public control.

Procurement creates path dependency. Once a system is installed, integrated, and relied upon, changing course is difficult. Contracts may be long-term. Data may be locked in proprietary formats. Users may be trained around the system rather than the law. What began as acquisition becomes embedded institutional dependency. The state continues to act, but through a structure it may not fully own, understand, or control.

The assumption that procurement is merely operational obscures the fact that it is frequently the first and most decisive point at which the state either yields or secures digital control. This paper therefore reconceives procurement as a governance gateway: the moment at which the state makes binding choices about the future conditions of its own administration.

3. The Doctrinal Foundation: Three Principles That Must Govern Procurement

3.1 Continuous Administration: The Foundational Obligation

At the heart of public administration lies a simple but powerful expectation: the state must continue to govern. Government institutions must remain capable of exercising their mandates across time, regardless of changes in political leadership, technological infrastructure, vendor relationships, or administrative personnel. This obligation is described in this paper as Continuous Administration.

Continuous Administration means that public authority must remain operational over time; institutional decision-making must remain attributable to the state; administrative responsibility cannot disappear into external systems; and the state must retain the capacity to supervise the instruments through which it governs.

Historically, this principle was largely taken for granted. Administrative tools, files, registers, records, workflows, and procedural structures were physically and institutionally contained within government. Digital transformation fundamentally changes this condition. The operational instruments through which the state now acts may be developed, hosted, maintained, or partially controlled outside institutional boundaries. This makes Continuous Administration a newly urgent governance concern.

The doctrine requires governments to ensure that the introduction of digital systems does not disrupt the state's ability to continue exercising authority, responsibility, and accountability over time. It is not enough for a system to work today. The question is whether the institution retains the authority to govern it tomorrow.

3.2 Administrative Hosting Capacity: The Institutional Mechanism

If Continuous Administration is the principle, Administrative Hosting Capacity is the institutional capability through which the principle is maintained. It asks a practical question: can the institution actually host and govern the digital systems through which it exercises public authority?

Hosting here does not mean technical server location. It refers to the institutional ability to contain the system within the administrative authority of the state. An institution with Administrative Hosting Capacity can supervise system operation; understand system outputs; intervene when problems arise; preserve accountability chains; retain authority over workflows and decisions; and maintain continuity even if vendors change or systems evolve.

Without such capacity, digital systems risk displacing administrative presence rather than strengthening it. The institution continues to act through the system, but it may no longer be governing it in any meaningful sense. The distinction between using a system and governing it is one of the central analytical contributions of this paper.

Administrative Hosting Capacity is not a post-procurement evaluation. It is a procurement criterion. The assessment of whether an institution can host a system must happen before the system is acquired because once it has been integrated, dependencies take hold and the governance problem becomes structural rather than correctable.

3.3 Procurement Entry Doctrine: The Gateway Moment

Procurement Entry Doctrine

The principle that digital and AI systems enter public administration through procurement decisions that determine whether the state retains the administrative continuity, institutional hosting capacity, and sovereign authority it is legally and constitutionally obligated to preserve.

Procurement is not peripheral to digital governance. It is constitutive of it.

Once Continuous Administration is understood as the foundational obligation, and Administrative Hosting Capacity as its institutional mechanism, procurement becomes the site where both must be operationalised. Procurement is the moment at which the state makes consequential choices about which systems will enter its administrative infrastructure, who will control them, and under what conditions the state may retain, modify, or exit from those arrangements. These choices are governance decisions, not administrative ones. They must be treated accordingly.

4. Digital State Power: What Enters Through Procurement

The phrase 'digital state power' refers to the operational capacity of the state as mediated, structured, or enabled by digital systems. This includes the ability to register, classify, monitor, allocate, verify, adjudicate, approve, deny, pay, audit, investigate, and coordinate through technology-enabled means. When digital systems are procured, several layers of state power may enter or be reshaped simultaneously.

Functional power is affected when a system performs, supports, or structures public functions such as licensing, tax processing, welfare disbursement, border clearance, or judicial administration. Informational power is affected when the system determines who controls data; its structure, portability, access permissions, retention, and analytics. Procedural power is affected when system workflows define what steps can be taken, in what order, and by whom, silently redesigning administrative procedure. Interpretive power is affected when AI-enabled or rules-based systems classify risk, score applicants, recommend actions, or prioritise cases. And infrastructural power is affected through hosting location, cloud arrangements, cybersecurity architecture, and maintenance obligations.

Procurement is thus a gateway not only to tools, but to layered forms of operational power. The governance question is whether public institutions remain capable of directing and containing that power and whether they have assessed that question before signing a contract.

4.1 Where AI Governance Actually Begins

Much of the AI governance field focuses on fairness, bias, explainability, privacy, and regulatory compliance during or after deployment. These are important. But in government contexts, AI governance begins before the system is switched on. It begins when the state chooses what system to procure, what function it will support, what data it will use, which vendor will configure it, and what safeguards are contractually required.

In public administration, the procurement stage is where foundational AI governance questions first arise: Is the public institution legally competent to use such a system for this function? Can the institution understand and contest system outputs? Does the contract require audit access and documentation? Can the state retrieve data and transition away from the vendor if necessary? Is error handling, appeals, overrides, and accountability mechanisms built in?

If these questions are not addressed at the procurement stage, later governance mechanisms, ethics committees, regulatory interventions, policy statements may be too weak or too late to correct structural design decisions embedded in contracts and architectures. Ethics oversight after deployment cannot recover what was not secured at entry.

5. Procurement as a Site of Administrative Delegation

One of the most important but overlooked consequences of digital procurement is the risk of unchecked administrative delegation. In administrative law, certain functions of the state cannot be transferred to private actors without proper legal authority, oversight, and accountability. Public functions involve duties of legality, fairness, reviewability, justification, and institutional responsibility.

Digital systems can blur the line between support and delegation. A vendor may build the workflow through which approvals are processed. A platform may determine what information is visible to officials. A proprietary rules engine may structure which cases are flagged for action. A managed service provider may control uptime, maintenance, access permissions, and system updates. In such cases, the institution retains nominal authority while losing practical control. Procurement has become a route of de facto delegation without explicit constitutional or administrative acknowledgement. The result is not outsourcing in the traditional sense. It is a partial displacement of administrative presence. The state continues to act, but through a structure it does not fully own, understand, or control.

This problem is especially acute where vendor contracts are opaque or weakly negotiated; where ministries lack digital legal expertise; where donor-supported systems are rapidly introduced without long-term state control planning; where public bodies cannot inspect or alter system logic; and where institutional staff become dependent on external technicians for ordinary governance functions. This is not a hypothetical concern. It is the governance condition in which several African states are currently operating.

6. The Administrative Law Foundation

This paper sits within an administrative law tradition concerned with lawful public authority. Administrative law asks how state institutions exercise power legitimately, accountably, and within defined legal bounds. Several of its core principles are directly implicated by digital procurement.

Institutional Competence requires that public power be exercised by institutions with a lawful mandate and operational capacity. This supports the doctrine of Administrative Hosting Capacity: digital systems must be situated within institutions capable of meaningfully governing them. Non-Delegable Functions recognises that some state functions require public judgment, public accountability, and lawful review. A system may support administrative decision-making, but it cannot absorb public authority without governance consequences. Traceability and Reviewability requires that administrative action be attributable and reviewable. Systems that obscure how decisions were made undermine this principle. Procurement must secure traceability by design.

Procedural Fairness requires that where systems affect rights, entitlements, access, sanctions, or exclusion, the public institution must preserve procedural safeguards, including appeal routes, override mechanisms, and explanation pathways. Continuity of Administration, discussed in Section 3, requires the state to remain capable of acting consistently and continuously, a capacity that procurement can either protect or erode.

These principles show that procurement is not external to administrative law. In the digital era, it is one of its most consequential frontiers. Every contract clause, every hosting decision, every data arrangement, every exit provision is an administrative law question.

7. Africa in Focus: What Procurement Failures Actually Look Like

The governance risks described in this paper are not theoretical. They are documented in procurement experiences across the African continent. Three cases are examined here as concrete illustrations of what happens when digital systems enter public administration without adequate governance architecture.

7.1 Uganda's Express Penalty Scheme: The Anatomy of a Procurement Failure

In June 2025, Uganda launched its Electronic Passenger Scheme (EPS) for traffic offences. The system was suspended less than a week after launch, with the government citing a 'lack of clarity' among government agencies. The explanation was procedurally accurate and substantively inadequate.

What the suspension exposed was a pattern of procurement failure that had been present long before launch. A Russian company, Joint Stock Company Global Security, had reportedly been granted 80 per cent of fine revenues generated by the system, despite contributing minimal investment, under arrangements that contained significant legal and procurement irregularities. There were no publicly accessible oversight mechanisms, no clear contracts, and no meaningful appeal avenues for citizens. Sensitive personal data was collected under conditions of limited transparency regarding who could access it. The state had acquired functionality. It had not retained governance.

Case: Uganda — Express Penalty Scheme (2025)

A foreign vendor was awarded the majority of public revenue from a state enforcement system, under opaque contractual terms, with no public audit mechanism, no appeal pathway, and no clear data governance framework. The procurement created a governance structure the state did not control and citizens could not contest. Suspension was the only corrective available. The lesson: functionality without governance architecture is not digital transformation. It is institutional exposure.

7.2 Uganda's National Digital ID: When Exclusion Is Procured

Uganda's national digital identity system; Ndaga Muntu was intended as a foundational public infrastructure enabling access to healthcare, education, and social protection. A 2021 report by the Centre for Human Rights and Global Justice documented how procurement and design choices embedded rigid registration requirements, created technical failure points with no recourse mechanisms, and resulted in millions of citizens disproportionately the elderly, women, and rural communities being excluded from basic public services.

The governance failure was not post-deployment. It was designed in at procurement stage: the system was built without adequate rights-impact assessment, without offline access protocols, and without grievance or remedy mechanisms embedded in its operational architecture. By the time these problems were visible, the system was operational and the architecture was fixed.

Case: Uganda — National Digital ID — Ndaga Muntu

Procurement choices embedded exclusion into foundational public infrastructure. The system was integrated with health, education, and social protection before governance safeguards were in place. The state could not easily correct what its own procurement had structurally embedded. The lesson:

for rights-affecting systems, governance architecture must precede deployment. It cannot be retrofitted.

7.3 Zimbabwe and the Cloudwalk Facial Recognition Programme

In 2018, Zimbabwe entered into an arrangement with the Chinese company Cloudwalk Technology to develop a national facial recognition system, framed as a smart financial services network with applications at airports, railway stations, and bus stations, and including the construction of a national facial database. The arrangement was conducted under the framework of China's Belt and Road Initiative.

The governance questions this arrangement raised were not primarily about the technology. They were about the procurement conditions under which the technology entered the state. Questions regarding data sovereignty, specifically who controls the national facial database and under what conditions, remain inadequately documented in the public domain. The cybersecurity legal framework that would govern the use of the data was criticised as insufficient at the time of the arrangement. These are procurement governance failures: decisions about data ownership, institutional control, and legal framework were not resolved before the system entered state administration.

Case: Zimbabwe — Cloudwalk Facial Recognition Programme (2018–present)

A foreign-designed and partially foreign-controlled biometric system entered state administration under governance conditions that left core questions of data sovereignty, institutional oversight, and legal framework unresolved. The procurement created ongoing governance obligations the state did not fully anticipate or secure. The lesson: for systems involving sensitive data and foreign control, every procurement decision is a sovereignty decision.

7.4 A Continent-Wide Pattern

These cases are not isolated failures. Research by CIPESA published in 2025 found that most e-government projects in Africa end in partial or total failure, commonly attributed to poor project design, lack of infrastructure, weak accountability frameworks, and insufficient governance planning. The pattern is one in which countries integrate complex, often foreign-managed digital systems into public governance without establishing frameworks for transparency, accountability, and institutional oversight.

In Kenya, a 2024 data centre partnership agreement raised serious concerns about long-term data sovereignty and control over critical digital infrastructure. In the Democratic Republic of Congo, a biometrics procurement valued at over one billion US dollars resulted in a system that remained largely non-functional, with civil servants raising alarms about financial irregularities, the World Bank refusing to fund the project, and only a small number of VIPs receiving identity documents after years of public expenditure. In each case, the governance problem had its origin at the point of procurement.

8. The Zimbabwe Context: Governing Digital Transformation from the Inside

Zimbabwe's current digital transformation presents a governance challenge that is simultaneously urgent and structurally complex. The country is acquiring digital systems across multiple sectors at a pace that has outrun the governance architecture needed to absorb them responsibly.

8.1 TaRMS and the Revenue Authority

ZIMRA's Tax Administration and Revenue Management System is the most significant digital procurement in Zimbabwe's public administration in recent years. It replaced a fragmented legacy architecture combining SAP and Microsoft platforms that had produced chronic downtime, delayed tax clearances, misallocated payments, and frustrated compliance. TaRMS has delivered measurable operational improvements: on-time filing increased from 14 per cent in 2023 to 38 per cent in 2024, and active taxpayer registrations grew substantially. These are real governance gains.

But TaRMS also illustrates the governance questions this paper raises. The system is being extended to incorporate AI and machine learning for fraud detection, predictive risk analysis, and intelligent case selection functions that directly affect taxpayer rights, enforcement prioritisation, and institutional discretion. As these AI functions are activated, the governance architecture must expand to match them. Key questions remain to be fully resolved: What are the auditability requirements for AI-generated risk scores? How will taxpayers contest algorithmic assessments? Who within ZIMRA retains meaningful oversight of the AI's case selection logic? Can the system be interrogated by the Auditor-General or Parliamentary oversight bodies? TaRMS is a significant institutional investment. The governance architecture surrounding its AI functions must be equally significant.

8.2 The Population Register and Digital Identity

Zimbabwe's Population Register is now the operational foundation for a growing number of state functions: civil servants audit, mobile phone registration, vehicle licensing, social welfare disbursement, and the planned integrated digital identity system. The integration of these functions into a single registry infrastructure creates both governance efficiency and governance risk. Operational integration without corresponding oversight integration means that failures, data breaches, or access errors in the registry can cascade across multiple service areas simultaneously.

The cybersecurity legal framework governing this infrastructure was identified as insufficient as early as the Cloudwalk programme. The Cyber and Data Protection Act (SI 155 of 2024) has since advanced Zimbabwe's data protection architecture. But the question for this paper is not only whether a data protection law exists. It is whether the institutions responsible for administering the Population Register have the Administrative Hosting Capacity to govern it: whether they can supervise its operation, respond to system failures, manage access disputes, and account for its outputs to oversight bodies.

8.3 ZAIRA and the Governance Frontier

Zimbabwe's proposed Zimbabwe Artificial Intelligence Regulatory Authority represents a significant governance commitment. It also raises a sequencing question that this paper considers fundamental: if AI systems are entering government through procurement decisions made before ZAIRA is operational, then ZAIRA will spend its early institutional life managing systems whose governance architecture was determined without it. Regulatory institutions established after digital adoption is underway face the structural challenge of governing what was not secured at entry.

The 2026–2030 National AI Strategy commits Zimbabwe to AI, blockchain, and 5G adoption. The procurement decisions that will operationalise that commitment will begin immediately. This paper's central argument applies directly: the governance work must happen at the procurement stage, not after deployment.

8.4 The Local Government Gap

The Local Authorities Digital System, introduced through the Commonwealth Local Government Forum and Harare Institute of Technology, reached six local authorities. Local authorities represent the administrative tier closest to citizens in licensing, billing, land administration, and service delivery. They also represent the tier with the least institutional digital governance capacity. Where procurement decisions at the local government level are made without adequate legal-technical expertise, without continuity planning, and without exit provisions, the governance gaps this paper identifies are most acute and least visible.

9. Why Existing Procurement Systems Are Inadequate for Digital Governance

Most public procurement regimes were not designed with AI or complex digital systems in mind. They assume that goods and services can be specified in relatively stable and observable terms. Digital systems are iterative, layered, opaque, and evolve after procurement is complete. Their long-term governance implications are difficult to capture through ordinary procurement templates.

Several structural gaps consistently arise. First, technical specifications are written without governance specifications: tender documents may define system features while omitting requirements for auditability, explainability, data portability, legal compatibility, and institutional authority retention. Second, procurement units and policy units operate separately, with insufficient shared analysis of governance risk. Third, most public institutions lack integrated legal-technical capacity teams that can examine legal, technical, contractual, and governance dimensions together. Fourth, donor-driven procurements are often conducted under project deadlines that are incompatible with the governance diligence digital systems require. Fifth, procurement is treated primarily as procedural compliance, and institutions may fail to recognise that they are making strategic choices about the future distribution of state power. These are not failures of intent. They are structural gaps in a procurement architecture built for a different era. Closing them requires new tools, new institutional practices, and a different understanding of what procurement is for.

10. The AGCIH Procurement Governance Matrix

The following matrix is a practical governance assessment tool for public institutions preparing to procure AI or complex digital systems. It operationalises the doctrines of Continuous Administration and Administrative Hosting Capacity as procurement criteria. It is designed to be applied by procurement teams, legal advisers, policy units, and oversight bodies before a procurement decision is finalised.

Each of the ten criteria is scored on a four-level scale. An institution assesses its current position honestly against each criterion and assigns a score from 1 (Minimal) to 4 (Strong). The total score out of 40 determines the institution's Governance Readiness status and recommended action.

Governance Criterion	Institutional Question	Level 1 Minimal	Level 2 Partial	Level 3 Adequate	Level 4 Strong
1. Mandate Fit	Is the system aligned with the institution's legal mandate?	No mandate analysis conducted	General mandate alignment assumed	Legal mandate formally documented and verified	Legal opinion obtained; function confirmed as digitisable
2. Continuous Administration	Will the state retain operational authority if the vendor changes or the system fails?	No continuity plan exists	Continuity is mentioned but not contractually secured	Continuity requirements included in contract clauses	Fully documented continuity plan with tested fallback protocols
3. Administrative Hosting Capacity	Can the institution supervise, understand, and remain accountable for the system?	No institutional capacity assessment conducted	Capacity assessed informally or by vendor only	Internal capacity review completed; gaps documented	Hosting capacity confirmed; capacity-building plan in place
4. Data Governance	Does the state control data ownership, access, extraction, and cross-border transfer?	Data ownership not addressed in contract	Data ownership asserted but extraction rights unclear	Data rights and portability documented in contract	Full data sovereignty plan with migration protocol and audit rights
5. Auditability and Traceability	Can outputs, decisions, and workflows be inspected by the institution and authorised oversight bodies?	No audit trail specified or available	Vendor provides reports on request only	Audit trail access required and specified in contract	Structured audit protocol with defined oversight body access rights
6. Function Sensitivity Assessment	Has the institution assessed whether the system affects rights, entitlements,	No rights-impact assessment conducted	Sensitivity informally acknowledged	Rights-impact assessment completed	Heightened safeguards applied; appeal and

Governance Criterion	Institutional Question	Level 1 Minimal	Level 2 Partial	Level 3 Adequate	Level 4 Strong
	exclusions, or sanctions?			and documented	override mechanisms confirmed
7. Accountability Architecture	Are human responsibility, override powers, escalation pathways, and remedy mechanisms preserved?	No accountability mapping conducted	Nominal accountability assumed without documentation	Accountability chains identified and documented	Accountability architecture embedded in contract and operational protocols
8. Vendor Lock-In Risk	Can the institution switch providers or recover autonomy at reasonable cost?	Proprietary system with no portability or exit clause	Exit acknowledged but no migration plan	Exit clause and data migration requirements in contract	Full vendor transition plan tested and documented
9. Continuity and Resilience	Can the institution continue operating during outages, cyber incidents, or connectivity failures?	No resilience or business continuity provisions	Resilience provisions mentioned but untested	Service continuity obligations specified in contract	Resilience plan tested; offline operating protocols documented
10. Fiscal Sustainability	Can the institution sustain total costs of ownership beyond the initial procurement cycle?	Only the initial acquisition cost considered	Recurring costs estimated informally	Total cost of ownership modelled for contract duration	Multi-year fiscal sustainability plan approved by budget authority

Scoring and Readiness Determination

Total the scores across all ten criteria. The maximum possible score is 40.

Score Range	Governance Readiness Status	Recommended Action
36–40	Strong — Procurement Governance Ready	Proceed with procurement. Maintain governance review schedule.
26–35	Adequate — Conditionally Ready	Proceed with identified conditions. Address gaps before deployment.
16–25	Partial — Significant Gaps	Pause procurement. Develop hosting capacity and governance plan before proceeding.
10–15	Minimal — Not Ready	Do not proceed. Governance architecture must be established first.

How to Use This Matrix

The matrix is not a compliance checklist. It is a governance readiness assessment. Its purpose is to enable institutions to make procurement decisions with a clear understanding of the governance conditions they are accepting, the risks they are creating, and the institutional work required before proceeding.

Where an institution scores at Level 1 or 2 on Criteria 2 (Continuous Administration) or 3 (Administrative Hosting Capacity), procurement should not proceed regardless of overall score. These criteria are foundational. A system that cannot be governed continuously and cannot be hosted institutionally should not enter the state regardless of its technical functionality.

Where an institution scores at Level 1 on any criterion, that criterion must be addressed in the procurement process either through contract provisions, pre-procurement capacity building, or restructuring of the proposed acquisition before the institution proceeds.

This matrix can form the basis of an AGCIH advisory product, a ministry-facing pre-procurement review tool, a regulatory condition attached to high-risk digital procurements, or an oversight body inspection framework. AGCIH intends to develop accompanying guidance notes for each criterion, including model contractual clauses and institutional readiness benchmarks.

11. Institutional Questions Before Any Procurement Decision

Before acquiring AI or complex digital systems, public bodies must ask a more disciplined set of institutional questions. These go beyond technical functionality and price competitiveness. They are governance questions.

What exact public function is this system intended to support, and is this function one that can be lawfully digitised in this manner? Which institution retains final accountability for outcomes, and does that institution have the governance structure to supervise the system? What data architecture is being created, and who controls it? What element of judgement, triage, or classification is the system performing, and how will errors be identified, challenged, and corrected? Can the institution extract all data and records if the contract ends? What level of dependence on the vendor is being created, and what does exit look like in practice?

What continuity arrangements exist for infrastructure failure, cyber incidents, or funding interruptions? Which oversight bodies will be able to inspect the system, and is that contractually guaranteed? Are we procuring a tool, or are we inadvertently redesigning the operational structure of public authority?

These questions are not obstacles to innovation. They are the foundation of responsible innovation in government. An institution that cannot answer them should not yet be procuring.

12. Procurement Risks in AI and Digital Government

A governance-sensitive understanding of procurement must be clear-eyed about the principal risks that arise when digital systems are acquired without adequate institutional design. The following risks are documented and recurring, not theoretical.

Vendor Lock-In occurs where systems are proprietary, non-portable, or deeply integrated without transition clauses, making provider change prohibitively difficult. Data Dependency arises where the state does not clearly control data schema, extraction rights, retention arrangements, or cross-border flows, weakening administrative sovereignty. Workflow Capture occurs when system design reflects vendor architecture more than legal mandate, privately restructuring administrative procedure. Reduced Auditability emerges where systems do not provide accessible logs, model documentation, or explanation pathways, undermining oversight bodies and legal review.

Governance Dilution Through Managed Services arises when operation, maintenance, upgrades, and permissions are externally controlled, eroding the institution's practical capacity to govern daily operations. Fragmented Institutional Ownership creates authority gaps where no single ministry, department, or agency retains clear governance responsibility. Inadequate Procurement Criteria results where tendering overemphasises technical compliance or price while failing to assess administrative fit, governance resilience, or legal compatibility. Long-Term Fiscal Exposure involves hidden recurring costs; subscriptions, licensing, maintenance, cybersecurity, and retraining that commit the state to enduring expenditure without institutional sustainability planning.

Systemic Dependence in Essential Services poses continuity risks in sectors such as health, justice, taxation, pensions, and public procurement itself, where system failure can disrupt core public functions. And perhaps most consequentially, Quiet Constitutional Effects arise where systems shape entitlement, suspicion, exclusion, or decision sequencing at scale, altering the character of governance without formal legislative or constitutional deliberation.

13. Conclusion: Procurement Is Where the Work Must Begin

Digital transformation in government is real, it is accelerating, and in Africa, it is happening now. Revenue systems are being rebuilt. Population registries are being integrated. Judicial and social protection functions are being digitised. Surveillance and identity infrastructure is being procured. The pace of adoption is outrunning the governance frameworks that should accompany it.

This paper has argued that the most consequential governance decisions in this transformation are made not at deployment, not at regulation, and not at public controversy, but at procurement. Procurement is the gateway through which digital systems, vendor dependencies, data architectures, and algorithmic logics enter the state. It is where public institutions first determine, often without full recognition, the future conditions of administrative control, institutional dependence, continuity, and accountability.

The three doctrines advanced here- Continuous Administration, Administrative Hosting Capacity, and the Procurement Entry Doctrine provide a governance framework for understanding why procurement is so consequential, and what must change for African public institutions to govern procurement with the seriousness digital transformation demands. They are not abstract principles. They are operational requirements. They translate into contractual provisions, institutional readiness assessments, oversight mechanisms, and scored governance criteria that procurement officers, legal advisers, and oversight bodies can apply.

For Zimbabwe and comparable contexts, the paper's implications are direct. Digital procurement decisions are being made now. TaRMS is being extended to include AI functions. The Population Register is being integrated across state services. ZAIRA is being established. The 2026–2030 Digital Roadmap is being operationalised. Each of these processes involves procurement decisions that will shape the administrative architecture of the state for years. Those decisions must be made with governance architecture in place, not after the fact.

The AGCIH Procurement Governance Matrix offers a starting point. It is not the complete answer. Governance readiness for digital public administration also requires updated public procurement legislation that incorporates digital-specific criteria; interdisciplinary procurement teams with legal, technical, and governance expertise; standard model clauses for digital and AI procurements that protect data sovereignty, auditability, and exit; and institutional capacity building that enables public bodies to supervise the systems they operate.

The task ahead is not to slow digital transformation. It is to ensure that when digital systems enter the state, they do so under conditions that preserve public authority, institutional continuity, and accountable governance. Procurement is where that task begins. It is also where it has most frequently been neglected.

AGCIH's contribution is to insist that this neglect be named, examined, and remedied before the next contract is signed.

References

The following sources are cited or drawn upon in this paper. Where documents are publicly available, URLs are provided. This working paper is Version 1.0 and the references list will be expanded in subsequent versions as additional literature is incorporated.

International and Multilateral Frameworks

OECD (2025). Governing with Artificial Intelligence. Organisation for Economic Co-operation and Development. Available at: oecd.org

OECD (2019). Recommendation of the Council on Artificial Intelligence. OECD/LEGAL/0449. Available at: oecd.org/going-digital/ai/principles

World Economic Forum (2020). AI Procurement in a Box: AI Government Procurement Guidelines. WEF / AI Commons. Available at: ai-procurement.org

African Union (2024). Continental Artificial Intelligence Strategy. Endorsed by the AU Executive Council, July 2024. African Union Commission, Addis Ababa.

United States Office of Management and Budget (2024). Memorandum M-24-10: Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence. Executive Office of the President. Available at: whitehouse.gov/omb

European Parliament and Council of the European Union (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, L Series.

Research and Policy Literature

GovLab, New York University (2023). AI Procurement Snapshot: Addressing the Governance Gaps in Government AI Acquisitions. The Governance Lab at NYU. Available at: thegovlab.org

AI Now Institute (2023). AI Now Report 2023. AI Now Institute, New York. Available at: ainowinstitute.org

CIPESA (2025). State of Internet Freedom in Africa 2025: Artificial Intelligence and Digital Rights. Collaboration on International ICT Policy for East and Southern Africa. Available at: cipesa.org

Research ICT Africa / Africa Just AI (2024). Towards Responsible AI in Africa: Governance, Procurement and Accountability. Research ICT Africa. Available at: researchictafrica.net

Centre for Human Rights and Global Justice, New York University School of Law (2021). Paved with Good Intentions: Rhodesia, Zimbabwe, and the Long Road to Digital Identity Abuse. NYU School of Law. Available at: chrgj.org

Carnegie Endowment for International Peace (2025). Insights on AI Governance in Africa. Technology and International Affairs Programme. Available at: carnegieendowment.org

Zimbabwe and Regional Context

Zimbabwe Revenue Authority (2024). ZIMRA Annual Report 2024: TaRMS Implementation and Revenue Performance. ZIMRA, Harare.

Government of Zimbabwe (2026). National Digital Transformation Roadmap 2026–2030. Ministry of Information Communication Technology, Postal and Courier Services, Harare.

Zimbabwe (2021). Data Protection Act [Chapter 11:22]. Government of Zimbabwe.

Zimbabwe (2024). Cyber and Data Protection (General) Regulations, SI 155 of 2024. Government of Zimbabwe.

Administrative and Public Law Foundations

Craig, P. (2012). Administrative Law (7th ed.). Sweet & Maxwell, London.

Harlow, C. and Rawlings, R. (2009). Law and Administration (3rd ed.). Cambridge University Press, Cambridge.

Cane, P. (2011). Administrative Law (5th ed.). Oxford University Press, Oxford.

Related AGCIH Publications

Kudya, D.H. (2026). Governing AI Before It Exists: Why Public Procurement Is the First Layer of AI Accountability. Africa Governance and Civic Innovation Hub, AGCIH Working Paper No. 001. www.agcih.africa

Kudya, D.H. (2026). AGCIH Working Paper No. 002. Africa Governance and Civic Innovation Hub. www.agcih.africa

---

This references list is Version 1.0. Additional sources will be incorporated as the paper develops. Readers who wish to suggest relevant literature are encouraged to contact AGCIH at admin@agcih.africa .

Companion Papers and AGCIH Research Programme

This paper is part of a developing AGCIH body of work on digital public authority. Planned companion papers include:

- Administrative Hosting Capacity: Governing Digital Systems Within Public Authority
- Continuous Administration in the Digital State: Doctrine and Practice
- Governance Readiness Before Digital Adoption: An Assessment Framework
- Electronic Government Procurement and the Integrity of Public Administration in Africa
- Vendor Dependence and Sovereign Administrative Authority
- AI in Revenue Administration: Accountability Architecture for Tax Systems

AGCIH also intends to publish practical toolkits derived from the Procurement Governance Matrix, including model contractual clauses for digital and AI procurements, sector-specific readiness benchmarks for health, justice, revenue, and social protection, and a guidance note on Procurement Entry Doctrine for use by Permanent Secretaries and oversight bodies.

Enquiries: admin@agcih.africa +263778227492