WORKING PAPER WP-2026-01 | HARARE, 2026

Administrative Risk

A Governance Framework for AI Infrastructure in Africa

Africa Governance and Civic Innovation Hub
agcih.africa
Harare, Zimbabwe | 2026

This working paper introduces an original governance framework for the AI infrastructure moment in Africa. It names a distinct category of institutional exposure called administrative risk, and advances two original governance concepts: institutional absorption and pro-governability. It argues that Africa's digital future requires a parallel investment in governance architecture alongside infrastructure ambition, and sets out the institutional design requirements that governance readiness demands.

Keywords: AI governance, administrative risk, institutional absorption, pro-governability, public procurement, digital infrastructure, Africa, state capacity, accountability

Suggested citation: Africa Governance and Civic Innovation Hub (2026). Administrative Risk: A Governance Framework for AI Infrastructure in Africa. AGCIH Working Paper WP-2026-01. Harare: AGCIH.

Abstract

Africa is in the midst of an infrastructure moment. Cloud environments, AI-enabled telecom products, national sovereign clouds, and government-facing digital platforms are being developed, procured, and deployed at increasing speed across the continent. This is a significant development that this paper welcomes unreservedly. But the governance conversation has not kept pace with the infrastructure conversation, and the gap between them carries institutional consequences that are structural, cumulative, and potentially irreversible.

This working paper introduces a governance framework organised around three original propositions. First, the expansion of digital infrastructure in African public institutions generates a distinct category of exposure called administrative risk, which is irreducible to technical, cyber, or ethical risk and demands its own institutional response. Second, institutional absorption, defined as the capacity of a public body to integrate new digital systems without losing administrative coherence, accountability, or continuity of authority, is the central governance challenge of the present moment and the most under-examined dimension of Africa's digital ambition. Third, pro-governability, defined as the institutional posture that insists digital transformation must remain governable throughout its lifecycle, is the appropriate response to both.

The paper engages the strongest objections to this framework directly, including the charge that it sets conditions that risk slowing digital transformation and the charge that capacity constraints in African public institutions render the framework aspirational rather than operational. It argues that both objections misread the framework's requirements, and that the cost of ignoring administrative risk is substantially higher than the cost of addressing it. Sovereignty in infrastructure is necessary but insufficient. Africa's public institutions need sovereign governance capacity around infrastructure, not merely local hosting of it.

Introduction: Africa's Infrastructure Moment and the Governance Gap

Something has shifted in the texture of Africa's digital conversation. For much of the past two decades, that conversation was shaped primarily by the language of access, adoption, and inclusion: connectivity gaps to be bridged, markets to be reached, populations to be brought within the orbit of the digital economy. That framing is no longer sufficient. Across the continent, the digital question is increasingly framed not only in terms of use, but in terms of infrastructure, compute, sovereignty, and public institutional capability.

African firms are presenting cloud environments, AI-enabled telecom products, local-language models, national sovereign-cloud architectures, and public-facing digital infrastructure propositions at the highest levels of global and continental policy discussion. African governments are not merely being courted by global technology providers; they are increasingly confronting questions of where AI systems will be hosted, on what terms digital capacity will be built, and how public institutions will retain meaningful control as these systems become operationally embedded. This paper does not resist that shift. It treats it as both necessary and consequential.

The paper is being published into a sharper and more consequential moment than even a year ago. Zimbabwe formally launched its National Artificial Intelligence Strategy on 13 March 2026. In February 2026, the African Union Commission and Google announced a partnership framed around Africa's sovereign AI and digital capacity. In March 2026, Cassava Technologies announced both a National Sovereign Cloud proposition for African governments and a further scaling of NVIDIA-powered AI infrastructure. These developments matter. They show that the infrastructure question is no longer abstract. It is institutional, contractual, and immediate.

What this paper argues is that this acceleration has not yet been matched by a governance conversation of comparable seriousness, and that the cost of that mismatch is accumulating.

> The infrastructure debate in Africa is robust and growing. The governance debate remains thinner than the moment requires. There are policy statements, ethics frameworks, and broad aspirational commitments,[2] but relatively few systematic attempts to name what is at stake institutionally when AI-enabled systems enter African public administration, and fewer still that speak from the particular conditions of African governance contexts rather than simply transposing frameworks

> designed for jurisdictions with different institutional histories, legal traditions, and state-capacity profiles.

This paper closes that gap by doing something specific: it introduces a governance framework. A framework of this kind is not a policy recommendation, an ethics checklist, or a strategic plan. It is a statement of principle about what the governance problem is, why it matters, and what institutional posture is required. It establishes the conceptual ground on which more applied instruments, including procurement standards, oversight frameworks, and accountability architectures, can then stand.

The framework rests on three propositions. First, that AI infrastructure expansion in public institutions generates **administrative risk**, a distinct category of institutional exposure that existing governance and accountability frameworks are not designed to address. Second, that **institutional absorption**, the capacity of public bodies to integrate new digital systems without losing administrative coherence, is both the hardest thing to build and the most consequential thing to lose. Third, that the **pro-governability posture**, the institutional commitment that transformation must remain governable, is the appropriate and necessary response to the present moment.[3]

The paper proceeds in seven sections. Section I names the problem: administrative risk as a distinct category, and addresses the objection that it is merely change management by another name. Section II examines the mechanism by which infrastructure outruns governance. Section III develops the concept of institutional absorption and addresses the capacity objection. Section IV confronts the limits of sovereignty in infrastructure and the particular conditions of African governance. Section V argues for pro-governability as an institutional posture. Section VI sets out the five questions that governance readiness requires public institutions to answer. Section VII draws implications for institutional design. The paper concludes with a summary of the framework and its call to action.

SECTION I Administrative Risk: Naming a Distinct Category

The word risk is used promiscuously in discussions of AI and digital technology. It appears in cybersecurity assessments, financial audits, ethical AI guidelines, and procurement evaluations, often without a shared understanding of what kind of risk is being described or what institutional response it demands. This imprecision matters. Different risk categories require fundamentally different responses, and conflating them produces governance frameworks that are simultaneously over-engineered in some dimensions and entirely silent in others.

The risk that this paper addresses is not cyber risk.[4] Cyber risk concerns the confidentiality, integrity, and availability of digital systems and is addressed through technical controls, security protocols, and incident-response capacity. It is a well-established category with its own professional community, regulatory frameworks, and institutional responses. Critically important as it is, it is not what is at stake here.

The risk this paper addresses is not financial risk, though financial consequences may follow from it. It is not reputational risk, though reputational damage may be one of its symptoms. It is not ethical risk in the sense deployed by AI ethics frameworks, such as those advanced by UNESCO[5] or the European Union's High-Level Expert Group on AI,[6] which focus principally on algorithmic fairness, bias, and individual rights. These are legitimate concerns, but they do not exhaust the governance problem, and they do not speak directly to what happens inside public institutions as they absorb digital systems into their administrative architecture.

A. The Distinctive Character of Administrative Risk

Administrative risk, as this framework defines it, is the risk that a public institution loses its capacity to govern itself in the presence of a digital system. It has four characteristics that distinguish it from the other risk categories named above.

It is structural, not incidental. Administrative risk does not arise from system failure, security breach, or individual error. It arises from the normal, intended operation of a digital system that has been inadequately integrated into an institution's governance architecture. The risk is latent in the arrangement itself, not the product of exceptional events. An institution can be subject to significant administrative risk even when every system in its portfolio is functioning exactly as designed.

It is cumulative, not episodic. Administrative risk does not appear suddenly. It accumulates as operational decision-making drifts towards vendor-managed

environments, as records are dispersed across systems the institution does not fully control, as accountability chains lengthen, and as institutional knowledge of how a system actually works erodes. By the time administrative risk becomes visible, it has typically been building for years.

It is institutional in locus. Administrative risk does not primarily affect individuals, though individuals experience its consequences. It affects the institution as an institution: its capacity to exercise authority, maintain records, assign accountability, supervise outputs, and remain intelligible to itself and to the public after digital transition.

It is potentially irreversible if unaddressed. Unlike a system failure, which can be corrected, or a data breach, which can be contained, administrative risk that is allowed to accumulate tends to compound. Institutions that lose operational clarity over how a consequential system works, or that allow accountability chains to dissolve across successive procurement cycles, rarely recover that clarity simply by drafting a better policy. The governance architecture must be built in, not retrofitted after the fact.

> Administrative risk is not a failure state. It is a governance gap, and governance gaps do not wait to be noticed before they begin to cause harm.

B. The Change Management Objection

The strongest objection to the concept of administrative risk as a distinct category is that it simply describes the change management challenges that accompany any significant organisational transformation. Every major technology adoption requires adjustment, retraining, and procedural adaptation. Why, the objection runs, should AI and digital systems be treated differently?[7]

This objection is understandable, but it does not hold. Change management risk is episodic: it is associated with a defined transition period and resolves, at least in principle, once the transition is complete. Administrative risk, as defined here, is not resolved by successful implementation. It is structural in the sense that it persists throughout the operational life of the system, and deepens as the institution's dependence on that system normalises. The very success of digital transformation, when a system is working well, widely used, and deeply embedded in workflows, is precisely the condition under which administrative risk accumulates most rapidly, because it is also the condition under which governance scrutiny most typically relaxes.

Change management frameworks are also designed primarily around the experience of the individual employee adapting to new tools. Administrative risk, by contrast, is a governance concept: it concerns institutional structures, authority allocations, accountability chains, and the constitutional conditions of public administration. These

are not the concerns of change management. They require a different conceptual framework and a different institutional response.

C. Why Existing Frameworks Do Not Address It

The reason administrative risk is under-addressed is that existing governance frameworks were designed for a different relationship between institutions and technology. Most public administration accountability frameworks assume that authority is exercised by identifiable officers acting within defined procedures, that records are maintained in formats accessible to the institution, and that the outcomes of institutional action can be traced, defended, and reviewed.[8] Those assumptions held reasonably well in environments of document-based administration and relatively simple digital tools.

They do not hold well when an institution's consequential decisions are shaped by AI-enabled systems that process data at scale, generate outputs that officials may not fully understand, operate through vendor-managed logic that is not fully transparent, and produce records that may be difficult to reconstruct or review. In those conditions, the standard accountability question, namely who did this and why, may become genuinely difficult to answer. Not because anyone has acted wrongly, but because the institutional architecture no longer supports a clear answer.

This is the governance gap. It is not addressed by cybersecurity protocols, procurement due diligence checklists, AI ethics guidelines, or digital transformation strategies, however well designed. None of these instruments is designed to ask: does this institution retain the administrative capacity to govern what it is acquiring? That is the question administrative risk puts to the fore.

SECTION II How Infrastructure Outruns Governance: The Mechanism

The proposition that infrastructure can outrun governance is widely acknowledged in retrospect. We can readily identify cases in which technology was deployed before the institutional frameworks required to govern it were in place. What is less well understood is the mechanism by which this happens: the sequence of steps through which governance capacity falls behind infrastructure expansion, and the points at which the gap becomes consequential.

The mechanism has four stages, each of which presents a governance opportunity that is commonly missed.

A. Acquisition Without Authority Mapping

The first stage is acquisition. A ministry, regulator, or public agency acquires a new digital system. The acquisition may be appropriately procured, technically sound, and strategically sensible. But at the moment of acquisition, it is rare for the acquiring institution to have mapped what the new system requires in terms of governance architecture. Which office will be responsible for authorising its use? Which officer will supervise its outputs? What decision-rights framework governs the boundary between automated outputs and human judgement? Who will be accountable if consequential outputs are incorrect, contested, or harmful?

These questions are commonly deferred. The assumption is that they will be worked out during implementation. In practice, implementation tends to be dominated by technical integration, staff training, and operational standup, none of which is the same as governance design. By the time the system is operational, the absence of governance architecture is rarely visible, because the system is functioning. The gap only becomes visible when something goes wrong, or when an accountability question is asked that cannot be answered.

B. Normalisation of Operational Dependence

The second stage is normalisation. Once a system is operational, institutions adapt to it. Staff learn to rely on its outputs. Workflows are restructured around its capabilities. Decision-making processes that once depended on officer judgement begin to depend on system-generated recommendations. The system becomes load-bearing.

This is not a problem in itself. Digital systems are acquired precisely because they improve institutional performance. The problem arises when normalisation is not accompanied by parallel governance adaptation: when institutional workflows adapt to a system's logic without that system having been brought within the institution's governance framework. Operational dependence then deepens without accountability structures keeping pace.

> The system becomes load-bearing before governance becomes load-ready. That asymmetry is precisely where administrative risk accumulates.

C. Authority Displacement

The third stage is authority displacement. As operational dependence deepens, the practical locus of certain decisions begins to shift. Not formally, because the legal authority of the relevant officer remains intact, but operationally. When an officer routinely accepts a system-generated output without independent review, when a ministry's decisions on complex matters are structured by platform logic rather than professional judgement, when the vendor's implementation team effectively determines how a contested output is interpreted, operational authority has drifted from where it is formally located.[9]

Authority displacement is difficult to detect from inside an institution, because at each individual step the displacement is small and the rationale is reasonable. It only becomes visible when the institution is asked to account for a consequential decision and discovers that it cannot reconstruct how that decision was reached, or that the reasoning it can offer is largely the system's output rather than the institution's independent judgement. At that point, the institution is not merely facing a process problem. It is facing a legitimacy problem.

D. Continuity Fragility

The fourth stage is continuity fragility. An institution that has normalised dependence on a system, and in which authority has been partially displaced towards that system, is fragile in a specific way: its capacity to function depends on the continued availability of a system it may not fully control. If the vendor exits, if the contract ends, if the system degrades, the institution may discover that it lacks the procedural memory, the data access, and the operational knowledge to continue its core functions independently.

This is the logical end state of normalised dependence without governance architecture. It is the point at which administrative risk becomes existential: an institution that cannot function without a vendor is not, in the most fundamental sense, a sovereign institution. It is an institution that has retained the name of sovereignty while transferring its practical content to a private arrangement.

SECTION III Institutional Absorption and Its Conditions

The concept of institutional absorption is introduced here as the positive formulation of the governance challenge. Where administrative risk names the problem, institutional absorption names the capacity required to address it. The concept is original to AGCIH's governance work and is intended to fill a gap in the existing vocabulary of digital governance.[10]

Institutional absorption is the capacity of a public institution to integrate a new digital system, including AI-enabled systems, cloud environments, platform-based services, and AI-assisted decision-support tools, without losing administrative coherence, accountability, or continuity of authority. An institution with high absorption capacity can take on complex new systems while remaining, in all governance-relevant senses, itself: able to exercise its functions, assign accountability, maintain records, supervise outputs, and remain intelligible to oversight bodies and the public it serves.

An institution with low absorption capacity may acquire technically advanced systems, host complex digital infrastructure, and present an impressive surface of digital transformation, while quietly losing the administrative coherence required to govern what it has acquired. The systems work. The institution is weaker.

> Institutional absorption is not a technical capacity. It is a governance capacity, and it is the most under-invested dimension of Africa's digital ambition.

A. The Conditions of Absorption

Institutional absorption is not a natural state or a fixed property of well-resourced institutions. It is produced by deliberate governance design. Several conditions are required.

The first is decision-rights clarity: a documented allocation of authority for each stage of the system's lifecycle, from procurement and commissioning through operation, review, and eventual decommissioning. Decision-rights clarity means that at every moment, an identifiable officer bears responsibility for each governance function, and that the boundaries between automated outputs and human judgement are specified rather than assumed.

The second is accountability architecture: institutional structures that ensure consequential outputs can be traced, reviewed, and contested. Accountability

architecture encompasses the record-keeping standards, audit pathways, review procedures, and officer-responsibility assignments that allow an institution to answer, credibly and completely, what happened and who was responsible. It is not simply a complaints mechanism. It is the institutional infrastructure of public answerability.

The third is hosting governance: a clear institutional understanding of where data is stored, who operates the hosting environment, what access rights the institution retains, how jurisdictional questions are addressed, and what the institution can and cannot do without vendor cooperation. Hosting governance is the infrastructural precondition for meaningful oversight.

The fourth is operational knowledge retention: the maintenance of sufficient in-house understanding of how a system works so that the institution is not entirely dependent on vendor explanation for its own operational decisions. This does not require institutions to employ AI engineers or data scientists in every department. It requires officers who understand the system well enough to ask meaningful questions, identify anomalies, and exercise informed oversight. The governance literature on algorithmic accountability has identified this as one of the most critical and most frequently neglected conditions of effective digital governance.[11]

The fifth is continuity planning: a documented and tested plan for how the institution would continue to function if the system became unavailable, and how it would lawfully transition away from a vendor at contract end or in the event of vendor failure. Continuity planning is the ultimate test of whether governance readiness is genuine or nominal.

B. The Capacity Objection

The most serious objection to the framework advanced in this section is the capacity objection: that the governance conditions described here exceed the current institutional capacity of most African public bodies, and that a framework built on standards that cannot yet be met in practice is aspirational rather than operational.

This objection deserves a serious answer, not dismissal.

The capacity constraints facing African public institutions are real. Across many jurisdictions, technically trained public-sector officers are scarce, procurement frameworks may not yet be adapted to complex digital acquisitions, accountability institutions are still being built, and legal frameworks for data and AI governance are at varying stages of development. These are not arguments for lower standards. They are arguments for building capacity, and for building it now, before digital systems become embedded at a scale that makes governance retrofitting prohibitively difficult.

The framework's five conditions are institutional design requirements, not individual competency benchmarks. The response to incapacity is investment in capacity, not

reduction of the governance standard. Moreover, the capacity burden can be distributed. Shared standards, regional governance frameworks, independent oversight institutions, and properly structured procurement guidance can all contribute to making the conditions of institutional absorption achievable in capacity-constrained environments. The framework does not assume that every ministry will build all five capacities independently from scratch. It assumes that all five conditions must be met for a system to sit on secure governance foundations, and that meeting them requires deliberate institutional investment.

The alternative, which is to adopt complex digital systems without building the governance conditions for institutional absorption, does not conserve capacity. It consumes it. Institutions that lack the governance architecture to manage the systems they have acquired spend institutional energy on crisis management, accountability failures, and vendor disputes that would not arise if the governance design work had been done at the outset.

SECTION IV Sovereignty in Infrastructure Is Not Sovereignty in Control

One of the most important clarifications this framework must make concerns the relationship between infrastructure sovereignty and institutional control. These are not the same thing, and conflating them is one of the most significant errors in current African AI governance discourse. The error is understandable, because the sovereign infrastructure narrative is doing important work: it is challenging historical patterns of technological dependency and asserting Africa's right to build and host the digital systems on which its future depends. That assertion is right. The error is in treating it as sufficient.

Infrastructure sovereignty refers to the location, ownership, and operational control of digital infrastructure: data centres, hosting environments, cloud platforms, communications networks, and computing resources. A sovereign cloud is a cloud environment that is locally hosted, operated under domestic jurisdiction, and not subject to the same extraterritorial exposure that characterises many international cloud arrangements.[12] These are legitimate and important gains. Local hosting can reduce legal vulnerability, support data residency requirements, and contribute to strategic autonomy in digital infrastructure. Recent African developments, including sovereign cloud propositions directed at government use and continental partnerships framed around sovereign AI capacity, make this distinction more urgent rather than less.

But infrastructure sovereignty does not produce institutional control. An institution that hosts its data in a nationally owned or domestically governed cloud has done something meaningful. It has not, by that act alone, built the governance capacity required to govern what happens to that data, to supervise the systems that process it, to preserve records and reasons in usable form, or to maintain accountability for the decisions those systems inform.

> A state can achieve infrastructure sovereignty and still be administratively dependent. The cloud can be local while the governance remains hollow. The contract can be national while operational leverage remains external. The infrastructure can be celebrated as sovereign while the institution still lacks audit access, exit capacity, effective supervision rights, or continuity arrangements that would allow it to function independently if the vendor relationship changed.

A. The Limits of Sovereign Hosting

The governance questions that sovereign hosting does not answer are precisely those addressed by the administrative risk framework. Who authorises the system's use within the hosting environment? Which officer supervises consequential outputs? What audit, inspection, and records access rights does the institution retain? How are accountability chains maintained when multiple systems, platforms, and service layers interact within the hosted environment? What happens to records, models, interfaces, and operational knowledge when a cloud contract is renegotiated, a service layer changes, or a vendor relationship ends?

These questions do not resolve themselves because infrastructure is locally hosted or African-built. They require the governance design work described in Section III. Without that work, a nationally hosted cloud can become a locally managed version of the same administrative risk that an internationally hosted arrangement would have created. Sovereignty in infrastructure is the beginning of the answer, not the whole of it. This framework is not opposed to the sovereign infrastructure proposition; it insists that the proposition be completed through procurement control, decision-rights clarity, accountability architecture, and tested continuity planning.

B. The African Governance Context: Why Origin Matters

A second objection sometimes advanced is that the governance challenges identified in this framework are not specific to Africa, and that framing them in African terms risks both over-generalising the African experience and under-connecting to a body of global governance thinking that has already grappled with these issues. The objection has some force, and this framework acknowledges it.

The challenge of governing AI-enabled systems in public administration is not unique to Africa. Every jurisdiction confronts questions of authority, accountability, and continuity as digital systems become embedded in public administration. The OECD AI Principles, UNESCO's Recommendation on the Ethics of Artificial Intelligence, and the growing literature on algorithmic accountability all address dimensions of this challenge from a global perspective.

What is specific to Africa is not the governance challenge in the abstract, but the institutional conditions in which it arises. The continent's governance institutions have particular histories, particular capacity profiles, and particular relationships to technology providers that shape the governance problem in ways that generic frameworks designed for OECD jurisdictions do not fully capture.[13] Africa's experience of technology adoption has been characterised by contractual arrangements that frequently embedded lock-in, by capacity-building commitments that did not survive vendor transitions, and by a pattern in which the terms of technological participation were set by providers rather than negotiated by recipients. These are governance conditions that a framework built for Africa must take seriously.

The response is therefore not to abandon global governance thinking, but to supplement it with frameworks built from African institutional realities outward. The administrative risk framework is designed for that purpose. It is Africa-grounded, not Africa-isolated, and it does not preclude productive engagement with international governance standards. It insists, however, that Africa's governance institutions should be the authors of the frameworks they operate within, not merely their recipients.

C. The National AI Strategy Moment

The governance stakes described in this paper are not hypothetical. Several African states, including Zimbabwe, have in 2025 to 2026 launched national AI strategies that explicitly provide for the use of AI systems in public administration and service delivery.[14] At the same time, continental and commercial actors are moving quickly to build cloud, compute, and sovereign-capacity propositions around those ambitions. This means the implementation question is no longer whether African institutions will encounter AI infrastructure. It is whether they will encounter it with sufficient governance architecture already in place.

The moment of strategy launch is therefore precisely the moment at which administrative risk and institutional absorption should be on the governance agenda. Before systems are procured, before contracts are signed, before AI-enabled platforms become operationally embedded in ministries and agencies, the five conditions of institutional absorption can still be designed in. After that point, the cost of design rises significantly, and the governance architecture must be retrofitted around systems that are already load-bearing. The strategy moment is not only a policy moment. It is a procurement, hosting, oversight, and institutional-design moment.

SECTION V Pro-Governability as an Institutional Posture

This framework requires a name for the correct institutional response to the challenge it describes. That name is **pro-governability**.[15]

Pro-governability is an institutional posture, not a policy position. It is the commitment, embedded in how institutions make decisions and design governance systems, that digital transformation must remain governable throughout its lifecycle. It holds that no digital system should be acquired, deployed, or scaled in a manner that undermines the institution's capacity to exercise authority over it, maintain accountability for its consequences, or transition away from it in an orderly manner.

The name is chosen deliberately. Pro-governability is neither anti-technology nor anti-innovation. It does not oppose digital transformation as such. It insists on a specific quality of transformation: that it remain subject to institutional governance rather than escape from it. Innovation that cannot be governed is not, from an institutional perspective, a gain. It is a transfer of authority from public institutions to technical systems or their vendors, presented in the language of progress.

> In that sense, pro-governability is not caution for its own sake. It is a defence of public authority under conditions of technological change.

A. The Speed Objection

The most practically pressing objection to the pro-governability posture is the speed objection: that requiring governance architecture alongside digital adoption will slow transformation at a moment when Africa needs to move quickly, and that the cost of delay is greater than the cost of imperfect governance.

This objection deserves a direct answer because it reflects a genuine strategic tension. Africa has historically adopted technology later than other regions, and the costs of that lag, in economic participation, in public service quality, and in institutional modernisation, are real. The argument that governance requirements should not become obstacles to necessary transformation has a legitimate basis.

The pro-governability framework does not, however, accept the terms of this objection. The objection assumes that governance architecture and digital adoption are in tension, specifically that building governance capacity takes time that could otherwise be spent on transformation. This is a false trade-off. Governance readiness does not require

transformation to stop while governance is built. It requires governance to be built alongside transformation, as a parallel investment. The pace of digital adoption does not determine whether governance architecture is built; it determines when it must be ready.

Moreover, the speed objection systematically underestimates the costs of ungoverned transformation. An institution that has acquired digital systems without governance architecture is not a fast institution that will add governance later. It is an institution carrying administrative risk that compounds with every additional system it adopts, every contract it signs, and every operational function it migrates to a vendor-managed environment. The remediation costs, which involve reconstructing accountability structures around systems that are already operational and load-bearing, are substantially higher than the cost of building governance architecture at the point of acquisition.

Speed and governance readiness are therefore not competing priorities. Ungoverned speed is not accelerated transformation. It is accelerated accumulation of administrative risk.

B. Pro-Governability and State Capacity

At its foundation, the pro-governability posture is a state-capacity argument. It holds that the quality of public administration is determined not only by the sophistication of the tools available to it, but by the degree to which those tools remain within the governance reach of the institutions that deploy them. A state with sophisticated digital infrastructure but weak governance capacity over that infrastructure is not a strong digital state. It is a state that has outsourced consequential functions while retaining nominal authority over them.

For Africa, this argument carries a particular resonance. The continent's governance institutions have, in many jurisdictions, spent decades building the administrative and legal frameworks required for effective public accountability. Those frameworks are unfinished projects in many states, but they are projects in earnest, and they represent real institutional investments. The risk of unmanaged digital transformation is that it erodes those frameworks faster than they can adapt: not through malice or misgovernance, but through the normal operation of systems whose governance implications were not addressed at the point of acquisition.

The pro-governability posture is therefore not a conservative or technology-sceptical stance. It is the stance of institutions that take both digital transformation and public accountability seriously, and that refuse to treat them as competing priorities. Properly understood, they are complementary requirements of a modern African state that is serious about both its digital future and its institutional integrity.

SECTION VI The Five Questions of Governance Readiness

This framework does not only name a problem. It specifies a test. The test of governance readiness is whether a public institution can answer five questions about any AI-enabled or digital system it is acquiring, operating, or evaluating for renewal. These questions are not a compliance checklist. They are governance questions in the full sense: questions whose answers require institutional design, legal clarity, and deliberate accountability architecture. They cannot be answered by reference to a vendor's documentation or a project manager's implementation plan. They require the institution itself to have built the governance capacity they assess.

Question 1: Who authorises the system's use?

This question asks for a specific, named, and legally grounded answer: which officer or body holds the authority to approve the system's deployment, define the scope of its use, approve changes to that scope, and withdraw authorisation if necessary. Authorisation is not a one-time act at procurement. It is an ongoing governance function that must be assigned, documented, and exercised throughout the system's operational life.

An institution that cannot answer this question has not yet built the decision-rights framework required for institutional absorption. It has acquired a capability without establishing who is accountable for its governance. In the context of AI-enabled systems that may evolve in their function over time, the absence of a clear authorisation architecture is a structural governance failure, not an administrative oversight.

Question 2: Who supervises the system's outputs?

This question asks which officer or body is responsible for the ongoing review of the system's consequential outputs: the decisions, recommendations, classifications, flags, or actions that the system produces and that the institution acts upon. Supervision is not technical monitoring. It is the governance function of ensuring that outputs are reviewed for accuracy, appropriateness, and consistency with legal and institutional standards, and that anomalies are identified, investigated, and addressed.

Supervision requires officers with sufficient understanding of the system's function to ask meaningful questions about its outputs, and with sufficient authority to require review or correction when outputs are problematic.[16] An institution that lacks this capacity has, in practice, delegated its decision-making function to a system it cannot

effectively govern. The public interest consequences of this delegation are not mitigated by the system's technical performance.

Question 3: Who is accountable for consequential outcomes?

This question asks which officer is answerable, to the institution, to oversight bodies, and to the public, for outcomes that result from the system's operation. Accountability in this sense is not collective or diffuse. It is specific and personal: there must be an identifiable officer who can be called upon to explain, defend, and if necessary accept responsibility for consequential outcomes.

The value of this question is that it resists the diffusion of accountability that complex digital systems can produce. In a multi-layered arrangement involving a ministry, a vendor, a hosting provider, and a platform operator, accountability can easily dissolve: each actor points to the others, and the public is left without a clear answer. The governance architecture must prevent that dissolution by assigning clear and non-negotiable accountability before the system becomes operational. Accountability assigned after a problem arises is almost always contested. Accountability assigned before the system is deployed is structurally embedded.[17]

Question 4: How are records and reasons preserved?

This question asks how the institution maintains the documentary record required for accountability, review, audit, and legal contestation. It asks not only whether records are kept, but whether they are kept in a form and location that allows the institution to access, use, and defend them independently of vendor cooperation. The records question is particularly significant in AI-enabled systems, because the reasoning that underlies an output may not be straightforwardly documentable.[18]

Where algorithmic processes contribute to a consequential outcome, the institution must be able to reconstruct, at a sufficient level of intelligibility, how that outcome was produced. The statement that the system recommended it is not an institutional record. It is a statement of administrative risk. An institution that can offer no more than this account of a consequential decision has not merely failed a record-keeping standard; it has failed the basic test of public accountability.

Question 5: How is continuity maintained if the system fails, changes, or exits?

This question asks whether the institution has a documented and tested plan for maintaining its core functions in the event that the system becomes unavailable, the vendor exits, the contract ends, or the system is decommissioned. Continuity planning is the ultimate test of institutional absorption: an institution that cannot function without a particular vendor has, in the most practical sense, transferred a portion of its sovereign administrative function to a private arrangement.

Continuity planning must be genuine. It must identify which functions the institution would need to sustain independently, what procedural and data resources would be required, how staff would be reoriented, and how long the transition would take. A continuity plan that amounts to saying that a replacement vendor would be found is not a plan. It is a statement of continued dependence.

> Where these five questions cannot be answered, infrastructure may still function technically. But it does not yet sit on secure governance foundations. That is the operational definition of administrative risk.

SECTION VII Implications for Institutional Design

The governance framework set out in this paper has implications that extend beyond individual procurement decisions or compliance frameworks. It speaks to the design of institutions themselves: to what capacities, structures, and cultures African public institutions need to build in order to navigate the present digital infrastructure moment with their governance functions intact.

A. Governance Design as a First-Order Investment

The most important institutional design implication of this framework is that governance design must be treated as a first-order investment, not a support function or a subsequent consideration. Ministries, regulators, and public agencies engaged in significant digital transformation must have access to governance design capacity: the expertise required to draft decision-rights frameworks, design accountability architectures, assess hosting arrangements, structure procurement terms that preserve institutional control, and produce and test continuity plans.

That capacity does not currently exist at scale in most African public institutions. Building it requires a different kind of investment than digital infrastructure investment: investment in legal and institutional expertise, in governance design methodology, and in the administrative cultures that treat governance readiness as a professional standard rather than a regulatory compliance exercise. Both forms of investment are necessary. Treating only one as a priority is a strategic error.

B. Procurement as a Governance Gateway

This framework has a specific implication for procurement: it must be treated as the primary governance gateway for AI and digital systems, not merely as an administrative process for acquiring goods and services.[19] AI rarely enters the state through abstract policy debate alone. It enters through contracts, enterprise systems, digital platform arrangements, cloud migration agreements, software integrations, managed services, and increasingly through infrastructure and compute partnerships presented as sovereign-capacity solutions. Procurement is typically the doorway through which technical capability becomes institutional fact. If that doorway is weakly governed, the consequences can be long-lasting, and by the time they are visible, the contractual and operational architecture that created them is already load-bearing.

Procurement governance for AI-enabled systems must therefore be designed to require answers to the five governance questions before acquisition is approved; to embed

accountability, audit, interoperability, records-access, and oversight obligations into contracts; to specify hosting and data-control terms that preserve institutional authority; to secure meaningful exit, transition, and continuity provisions; and to require continuity planning as a condition of procurement approval. These are achievable standards. They do not require new primary legislation in most cases. They require adaptation of existing procurement frameworks, development of technical guidance, and training of procurement officers in the governance dimensions of digital acquisition.

C. The Role of Independent Governance Institutions

The framework also has implications for independent governance institutions, including oversight bodies, regulatory commissions, accountability institutions, and governance-focused civil society organisations operating in the digital space. These actors perform a critical function in the pro-governability architecture: establishing standards, conducting assessments, providing technical assistance, and holding public institutions accountable for the quality of their governance design around digital systems.

In the African context, this function is particularly significant because the capacity constraints facing individual ministries and agencies are genuine. Not every public institution will build deep in-house governance design capacity from scratch. Independent institutions that can provide shared standards, assessment frameworks, and technical support play a vital role in ensuring that the pro-governability posture is operationally achievable rather than merely aspirationally desirable. The existence of such institutions is itself a measure of governance maturity.

D. Governance Readiness Before Scale

Perhaps the most practically significant implication concerns sequencing. Africa's digital infrastructure ambitions are, in many jurisdictions, ambitious in scale. The combination of sovereign cloud developments, AI-enabled government services, national digital platforms, telecom-integrated public systems, and new sovereign-compute propositions represents a significant expansion of the digital footprint of public administration.[20] The framework's implication is clear: governance readiness must be built before scale, not after it.

Scale that precedes governance readiness is not accelerated transformation. It is accelerated accumulation of administrative risk. An institution that has expanded its digital systems quickly without building the governance architecture required to absorb them has compounded its exposure at every point of expansion. The cost of remediation, which involves reconstructing governance architecture around systems that are already operational and load-bearing, is substantially higher than the cost of building it correctly at the outset.

This is the framework's practical counsel: invest in governance readiness now, at the moment of infrastructure ambition, not when the consequences of its absence become visible. The African states best positioned for the digital future will be those that made this investment deliberately, at the right moment, with the appropriate understanding of what institutional absorption requires.

Conclusion: The Framework and Its Call

The governance framework introduced in this paper can be stated plainly.

Africa is in an infrastructure moment. That moment is important and should be pursued with ambition and confidence. But infrastructure without governance architecture generates administrative risk: the structural, cumulative erosion of an institution's capacity to exercise authority, maintain accountability, and preserve continuity in the presence of digital systems it cannot fully govern. Recent developments across the continent only sharpen this point. The sovereign cloud, sovereign compute, and digital-capacity agenda is accelerating. Governance readiness must accelerate alongside it.

The central governance challenge is institutional absorption: the capacity of public bodies to integrate new digital systems without losing administrative coherence. Absorption is not a technical capacity. It is a governance capacity. It requires decision-rights clarity, accountability architecture, hosting governance, operational knowledge retention, and continuity planning. These are not secondary concerns. They are the conditions under which public institutions survive technological transition with their governance functions intact.

Sovereignty in infrastructure is necessary but insufficient. A nationally hosted cloud environment that is not matched by genuine institutional control over what runs within it is sovereignty in form without sovereignty in substance. The same is true of continental capacity partnerships or government-facing sovereign cloud offers if they are not matched by clear decision-rights, audit access, records control, accountability assignments, and continuity provisions. The goal is not an Africa that hosts more systems locally. It is an Africa whose public institutions exercise real authority over the systems they host, deploy, and depend upon.

The pro-governability posture is the appropriate institutional response. It does not oppose digital transformation. It insists that transformation remain governable. Innovation that escapes institutional governance is not a gain for the state or for the public it serves. It is a transfer of authority concealed beneath the language of modernisation.

The four objections engaged in this paper, namely that administrative risk is merely change management, that the governance standard exceeds current African capacity, that the framework risks slowing transformation, and that governance challenges are not Africa-specific, all fail for the same reason. They misread what the framework is asking. It does not ask for governance perfection before adoption. It asks for governance

architecture alongside adoption, as a parallel investment. It does not set a standard that cannot be met; it sets a standard that must be built towards, because the alternative is more costly than the investment. And it is Africa-grounded not because governance challenges are unique to Africa, but because the institutional conditions in which they arise are, and frameworks built for those conditions must be designed from them outward.

> The real test of Africa's digital maturity will not be whether institutions can announce new systems. It will be whether they remain able to direct, supervise, explain, and lawfully own the consequences of what they adopt.

The framework's call is therefore this: invest in governance readiness as a first-order institutional commitment. Build the decision-rights frameworks, accountability architectures, procurement standards, hosting-governance terms, records safeguards, audit rights, and continuity plans required for institutional absorption before scale, not after it. Insist that every significant digital acquisition be subject to the five governance questions, and treat unanswered questions as conditions requiring governance design, not obstacles to be managed.

Africa does not need infrastructure alone. It needs governable infrastructure. And the institutions that build governability into the foundations of their digital transformation, rather than attempting to retrofit it after the fact, will be the institutions that can credibly claim to have led their countries, and the continent, into a digital future that is as strong institutionally as it is technologically.

That is what it means to govern well in this moment. That is what this framework requires.

Notes

[1] The shift in how Africa's digital position is narrated is reflected in a range of recent developments, including presentations at Mobile World Congress 2025 by African technology firms, the formal launch of Zimbabwe's National Artificial Intelligence Strategy on 13 March 2026, the African Union Commission's February 2026 partnership announcement with Google on sovereign AI and digital capacity, and Cassava Technologies' March 2026 announcements on a National Sovereign Cloud for African governments and further NVIDIA-powered AI infrastructure expansion. These developments illustrate a clear move from a language of access and adoption towards a language of infrastructure, capacity, and institutional control.

[2] The governance gap between infrastructure ambition and institutional readiness is a recurring observation in the literature on digital governance in developing economies. Research ICT Africa has documented this gap in several contexts. See Research ICT Africa (2023) for relevant empirical analysis of governance readiness across African jurisdictions.

[3] All three concepts, namely administrative risk, institutional absorption, and pro-governability, are original to AGCIH's governance work. They fill a conceptual gap in existing AI governance literature that addresses technical, ethical, and financial risk but has not adequately named the structural governance risk arising from inadequate institutional design around digital systems.

[4] Cybersecurity risk in the African context is addressed by a growing body of national and regional frameworks, including the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention, 2014) and domestic frameworks such as Zimbabwe's Cyber and Data Protection Act (2021). These frameworks address a distinct risk category from the one this paper names.

[5] UNESCO (2021). Recommendation on the Ethics of Artificial Intelligence. Paris: UNESCO. The Recommendation addresses algorithmic fairness, transparency, accountability, and human rights dimensions of AI but does not specifically address the structural governance risk to public institutions arising from inadequate absorption capacity.

[6] High-Level Expert Group on Artificial Intelligence (2019). Ethics Guidelines for Trustworthy AI. Brussels: European Commission. The HLEG framework is among the most developed of its kind but is designed for a different institutional context and does not translate directly to the governance conditions of African public administration.

[7] The change management objection reflects a tradition in public management literature that treats technology adoption as primarily an organisational adaptation challenge. See Osborne (2010) on new public governance, which addresses institutional adaptation but does not specifically address the structural accountability implications of AI-enabled systems in public administration.

[8] On accountability frameworks in public administration, see Bovens, Schillemans and Goodin (eds) (2014), The Oxford Handbook of Public Accountability. Oxford: Oxford University Press. The handbook provides a comprehensive treatment of accountability in public institutions but predates the AI infrastructure moment and does not address the specific governance implications of AI-enabled decision-making at scale.

[9] The concept of authority displacement in AI-enabled environments is addressed in Pasquale (2015), The Black Box Society. Cambridge MA: Harvard University Press. Pasquale's analysis focuses on the private sector but the displacement dynamic he describes is equally applicable to public administration contexts.

[10] The concept of institutional absorption is original to AGCIH's governance work. Related concepts appear in the organisational learning literature, particularly Zahra and George (2002) on absorptive capacity, and in the public management literature on institutional resilience, but neither directly addresses the governance dimensions of AI system integration in public administration that this framework specifies.

[11] On operational knowledge retention as a condition of effective digital governance, see Diakopoulos (2016), 'Accountability in Algorithmic Decision Making', Communications of the ACM, 59(2), 56-62.

Diakopoulos identifies the inability of institutions to interrogate algorithmic outputs as one of the most significant practical barriers to accountability in automated decision-making.

[12] On digital sovereignty and its conceptual dimensions, see Pohle and Thiel (2020), 'Digital sovereignty', Internet Policy Review, 9(4). Pohle and Thiel distinguish between different dimensions of digital sovereignty, including infrastructure sovereignty, data sovereignty, and regulatory sovereignty. This paper's argument that infrastructure sovereignty is insufficient without institutional control maps onto and extends their analysis.

[13] Research ICT Africa's work on AI governance readiness across African jurisdictions provides empirical grounding for the observation that generic governance frameworks designed for OECD contexts do not adequately account for the institutional conditions of African public administration. See Research ICT Africa (2022, 2023).

[14] Zimbabwe's National Artificial Intelligence Strategy was formally launched on 13 March 2026, making Zimbabwe one of a growing number of African states with a formal national AI strategy providing for AI deployment in public services. The administrative risk framework is directly relevant to the strategy's implementation because the strategy moment is also a procurement, hosting, and institutional-design moment, not only a policy moment.

[15] The concept of pro-governability is original to AGCIH's governance work. It is introduced here as an institutional posture rather than a policy preference, reflecting AGCIH's position that effective AI governance in Africa requires an orientation embedded in how institutions are designed, not only in the policies they adopt.

[16] On the governance conditions required for effective oversight of AI outputs, see Yeung (2018), 'Algorithmic regulation: A critical interrogation', Regulation and Governance, 12(4), 505-523.

[17] On accountability assignment and the diffusion problem in AI decision chains, see Cobbe, Kumar and Singh (2021), 'Reviewable Automated Decision-Making: A Framework for Accountable Algorithmic Systems', Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency (FAccT). New York: ACM.

[18] On records and traceability in algorithmic decision-making, see Brownsword, Scotford and Yeung (eds) (2017), The Oxford Handbook of Law, Regulation and Technology. Oxford: Oxford University Press.

[19] The proposition that procurement is the primary governance gateway for AI in the public sector is developed at length in AGCIH (2026b), the procurement-focused companion piece to this working paper. The present paper introduces the proposition as one implication of the administrative risk framework; current developments in sovereign cloud, compute, and managed digital-capacity partnerships only reinforce procurement's significance as the point at which institutional dependence, audit rights, exit options, and continuity obligations must be structured before deployment.

[20] The scale of Africa's digital infrastructure ambitions is reflected not only in the African Union's AI Continental Strategy (2024), which anticipates significant expansion of AI-enabled public services across the continent, but also in the more recent acceleration of sovereign cloud, sovereign compute, and public-facing digital infrastructure offers announced in 2026. The governance readiness implications of that scale of adoption are the direct concern of the framework advanced in this paper.

Bibliography

A. Primary and Institutional Sources

Africa Governance and Civic Innovation Hub (2026a). Administrative Risk: A Governance Framework for AI Infrastructure in Africa. AGCIH Working Paper WP-2026-01. Harare: AGCIH.

Africa Governance and Civic Innovation Hub (2026b). Procurement Is Where AI Enters the State. AGCIH Insight Brief. Harare: AGCIH.

African Union Commission (2024). A United Africa in the Age of Artificial Intelligence: The African Union Artificial Intelligence Continental Strategy for Africa 2024 to 2034. Addis Ababa: African Union Commission.

African Union (2014). African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention). Addis Ababa: African Union.

High-Level Expert Group on Artificial Intelligence (2019). Ethics Guidelines for Trustworthy AI. Brussels: European Commission.

OECD (2019). Recommendation of the Council on Artificial Intelligence. OECD/LEGAL/0449. Paris: Organisation for Economic Cooperation and Development.

Research ICT Africa (2022). AI Governance in Africa: Mapping the Landscape. Cape Town: Research ICT Africa.

Research ICT Africa (2023). Governing AI in the Public Sector: Readiness and Risk in African Jurisdictions. Cape Town: Research ICT Africa.

UNESCO (2021). Recommendation on the Ethics of Artificial Intelligence. Paris: United Nations Educational, Scientific and Cultural Organisation.

Zimbabwe (2021). Cyber and Data Protection Act [Chapter 12:07]. Harare: Government of Zimbabwe.

Zimbabwe (2026). National Artificial Intelligence Strategy. Harare: Ministry of Information Communication Technology, Postal and Courier Services.

African Union Commission (2026). African Union Commission and Google Sign Landmark Partnership to Advance Africa's Sovereign AI and Digital Capacity. Press release, 17 February 2026. Addis Ababa: African Union Commission.

Cassava Technologies (2026a). Cassava Technologies Announces National Sovereign Cloud to Support Secure Digital Infrastructure for African Governments. March 2026.

Cassava Technologies (2026b). Cassava Scales African AI Infrastructure with NVIDIA-Powered AI Factories to Accelerate Sovereign Data Capabilities. March 2026.

UNESCO (2026). Zimbabwe Launches National Artificial Intelligence Strategy. News article, 25 March 2026. Paris: UNESCO.

B. Books and Book Chapters

Bovens, Mark, Schillemans, Thomas, and Goodin, Robert E. (eds) (2014). The Oxford Handbook of Public Accountability. Oxford: Oxford University Press.

Brownsword, Roger, Scotford, Eloise, and Yeung, Karen (eds) (2017). The Oxford Handbook of Law, Regulation and Technology. Oxford: Oxford University Press.

Osborne, Stephen P. (ed.) (2010). The New Public Governance: Emerging Perspectives on the Theory and Practice of Public Governance. London: Routledge.

Pasquale, Frank (2015). The Black Box Society: The Secret Algorithms That Control Money and Information. Cambridge MA: Harvard University Press.

C. Journal Articles and Conference Papers

Cobbe, Jennifer, Kumar, Mehtab, and Singh, Jatinder (2021). 'Reviewable Automated Decision-Making: A Framework for Accountable Algorithmic Systems'. Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency (FAccT). New York: ACM.

Diakopoulos, Nicholas (2016). 'Accountability in Algorithmic Decision Making'. Communications of the ACM, 59(2), 56-62.

Pohle, Julia and Thiel, Thorsten (2020). 'Digital sovereignty'. Internet Policy Review, 9(4). https://doi.org/10.14763/2020.4.1532.

Yeung, Karen (2018). 'Algorithmic regulation: A critical interrogation'. Regulation and Governance, 12(4), 505-523.

Zahra, Shaker A. and George, Gerard (2002). 'Absorptive capacity: A review, reconceptualisation, and extension'. Academy of Management Review, 27(2), 185-203.

About AGCIH

The Africa Governance and Civic Innovation Hub (AGCIH) is an independent governance institution that works at the intersection of public law, institutional design, and emerging technology governance. AGCIH supports governments, regulators, and oversight bodies in building the governance architecture required to manage high-impact digital and AI-enabled systems in public administration.

AGCIH's work is grounded in the particular institutional realities of African governance contexts. It proceeds from the conviction that effective AI governance in Africa must be designed for Africa, built from African governance conditions, legal traditions, and institutional histories, not imported wholesale from frameworks designed for different jurisdictions.

AGCIH does not position itself against digital transformation or against the institutions and firms driving it. It positions itself as the governance institution that ensures transformation remains governable: that public authority remains intact, accountability is preserved, and the digital future of African states is built on secure institutional foundations.

agcih.africa

AGCIH Working Paper WP-2026-01 | Harare, Zimbabwe