



MODERNISING GOVERNMENT ACCOUNTING AND PROTECTING PUBLIC FINANCIAL DATA IN SIERRA LEONE: A STRATEGIC FRAMEWORK FOR DIGITAL GOVERNANCE AND FINANCIAL ACCOUNTABILITY

Joseph Momoh Conteh¹ⁱ,
Musa Abdullah Kargbo²,
Abdul Rahman N'Jai³,
Mohamed Sahid Sesay⁴

¹Peking University,
Beijing, China

²Fourah Bay College,
University of Sierra Leone,
Sierra Leone

³Institute of Public Administration and Management (IPAM),
University of Sierra Leone,
Sierra Leone

⁴Rokel Commercial Bank Sierra Leone Limited,
Sierra Leone

Abstract:

Sierra Leone presents a paradox that should trouble anyone who studies public financial management reforms in low-income countries. Two decades of sustained investment, five independent Public Expenditure and Financial Accountability (PEFA) assessments and three successive reform strategies have produced genuine achievements: a Treasury Single Account (TSA), an upgraded Integrated Financial Management Information System (IFMIS) covering thirty ministries, departments and agencies, adoption of Cash Basis International Public Sector Accounting Standards (IPSAS), an operational electronic procurement platform and an 'A' rating for budget classification in the 2021 to 2022 PEFA assessment. Yet, in December 2025 the Financial Secretary warned publicly that fragmented data systems were bleeding value from payroll and pension administration, observing that *"somebody will still continue to benefit from one system while the other system is losing"*. This article takes that warning as its organising diagnosis. It argues that Sierra Leone has reached the limits of system-by-system modernisation and that the next generation of reform must treat three agendas as a single problem: interoperability across government financial systems, cyber-security and data protection for the financial information those systems generate, and institutional accountability for how that information is used. The article traces the reform trajectory from the Integrated Public

ⁱ Correspondence: email josephmconteh2004@yahoo.com

Financial Management Reform Project (2008 to 2013) through the current interoperability roadmap, evaluates the emerging Data Protection and Right to Access Information Act and its unified dual-mandate authority, and analyses the persistent gap between transactional automation and data governance. It then proposes an integrated digital governance framework built on four pillars, digital infrastructure and systems integration, legal and regulatory enablement, institutional capacity and human capital, and oversight with citizen engagement, resting on a cross-cutting foundation of security and data protection by design, with a sequenced sixty-month implementation roadmap ‘costed’ against realistic institutional capacity and the financing envelope available from the IMF Extended Credit Facility, World Bank and African Development Bank operations. Sierra Leone’s experiment in fusing access to information and data protection within one authority, and in wiring anti-corruption oversight directly into digital PFM systems, offers lessons of genuine comparative significance for the Global South.

JEL: M40, M41, M48, G00, H00

Keywords: accountability, cybersecurity, data protection, digital governance, government accounting, IFMIS, interoperability, IPSAS, public financial management, Sierra Leone

1. Introduction

In December 2025, Sierra Leone’s Financial Secretary, Mathew Dingie, said something that finance ministries rarely admit in public. Fragmented data systems, he warned, were creating costly inefficiencies in payroll and pension administration and undermining the wider public financial management reform programme, because “*somebody will still continue to benefit from one system while the other system is losing*” (Government of Sierra Leone [GoSL], 2025). The sentence deserves close reading. It is not a complaint about missing technology. Sierra Leone has technology: an Integrated Financial Management Information System (IFMIS) running in thirty ministries, departments and agencies (MDAs), an Integrated Tax Administration System (ITAS), an electronic government procurement platform, a TSA, encrypted EFT between the Accountant General’s Department (AGD) and the Bank of Sierra Leone (BSL)’s T24 core banking application. It is a complaint about what happens between technologies. When the payroll system and the pension system cannot see each other, a retired officer can remain on the active payroll while drawing a pension; a ghost worker deleted from one register survives in another. Each system, taken alone, works; taken together, they leak.

That admission crystallises the argument of this article. Sierra Leone has spent more than two decades and hundreds of millions of dollars of domestic and donor resources modernising government accounting, and the effort has not been wasted. Five independent Public Expenditure and Financial Accountability (PEFA) assessments,

conducted in 2007, 2010, 2014, 2017 and 2021 to 2022, chart a slow but real improvement in the machinery of public finance, culminating in an 'A' rating for budget classification and budget transfers in the most recent assessment (PEFA Secretariat, 2023). Yet the same assessment found that only eight of thirty-one indicators moved favourably against 2017, while two deteriorated. The reform model that produced these results - procure a system, deploy it in an institution, train its users, move to the next system - has reached its ceiling. What remains is not a systems problem but a data problem: how financial information flows, or fails to flow, across institutional boundaries; how it is secured against a threat environment that has changed beyond recognition since IFMIS was first specified; and who is accountable when it is corrupted, stolen or quietly exploited.

I write about this problem from inside it. Years of coordinating governance reform, ICT infrastructure, procurement and donor-funded programmes within Sierra Leone's justice sector taught me that the binding constraint on reform in Freetown is almost never the absence of a plan or a platform. It is the seam between institutions: the memorandum of understanding that is drafted but never signed, the data-sharing arrangement that depends on a flash drive carried across Tower Hill, the reconciliation that waits three weeks for a spreadsheet. The Financial Secretary's warning names that constraint at the apex of the state's financial machinery, and the government's own responses - a July 2025 stakeholder roadmap for a PFM Interoperability Framework, a consolidated interagency approach to systems interoperability, and Cabinet approval of a new Data Protection and Right to Access Information Act - show that the diagnosis is now official policy. What is missing is a strategic framework that binds these initiatives into a coherent whole and confronts their joint implication: a government that integrates its financial data multiplies both the value of that data and the consequences of losing control of it.

This article supplies that framework. Its contribution is threefold. First, it offers the most complete diagnostic yet assembled of Sierra Leone's digital PFM transition, drawing together the PEFA record, the IFMIS and International Public Sector Accounting Standard (IPSAS) trajectories, the interoperability agenda and the emerging data protection regime, materials that have so far been analysed in isolation by separate professional communities of accountants, technologists and lawyers. Second, it advances an original conceptual claim: that accounting modernisation, interoperability and data protection are not three reforms but one, connected by the object they all govern, public financial data, and that treating them separately is precisely what produces the leakage the Financial Secretary described. Institutional theory, agency theory and socio-technical systems theory each illuminate part of this claim, and Section 7 develops the synthesis into a four-pillar strategic framework with a phased sixty-month implementation roadmap. Third, the article positions Sierra Leone's institutional choices, above all the decision to merge data protection and access to information into a single dual-mandate authority, within comparative debates on digital governance in developing countries, and argues that they constitute a genuine innovation from which other states in the

Global South can learn, provided the well-documented risks of concentrated regulatory power are managed.

The stakes extend beyond fiscal arithmetic. Public financial data is the evidentiary substrate of democratic accountability: the audit trail that lets the Audit Service Sierra Leone (ASSL) qualify an account, the payroll record that lets the Anti-Corruption Commission prosecute a ghost-worker scheme, the procurement dataset that lets a journalist ask why one supplier keeps winning. A state that cannot protect the integrity of that data cannot credibly promise its citizens either honest government or effective services, and in a country where the IMF’s Governance and Corruption Diagnostic has documented governance vulnerabilities across key state functions (International Monetary Fund [IMF], 2025a), the credibility of financial information is a first-order development question. At the same time, the multilateral financing on which reform depends - an IMF Extended Credit Facility arrangement whose first and second reviews unlocked US\$79.8 million in December 2025, a proposed World Bank operation on accountability and local oversight, and an African Development Bank policy-based operation carrying US\$11.5 million for 2026 after a three-year suspension of budget support - is explicitly conditioned on PFM performance. Data governance has become, quite literally, bankable.

The article proceeds as follows. Section 2 reconstructs the evolution of PFM reform in Sierra Leone since 2002 and interrogates the PEFA record. Section 3 analyses the digital transformation of government accounting through IFMIS, Cash Basis IPSAS and the new digital revenue, procurement and asset-declaration platforms. Section 4 dissects the data fragmentation problem and the interoperability response. Section 5 examines the cyber threat environment and the emerging data protection framework. Section 6 presents the integrated strategic framework and its implementation roadmap. Section 7 places Sierra Leone in comparative perspective; Section 8 confronts risks and mitigation, and Section 9 concludes with recommendations for government, development partners and civil society.

2. The Evolution of Public Financial Management in Sierra Leone

2.1 Historical Context and Reform Trajectory

Sierra Leone’s modern PFM reform programme is a child of the post-conflict settlement. When the civil war ended in 2002, the state’s financial machinery was in ruins: budget execution was largely discretionary, the ledger of record was a legacy Financial Management and Accounting System (FMAS) that could not be sustained, arrears were unrecorded and external audit was years behind. The World Bank’s early governance operations treated the reconstruction of financial control as a security question as much as an economic one, on the reasoning, since vindicated by a generation of state-building scholarship, that a state which cannot account for public money cannot hold the loyalty of those it taxes (Andrews et al., 2017). From roughly 2002 onwards, PFM reform in Sierra

Leone has run as a continuous, donor-supported enterprise, punctuated by three formal strategies: the Integrated Public Financial Management Reform Project (IPFMRP) of 2008 to 2013, the PFM Reform Strategy 2014 to 2017, and the PFM Reform Strategy 2018 to 2021.

The three strategies trace a recognisable arc. The IPFMRP concentrated on foundations: a legal framework, the chart of accounts, the beginnings of IFMIS, payroll cleansing and the machinery of external audit. The 2014 to 2017 strategy, drafted in the shadow of the Ebola epidemic and the iron-ore price collapse, both of which devastated revenue and exposed the fragility of commitment controls, shifted towards consolidation: extending IFMIS coverage, deepening the TSA and strengthening cash management. The 2018 to 2021 strategy, aligned with the change of government in 2018, foregrounded revenue mobilisation through the Integrated Tax Administration System, procurement reform and fiscal transparency. Each strategy was informed by the PEFA assessment that preceded it, a discipline of externally benchmarked self-examination that few low-income countries have maintained across five cycles, and that itself deserves recognition as an institutional achievement.

The political economy of this trajectory deserves candour, because it explains features of the present that a purely technical history cannot. PFM reform in Sierra Leone has been, throughout, a negotiated enterprise between a government whose commitment has been genuine but episodic and a donor community whose financing has been indispensable but fragmenting. Budget support gave external partners standing in the reform dialogue that few domestic constituencies possessed, and the reform agenda therefore tracked the instruments partners could finance: systems, assessments, technical assistance. This produced real assets, but it also produced the project-by-project acquisition pattern whose consequences Section 4 dissects, and it left reform ownership concentrated in a thin senior stratum of the Ministry of Finance (MoF) and the AGD rather than diffused through the administration that must operate the results. The exogenous shocks of the period compounded the pattern. The Ebola epidemic of 2014 to 2016 and the simultaneous collapse of iron-ore revenues forced emergency expenditure through whatever channels could move money fastest, normalising exactly the off-system practices that commitment controls existed to prevent; the COVID-19 period repeated the lesson. A control environment that suspends itself in every crisis teaches its users that the controls are ornamental, and the override economy documented later in this article has roots in those episodes, not merely in software configuration. Any honest account of the next reform phase must therefore build for the crisis case, with emergency procedures that are fast but logged, rather than assume the fair-weather state.

The pattern across the three strategies also reveals the reform model’s underlying logic, and its limitation. Each strategy defined reform as a portfolio of systems and institutional fixes: build IFMIS, adopt the Treasury Single Account, computerise tax administration, and strengthen the Audit Service. This is the logic that Andrews (2013) calls “solution-driven” reform: the solution is specified in advance, usually by reference

to international good practice, and implementation is measured by whether the artefact exists rather than whether the underlying function has changed. Sierra Leone implemented artefacts with reasonable fidelity. What the model never asked was how the artefacts would talk to one another, and it is exactly at those unexamined interfaces that the Financial Secretary located the leakage in December 2025.

2.2 PEFA Performance: What Five Assessments Actually Show

The five PEFA assessments of 2007, 2010, 2014, 2017 and 2021 to 2022 constitute the longest continuous externally validated performance record of any governance function in Sierra Leone, and they repay careful reading precisely because they resist a triumphalist narrative. The 2021 to 2022 assessment recorded improvement on eight indicators relative to 2017 and deterioration on two; the remaining twenty-one were broadly static (PEFA Secretariat, 2023). Eight of thirty-one moving favourably after four years of strategy implementation is not failure, but it is a rate of institutional change that should chasten anyone who believes technology adoption translates mechanically into performance.

The composition of the scores matters more than the count. Sierra Leone earned an ‘A’ overall for budget classification and for budget transfers, both core elements of the Transparency of Public Finances pillar. These are, tellingly, the dimensions most directly determined by system configuration: a modern chart of accounts embedded in IFMIS produces compliant classification more or less automatically. The weaker performance clusters in dimensions that depend on behaviour across institutions, asset and liability management, predictability of in-year resource allocation, and follow-up on audit findings, where no single system can compel compliance and where the seams between institutions dominate. Table 1 summarises the pattern, and Figure 1 characterises pillar-level performance in radar form. The lesson we draw, consistent with the cross-country evidence that IFMIS investments improve transaction processing long before they improve fiscal outcomes (Dener et al., 2011; Hashim, 2014), is that Sierra Leone’s PEFA record is a portrait of automated transactions coexisting with unintegrated institutions.

Table 1: PEFA performance trends in Sierra Leone, 2007 to 2022 (summary characterisation; indicator-level scores to be verified against published PEFA reports)

Dimension of performance	2007 to 2014 trajectory	2017 assessment	2021 to 2022 assessment	Principal driver
Budget classification	Weak to moderate	Improving	A	IFMIS chart of accounts
Transfers and budget documentation	Weak	Moderate	A (transfers)	Standardised formats, TSA
Aggregate expenditure out-turn	Volatile	Weak	Mixed	Shocks; commitment control gaps
Asset and liability management	Weak	Weak	Weak	No integrated registers

Predictability and control in execution	Weak	Moderate	Moderate; overrides persist	Manual workarounds outside IFMIS
Accounting and reporting	Weak	Moderate	Improving	Cash Basis IPSAS, GPFS formats
External scrutiny and audit	Improving	Moderate	Moderate	ASSL capacity; weak follow-up
Overall movement vs prior assessment	n/a	Mixed	8 of 31 indicators improved; 2 deteriorated	Systems ahead of institutions

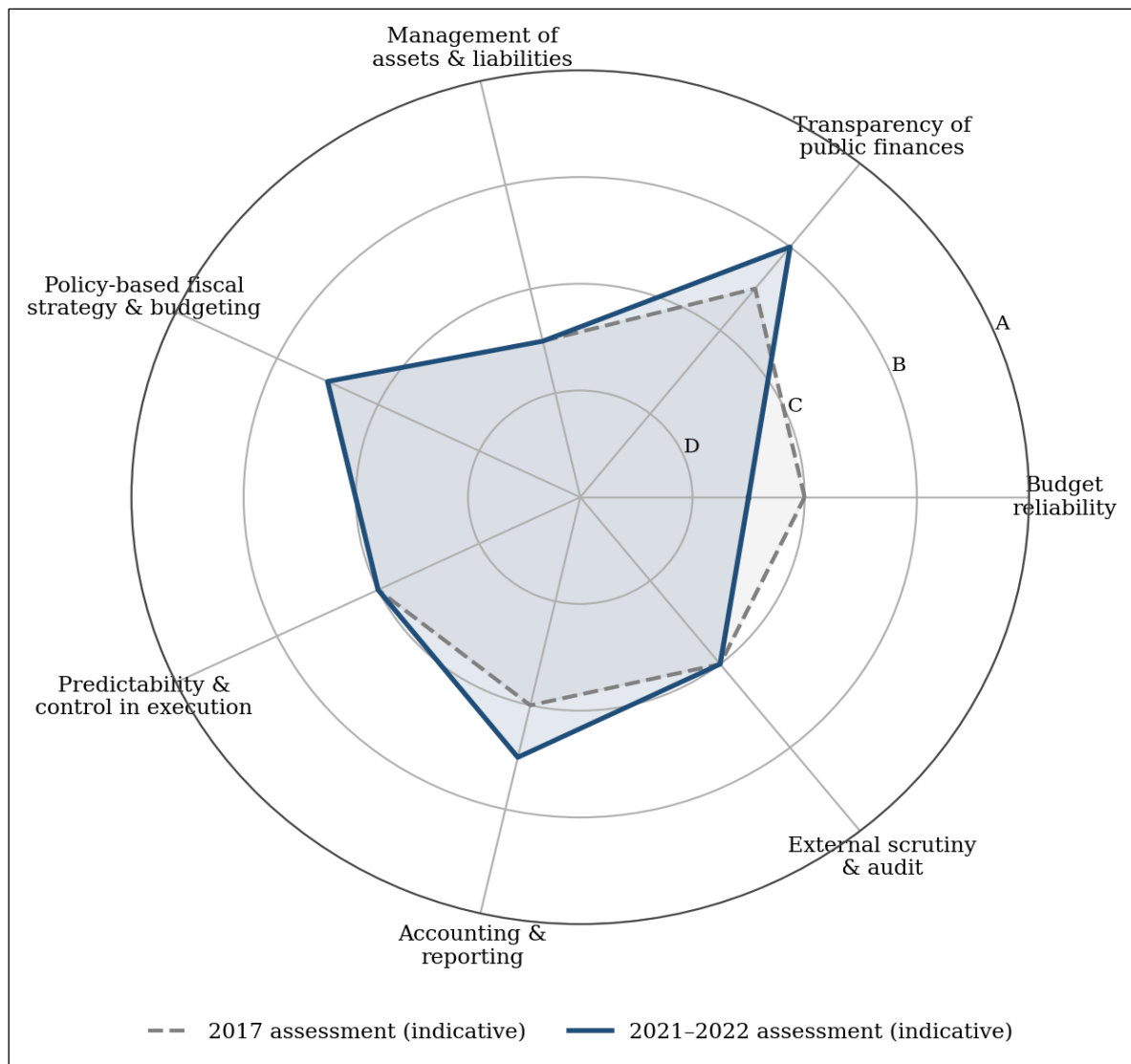


Figure 1: Indicative characterisation of Sierra Leone’s PFM performance across PEFA pillars, 2017 versus 2021 to 2022. Ordinal positions are illustrative and must be verified against the published assessments before submission

Two further observations follow from the PEFA record. First, the deterioration on two indicators between 2017 and 2021 to 2022 coincided with the period of maximum

system deployment, which supports the socio-technical reading advanced throughout this article: introducing systems faster than institutions can absorb them creates new control gaps, notably the high volume of transactions approved outside IFMIS through system overrides, even as it closes old ones. Second, the stability of the middle of the distribution, twenty-one indicators essentially unchanged, suggests that the marginal return to further stand-alone system investment is now low. The 2021 to 2022 PEFA is, in effect, an empirical argument for the interoperability turn that the government adopted in 2025.

2.3 The Legal and Institutional Framework

The Public Financial Management Act 2016 is the constitutional core of the reform architecture. It consolidated budget preparation, execution, banking and reporting rules that had previously been scattered across the Government Budgeting and Accountability Act 2005 and subsidiary instruments, entrenched the Treasury Single Account, and gave statutory force to fiscal responsibility principles. Planned revisions to the Act, signalled in the current reform dialogue with the IMF and World Bank, are expected to address the gaps that a decade of implementation has exposed: the treatment of state-owned enterprises and sub-vented agencies, sanctions for control violations, and, critically for this article’s argument, the legal status of electronic financial records and inter-agency data sharing. A PFM statute drafted in 2016 could take the paper record as its implicit default; a statute revised in the interoperability era cannot.

Around the Act stands a crowded institutional field. The MoF owns policy and the budget; the AGD operates IFMIS, the TSA and government accounting; the NPPA regulates procurement and now operates the e-GP platform; the ASSL provides external audit; the Anti-Corruption Commission (ACC) investigates and prosecutes; the National Revenue Authority (NRA) administers ITAS; the BSL settles government payments through T24; NaSSIT holds pension records; and the National Civil Registration Authority holds the identity registry against which every payroll and pension record ultimately ought to resolve. Each of these bodies has a statute, a governance structure and, in most cases, its own information system. None of them has, as yet, a binding legal duty to expose its data to the others through defined interfaces. That absence, more than any technical deficiency, is the institutional root of the fragmentation analysed in Section 4, and it is why the legal pillar of the framework proposed in Section 6 carries as much weight as the technological one.

Two further weaknesses in the current legal settlement bear directly on the article’s argument. The first concerns sanctions. The PFM Act 2016 creates duties in abundance and consequences in scarcity: the officer who authorises expenditure outside the system, the vote controller who ignores an audit recommendation, the agency head who declines to supply data face, in practice, administrative correspondence rather than personal liability, and twenty years of Auditor-General’s reports itemising repeated findings against the same institutions are the measure of what unsanctioned duties

achieve. Comparative experience is blunt on this point: Rwanda’s enforcement of personal accountability for audit findings and Kenya’s slow movement in the same direction under its PFM Act mark the difference between audit as literature and audit as deterrent. The second weakness concerns the perimeter. Sub-vented agencies, state-owned enterprises and local councils hold substantial public resources and generate substantial fiscal risk, yet they sit at the edges of both the Act’s operational grip and the systems estate, reporting late, on varied bases, through manual channels. Any revision of the Act that modernises the electronic core while leaving the perimeter analogue will simply relocate the arbitrage the Financial Secretary described from the centre of government to its edges, where visibility is worst.

3. The Digital Transformation of Government Accounting

3.1 The IFMIS Journey

IFMIS is the spine of Sierra Leone’s government accounting, and its history compresses every lesson the international literature has learned about financial management information systems in low-income countries. The system replaced FMAS, which had become technically unsustainable, and its rollout has now run for well over a decade. Coverage stands at thirty MDAs, against an original plan to reach all MDAs and sub-vented agencies by 2021, a target that slipped for reasons the government itself has candidly identified: procurement delays, technical infrastructure constraints, limited connectivity outside Freetown, and coordination challenges among the institutions that must jointly deliver each site (GoSL, 2025). Figure 2 sketches the trajectory. Table 2 summarises coverage by entity category.

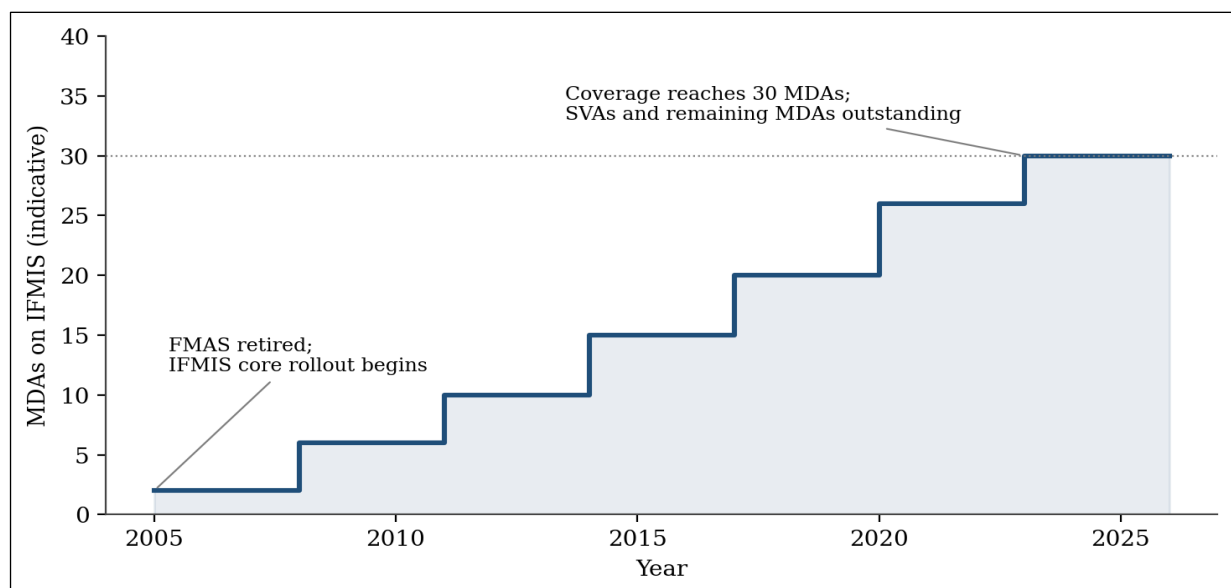


Figure 2: Indicative IFMIS rollout trajectory, from the retirement of FMAS to current coverage of thirty MDAs. Intermediate values are illustrative; the endpoint reflects officially reported coverage

Table 2: IFMIS rollout status by entity category (to be verified against AGD records)

Entity category	Approximate population	IFMIS status	Principal constraint
Central MDAs (budget-funded)	c. 50+	30 connected; remainder outstanding	Connectivity, site readiness, coordination
Sub-vented agencies	Numerous	Largely outside IFMIS; GPFS reporting via Cash Basis IPSAS formats	Capacity, financing of rollout
Local councils	22	Separate PETRA-lineage systems; not integrated	Interoperability, connectivity
State-owned enterprises	c. 20+	Own accounting systems; consolidated reporting weak	Legal mandate, standards alignment
Missions abroad	c. 20	Manual or semi-manual returns	Connectivity, cost

Three features of the IFMIS experience matter for the argument. The first is the persistence of transactions approved outside the system. The government acknowledges a high volume of overrides, expenditures processed through manual or parallel channels and regularised later, if at all. In control terms, an override is not a workaround; it is a hole in the control environment, because every commitment control, budget check and audit trail that IFMIS enforces is suspended for exactly the transactions most likely to need scrutiny. The international evidence is unambiguous that FMIS benefits are conditional on comprehensive use, and that partial coverage combined with tolerated bypasses can leave fiscal control worse than a disciplined manual system, because it manufactures an appearance of automation that oversight bodies may be tempted to trust (Hashim, 2014; Diamond & Khemani, 2006).

The second feature is the Electronic Funds Transfer (EFT) arrangement, which deserves more attention than it usually receives. Payment instructions leave IFMIS at the AGD as encrypted electronic CSV files and are transmitted to the T24 core banking application at the BSL for settlement. This is, on one hand, a real achievement: it removed the cheque, and with it an entire class of fraud. On the other hand, a file-based interface between the two most consequential financial systems in the state is a fragile, point-to-point integration of exactly the kind that the interoperability literature warns against. A CSV file, however well encrypted in transit, is generated, staged and consumed at endpoints where it can in principle be altered, duplicated or replayed; its security depends on operational discipline rather than architecture. The EFT link is simultaneously the proof that integration pays and the clearest illustration of why Sierra Leone needs to move from file exchange to governed, authenticated, logged service interfaces.

The third feature is what IFMIS has quietly built beneath the transactions: a standardised chart of accounts, a single budget classification, and a body of accountants and ICT officers who have operated a modern ERP-class system for a decade. These are the assets, intangible and rarely ‘costed’, on which the interoperability agenda can now draw. The rollout’s slowness has been expensive, but it has also been formative, and any

strategy that treats the existing IFMIS estate as a liability to be replaced rather than a platform to be federated would repeat the most common and costly error in the global FMIS record (Dener et al., 2011).

3.2 IPSAS Adoption and the Modernisation of Financial Reporting

Alongside the systems agenda runs a standards agenda. The Government of Sierra Leone has formally adopted the IPSAS for Financial Reporting under the Cash Basis of Accounting, and the AGD has developed standardised General Purpose Financial Statement (GPFS) formats on that basis for sub-vented agencies and other government entities. The national standard-setting infrastructure predates this adoption: the Corporate and Sector Accounting Advisory Group (CSAAG) was established in 2008 under the sponsorship of the Institute of Chartered Accountants of Sierra Leone (ICASL), giving the country a domestic professional anchor for standards work that many peers lack.

IPSAS Cash Basis is often dismissed as the modest end of the reporting spectrum, and the comparative record does show most value accruing to countries that eventually transit to accrual (IPSASB, 2022; IFAC & CIPFA, 2021). But the dismissal misreads the sequencing problem in a country at Sierra Leone’s stage. The binding constraint on financial reporting in Freetown has never been the sophistication of the measurement basis; it has been completeness, timeliness and consistency, whether every entity reports, on time, in the same format, covering all cash flows including donor funds. IPSAS Cash Basis, faithfully applied through standardised GPFS formats, attacks exactly that constraint, and it does so with data that IFMIS already produces. The strategic question is not whether cash-basis reporting is ambitious enough but whether the transition to accrual, which Section 6 places in the medium-term phase, is prepared deliberately: asset registers built, liabilities recognised progressively, and the accounting cadre trained ahead of need rather than after it. Table 3 summarises the current position.

Table 3: IPSAS compliance status by entity type (characterisation; to be verified)

Entity type	Reporting basis	GPFS format status	Principal gap
Central government (consolidated)	IPSAS Cash Basis	Standardised	Coverage of extra-budgetary flows
Sub-vented agencies	IPSAS Cash Basis	Standardised formats issued by AGD	Consistent application, timeliness
Local councils	Cash-based statutory formats	Partial alignment	Capacity, system support
State-owned enterprises	IFRS or national standards	Outside GPFS regime	Consolidation, fiscal risk disclosure
Transition to accrual IPSAS	Not yet commenced	n/a	Asset registers, valuation, skills

The reporting agenda also carries a data governance implication that is rarely stated. Standardised GPFS formats are, in effect, a data standard: they define entities,

classifications and aggregation rules. Every step towards reporting consistency is therefore also a step towards interoperability, because systems that must produce the same statement from the same classification are systems that can, with modest additional effort, exchange the underlying records. The accountants and the technologists are building the same road from opposite ends; the strategic framework in Section 6 asks them to meet in the middle.

3.3 E-Procurement, Digital Revenue and Digital Integrity Systems

The third stream of digitalisation lies upstream and downstream of the accounts. Upstream, the ITAS has modernised the NRA’s core processes, and the launch of the Electronic Government Procurement system marks a decisive step in digitalising the spending pipeline at its point of origin, with the National Public Procurement Authority (NPPA) already piloting training on digital Annual Procurement Plans and Disbursement Forecasts. Downstream, two integrity platforms are under construction: the Sierra Leone Asset Declaration System (SL-ADS), developed with the Directorate of Science, Technology and Innovation to replace a declaration process whose past weaknesses were well documented, and a dedicated software platform through which the Government Audit Committee will track the status of every audit recommendation in real time, open, on-going or completed, with the Anti-Corruption Commission (ACC) holding direct access under a memorandum of understanding now being drafted between the ACC and the GAC.

Read together, these initiatives disclose an emergent architecture of digital accountability that is more coherent than any single project document admits. e-GP creates a structured record of who was invited, who bid, who won and at what price; IFMIS records the commitment and the payment; EFT settles it; ITAS records the winner’s tax behaviour; SL-ADS records the officials’ declared interests; and the audit-tracking platform records whether findings about any of it were ever acted upon. Every link in the accountability chain is acquiring a digital expression. The chain, though, is only as strong as its joins. An e-GP contract award that cannot be matched automatically to an IFMIS commitment, or an audit recommendation that references a transaction the tracking platform cannot retrieve, reproduces in digital form the same seams that defeated paper-based oversight. The promise of these systems is conditional on the interoperability agenda to which the article now turns, and their peril, a concentration of sensitive personal and financial data in connected platforms, is the subject of Section 5.

3.4 Emerging Technologies: Promise Under Discipline

No strategic treatment of government accounting modernisation can now avoid the technologies that dominate the reform conversation, artificial intelligence, cloud computing, block-chain and big data analytics, and none should discuss them without discipline, because the gap between their rhetorical and their realised value in public finance is wide. The test I apply to each is the practitioner’s test: what problem in Sierra

Leone’s actual control environment does the technology solve, at what recurrent cost, with what new dependency, and what must exist first.

Analytics and machine learning pass the test most convincingly, but only after the interoperability programme creates their raw material. The characteristic frauds of Sierra Leone’s payroll and payments environment, duplicates across registers, dormant records reactivated, payment patterns that cluster around thresholds, are precisely the patterns that anomaly-detection methods find cheaply once the underlying registers are joined. The sequencing implication is uncomfortable for enthusiasts: an ML model trained on fragmented, manually reconciled data automates the errors it is fed. The data warehouse endorsed by Cabinet is therefore not an analytics project with an integration prerequisite; it is an integration project whose analytics are the dividend. The supreme audit institutions that have operationalized data-driven audit, Brazil’s TCU is the most studied case, all built the data pipeline before the models, and the ASSL should plan on the same order.

Cloud computing presents Sierra Leone with a genuine dilemma rather than a simple choice. Domestic data-centre capacity is limited, power-constrained and expensive to secure to the standard that treasury systems require; commercial cloud providers offer resilience, patching discipline and security engineering that no institution in Freetown can currently replicate. Against that stand three considerations: sovereignty over the state’s most sensitive records, the foreign-exchange exposure of perpetual subscription costs, and the requirements the new data protection statute will impose on cross-border transfer of personal data. The defensible position is a classified hybrid: public and low-sensitivity workloads to accredited cloud services under contracts that satisfy the statute; the transactional core and the identity registry on sovereign or regionally controlled infrastructure hardened with partner support; and, in all cases, exit provisions negotiated at signature, because a treasury that cannot leave its provider has privatised a piece of its sovereignty.

Block-chain earns the most scepticism and the narrowest endorsement. The comparative record of distributed-ledger pilots in government finance is largely a record of quiet abandonment, because the technology answers a question, how can mutually distrusting parties share an append-only record without a trusted operator, that most public financial processes do not ask; the state is the trusted operator, and a well-governed database with proper logging is cheaper, faster and easier to fix. The exception worth watching is audit-trail integrity in the interoperability layer itself: an append-only, hash-chained log of inter-agency data access, distributed across the oversight institutions so that no single administrator can rewrite history, addresses a real threat, insider tampering with the evidence of insider tampering, and can be implemented with modest ledger techniques without token infrastructure. That narrow use belongs in the Phase 2 design; a block-chain general ledger does not belong anywhere in this programme.

Artificial intelligence (AI) in the wider sense, including the large language models now entering administrative work, will reach Sierra Leone’s public service through the

pockets of its staff long before it arrives through any procurement, and the governance implication is immediate rather than futuristic: officials pasting financial records into consumer AI services constitute a data-protection incident in progress, and the new authority’s early guidance should say so plainly. The affirmative uses - drafting support, translation of financial reports into accessible summaries for the transparency portals, first-line query handling for suppliers and pensioners - are real but secondary. The strategic principle across all four technologies is the same one this article applies throughout: capability follows data governance. Every one of these tools amplifies the quality of the records it touches, integrating and protecting records into insight, and transforming fragmented and insecure records into confident error.

4. The Data Fragmentation Challenge

4.1 Symptoms and Consequences

The Financial Secretary’s December 2025 warning was specific: fragmentation is producing costly inefficiencies in payroll and pension administration, and the losses are not abstract. *“Somebody will still continue to benefit from one system while the other system is losing”* is a precise description of arbitrage across unreconciled registers. Payroll and pensions are where fragmentation bites hardest because they sit at the intersection of the largest number of systems: the payroll itself, IFMIS which pays it, NaSSIT which holds contribution and pension records, the civil registry at NCRA which establishes that a person exists and remains alive, and the human resource records of employing MDAs. Any pair of these registers that disagrees creates an exploitable gap, and pairs that are reconciled manually, monthly at best, disagree by construction for weeks at a time.

The government’s own diagnosis extends well beyond payroll. Multiple systems, those of the MoF, the AGD, the NPPA, the ASSL, the BSL, NaSSIT and NCRA, rely on one another for information yet depend on manual data-sharing processes that compromise data quality (GoSL, 2025). Dr Simeon Jonjo, Director of the Directorate of Financial Management and Systems Technology, put the point bluntly at the July 2025 interoperability workshop: most government systems operate independently, without interconnectivity, despite significant investment over the past decade. Figure 3 maps the current position. The dashed lines, manual or semi-manual exchange, dominate; the single automated link is the encrypted EFT channel to T24.

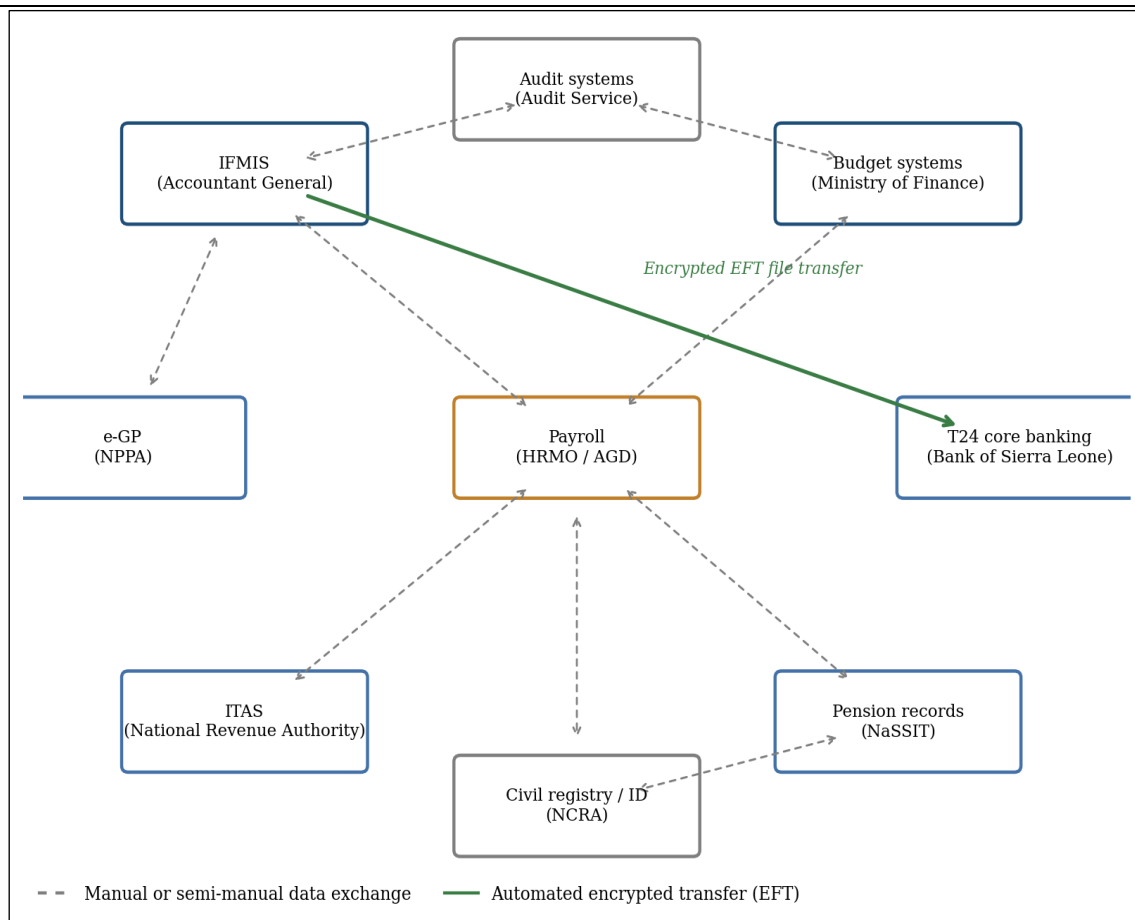


Figure 3: Sierra Leone’s principal government financial systems and their current data exchange arrangements. Dashed connections denote manual or semi-manual exchange; the solid connection denotes the automated encrypted EFT transfer from IFMIS to the BSL’s T24 application.

The consequences run along four channels. Fiscal leakage is the most visible: duplicate and ghost payments that survive because no register is authoritative. Decision degradation is subtler: a Minister of Finance setting the wage bill ceiling from a payroll extract that disagrees with NaSSIT’s records is planning on corrupted inputs, and the Cabinet’s stated ambition of data warehousing, analytics and business intelligence for informed decision-making is unachievable while the warehouse would have to be filled by hand. Oversight friction is the third channel: the ASSL and the ACC spend scarce forensic capacity reconstructing data flows that an integrated architecture would log automatically, which is one reason implementation of audit recommendations across MDAs, state-owned enterprises and local councils has remained persistently weak. The fourth channel is the citizen-facing one identified in the government’s own digital identity work: siloed systems and the absence of a data protection framework block safe use of the national ID for digital payments, education, health and social protection, so fragmentation inside government reproduces exclusion outside it.

The macro-fiscal arithmetic sharpens the point. The wage bill and pensions together absorb one of the largest shares of Sierra Leone’s domestically financed expenditure, and in a programme environment where the IMF arrangement disciplines the primary balance and the AfDB’s renewed budget support carries explicit reform measures, every Leone leaking through register arbitrage is a Leone unavailable for the health worker, the classroom or the debt service that the programme protects. Fragmentation losses are, in effect, an unbudgeted expenditure line whose beneficiaries are unknown and whose size the government cannot currently state, which is itself the strongest argument for the baseline measurement this article urges. There is also a compounding temporal cost: because manual reconciliation is slow, errors persist for months before detection, and recovery of amounts wrongly paid is far more expensive, administratively and politically, than prevention. Systems that reconcile continuously convert an open-ended contingent liability into a bounded operating cost, and that conversion, more than any efficiency statistic, is what the MoF is buying with the interoperability programme.

4.2 Root Causes

It would be convenient to blame technology procurement, and procurement played its part: each system was specified, financed and delivered as a project, usually by a different partner, on a different platform, with integration listed among future phases that budgets never reached. But the deeper causes are institutional, and the theoretical literature names them accurately. In institutional terms (DiMaggio & Powell, 1983), each agency adopted the system that its own field legitimated; revenue administrations buy tax systems, treasuries buy FMIS, procurement regulators buy e-GP, and legitimacy attached to possessing the artefact, not to connecting it. In agency terms (Jensen & Meckling, 1976), information is power in budget negotiations, and an MDA that surrenders unilateral control of its data surrenders discretion; the absence of any statutory duty to share meant the default, hoarding, prevailed. In socio-technical terms (Heeks, 2002), each system was optimised around the workflows of its host institution, so the design gaps between systems mirror, precisely, the coordination gaps between the institutions themselves. Fragmented systems are not an accident that befell a coherent government; they are a faithful digital portrait of an incoherent one.

That diagnosis matters because it dictates the remedy. If fragmentation were technical, middleware would cure it. Because it is institutional, the cure must combine architecture with authority: interoperability standards that are binding rather than advisory, a governance body with the mandate to enforce them, data ownership and stewardship rules that make sharing a legal duty rather than a favour, and financing that rewards connection rather than acquisition. This is the reasoning behind the government’s consolidated interagency approach to systems interoperability, and it is why the framework in Section 6 pairs every technical measure with a legal or institutional one.

4.3 The Interoperability Imperative

The July 2025 stakeholder workshop that produced the roadmap for the PFM Interoperability Framework is therefore the most consequential PFM event in Sierra Leone since the adoption of the Treasury Single Account, even though it committed no expenditure. It marked the official abandonment of the system-by-system model and the adoption of an architectural one: a consolidated interagency approach intended to support data warehousing, analytics, business intelligence and informed decision-making. The natural technical expression of that approach, familiar from government service bus implementations elsewhere and consistent with the direction of the roadmap, is a governed exchange layer through which systems publish and consume data via authenticated, logged interfaces against agreed standards, replacing the current lattice of files, spreadsheets and flash drives.

The comparative evidence for this architectural pattern is strong. Estonia’s X-Road data exchange layer is the canonical case, but the more instructive comparators for Freetown are closer: Rwanda’s integration of its IFMIS with tax, payroll and identity systems, and India’s India Stack, which demonstrated that identity-anchored interoperability can operate at extreme scale on modest per-transaction cost, are both routinely credited with material reductions in payment leakage, with India’s direct benefit transfer reforms alone estimated by its MoF to have saved several billion dollars by eliminating duplicate and ghost beneficiaries (World Bank, 2022). The mechanisms are the same ones the Financial Secretary described in reverse: where registers reconcile automatically and continuously, the arbitrage between them disappears. Table 4 sets out the principal benefit channels for Sierra Leone; I deliberately present them qualitatively, because credible country-specific quantification requires baseline measurement of override volumes, reconciliation lags and payroll-pension mismatches, which should itself be a first-phase deliverable of the interoperability programme rather than an assumption smuggled into its business case.

Table 4: Principal benefit channels of PFM systems interoperability in Sierra Leone

Benefit channel	Mechanism	Primary beneficiary institutions	Measurement baseline required
Payroll and pension integrity	Continuous reconciliation of payroll, NaSSIT and NCRA registers	AGD, MoF, HRMO, NaSSIT	Current mismatch and duplicate rates
Commitment-to-payment control	Automatic matching of e-GP awards, IFMIS commitments and EFT payments	AGD, BSL, NPPA	Override volume and value outside IFMIS
Revenue assurance	Cross-matching of ITAS records with procurement winners and payees	NPPA, NRA	Compliance gap among government suppliers
Audit and investigation efficiency	System-generated trails; real-time recommendation tracking	ASSL, ACC, GAC	Average evidence retrieval and follow-up time

Fiscal reporting and analytics	Warehouse fed by system interfaces rather than manual returns	Cabinet, MoF, Parliament	Reporting lag and error rates
Citizen service access	Safe ID-anchored eligibility checks for payments and services	Social protection, health, education MDAs	Exclusion and duplication rates in beneficiary lists

One caution belongs here rather than in the risk section, because it shapes the whole argument that follows. Interoperability concentrates value. A lattice of disconnected systems is inefficient but compartmentalised; a governed exchange layer through which payroll, pensions, identity, tax and payments all flow is efficient and a single, supremely attractive target. Every kilometre of integration Sierra Leone builds raises the stakes of the security and data protection regime that must protect it. That is why this article insists on treating Sections 4 and 5 as one problem, and why the government’s parallel movement on data protection legislation is not a separate reform that happens to be contemporaneous but the necessary condition of the interoperability programme’s legitimacy.

5. Protecting Public Financial Data

5.1 The Cyber-security Threat Environment

Government financial systems have become primary targets of cybercrime worldwide, and the African public sector’s exposure has grown faster than its defences. The ITU’s Global Cyber-security Index places most West African states, Sierra Leone among them, in the lower tiers of institutional cyber readiness (International Telecommunication Union [ITU], 2021), while INTERPOL’s African cyber-threat assessments document sustained growth in ransomware, business email compromise and payment-flow interception directed at both public and financial institutions across the region (INTERPOL, 2024). The pattern of publicly reported incidents against African governments in recent years, ransom-ware against national treasuries and revenue authorities, compromise of payroll portals, exfiltration of citizen registries - describes with uncomfortable precision the asset classes Sierra Leone is now digitalising and connecting.

Sierra Leone’s specific vulnerability profile has four layers, and Figure 4 organises the threat taxonomy against them. The first is infrastructural: limited and unevenly distributed data storage capacity, dependence on constrained power and connectivity, and consequent improvisation, the unofficial cloud account, the personal laptop, the flash drive, that no security policy reaches. The second is the interface layer already described: manual and file-based data exchange multiplies the points at which financial data exists outside any system’s control environment, and the EFT arrangement, for all its encryption in transit, terminates in endpoints whose security is operational rather than architectural. The third layer is human: a small cadre of security-skilled professionals,

thinly spread, facing an adversary market that recruits globally; capacity building needs and financial constraints are acknowledged in the government’s own data protection diagnosis. The fourth is institutional: until the current reforms, no authority combined the mandate, the technical competence and the enforcement power to hold data controllers, public or private, to a standard. The National Cyber Security Coordination Centre, established under the Cyber-security and Crime Act 2021, supplies part of that architecture; the new data protection authority is designed to supply the rest.

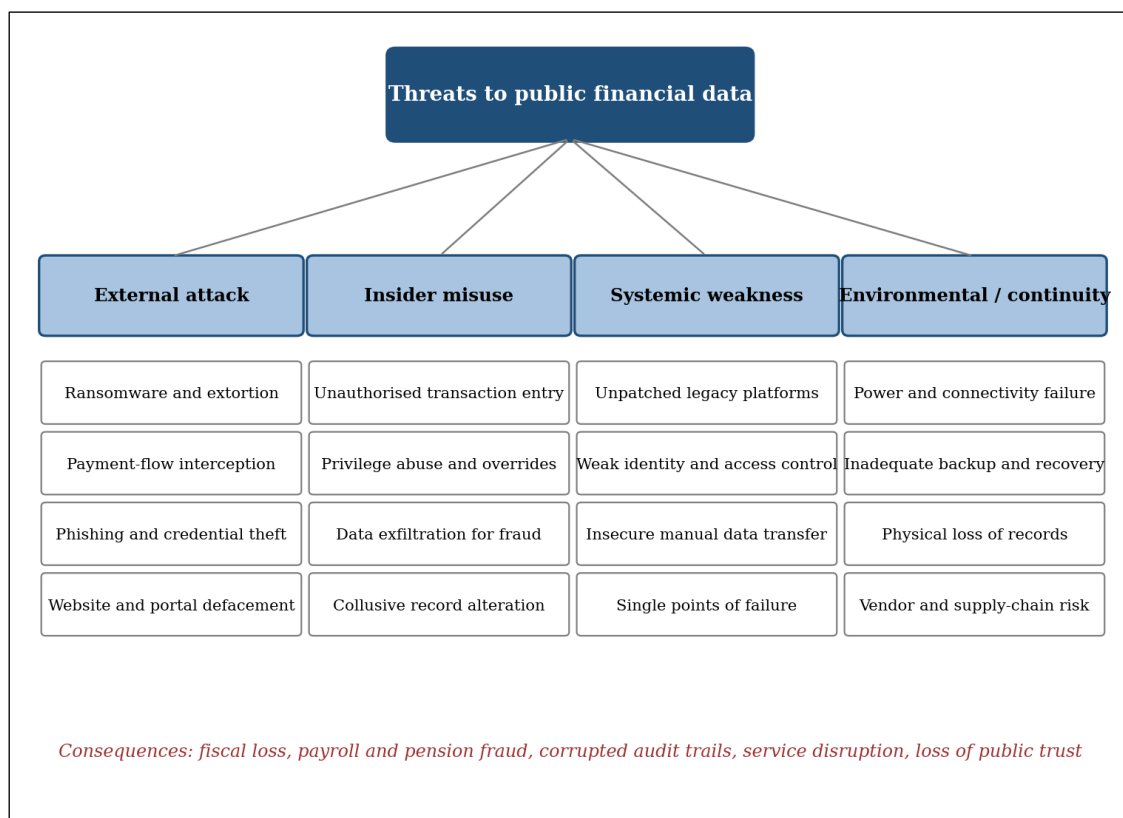


Figure 4: Taxonomy of threats to public financial data in Sierra Leone organised by threat class, with principal consequences

The economics of the threat deserve as much attention as its taxonomy, because they determine what defence must cost. Cybercrime against financial systems is an industry with falling entry costs: ransomware is sold as a service, phishing kits are commoditised, and generative AI has cut the price of convincing social engineering, fluent spear-phishing in any register, cloned voices for payment authorisation fraud, to nearly nothing. The attacker’s economics scale globally while the defender’s do not, and this asymmetry bears hardest on small states, which present the same asset classes as large ones - treasuries, payrolls, citizen registries - behind a fraction of the defensive investment. The regional record makes the exposure concrete: recent years have seen ransomware operations paralyse government networks in more than one African state for weeks, revenue authorities lose taxpayer data, and payment-diversion frauds

executed through compromised official email against ministries of finance. Sierra Leone has no exemption from this market; it has, until now, had a smaller digital surface, and the entire thrust of the reform programme this article endorses is to enlarge that surface. Honest strategy states the bargain plainly: integration is being purchased with exposure, and the purchase is worth making only if the security investment is priced into it from the first budget line, not appended when the first incident forces the question.

Two features of this threat environment deserve emphasis because they cut against comfortable assumptions. First, the insider threat dominates in systems like Sierra Leone’s. The high volume of overrides outside IFMIS is usually discussed as a control weakness; it is equally a security finding, because a tolerated bypass is indistinguishable, in the logs, from an attack. Information security theory has long held that controls defeated by authorised users are the characteristic failure mode of financial systems (Anderson, 2020), and the payroll-pension arbitrage the Financial Secretary described is, in security terms, a long-running insider exploitation of an integrity gap. Second, the fiscal consequences of a successful attack on an integrated PFM core would not be limited to the ransom or the loss. A treasury that cannot certify the integrity of its ledgers cannot close its accounts; a payroll that cannot be trusted cannot be paid without manual verification of tens of thousands of records; and a government mid-programme with the IMF would face its reviews with ‘unauditable’ data. Cyber resilience, the capacity to withstand, contain and recover, is therefore a fiscal policy variable, which is precisely how the NIST Cybersecurity Framework’s current revision and the enterprise risk management tradition ask organisations to treat it (National Institute of Standards and Technology [NIST], 2024; COSO, 2017).

5.2 The Emerging Data Protection Framework

Against this background, the legal reforms approved by Cabinet in 2025 constitute the most significant development in Sierra Leone’s information governance since the Right to Access Information Act 2013. Government has approved a National Data Protection Policy and authorised the repeal of the Right to Access Information Commission Act and the enactment of a new Data Protection and Right to Access Information Act. The design choice at the heart of the legislation is unusual and deliberate: a single unified authority with a dual mandate covering both access to public information and protection of personal data. The existing Right to Access Information Commission will be transformed into a stronger institution with enhanced investigative, compliance and enforcement powers over both public and private sector data handling, and the statute mandates stricter data protection protocols for banks, mobile network operators (MNOs) and government agencies. Minister of Information and Civic Education Chernor Bah has described the reform as *“a turning point in safeguarding citizens’ privacy and improving transparency”* and among the most forward-looking legislation in the country’s recent history (GoSL, 2025).

Table 5 places the design in comparative context. Most African data protection regimes, Ghana’s Act 843 of 2012, Kenya’s Data Protection Act 2019, Nigeria’s Data Protection Act 2023, follow the European model of a stand-alone data protection authority, with access to information governed separately where it is governed at all, the pattern the EU itself embeds by assigning the GDPR and freedom of information to different instruments (European Union, 2016). Sierra Leone’s fusion of the two mandates is rarer, and its logic is strongest exactly in the public financial data domain this article examines. Transparency and privacy are not opposing values that happen to share a regulator; they are two rulings on the same question: who may see this record, and a single authority can develop a coherent jurisprudence of that question where two authorities would generate boundary disputes. A procurement record contains a supplier’s bank details and beneficial owners; a payroll contains both a public wage bill and thousands of private identities; an asset declaration is simultaneously an integrity instrument and a dossier of personal financial information. Every consequential PFM dataset sits astride the access-privacy line, and Sierra Leone has, alone among its peers, built its regulator astride the same line.

Table 5: Comparative design of data protection frameworks relevant to public financial data

Design dimension	Sierra Leone (Bill, 2025)	Ghana (Act 843, 2012)	Kenya (DPA, 2019)	Nigeria (NDPA, 2023)	EU benchmark (GDPR, 2016)
Regulator model	Unified authority, dual mandate (access + protection)	Stand-alone Data Protection Commission	Office of the Data Protection Commissioner	Nigeria Data Protection Commission	DPAs; access governed separately
Access to information	Integrated in same statute and authority	Separate RTI Act 2019	Separate ATI Act 2016	Separate FOI Act 2011	Separate instruments
Public sector coverage	Explicit; government agencies bound	Yes, uneven enforcement	Yes	Yes	Yes
Financial sector obligations	Stricter protocols for banks and MNOs mandated	General	General plus sectoral rules	General plus sectoral rules	General plus sectoral law
Enforcement powers	Enhanced investigative and compliance authority	Moderate	Growing; active enforcement record	New; developing	Strong; substantial fines
Continental alignment	Consistent with AU Malabo Convention direction	Malabo signatory context	Malabo-aligned	Malabo-aligned	n/a

Note: Characterisations are the author’s; statutory details to be verified against the enacted texts.

The comparative point should not become congratulation. A dual-mandate authority is only as good as its independence, budget and technical depth, and the enforcement record of first-generation African data protection authorities is cautionary: statutes passed quickly, commissions funded slowly, enforcement arriving years later if at all. The design also concentrates power, an authority that decides both what government must disclose and what it must withhold is a formidable institution, and its capture would be correspondingly damaging. These risks are addressed in Section 8; here the analytical claim is narrower: for the specific problem of governing public financial data in an interoperable architecture, the unified model is a better fit than the imported standard design, and it is a genuine Sierra Leonean institutional innovation rather than a transplant.

5.3 Transparency and Privacy in the Same Ledger

The dual mandate forces a discipline that PFM reformers usually postpone: deciding, dataset by dataset, where the access-privacy line runs. The framework this article proposes treats that decision as an architectural input, not an afterthought, through three operating principles. First, transparency of aggregates, protection of identities: budget execution, procurement outcomes and audit findings should be published proactively at a granularity that supports accountability, while the personal data embedded in the same records, bank accounts, identity numbers, family details in declarations - is protected by design, with disclosure decisions reasoned under the statute rather than improvised by records officers. Second, purpose limitation inside government: interoperability is not a licence for every agency to see everything, and the exchange layer must enforce, technically, the legal basis on which each institution accesses each dataset, the ACC’s access to the audit-tracking platform being the model of a defined, logged, purpose-bound connection. Third, the citizen as data subject of the state: the same identity registry that anchors payroll integrity also anchors surveillance risk, and the legitimacy of the whole architecture depends on citizens experiencing the data protection authority as their instrument rather than the government’s. A worked example shows the discipline in operation. Consider the Sierra Leone Asset Declaration System. An asset declaration serves accountability only if someone can check it, yet it contains the most sensitive personal financial information the state ever collects about an individual, and it implicates third parties, spouses, children, and business partners, who declared nothing and consented to nothing. Under a separate-regulator model, the access commission would face demands for publication and the data protection authority would face complaints about it, with the declarant’s lawyers arbitrating between them. Under the unified statute, one authority must produce a single reasoned settlement, and the settlement that comparative practice supports is a tiered one: verification access for the ACC as of right, purpose-bound and logged; publication of a defined summary layer, offices held, categories and bands of assets, registrable interests, sufficient for journalistic and civic scrutiny; and protection of the granular layer, account numbers, addresses,

minor children, absent a reasoned public-interest determination. The same tiering logic then generalises across the PFM estate: full-granularity procurement data to the NPPA and the Audit Service, contract-level publication to the portal with commercial and personal fields governed; transaction-level payroll to the AGD and HRMO, aggregate wage bill data by grade and MDA to Parliament and the public. Designing these tiers, dataset by dataset, is unglamorous regulatory work, and it is exactly the work that determines whether digital transparency and data protection reinforce or destroy each other.

International alignment carries practical weight here too: credible data protection is increasingly a condition of cross-border financial integration, correspondent banking confidence and participation in continental digital trade under the African Continental Free Trade Area’s digital protocol, so the statute is an economic instrument as much as a rights instrument.

6. A Strategic Framework for Digital Governance and Financial Accountability

6.1 Conceptual Foundation

The framework proposed here rests on a synthesis of the theoretical traditions that each explains part of Sierra Leone’s predicament. Institutional theory explains why systems were adopted without connection and warns that interoperability will be resisted wherever it threatens legitimated autonomy; the remedy it prescribes is to change what counts as legitimate, which is the function of binding standards and public performance measurement. Agency theory explains the information hoarding and the override economy, and prescribes realigned incentives: statutory duties to share, sanctions with teeth, and audit trails that raise the price of discretion. Stewardship and public value theory (Moore, 1995) supply the affirmative case, that most officials will use integrated data well if the architecture makes good behaviour the path of least resistance. New Public Management explains the first two decades of reform, efficiency through systems and measurement, while New Public Governance (Osborne, 2006) explains why the next phase must be networked: no single institution owns the interoperability problem, so its governance must be collegial by design. The resource-based view and dynamic capability theory (Barney, 1991; Teece et al., 1997) reframe the decade of IFMIS operation as an accumulated capability to be extended rather than replaced, and locate the scarcest strategic resource accurately: not hardware but the human capacity to reconfigure systems as needs change. The Technology Acceptance Model and diffusion theory (Davis, 1989; Rogers, 2003) explain the override problem from the user’s side: systems bypassed because bypassing was easier, and instruct that the integrated architecture must beat the workaround on usefulness and ease, not merely prohibit it. Information security theory, the enterprise risk management tradition and the cyber resilience literature (Anderson, 2020; COSO, 2017; NIST, 2024) supply the cross-cutting foundation, while socio-technical systems theory disciplines the whole: every technical layer must be

paired with the institutional arrangement that operates it, because in Sierra Leone’s record it is always the unpaired layer that fails.

From this synthesis the framework draws its structure: four pillars on one foundation, shown in Figure 5. The pillars are digital infrastructure and systems integration; legal and regulatory enablement; institutional capacity and human capital; and oversight, accountability and citizen engagement. The foundation, deliberately drawn beneath all four rather than as a fifth pillar, is cyber-security and data protection by design. The geometry is the argument: security and data protection are not a component of the reform but the condition on which every component stands, and a programme that treats them as a parallel work-stream will discover, as the interoperability layer concentrates value, that it has built the target before the shield.

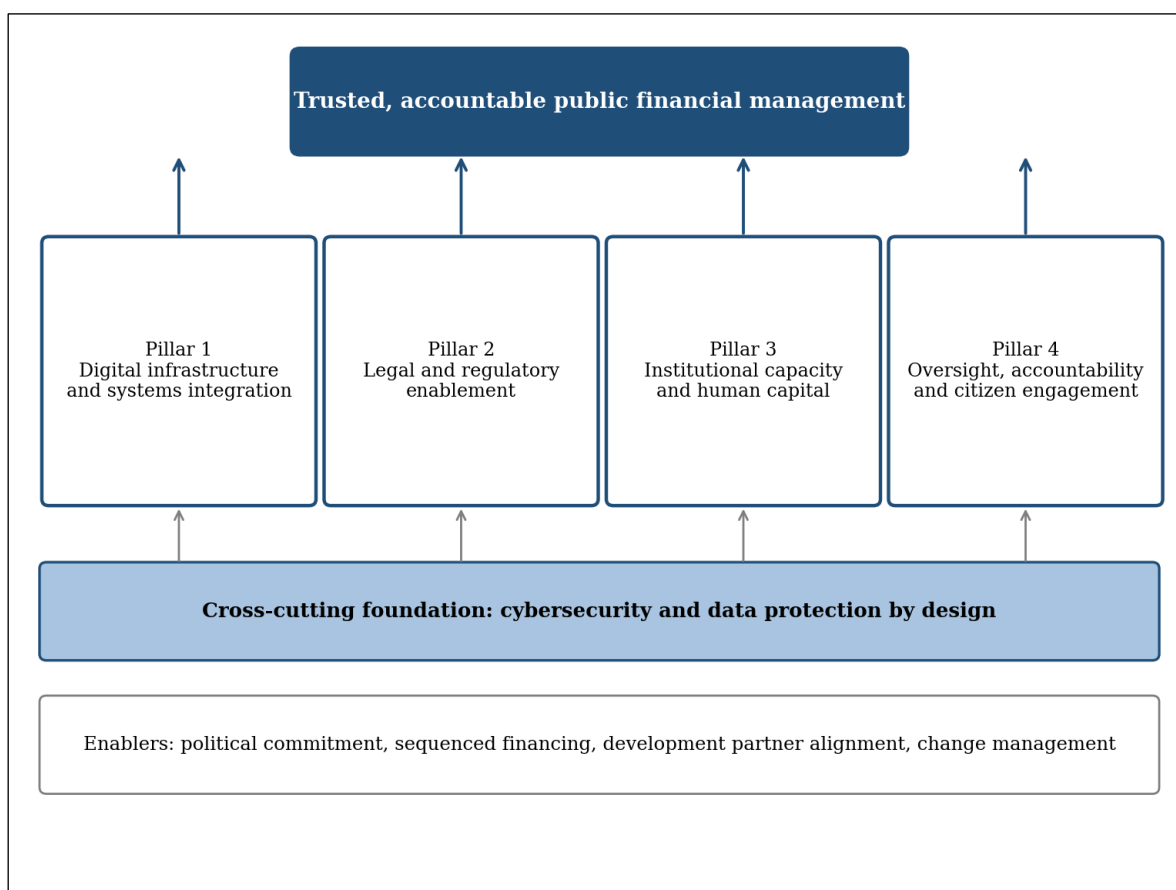


Figure 5: The Integrated Digital Governance Framework: four pillars on a cross-cutting foundation of cyber-security and data protection by design

Pillar 1, digital infrastructure and systems integration, completes the IFMIS estate, replaces file-based exchange with a governed interoperability layer implementing the PFM Interoperability Framework, and builds the data warehouse and analytics capability Cabinet has endorsed, anchored on the NCRA identity registry as the resolution point for every person-linked record. Emerging technologies enter here on strict subsidiarity: cloud services where sovereign hosting and the data protection statute permit, because

they buy resilience Sierra Leone cannot yet build domestically; analytics and machine-learning methods for anomaly detection in payroll and payments, where the data warehouse creates the substrate; and distributed-ledger techniques only for the narrow uses where an append-only shared record among mutually distrusting institutions genuinely beats a governed database, audit-trail integrity being the plausible candidate, not the general ledger itself. The comparative record of blockchain pilots in government finance is a record mostly of abandoned pilots, and Sierra Leone’s scarce engineering capacity should not be spent relearning it.

Pillar 2, legal and regulatory enablement, carries the PFM Act revision (electronic records, mandatory data sharing duties, sanctions for override abuse), the enactment and commencement of the Data Protection and Right to Access Information Act, subsidiary instruments defining data standards and interface obligations, and the classification exercise of Section 5.3 that draws the access-privacy line dataset by dataset. Pillar 3 confronts the human constraint directly: a professionalised cadre of government accountants progressing towards accrual IPSAS, a public service ICT and security career stream competitive enough to retain scarce skills, and the change management that the Technology Acceptance Model shows determines adoption. Pillar 4 wires the oversight institutions into the architecture as first-class users: the audit recommendation platform with ACC access, SL-ADS, parliamentary access to execution data, and citizen-facing transparency portals that publish what the classification exercise deems public, because published data is the cheapest audit function a poor state can buy.

The pillars are not independent work-streams to be assigned to separate committees; the framework’s causal claims run across them, and stating those claims explicitly is what distinguishes a framework from a diagram. Pillar 1 without Pillar 2 produces integration without authority, an exchange layer that agencies may lawfully ignore, which is the Ghanaian and Nigerian experience of interoperability initiatives that plateaued at pilot scale. Pillar 2 without Pillar 1 produces the opposite pathology, familiar from first-generation African data protection regimes: rights on paper that no architecture enforces, so compliance becomes a filing exercise. Pillars 1 and 2 without Pillar 3 produce the classic donor artefact, a system and a statute that decay together as the trained cohort disperses, and the resource-based reading of Sierra Leone’s IFMIS decade shows that the durable asset was always the people. And the first three pillars without the fourth produce something more dangerous than failure: an efficient, well-governed data machine whose outputs nobody outside the executive can interrogate, which would modernise the state’s capacity without modernising its accountability, inverting the purpose of the entire enterprise. The foundation interacts with all four: security failures destroy the trust on which Pillar 4’s citizen engagement depends, and data protection failures give every reluctant agency in Pillar 1 a respectable reason to withhold connection. The framework therefore prescribes joint governance, the interagency council of Section 8, precisely because its logic cannot be executed in

institutional silos; a siloed implementation of an anti-silo framework would be its own refutation.

6.2 Implementation Roadmap

Sequencing is where strategic frameworks for low-capacity states usually fail, by front-loading ambition that the institutions cannot absorb. The roadmap below is disciplined by three rules drawn from the problem-driven iterative adaptation literature (Andrews et al., 2017): every phase must deliver a visible win that builds the coalition for the next; nothing enters a phase whose institutional precondition was not met in the previous one; and measurement baselines precede investment cases. The phases align deliberately with the financing calendar, the IMF Extended Credit Facility reviews, the AfDB policy-based operation’s 2026 reform measures, and the preparation of the World Bank’s proposed Strengthening Accountability and Local Oversight for the New Generation Public Financial Management Project, because in Sierra Leone reform momentum and disbursement momentum are the same phenomenon.

Phase 1 (0 to 18 months) concentrates on completion and legal foundation: finish the IFMIS rollout to the remaining MDAs, enact and commence the Data Protection and Right to Access Information Act with the transformed authority minimally staffed, deploy the audit recommendation tracking platform with the ACC connection live, sign the ACC-GAC memorandum, and, crucially, measure the baselines, override volumes, reconciliation lags, payroll-pension mismatch rates, that Phase 2’s business case requires. A single high-visibility interoperability pilot belongs here: continuous payroll-NaSSIT-NCRA reconciliation, chosen because it attacks the exact leakage the Financial Secretary named and can show savings within the phase.

Table 6: Phase 1 priority actions (0 to 18 months)

Action	Lead responsibility	Success metric
Complete IFMIS rollout to remaining MDAs	AGD with MoF	All budget-funded MDAs transacting on IFMIS
Enact and commence Data Protection and RAI Act	Ministry of Information and Civic Education; Parliament	Act in force; authority board and core staff appointed
Deploy audit recommendation tracking platform	GAC with ASSL; ACC access	Platform live; 100% of new recommendations tracked
Sign and operationalize ACC-GAC MoU	ACC, GAC	MoU signed; joint follow-up protocol in use
Payroll-pension-identity reconciliation pilot	AGD, HRMO, NaSSIT, NCRA	Continuous matching live; mismatch register published internally
Baseline measurement programme	MoF (DFMST)	Override, reconciliation-lag and mismatch baselines documented
Security uplift of EFT endpoints and IFMIS estate	AGD, BSL, NCSCC	Independent security assessment completed; critical findings closed

Phase 2 (18 to 36 months) builds the architecture on those foundations: implement the PFM Interoperability Framework as a governed exchange layer across the core systems mapped in Figure 3; commence the transition to accrual-basis IPSAS with asset registers and a published migration path; and operationalize the unified data protection authority as a working regulator, completing the dataset classification exercise and issuing the financial-sector and government data protocols the statute mandates. The e-GP-to-IFMIS commitment match and the ITAS-supplier cross-match enter service in this phase, converting the digital accountability chain of Section 3.3 from aspiration to plumbing.

Table 7: Phase 2 priority actions (18 to 36 months)

Action	Lead responsibility	Success metric
Deploy PFM interoperability exchange layer	MoF (DFMST) with participating institutions	Priority interfaces live: payroll, pensions, identity, e-GP, ITAS, audit
Commence accrual IPSAS transition	AGD with CSAAG and ICASL	Asset register programme underway; migration path published
Operationalize unified data authority	Transformed RAIC successor	Classification of core PFM datasets completed; first enforcement actions
e-GP to IFMIS commitment matching	NPPA, AGD	Awards auto-matched to commitments; exceptions reported monthly
Government data warehouse, first release	MoF (DFMST)	Warehouse fed by interfaces, not manual returns, for core datasets
Security operations capability	NCSCC with AGD and BSL	Monitoring of PFM core live; incident response tested

Phase 3 (36 to 60 months) is the integration horizon: full digital integration across PFM systems, advanced analytics and business intelligence in routine use for budget preparation, wage bill management and fraud detection, citizen-facing transparency portals publishing classified-as-public data by default, and the accrual transition reaching consolidated statements. By this phase the reform’s measure of success shifts from systems delivered to behaviour changed: overrides rare and individually explained, audit recommendations implemented on pain of visible escalation, and the next PEFA assessment testing whether the middle of the indicator distribution finally moves.

Table 8: Phase 3 priority actions (36 to 60 months)

Action	Lead responsibility	Success metric
Full systems integration across PFM estate	MoF (DFMST)	Manual inter-agency data transfers eliminated for core processes
Analytics and BI in routine fiscal management	MoF, AGD	Wage bill, cash and fraud analytics in monthly management use
Citizen transparency portals	MoF with unified data authority	Budget, procurement and audit data published by default
Consolidated accrual-basis reporting	AGD	First consolidated statements on accrual migration path

Institutionalised capacity programme	HRMO, ICASL, universities	Accredited PFM-digital career streams operating
Independent evaluation and next PEFA	MoF with partners	Majority of previously static indicators improved

6.3 Financing and Partnership Strategy

The financing logic follows the sequencing logic. Phase 1 is largely fundable within existing envelopes: the ECF programme’s structural benchmarks can carry the legislative and baseline actions, the AfDB operation’s 2026 reform measures align naturally with enactment and rollout completion, and the proposed World Bank accountability operation is the natural home for the oversight platforms and the interoperability layer’s core investment. Three principles should govern the partnership: first, one architecture, many financiers, partners fund components of the single interoperability design rather than systems of their own choosing, reversing the pattern that produced the fragmentation; second, recurrent cost realism, every component enters service with its maintenance, licensing and staffing provided in the domestic budget, because the graveyard of African government systems is filled with platforms that died at the end of their project financing; third, capability purchase over capacity substitution, technical assistance contracted to build the DFMST, AGD and authority teams rather than to perform their functions, with public-private participation confined to delivery roles under government architectural control. Domestic resource mobilisation is not decorative here: a government asking citizens to fund data systems about themselves has an additional reason to make the data protection authority visibly independent and the transparency portals visibly useful.

The instruments themselves reward closer specification. The ECF arrangement is the programme’s macro-fiscal spine, and its review calendar, the December 2025 disbursement of US\$79.8 million followed by a third disbursement in 2026, gives the government roughly semi-annual moments at which reform commitments become verifiable; the discipline of Section 6.2’s roadmap is designed to place a completed, evidencable action at each such moment, because programmes accumulate credibility transaction by transaction. The AfDB policy-based operation carries a different kind of leverage: after a three-year suspension of budget support, the US\$11.5 million attached to the 2026 reform measures is less significant as financing than as a signal that the Bank’s confidence has been re-established, and the measures should therefore be chosen from the roadmap’s Phase 1 actions that are fully within government control, enactment, commencement, coverage completion, rather than from outcomes that depend on multi-year behaviour change. The proposed World Bank operation on accountability and local oversight is the natural investment vehicle for the durable assets, the exchange layer, the oversight platforms, the local council connectivity that no other financier will touch, and its preparation phase is the right moment to bind all three institutions to the single-architecture principle through a jointly endorsed programme document rather than three parallel results frameworks. On public-private participation, the boundary worth

drawing in advance is between delivery and control: systems integration, adapter engineering, security operations support and data-centre services are legitimately contractible; architectural authority, data ownership, the classification of datasets and the operation of the exchange layer’s governance are not, and a concession that blurs that boundary would trade a capacity gap today for a sovereignty problem for a generation.

7. International Comparative Analysis

7.1 Regional Context

Sierra Leone’s position among African peers is easily misread in both directions. On core FMIS coverage, it sits behind the regional leaders: Ghana’s GIFMIS and Uganda’s IFMS reach substantially more of central government, Kenya’s IFMIS is coupled to an advanced revenue and payments ecosystem, and Cabo Verde, the small-state outlier, has run a near-fully integrated state financial system (SIGOF) for years, demonstrating that scale is not the binding constraint. Nigeria’s experience runs the other way: GIFMIS, the TSA and the Integrated Payroll and Personnel Information System (IPPIS) payroll platform were deployed at great scale, and the TSA consolidation famously recovered large idle balances, yet payroll integrity scandals persisted for years afterwards because the payroll, identity and pension registers remained imperfectly reconciled, precisely the pathology Sierra Leone’s Financial Secretary has diagnosed at home. Figure 6 positions the group on the two dimensions this article distinguishes: core system coverage and interoperability with data governance. The reading is deliberately indicative rather than an index, because published measures (the World Bank’s GovTech Maturity Index, the UN E-Government Survey) blend these dimensions in ways that obscure the point at issue (World Bank, 2022; United Nations, 2024).

The instructive gap in Figure 6 is the second bar, not the first. Rwanda scores strongly there for reasons that have little to do with wealth and everything to do with governance choices: a single centre of digital authority, mandatory standards, and the early decision to anchor systems on a reliable identity registry. Sierra Leone trails on both dimensions but, and this is the comparative claim worth making, its 2025 policy turn addresses the second dimension directly at an earlier relative stage than most peers did. Ghana and Kenya built extensive systems first and are retrofitting data governance under the pressure of enforcement actions and breach incidents; Sierra Leone has the chance, precisely because its integration is unbuilt, to construct the exchange layer and the protection regime as one artefact.

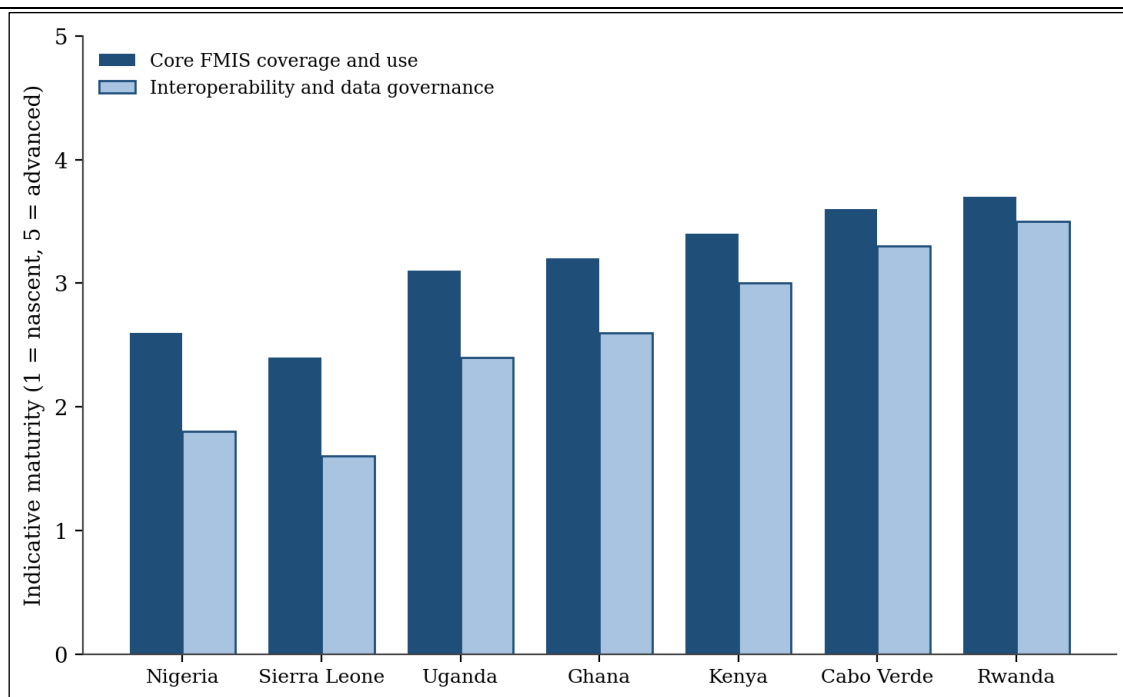


Figure 6: Indicative positioning of Sierra Leone and regional comparators on core FMIS coverage and on interoperability and data governance. Positions are the author’s characterisation for analytical purposes, not index scores

7.2 Global Lessons

Three bodies of international experience bear directly on the framework. The first is the FMIS record itself: the World Bank’s synthesis of decades of FMIS lending finds that the projects which endure are those that secured comprehensive use before functional sophistication, held a single architectural authority against vendor and donor fragmentation, and budgeted recurrent costs from the outset (Dener et al., 2011; Hashim, 2014). Sierra Leone’s roadmap encodes all three lessons, most visibly in the Phase 1 insistence on completing coverage and closing the override economy before the analytics ambitions of Phase 3.

The second is the interoperability experience of the digital-government leaders. Estonia’s X-Road demonstrates the architectural pattern, a governed exchange layer with authenticated, logged interfaces, but the transferable lesson is institutional: X-Road works because participation is mandatory, standards are law, and every query is attributable. India’s identity-anchored direct benefit transfer architecture demonstrates the fiscal payoff of register reconciliation at scale, with official estimates of cumulative leakage savings in the tens of billions of dollars across schemes, and South Korea’s dBrain shows a treasury system conceived from the start as an integrated data platform rather than a transaction processor. None of these architectures is importable wholesale; what travel is the design grammar, mandatory participation, identity anchoring, logged access, and the confirmation that the returns accrue at the joins between systems, never inside them.

Organisation for Economic Co-operation and Development (OECD) experience adds a fourth strand that is easy to overlook from Freetown because it concerns direction rather than distance. The digital-era treasuries of the OECD are converging on a common operating pattern: spending controls embedded in systems rather than exercised through prior approvals, near-real-time fiscal data replacing periodic returns, open publication of budget and procurement data as the default, and privacy regulation applied to the state’s own data holdings with the same force as to the private sector’s (OECD, 2023). None of this describes where those countries began; it describes where thirty years of iteration took them, and the value of the pattern for Sierra Leone is that it identifies the destination against which each phase of the roadmap can be checked. Two OECD lessons translate with particular force. The first is that embedded controls change the audit function: when the system enforces the rule, the auditor’s question shifts from whether the rule was followed to whether the system’s configuration and its exceptions were governed, which is why the security and logging architecture of Section 5 is also an audit reform. The second is that transparency infrastructure only earns its cost when publication is automatic; every OECD administration that relied on manual publication processes saw them decay, and Sierra Leone’s portals should therefore be fed by the exchange layer itself, not by officials remembering to upload.

The third body of experience concerns IPSAS transitions in developing countries. The cross-country record shows cash-to-accrual journeys of a decade or more even in well-resourced administrations, with the recurrent failure mode being an announced accrual adoption unaccompanied by asset registers, valuation capacity or trained staff, producing statements that assert a basis they cannot substantiate (IFAC & CIPFA, 2021). Sierra Leone’s disciplined use of Cash Basis IPSAS with standardised GPFs formats is, against that record, a strength to be extended on the deliberate path Section 6 sets out, not an embarrassment to be leapt over.

7.3 Sierra Leone’s Distinctive Contributions

Comparative analysis usually casts countries like Sierra Leone as importers of practice. The record assembled here supports a different reading: on at least three design choices, Sierra Leone is exporting. Table 9 summarises.

Table 9: Sierra Leone’s distinctive PFM reform designs and their wider significance

Design choice	What is distinctive	Why it matters beyond Sierra Leone
Unified dual-mandate data authority	Access to information and data protection fused in one statute and one regulator	Offers a coherent jurisprudence of the access-privacy line that separate-regulator models generate by dispute; directly suited to PFM datasets that straddle the line
Anti-corruption wired into digital PFM	ACC direct access to real-time audit recommendation tracking; digital asset declarations (SL-ADS) built with DSTI	Converts audit follow-up, the weakest link in most African accountability chains, from correspondence into observable system state

Interoperability-first reform turn	Consolidated interagency interoperability framework adopted before, not after, full systems build-out	Demonstrates a sequencing option for late-integrating states: build the exchange layer and the protection regime as one artefact
Sustained PEFA discipline	Five assessments across fifteen years informing successive strategies	A model of externally benchmarked iteration few low-income countries have maintained

The claim is not that these designs are proven; two of the four are commitments rather than accomplishments, and Section 8 treats their failure modes seriously. The claim is that they are original responses to problems the standard reform template does not solve, and that the international PFM community, which has documented the template’s limits exhaustively (Andrews, 2013; Schick, 1998), has an interest in watching whether they work. A landlocked view of reform transfer, from Washington and Brussels outward, has always been empirically wrong; Sierra Leone’s current programme is a live case of institutional innovation moving in the other direction.

8. Challenges, Risks and Mitigation Strategies

8.1 Technical Challenges

The technical risks are the familiar ones, and familiarity should sharpen rather than dull attention to them. Connectivity remains the hardest physical constraint: an exchange layer is only as available as the links that reach it and MDA sites outside Freetown, local councils above all, operate on power and bandwidth that fail routinely. The mitigation is architectural honesty, designing for intermittent connectivity with store-and-forward interfaces and local resilience, rather than assuming away the grid. Legacy integration is the second technical front: IFMIS, ITAS, T24, NaSSIT’s systems and the NCRA registry were built on different platforms by different vendors under different contracts, and the practical work of interoperability is less about the exchange layer itself than about building and maintaining the adapters at each system’s edge, work that is unglamorous, recurrent and chronically under-budgeted. The EFT channel illustrates a third risk: transitional arrangements harden into permanent ones. Every interim file-based interface tolerated during migration must carry an explicit retirement date, or the programme will end with the old lattice running quietly beneath the new layer.

8.2 Institutional Challenges

The institutional risks are larger. Capacity is the first: the DFMST, the AGD, the NCSCC and the transformed data authority must collectively field skills, integration engineering, security operations, data protection law, accrual accounting, that the domestic labour market produces in small numbers and the international market prices beyond public salaries. The mitigations are the Pillar 3 measures: credible career streams, partnership with ICASL and the universities, and technical assistance contracted to transfer capability

rather than substitute for it. Resistance is the second institutional risk, and it will be rational rather than obstinate: interoperability strips discretion from every actor who currently benefits from reconciliation lag, and the December 2025 warning is precise about the existence of such actors. Resistance will therefore present as technicality, data quality concerns, legal doubts, sequencing objections, and the programme’s governance must be able to distinguish genuine caution from strategic delay.

Change management is the third institutional front, and it is where the Technology Acceptance Model earns its place in the framework rather than in the literature review. The users who will make or break the integrated architecture are not the senior officials who attend the workshops; they are the accountants, payroll clerks, procurement officers and records staff in several dozen MDAs whose daily work the new interfaces will change, and whose current workarounds, the spreadsheet kept beside the system, the transaction held for batch entry, the override requested as routine, are rational adaptations to systems that were slower than the job. If the integrated processes are harder to use than the workarounds they replace, they will be worked around, whatever the statute says, because that is what the entire history of information systems in low-capacity administration teaches (Heeks, 2002; Davis, 1989). The practical programme this implies is unheroic: user involvement in interface design before procurement rather than training after it, process simplification as a design objective with equal standing to control, help-desk and super-user structures resourced as permanent establishment, and a feedback channel through which front-line staff can report, without career risk, where the system and the job diverge. The reform’s most reliable early-warning indicator will not be found in any dashboard; it will be the reappearance of the parallel spreadsheet, and the programme should treat everyone it finds as a design finding rather than a disciplinary matter. Table 10 assembles the principal risks.

Table 10: Risk assessment matrix

Risk	Likelihood	Impact	Principal mitigation
Connectivity and power failures degrade integrated operations	High	Medium	Offline-tolerant design; store-and-forward interfaces; site resilience investment
Legacy adapter build and maintenance under-resourced	High	High	Adapter work costed and staffed as recurrent, not project, expenditure
Skills attrition from key technical units	High	High	Career streams, retention premiums, structured TA with transfer obligations
Institutional resistance disguised as technical objection	Medium-High	High	Interoperability duties in law; public interface scorecard; political sponsorship at Cabinet level
Data authority under-funded or captured	Medium	Very high	Statutory funding floor; transparent appointments; published enforcement reporting

Cyber incident against integrated PFM core	Medium	Very high	Security by design; NCSCC monitoring; tested recovery; segmentation of the exchange layer
Political transition stalls the programme	Medium	High	Cross-party parliamentary anchoring; embedding in statute and IMF/World Bank/AfDB frameworks
Donor fragmentation re-emerges around new systems	Medium	Medium-High	Single architecture governance; partners fund components, not parallel systems
Accrual transition announced before substantiated	Medium	Medium	Migration path with published preconditions; CSAAG gatekeeping
Privacy failure erodes citizen legitimacy	Low-Medium	Very high	Dataset classification; purpose-bound access enforced technically; authority independence

8.3 Political and Governance Risks

Two political risks tower over the rest. The first is sustainability across electoral transitions. Sierra Leone’s reform strategies have each spanned a political cycle, and the 2018 transition demonstrated both that reform can survive a change of government and that its emphasis will be rewritten by the incoming one. The programme’s defence is depth of embedding: duties written into the revised PFM Act and the data protection statute, financing conditionality across the IMF, World Bank and AfDB frameworks that no incoming government can costlessly discard, and, more durably, constituencies inside and outside the state, the ASSL, the ACC, the accountancy profession, civil society users of the transparency portals, whose interests the architecture serves. Figure 7 maps the stakeholder field; the strategic task it depicts is to move the high-interest, low-influence actors, civil society, the press and the general public, into effective coalition with the high-influence institutions whose commitment fluctuates.

The second political risk is the concentration-of-power problem inherent in the programme’s own success. An integrated financial data architecture plus a unified information authority is an instrument of accountability in one set of hands and of control in another. The mitigations are the classical ones: independence guarantees, transparency of the authority’s own operations, purpose limitation enforced in the architecture rather than merely promised in policy, parliamentary oversight of the overseers, and they deserve to be treated as first-order design requirements, because the surest way to lose public consent for data integration is a single well-publicised abuse.

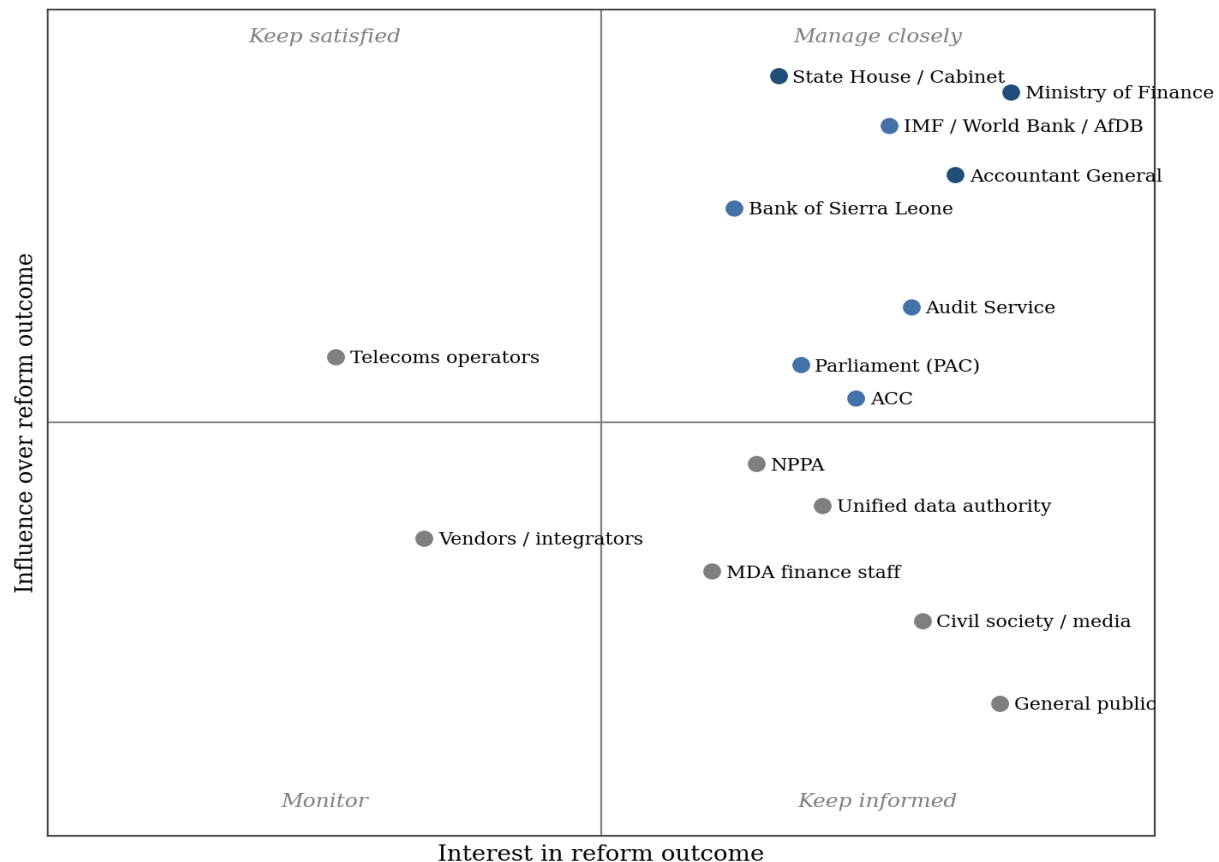


Figure 7: Stakeholder analysis for the digital PFM reform programme, mapped by interest in and influence over the reform outcome

8.4 The Mitigation Logic

Across Table 10, a common logic runs, and it is worth stating as doctrine. Every mitigation pairs an institutional instrument with a technical one: the law mandates sharing and the exchange layer logs it; the authority protects data and the architecture enforces purpose limits; the Cabinet sponsors the programme, and the scorecard makes each institution’s interface performance public. Phased implementation with early visible wins builds the coalition; continuous capacity building holds it; multi-stakeholder governance, a standing interagency council chaired at the centre of government, with the oversight institutions and, for the transparency agenda, civil society at the table, arbitrates it. Socio-technical pairing, sequenced wins and collegial governance are not three separate mitigations; they are one strategy for making reform survivable in a political environment, and the evidence of Sierra Leone’s own twenty-year record is that reforms designed this way - the PEFA cycle, the TSA - endure, while unpaired artefacts decay.

9. Conclusion and Recommendations

9.1 What the Evidence Shows

This article began with a Financial Secretary’s admission and has tried to take it as seriously as it deserves. The evidence assembled supports four findings. First, Sierra Leone’s two decades of PFM reform produced real and measurable modernisation, an IFMIS estate, a TSA, Cash Basis IPSAS reporting, digital tax, procurement and integrity platforms, and a PEFA record whose ‘A’ ratings for budget classification and transfers are earned, but the model that produced them has exhausted its returns: eight of thirty-one indicators improving across a full strategy cycle is the signature of systems outrunning institutions. Second, the binding constraint is now the seams: manual data exchange among the MoF, the AGD, the NPPA, the ASSL, the BSL, NaSSIT and NCRA degrades data quality, sustains the payroll-pension arbitrage the Financial Secretary described, and blocks the analytics ambitions the Cabinet has endorsed. Third, the government’s 2025 policy turn, the PFM Interoperability Framework roadmap and the Data Protection and Right to Access Information Act with its unified dual-mandate authority, is the correct diagnosis translated into commitments, and the dual-mandate design in particular is an institutional innovation of genuine comparative interest. Fourth, integration and protection are one problem: every step that connects Sierra Leone’s financial data multiplies both its value and its attack surface, so the security and data protection foundation is the condition of the whole enterprise, not a workstream within it.

9.2 Strategic Recommendations

For the Government of Sierra Leone, five actions carry the programme. Enact and commence the Data Protection and Right to Access Information Act, and fund the transformed authority to a statutory floor, before the interoperability layer concentrates data worth protecting. Revise the PFM Act to make inter-agency data sharing a legal duty with defined interfaces, to give electronic records unambiguous status, and to attach personal consequences to unauthorised overrides. Complete IFMIS coverage and run the payroll-pension-identity reconciliation pilot inside eighteen months, publishing the savings, because the coalition for Phase 2 will be built on Phase 1’s visible arithmetic. Hold one architecture under one governance, the interagency council with DFMST as its technical arm, and require every financier to fund components of it rather than systems beside it. And measure first: baseline the overrides, the reconciliation lags and the register mismatches now, so that this reform, unlike its predecessors, can prove what it changed. For development partners, the recommendation is a discipline as much as a commitment. The IMF’s structural benchmarks, the AfDB’s 2026 reform measures and the World Bank’s proposed accountability operation should be mutually mapped onto the single roadmap, with the interoperability layer and the data authority treated as the shared critical path. Partners should finance recurrent capability, adapter maintenance, security

operations, authority staffing, not only capital artefacts, and should accept government architectural authority as the price of coherence, because the fragmentation this article documents is partly their bequest.

For civil society, the professions and the universities, the architecture creates roles that did not previously exist. The transparency portals will be worth exactly what their users make of them: journalists and civic organisations that build the habit of interrogating published budget, procurement and audit data become the cheapest and most durable layer of the accountability system. ICASL and the universities hold the supply line for the accrual transition and the security cadre. And the data protection authority’s independence will be defended, in the end, not by its statute but by a public that has learned to regard its own data as something the state holds on trust.

9.3 Beyond Sierra Leone

The wider significance of this case lies in the question it poses to the international PFM community. The reform template that the community has exported for thirty years - systems, standards, assessments - has been implemented in Freetown with unusual persistence, and the result is a state that can classify a budget to an ‘A’ standard while a retiree’s record leaks value between two computers that have never been introduced. The next template, if the term still applies, will be built at the joins: exchange layers rather than applications, data governance rather than data entry, authorities that rule on who may see a record rather than clerks who decide by default. Sierra Leone, by adopting an interoperability-first roadmap and fusing transparency and privacy in a single regulator, has committed itself earlier and more coherently to that next template than most of its peers, richer ones included. Whether it succeeds will depend on the unglamorous variables this article has laboured: adapters maintained, baselines measured, careers built, an authority funded, a Cabinet that keeps chairing the council after the communiqués stop. If it does succeed, the country that once borrowed every element of its PFM system will have something to lend: a working demonstration that, for the digital state now being built across the Global South, financial accountability and data protection are not competing reforms but the same reform, and that a small, fiscally constrained country can design that reform for itself.

Creative Commons License Statement

This research work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit <https://creativecommons.org/licenses/by-nc-nd/4.0>. To view the complete legal code, visit <https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode.en>. Under the terms of this license, members of the community may copy, distribute, and transmit the article, provided that proper, prominent, and unambiguous attribution is given to the authors, and the material is not used for commercial purposes or modified in any way. Reuse is

only allowed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.

Conflict of Interest Statement

The authors declare no conflicts of interest. None of the authors has received financial assistance, employment, consultancy engagements, shareholdings, honoraria, or remunerated expert testimony from any organisation holding a financial stake in the subject of this study. Every source of funding is acknowledged in the acknowledgements section.

About the Authors

Joseph Momoh Conteh is a PhD candidate in Theoretical Economics at the Institute of South-South Cooperation and Development (ISSCAD), Peking University, Beijing, China (<https://www.isscad.pku.edu.cn/>). He is the ICT/Administrative Director at the Justice Sector Coordination Office (<https://jsco.gov.sl>), where he has served for 16 years. His research addresses national development, spanning aid and development, international cooperation, trade, information and communication technology for development, administration, policy development, and finance. His doctoral work is directed at advancing economic theory while generating practical insights capable of informing sustainable development policy throughout the Global South. His academic profiles:

Academia.edu: <https://ufl.academia.edu/JosephConteh>,

ORCID: <https://orcid.org/0009-0004-1690-508X>

ResearchGate: https://www.researchgate.net/profile/Joseph-Conteh-6?ev=hdr_xprf.

Musa Abdullah Kargbo, BSc, MFA, FCCA, FCA(SL), is a Chartered Accountant with more than fifteen years in banking and government service. As Head of Finance at the Ministry of Information and Civic Education, he oversees budgets, financial reporting, treasury and compliance. A Fellow of ACCA and of the Institute of Chartered Accountants of Sierra Leone, he is reading for an MPhil in Accounting on foreign direct investment in Sierra Leone and writes on public finance, governance and development.

Abdul Rahman N’Jai is an Associate Lecturer at Njala University and Part-Time Lecturer in the Faculty of Accounting and Finance, Institute of Public Administration and Management (IPAM). He teaches undergraduate and postgraduate courses in Accounting and Finance.

Mohamed Sahid Sesay, FCCA, is a finance and risk management professional with over 24 years of experience in financial accounting, auditing, compliance, strategic management, and enterprise risk management. He currently serves as Senior Manager for Enterprise Risk Management at Rokel Commercial Bank Sierra Leone Limited. A Fellow of the Association of Chartered Certified Accountants (ACCA-UK) and the Institute of Chartered Accountants of Sierra Leone, his research interests include financial governance, banking regulation, internal controls, and corporate strategy.

References

- Anderson, R. (2020). *Security engineering: A guide to building dependable distributed systems* (3rd ed.). Wiley. Retrieved from <https://onlinelibrary.wiley.com/doi/book/10.1002/9781119644682>
- Andrews, M. (2013). *The limits of institutional reform in development: Changing rules for realistic solutions*. Cambridge University Press. <https://doi.org/10.1017/CBO9781139060974>
- Andrews, M., Pritchett, L., & Woolcock, M. (2017). *Building state capability: Evidence, analysis, action*. Oxford University Press. <https://doi.org/10.1093/acprof:oso/9780198747482.001.0001>
- Barney, J. (1991). Firm resources and sustained competitive advantage. *Journal of Management*, 17(1), 99–120. <https://doi.org/10.1177/014920639101700108>
- Cangiano, M., Curristine, T., & Lazare, M. (Eds.). (2013). *Public financial management and its emerging architecture*. International Monetary Fund. <https://doi.org/10.5089/9781475531091.071>
- COSO (Committee of Sponsoring Organizations of the Treadway Commission). (2017). *Enterprise risk management: Integrating with strategy and performance*. COSO. Retrieved from https://books.google.ro/books/about/Enterprise_Risk_Management_Integrating_w.html?id=U28O0QEACAAJ&redir_esc=y
- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319–340. <https://doi.org/10.2307/249008>
- Dener, C., Watkins, J., & Dorotinsky, W. L. (2011). *Financial management information systems: 25 years of World Bank experience on what works and what doesn't* (World Bank Study). World Bank. <https://doi.org/10.1596/978-0-8213-8750-4>
- Diamond, J., & Khemani, P. (2006). Introducing financial management information systems in developing countries. *OECD Journal on Budgeting*, 5(3), 97–132. <https://doi.org/10.1787/budget-v5-art17-en>
- DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review*, 48(2), 147–160. <https://doi.org/10.2307/2095101>
- European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation). *Official Journal of the European Union*, L119, 1–88.
- Government of Ghana. (2012). *Data Protection Act, 2012 (Act 843)*. Government Printer.
- Government of Kenya. (2019). *The Data Protection Act, No. 24 of 2019*. Government Printer.
- Government of Nigeria. (2023). *Nigeria Data Protection Act, 2023*. Federal Government Printer.

- Government of Sierra Leone. (2016). *Public Financial Management Act, 2016*. Government Printing Department.
- Government of Sierra Leone. (2021). *Cybersecurity and Crime Act, 2021*. Government Printing Department.
- Government of Sierra Leone. (2025). *Communications of the Ministry of Finance and the Ministry of Information and Civic Education on PFM interoperability, payroll and pension data fragmentation, and the Data Protection and Right to Access Information Bill* [Official statements and workshop proceedings, July–December 2025; to be verified against gazetted texts and official releases].
- Hashim, A. (2014). *A handbook on financial management information systems for government: A practitioner’s guide for setting reform priorities, systems design, and implementation* (Africa Operations Services Series). World Bank. Retrieved from <https://documents.worldbank.org/en/publication/documents-reports/documentdetail/147241467987856662>
- Heeks, R. (2002). Information systems and developing countries: Failure, success, and local improvisations. *The Information Society*, 18(2), 101–112. <https://doi.org/10.1080/01972240290075039>
- Hood, C. (1991). A public management for all seasons? *Public Administration*, 69(1), 3–19. <https://doi.org/10.1111/j.1467-9299.1991.tb00779.x>
- IFAC & CIPFA (International Federation of Accountants & Chartered Institute of Public Finance and Accountancy). (2021). *International public sector financial accountability index: 2021 status report*. IFAC. Retrieved from <https://www.ifac.org/knowledge-gateway/public-sector/publications/international-public-sector-financial-accountability-index-2021-status-report>
- International Monetary Fund. (2025a). *Sierra Leone: Governance and corruption diagnostic assessment* [Country report; details to be verified]. IMF. Retrieved from <https://www.imf.org/en/publications/technical-assistance-reports/issues/2025/12/10/sierra-leone-technical-assistance-report-governance-and-corruption-diagnostic-572467>
- International Monetary Fund. (2025b). *IMF Executive Board completes the first and second reviews of the Extended Credit Facility arrangement with Sierra Leone* [Press release, December 2025; to be verified]. IMF. Retrieved from <https://www.imf.org/en/news/articles/2025/12/16/pr-25425-sierra-leone-imf-completes-1st-and-2nd-reviews-arrangement-under-ecf>
- INTERPOL. (2024). *African cyberthreat assessment report*. INTERPOL. Retrieved from <https://afripol.africa-union.org/resources/interpol-african-cyberthreat-assessment-report-2024>
- IPSASB (International Public Sector Accounting Standards Board). (2017). *Financial reporting under the cash basis of accounting* (revised). IFAC.
- IPSASB (International Public Sector Accounting Standards Board). (2022). *Handbook of international public sector accounting pronouncements*. IFAC.

- ITU (International Telecommunication Union). (2021). *Global Cybersecurity Index 2020*. ITU. Retrieved from <https://www.itu.int/epublications/ru/publication/d-str-gci.01-2021-htm-e>
- Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics*, 3(4), 305–360. [https://doi.org/10.1016/0304-405X\(76\)90026-X](https://doi.org/10.1016/0304-405X(76)90026-X)
- Meyer, J. W., & Rowan, B. (1977). Institutionalized organizations: Formal structure as myth and ceremony. *American Journal of Sociology*, 83(2), 340–363. <https://doi.org/10.1086/226550>
- Moore, M. H. (1995). *Creating public value: Strategic management in government*. Harvard University Press.
- National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29). U.S. Department of Commerce. <https://doi.org/10.6028/NIST.CSWP.29>
- OECD (Organisation for Economic Co-operation and Development). (2023). *2023 OECD Digital Government Index* (OECD Public Governance Policy Papers). OECD Publishing.
- Osborne, S. P. (2006). The new public governance? *Public Management Review*, 8(3), 377–387. <https://doi.org/10.1080/14719030600853022>
- PEFA Secretariat. (2023). *Sierra Leone: Public expenditure and financial accountability (PEFA) performance assessment report, 2021–2022* [Report details to be verified]. PEFA Secretariat. Retrieved from <https://www.pefa.org/node/5185>
- Rogers, E. M. (2003). *Diffusion of innovations* (5th ed.). Free Press. Retrieved from <https://doi.org/10.4324/9780203710753-35>
- Schick, A. (1998). Why most developing countries should not try New Zealand’s reforms. *The World Bank Research Observer*, 13(1), 123–131. <https://doi.org/10.1093/wbro/13.1.123>
- Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic Management Journal*, 18(7), 509–533. [https://doi.org/10.1002/\(SICI\)1097-0266\(199708\)18:7<509::AID-SMJ882>3.0.CO;2-Z](https://doi.org/10.1002/(SICI)1097-0266(199708)18:7<509::AID-SMJ882>3.0.CO;2-Z)
- United Nations. (2024). *United Nations e-government survey 2024*. UN Department of Economic and Social Affairs. Retrieved from <https://publicadministration.un.org/egovkb/en-us/reports/un-e-government-survey-2024>
- World Bank. (2022). *GovTech maturity index: The state of public sector digital transformation* World Bank. Retrieved from <https://documents.worldbank.org/en/publication/documents-reports/documentdetail/298661631773566870>