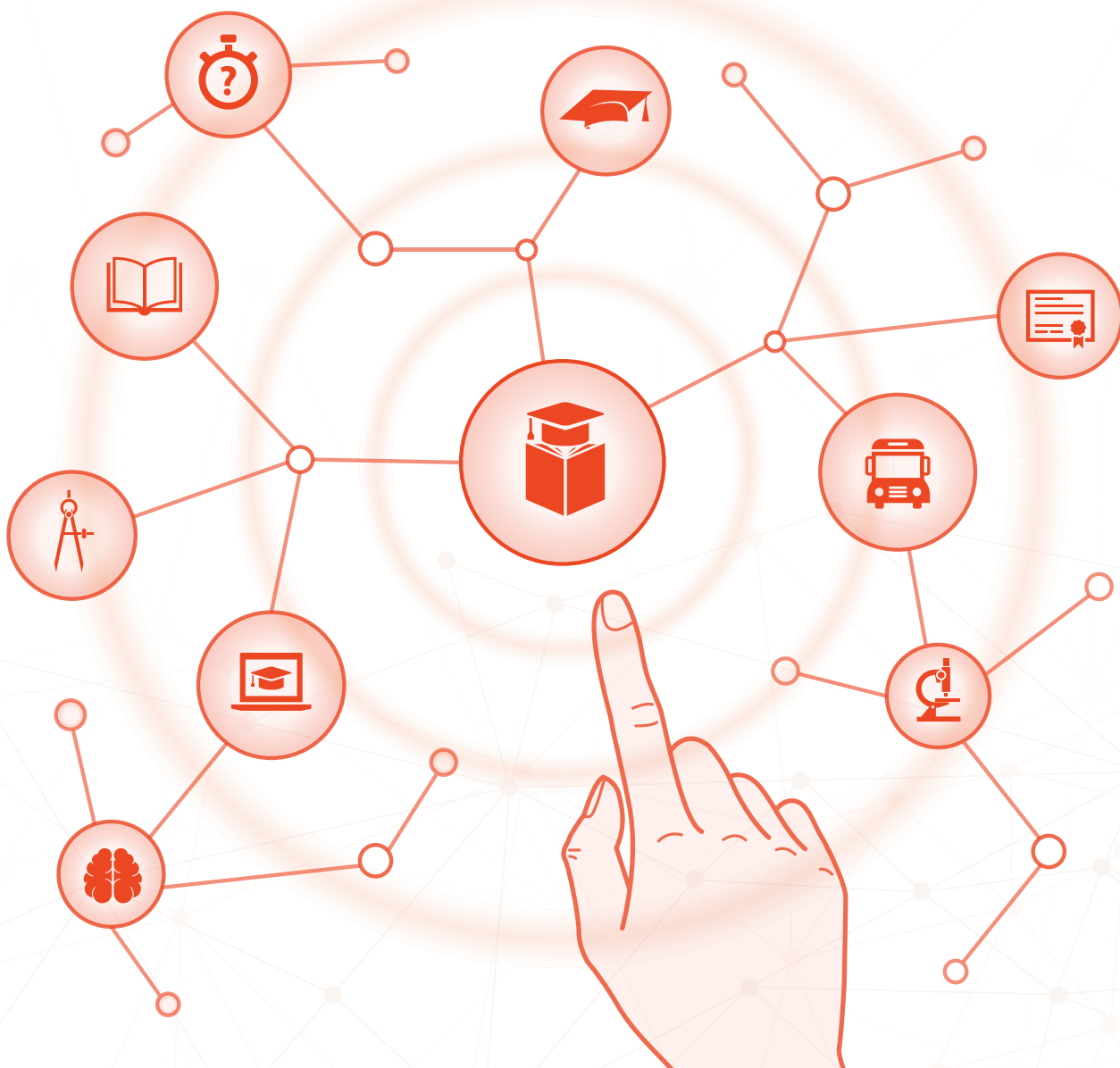




e-Readiness Assessment of Somali Higher Education Institutions 2026

Executive Summary Report



Contents

List of Abbreviations.....	iii
Executive Summary	iv
1 Introduction and Context	6
1.1 Why Readiness Matters.....	7
1.2 Why a System Approach.....	7
2 Scope and Approach.....	8
2.1 Scope.....	8
2.2 Coverage	8
2.3 Data sources, coverage and limitations	9
3 Readiness Tiers	10
3.1 How to Use Tiers	10
3.2 Tier Definitions	11
3.3 Gating Conditions for Progression.....	11
3.4 National Distribution Across Tiers	12
4 Key Findings.....	13
4.1 Connectivity Adequacy and Reliability.....	13
4.2 Financial Sustainability	15
4.3 Operational Capacity and Service Management	16
4.4 Core systems and Integration.....	17
4.5 Security and Continuity.....	19
4.6 Governance and Decision Pathways	21
5 Implications by Tier.....	23
5.1 What Each Tier Enables	23
5.2 How Institutions Progress	24
5.3 Targeting Support by Tier.....	25
6 Recommendations and Sequencing	18
6.1 Priority Actions (0–6 months).....	25
6.2 Scaling Actions (6–18 months).....	26
6.3 Consolidation Actions (18–36 months).....	20
7 Delivery and Financing	21

7.1	SomaliREN as a Delivery Platform	21
7.2	EARDIP as a Catalytic Window	21
7.3	Sustainability Principles	22
8	Implementation	23
8.1	Roles and Responsibilities	31
8.2	Milestones and Monitoring Cadence	32

List of Abbreviations

Abbreviation	Meaning / Expansion
AUP	Acceptable Use Policy
CapEx	Capital expenditure
EA-RDIP	Eastern Africa Regional Digital Integration Project
ERP	Enterprise Resource Planning
FGS	Federal Government of Somalia
FMS	Federal Member States
HEI	Higher Education Institution (plural: HEIs)
HRIS	Human Resources Information System
ICT	Information and Communication Technology
ICT Policy	Information and Communication Technology Policy
ISP	Internet Service Provider
IT	Information Technology
ITU	International Telecommunication Union
KII	Key Informant Interview
LAN	Local Area Network
LMS	Learning Management System
MoCT	Ministry of Communications and Technology
MoECHE	Ministry of Education, Culture and Higher Education
NOC	Network Operations Centre
NREN	National Research and Education Network (plural: NRENs)
OpEx	Operational expenditure
PIU	Project Implementation Unit
PPP	PublicPrivate Partnership
QA	Quality assurance
QoS	Quality of Service

Executive Summary

This policy note presents the findings of the SomaliREN Higher Education E-Readiness Assessment, translating them into a staged, decision-oriented pathway to strengthen digital service delivery across Somalia's higher education sector. The assessment establishes an institutional baseline of the conditions that enable, or constrain, the reliable operation and long-term sustainability of digital services that support core academic and administrative functions. It does not measure individual digital skills or student access, nor does it rank institutions.

The assessment targeted 55 institutions and received responses from 50 through a structured institutional survey primarily administered to ICT leadership. The findings were analysed across six domains: **infrastructure and systems; human resources and capacity; governance and planning; core digital systems; budgeting and financial sustainability; and security and risk management**. The results are synthesised through a four-tier readiness framework intended as a staging and sequencing tool, to inform realistic policy, investment and partnership decisions.

Readiness tiers and what they imply.

Participating institutions are distributed across **Tiers 1 to 3**, with none at Tier 4. Tier 4 is retained as an aspirational benchmark aligned with good practice. Overall, readiness is uneven and often fragile: while many institutions have acquired connectivity and deployed basic systems, or established ICT units, but constraints regarding reliability and sustainability remain common. Tier placement reflects the configuration of enabling conditions—reliability, operating capacity, governance and sustainable financing—rather than institutional effort or ambition.

Binding constraints. The assessment identifies six constraints that most strongly determine whether assets translate into dependable services: (i) connectivity, which must be adequate and reliable, incurring a scale penalty as institutions grow; (ii) financial sustainability, where ICT funding is often project-based rather than covering recurring services with predictable renewals; (iii) operational capacity and service management, with weak routines for monitoring, support and documentation; (iv) fragmented and limited integration of core systems, where systems exist but are unevenly used and poorly supported; (v) security and continuity gaps, particularly where backups are not matched by recovery readiness; (vi) governance and decision pathway weaknesses, which limit standard-setting and coordinated delivery.

Strategic direction: The most persistent bottlenecks, such as high and volatile connectivity costs, limited bargaining power, duplication, inconsistent security practices and dependence on short-term funding, cannot be solved efficiently through campus-by-campus approaches. A system delivery model is required. Strengthening SomaliREN as a platform for pooled procurement and shared services could improve value for money, raise baseline quality and reduce fragmentation. EARDIP provides a time-bound opportunity to finance shared foundations and delivery capacity, such as standards, shared services, and operating capability, rather than fragmented upgrades. The recommendations are sequenced over 0–6, 6–12 and 12–18 months. Implementation will be light, with 6-monthly governance reviews and an annual tier-based progress review.



1 Introduction and Context

This policy note summarises the findings of the SomaliREN Higher Education E-Readiness Assessment, proposing actions to strengthen the delivery of digital services across Somalia’s higher education sector. It is intended for **senior government officials, higher education leaders, and development partners** who are shaping policy, investment priorities, and delivery arrangements—including decisions relating to SomaliREN and catalytic programmes, such as EARDIP. The note is designed to facilitate rapid understanding and decision-making; detailed evidence and methodological information are provided in the full report and annexes.



1.1 Why Readiness Matters

Higher education increasingly depends on reliable digital services. Connectivity, core systems and secure information management underpin admissions and registration, finance and HR management, communications and the continuity of teaching and learning. When services are dependable, institutions can improve efficiency, strengthen accountability, expand access to learning resources, support research collaboration, and develop skills for national development. However, when services are unreliable, institutions revert to manual workarounds, duplication increases and returns on investment are limited.

Readiness is often more constrained by the lack of the necessary **foundations to operate and sustain digital services**, such as reliable infrastructure, operational routines, predictable financing, governance, security and continuity practices, than by the absence of technology. Strengthening these foundations is therefore necessary to improve outcomes and build sector resilience.



1.2 Why a System Approach

Somalia's higher education sector has made progress through institutional initiatives and project-based support. However, investments risk remaining **fragmented and institution-specific**, which can lead to uneven quality, duplicated costs, incompatible systems, and weak sustainability. Furthermore, fragmentation increases security and continuity risks when institutions expand their digital footprint without consistent standards or shared support capacity.

A system approach offers a more credible path to sustainable improvement. By pooling demand, standardising requirements, and delivering shared services, SomaliREN and its partners can improve value for money, raise the baseline quality of services, and reduce duplication. This approach also enables the development of sector-wide standards for service performance and security, strengthens accountability and supports tier-based sequencing, ensuring that investments match institutions' starting points and build dependable, enduring services.

2 Scope and Approach

This policy note summarises the results of an institutional e-readiness assessment of Somali higher education institutions. The assessment is designed to identify the system conditions that enable or constrain the reliable and sustainable use of digital technologies in support of teaching, learning, research and institutional administration.

2.1 Scope

The assessment focuses on **institutional readiness**—the capabilities and enabling conditions required for digital services to function reliably rather than as fragile assets. It examines six interrelated areas:



Infrastructure and connectivity: external connectivity, internal distribution, power reliability and the basic network environment required to run services.



Core digital systems: the availability and operational status of systems that support academic and administrative functions.



Governance and planning: institutional decision pathways, policies, accountability arrangements and planning practices for ICT.



Operations and capacity: staffing, service management routines (monitoring, support and documentation) and the ability to sustain day-to-day ICT delivery.



Finance and sustainability: budget structures, the predictability of recurrent funding, renewal discipline and cost-sharing or cost-recovery practices.



Security and continuity: baseline security controls, backup and recovery readiness, and the minimum trust conditions required for shared services.

This scope reflects the premise that digital transformation in higher education is less constrained by single technology choices and more by the presence of these institutional foundations.

2.2 Coverage

In order to keep the assessment focused, the following are not covered:



Measuring the digital skills of individual students, faculty or administrators.



Assessing student access and inclusion (e.g. device ownership, affordability or home connectivity) or wider digital inclusion barriers;



Ranking institutions or producing league tables. The tier framework used in this note is a staging tool for sequencing and targeting support; it is not a measure of institutional prestige or quality.



Evaluating pedagogy or learning outcomes directly. Where teaching and learning systems are referenced, the emphasis is on the existence and operability of institutional systems and services, rather than end-user experience.

2.3 Data sources, coverage and limitations

The assessment **targeted 55 institutions across Somali regions** in order to establish a representative institutional baseline of digital readiness that reflects variations in size, ownership and operating models. **Responses were received from 52 institutions, including 50 higher education institutions and two research institutions.** This represents a high overall response rate and broad sector coverage. The responding higher

education institutions (HEIs) reflect substantial variation in scale. Table 1 summarises enrolment-based groupings derived from the observed distribution of reported student populations. The majority of students are enrolled in large institutions: large HEIs account for 58.2% of total reported enrolment, compared with 35.2% in medium institutions and 6.6% in small institutions.

Table 1: Distribution of institutions by size category and student enrolment

Size of institution	Number of institutions	Proportion (%)	Total number of students	Proportion of students (%)
Small (< 1,000)	17	34	9,311	6.6
Medium (1,000 – 3,999)	21	42	49,259	35.2
Large (≥ 4,000)	12	24	81,555	58.2

The assessment primarily draws on structured institutional data collection and validation processes, combining reported information with basic consistency checks and follow-up clarification where required. Findings should be interpreted as an indication of institutional readiness at the time of assessment.

As with most institutional surveys in constrained environments, limitations apply. Some indicators

rely on self-reported information and may reflect variation in record-keeping maturity across institutions. Additionally, the assessment is designed to describe patterns of readiness and constraints rather than attribute causality or predict performance outcomes. Despite these limitations, the assessment’s core value remains intact: identifying the practical conditions that must be strengthened to convert existing assets into reliable, sustainable digital services.

3 Readiness Tiers

This policy note uses a four-tier readiness framework to interpret the findings and guide the sequencing of actions. The tiers provide a practical staging tool that describes the conditions under which digital services can operate reliably within higher education institutions, covering infrastructure, governance, operations, financing and security. The framework is designed to support targeted support and system planning and is not intended to rank universities or be used for league tables or reputational comparisons.

3.1 How to Use Tiers

Use tiers as a lens for **planning and sequencing**. They can help policymakers and partners to identify what can be credibly achieved in the near term, what prerequisites are missing and which system-level interventions can accelerate progress across institutions. Tiers also support **targeting**. Tier 1–2 institutions usually need foundational reliability and operating capacity, whereas Tier 3–4 institutions can consolidate services, improve quality standards and extend advanced capabilities.

What tiers are not:

- » **They are not a ranking** of institutions, performance, or prestige.
- » **They are not a measure of the digital skills** of individual students or staff.
- » **They are not a checklist where any single asset implies readiness** (e.g. having an LMS does not mean that services are reliable).
- » **They are not static**; institutions can move tiers as minimum conditions are met and services become institutionalised.

3.2 Tier Definitions



Tier 1 — Foundational

Digital services exist in a basic form but are **not yet reliable**. Frequent connectivity and power interruptions disrupt operations, and systems may be present but are not consistently supported or used. ICT delivery is largely reactive and the institution's ability to sustain routine digital services is fragile.



Tier 2 — Emerging

Institutions maintain **basic functional services**, but reliability and coverage remain inconsistent. Some core systems may be in place and there may be ICT staff, yet service routines such as monitoring, support, documentation and renewals are still developing. Financing is often short-term or ad hoc, which limits stability and scale.



Tier 3 — Developing

Institutions operate a **more reliable set of core digital services** with clearer responsibilities and more consistent operational routines. Monitoring and user support are in place, and documentation and renewal practices are improving. Financing tends to be more predictable. However, quality standards, continuity practices and sustainability mechanisms have not yet been fully institutionalised.



Tier 4 — Established

Institutions deliver **well-managed, resilient digital services** that are aligned to institutional priorities and supported by mature operational processes and service standards. Security and continuity practices are stronger, including recovery planning and testing, and the institution is positioned to benefit from shared services, cost efficiencies and continuous improvement.

Table 2: Tier definition and gating conditions

Tier	Label	Service reality	Priority focus to move up
1	Foundational	- Services may exist but are not yet dependable - Frequent interruptions; reactive ICT delivery	- Stabilise power/connectivity for critical services - Basic operations: support, monitoring, inventory - Minimum recurrent ICT budget line
2	Emerging	- Basic services function, but reliability/coverage are uneven - Core systems may exist; routines and financing remain ad hoc	- Right-size bandwidth; improve reliability (pooled procurement) - Strengthen service management (roles, routines, documentation) - Minimum security baseline + regular backups
3	Developing	- More reliable core services with clearer roles and routines - Monitoring and support improving; continuity and standards still maturing	- Adopt service standards (SLAs) and performance reporting - Strengthen continuity: recovery plans and periodic testing - Move toward sustainable financing; shared-service participation
4	Established	- Resilient, standards-based services with continuous improvement - Strong security/continuity enables scaling and advanced capabilities	- Optimise shared services and efficiencies - Assurance, risk management and continuous improvement - Scale standards/mentorship to lower-tier institutions

3.3 Gating Conditions for Progression

Movement between tiers depends on meeting a small number of minimum conditions that transform assets into reliable services. The most consequential gating conditions in this assessment include:

- i. **Foundational reliability:** stable power and network performance sufficient to sustain routine operations.
- ii. **Adequacy of connectivity:** bandwidth aligned to institutional scale and service demand (not just ‘a link exists’).
- iii. **Operational capacity:** an ICT function with defined roles, basic monitoring, user support and documentation routines.
- iv. **Predictable financing:** recurrent funding for core service costs (connectivity, system maintenance, licences, security).
- v. **Security and continuity baseline:** basic controls plus backup practices, with at least minimal recovery/continuity planning.
- vi. **Governance and decision pathways:** clear accountability for ICT priorities, standards and procurement decisions.

3.4 National Distribution Across Tiers

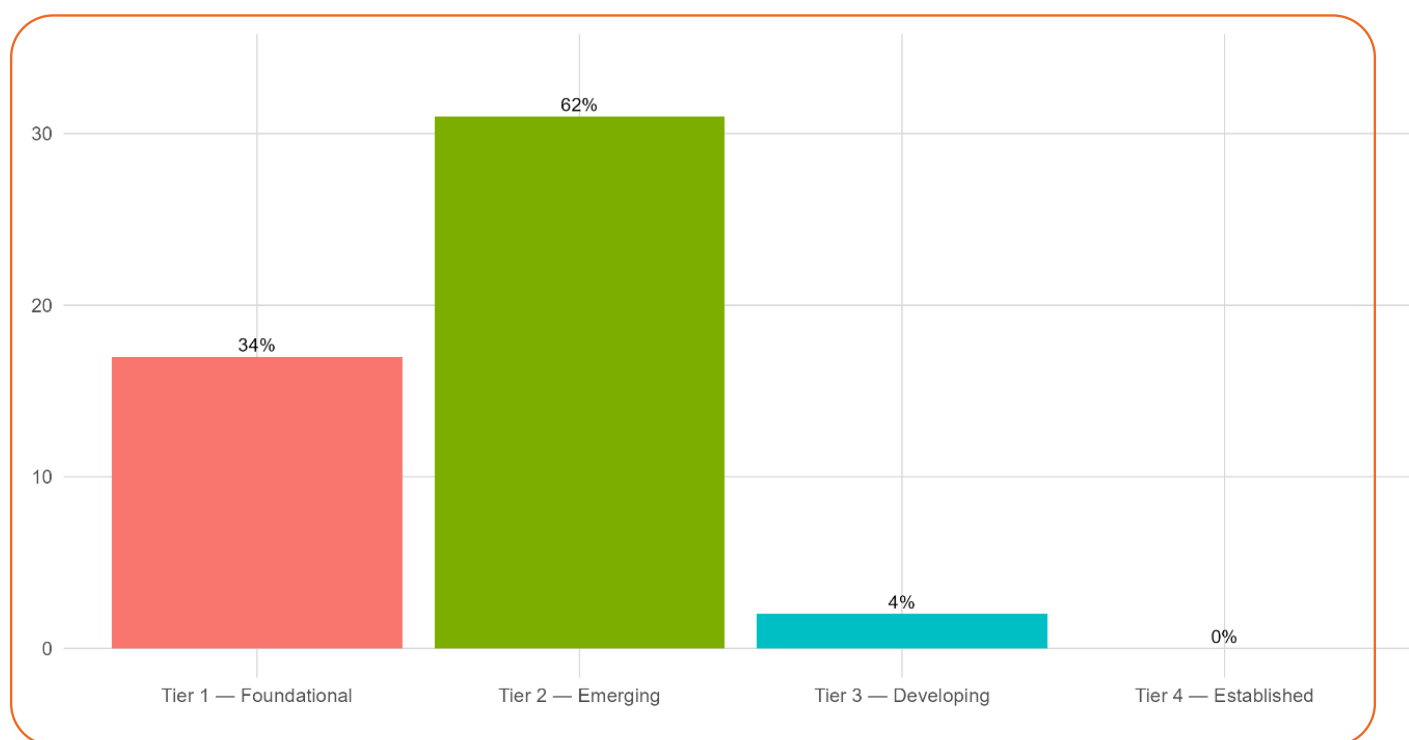


Figure 1: *Distribution of institutions by readiness tier*

The national distribution across tiers shown in Figure 1 suggests that progress within the system will depend on **tier-appropriate, sequenced interventions** rather than uniform, “one-size-fits-all” investments. Where large proportions of institutions remain in the lower tiers, the most credible near-term results focus on foundational reliability, minimum operating capacity and shared procurement efficiencies. As more institutions reach Tier 3 and above, attention can shift towards service standards, shared services and sustainability mechanisms that improve quality and reduce recurrent costs.

Implications for policy and investment:

- » In the short term, prioritise interventions that raise the floor (minimum trust baseline, operational routines and predictable financing).
- » Use SomaliREN and partner support to accelerate tier progression at scale through pooled procurement and shared services.
- » Link major capital investments to evidence that gating conditions are being met to prevent the accumulation of assets without ensuring service reliability.

4 Key Findings

The assessment findings indicate that a small number of binding constraints determine whether digital technologies function as dependable institutional services or remain fragile assets. These constraints cut across the domain structure of the assessment and explain why progress can appear uneven. Institutions may have systems

in place, but the reliability, operating capacity, financing and continuity of these systems are often insufficient to sustain services. The following sections summarise the most significant constraints and highlight implications for policy, investment and delivery at different tiers.

4.1 Connectivity Adequacy and Reliability

Evidence

Basic external connectivity is now widespread, with all surveyed institutions reporting an active internet connection. However, service adequacy and manageability are far more limited. Only 28% have internet monitoring in place, which limits visibility of performance, outages and vendor quality.

When bandwidth is assessed relative to institutional size, the issue becomes apparent. The median institution has 2,069 users (students and staff combined) and contracts 77.5 Mbps, equivalent to **0.04 Mbps per user — around 40 Mbps per 1,000 users**. This level is unlikely to support the routine use of cloud services, digital libraries, learning platforms, video conferencing and online research tools.

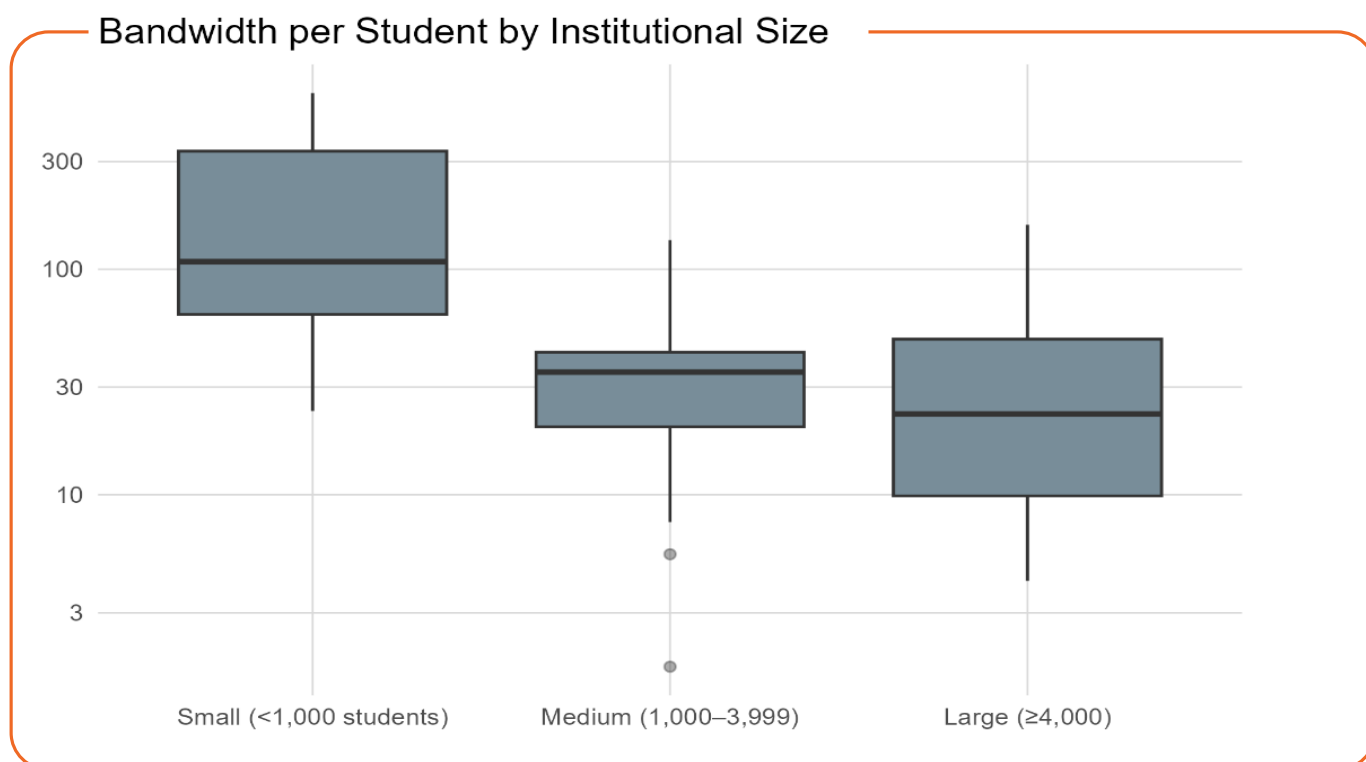


Figure 2: Bandwidth per student by institutional size

A consistent scale penalty emerges as institutions grow as shown in Figure 2. Small institutions (with fewer than 1,000 students) report a median of **107.9 kbps per student**, compared with **35.0 kbps** for medium-sized institutions (with 1,000–3,999 students) and **23.1 kbps** for large institutions (with 4,000 or more students). In practical terms, this equates to approximately **35 Mbps per 1,000 students** for medium-sized institutions and **23 Mbps per 1,000 students** for large institutions, suggesting that capacity has not kept pace with enrolment growth. The World Bank has recommended that African higher education institutions progressively achieve a broadband target of at least **0.2 Gbps (200 Mbps) per 1,000 users** as a baseline for supporting digital learning and research-intensive activities, equivalent to 1 Gbps for a 5,000-student campus.¹

Implications

The question is no longer whether there is any connection, but whether the connectivity is **adequate and reliable on an institutional scale**. Insufficient bandwidth leads to persistent congestion during peak periods, forcing institutions to ration resources and implement workarounds that hinder the adoption of core academic and administrative systems. This also reduces value for money: institutions may invest in systems, platforms and content, but fail to realise the benefits because the underlying service is too limited to support routine use on a large scale.

Actions (tier-sensitive)

- » **Tier 1 (Foundational):** Prioritise stabilising ‘minimum viable’ connectivity for critical functions (administration, communications and core services), alongside basic power and network reliability improvements. Do not invest in complex systems until a minimum reliability baseline is in place.
- » **Tier 2 (Emerging):** Shift from ‘any link is enough’ to adequacy planning — right-size bandwidth to institutional demand and improve resilience (provider redundancy where feasible, better uptime monitoring and campus distribution improvements).
- » **Tier 3–4 (Developing/Established):** Move towards service standards (targeted uptime, response times and traffic management) and consolidate gains through shared procurement, performance benchmarking and continuous improvement.

System-level opportunities

The wide dispersion in bandwidth adequacy and the persistent scale penalty reinforce the case for **pooled procurement and shared contracting support**. SomaliREN and its partners can help institutions to secure better pricing and clearer service levels, strengthen performance monitoring and reduce fragmentation by aggregating demand and standardising requirements, especially for medium-sized and large campuses, where the bandwidth adequacy gap is most severe.

¹ <https://documents1.worldbank.org/curated/en/320071626434508906/pdf/Feasibility-Study-to-Connect-all-African-Higher-Education-Institutions-to-High-Speed-Internet.pdf>

4.2 Financial Sustainability

Evidence

Financial sustainability is a key issue: many institutions find it difficult to fund ICT as an ongoing service rather than a one-off purchase. Where budgets exist, they are often fragmented across units, dependent on short-term projects or insufficient to cover ongoing costs such as connectivity, licensing, maintenance, security, backup arrangements and ICT staffing. Consequently, services established during a project phase often deteriorate over time due to delayed renewals, inadequate maintenance, and unplanned outages.

Implications

Without predictable recurrent financing, institutions cannot transition from having assets to providing enduring services. This creates a cycle of reinvestment in the same basics — connectivity upgrades, equipment replacement and re-installation — without the institutionalisation required for reliability. For governments and their partners, weak sustainability also increases fiduciary risk: investments may fail to deliver the expected outcomes if operating funding, responsibility structures and minimum service standards are not secured simultaneously.

Actions (tier-sensitive)

- » Tier 1 (Foundational): Establish a minimum recurrent funding approach focused on essential services (connectivity, basic operations and protective maintenance). Even small, reliable allocations can reduce repeated 'restart costs'.
- » Tier 2 (Emerging): Introduce budget lines and renewal discipline (licences, maintenance and subscriptions) and provide basic cost visibility, i.e. what it costs per month to keep services running. This tier benefits greatly from pooled procurement to reduce unit costs.
- » Tier 3–4 (Developing/Established): Consolidate sustainability through multi-year ICT plans that are aligned to institutional strategy and that include cost-sharing mechanisms and service standards which clarify what is funded and what performance is expected.

System-level opportunities

Rather than campus-by-campus equipment alone, EARDIP and its partners should prioritise investments that strengthen system delivery capacity, such as shared procurement, shared services, service standards, and operating capacity. This approach helps to reduce recurrent cost pressures, improve predictability and prevent fragmentation.

4.3 Operational Capacity and Service Management

Evidence

Across institutions, the ability to deliver dependable services often hinges on having the right operational capacity. Many institutions report having limited ICT staff, unclear responsibilities, and inconsistent routines for monitoring, user support, documentation, asset management, vendor management, and renewals. Where services do exist, they are often maintained through individual effort rather than institutionalised processes, which makes performance fragile and highly sensitive to staff turnover, outages and procurement delays.

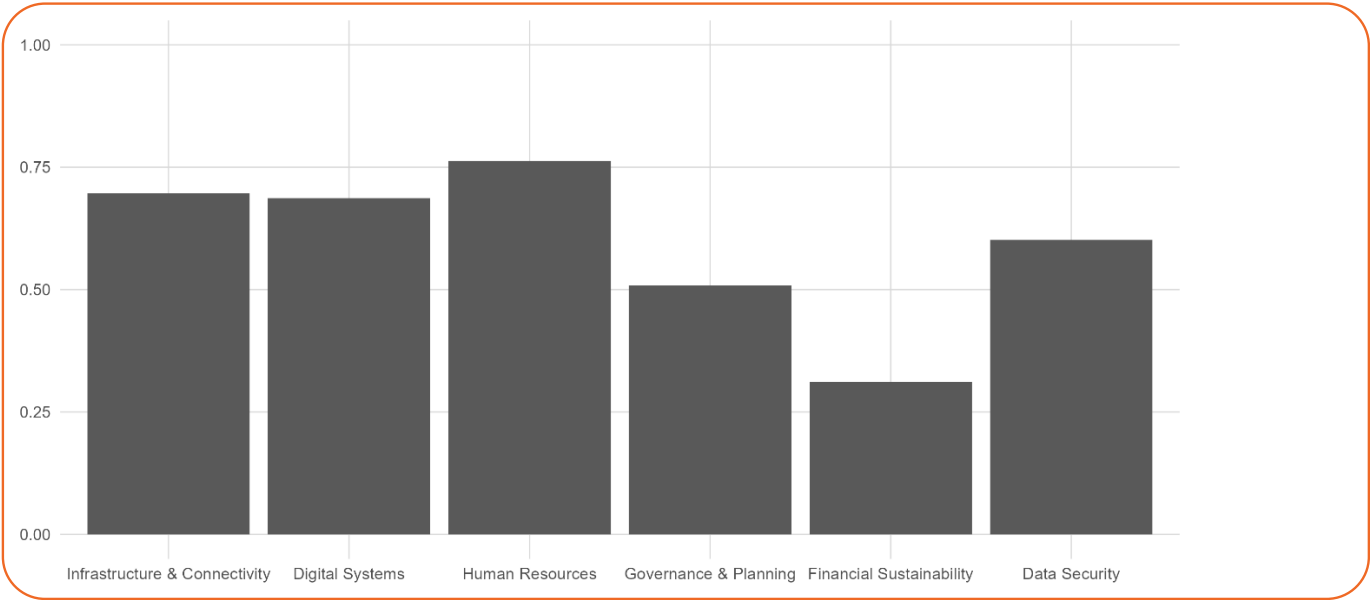


Figure 3: Mean domain scores across institutions

Implications

Poor service management reduces the value of connectivity and systems investments. Downtime persists, minor issues accumulate into major outages and user trust in digital systems declines, leading to parallel manual processes and lower uptake in teaching, learning and administration. It also constrains scalability: even when external connectivity improves, institutions struggle to translate this into stable, campus-wide services without minimum operating routines and clear accountability for day-to-day ICT delivery.

Actions (tier-sensitive)

- » Tier 1 (Foundational): Establish a minimum ICT operating model comprising a basic helpdesk function, simple monitoring (uptime/logs), asset inventory and a small set of critical service routines (patching, backups and access management).
- » Tier 2 (Emerging): Formalise roles and routines (support, monitoring, documentation and renewals); introduce service logs; and standardise basic processes. Prioritise reliability and user support before expanding the scope of systems.
- » Tier 3–4 (Developing/Established): Introduce service standards (SLAs), routine performance reporting, change management and continuous improvement. Participate in shared services that reduce the operational burden and improve quality, such as shared NOC/

SOC-lite, shared procurement support and shared hosting/identity services, where feasible.

System-level opportunities

The operational capacity gap lends itself well to system delivery. SomaliREN and its partners can alleviate the pressure on individual institutions by offering shared operational support, such as common monitoring tools, a helpdesk and escalation pathways, and by encouraging the adoption of a minimum operating model for service management. Standardised templates, playbooks, and tier-linked service expectations can help institutions to establish reliable routines without duplicating effort.

4.4 Core systems and Integration

Evidence

Many institutions have deployed elements of the core digital systems stack, such as student information and administration tools, learning platforms, finance or HR modules, and institutional email and collaboration tools. However, their capabilities are often constrained by partial implementation, uneven usage across departments, limited interoperability between systems and weak supporting processes, such as identity management, data governance, user support and routine administration. Consequently, although systems may exist, they do not consistently function as integrated institutional services that streamline workflows and generate reliable management information.

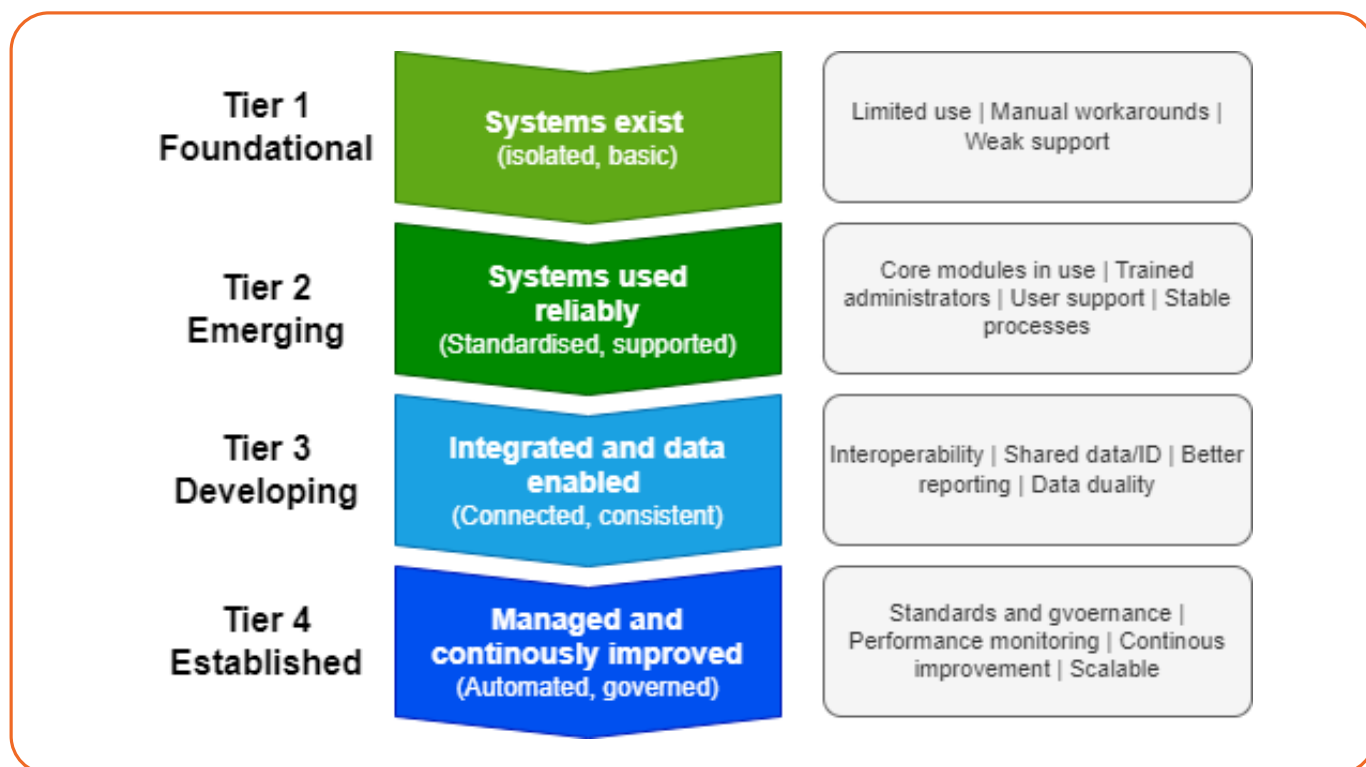


Figure 4: Core systems maturity ladder (tier 1 to 4)

Implications

When core systems are fragmented or underused, institutions fail to realise the productivity and accountability gains promised by digital transformation. Manual workarounds persist, reporting remains slow and inconsistent, and data quality suffers, limiting evidence-based decision-making and weakening trust in digital processes. This is important for partners and the government because investments can result in the installation of systems without delivering sustained improvements in service delivery, operational efficiency or learning outcomes.

Actions (tier-sensitive)

- » Tier 1 (Foundational): Focus on a small number of critical, low-burden systems that can be sustained, such as institutional email/collaboration and basic student administration, and avoid expanding the scope of

systems until minimum reliability and operational routines are in place.

- » Tier 2 (Emerging): Stabilise and standardise the core stack, ensuring consistent usage. Assign system owners, train administrators and strengthen user support. Prioritise ‘making what exists work reliably’ over acquiring new platforms.
- » Tier 3–4 (Developing/Established): Improve integration and data quality by introducing basic interoperability approaches (shared identity, common data standards and integration where feasible), strengthening data governance and using management information for planning and accountability. Consider shared platforms or hosting/services where these reduce costs and improve reliability.

System-level opportunities

System fragmentation can be reduced through common standards and shared services. Agreeing on minimum interoperability and reporting standards (e.g. identity approaches, core data fields, and output formats) would improve coherence and enable aggregation over time. Where appropriate, shared platforms or shared hosting/support services, delivered through SomaliREN or trusted partners, can improve reliability and reduce unit costs. Reference architectures and model specifications can also prevent incompatible procurement.

4.5 Security and Continuity

Evidence

Security controls and continuity practices vary across institutions. While basic measures such as antivirus software, passwords and ad hoc backups may exist, they are not consistently implemented as part of a managed security strategy. Crucially, many institutions lack routine practices for recovery and continuity, including documented recovery procedures, regular backup validation, incident response routines and clear accountability for managing security events. This creates a persistent gap between having data copies and being able to reliably restore services after an outage, cyber incident or equipment failure.

Table 3: Data protection and backup practices

Indicator	Summary
Institutions that back up institutional data	94%
Regularity of institutional data backups	Yes – regularly
Backup automation status	Automated
Institutions that have tested data restoration or disaster recovery processes	47%
Institutions providing cybersecurity or data protection training to ICT staff	41%

Implications

Inadequate security and continuity measures undermine trust in digital systems and increase the risk of service disruptions escalating into prolonged institutional crises. For governments and their partners, this poses not only an institutional risk, but also a systemic one: as shared services expand (e.g. connectivity pooling, shared platforms, federated identity and shared hosting), the minimum security baseline required for safe participation becomes increasingly important. Without a 'minimum trust baseline', scaling digital services can increase exposure and reputational risk and erode confidence in sector-wide digital transformation efforts.

Actions (tier-sensitive)

- » **Tier 1 (Foundational):** Establish a minimum trust baseline comprising basic access controls, regular backups of critical systems and data, defined administrator accounts and simple incident reporting. Start with a small set of critical services and protect them well.
- » **Tier 2 (Emerging):** Institutionalise security routines, such as patching and updates, backup schedules, basic logging and backup validation. Clearly assign responsibility for security tasks and begin continuity planning (decide what to restore first and how).

- » **Tier 3–4 (Developing/Established):** Move towards managed security and continuity, including documented incident response, periodic recovery testing, role-based access, stronger authentication where feasible and compliance-oriented practices. Participate in shared security support (e.g. SOC-lite services, shared awareness and playbooks) to reduce the burden and improve quality.

System-level opportunities

Security and continuity require a minimum trust baseline across the entire system, especially as shared services expand. SomaliREN and its partners can define baseline controls and continuity practices as conditions for participation and provide shared support, such as incident reporting channels, standard response playbooks and periodic exercises. Pooled options for backup and recovery testing support can also raise continuity readiness more efficiently than institution-by-institution approaches.

4.6 Governance and Decision Pathways

Evidence

Governance arrangements for ICT are often not clearly defined enough to support consistent prioritisation, standard-setting, procurement discipline and accountability. Many institutions lack clear decision pathways that connect leadership intent (strategy) to operational

execution (standards, budgets and enforcement). There are also coordination gaps at the system level: without agreed service standards and shared delivery mechanisms, institutions are incentivised to pursue isolated solutions, resulting in duplication, uneven quality and high unit costs.



Figure 5: Governance stack for system delivery

Implications

Governance is a binding constraint because it determines whether investment leads to coordinated service delivery or fragmented procurement. Without clear mandates, standards and accountability, even well-funded initiatives risk producing incompatible systems, weak sustainability and inconsistent

security practices. Strong governance is also necessary to leverage SomaliREN as a delivery platform. Shared procurement, shared services and performance monitoring require rules to be established, such as who sets standards, who enforces them, how exceptions are handled and how costs are shared.

Actions (tier-sensitive)

- » Tier 1 (Foundational): Create clear institutional accountability by designating ICT leadership responsibility, defining minimal decision-making routines (e.g. budgeting and procurement approvals) and ensuring alignment between leadership priorities and the minimum operating model.
- » Tier 2 (Emerging): Introduce basic policies and standards (e.g. procurement specifications, minimum security baseline, service expectations) and establish simple monitoring and reporting routines. Reduce ad hoc decisions by formalising renewals and vendor management.
- » Tier 3–4 (Developing/Established): Strengthen governance to enable growth by adopting service standards (SLAs), performance reporting, audit and assurance routines, and participation rules for shared services and pooled procurement. Use tier-based targeting to allocate support and track progress over time.

System-level opportunities

Governance enables coordinated investment and delivery at scale. A light but explicit coordination mechanism linking government, SomaliREN, and institutional representation can set standards, prioritise investments, and monitor performance. Using tiers as the agreed targeting tool (including for EARDIP resourcing) and formalising a SomaliREN service catalogue with basic service levels can reduce fragmentation and strengthen accountability.

5 Implications by Tier

This section translates the tier framework into practical implications for planning, targeting support and sequencing investments. Read this section alongside Table 2 and Figure 1, which were presented earlier.

5.1 What Each Tier Enables

Tier 1: Foundational

Institutions at Tier 1 can maintain a limited number of basic digital functions, but these are fragile and subject to frequent interruption. The priority is to stabilise essential services such as connectivity and power for critical ICT, as well as basic support routines, while avoiding expanding the systems footprint faster than the institution can operate and sustain.

Tier 2: Emerging

Tier 2 institutions have basic services in place, but reliability and coverage remain uneven, and operational routines are still being developed. The practical priority is to ensure consistent operation of existing systems: right-sizing and stabilising connectivity, establishing minimum service management routines, and introducing predictable funding and renewal discipline.

Tier 3: Developing

Tier 3 institutions operate a more reliable core service stack with clearer roles and routines. However, standards, continuity practices, integration and sustainability mechanisms have not yet been fully institutionalised. The practical priority is to formalise service standards, strengthen continuity and security, and begin integration and performance reporting.

Tier 4: Established

Tier 4 institutions deliver resilient,

standards-based services with continuous improvement. The practical priority shifts from building basic capability to optimisation and scaling up, including improving efficiency, deepening integration, adopting advanced practices and supporting system-level initiatives such as shared services, mentoring and benchmarking.

5.2 How Institutions Progress

Progress is less about acquiring new systems and more about achieving dependable services.

- **Reliability first:** fewer interruptions and predictable uptime for core services
- **Institutionalisation:** involves documented routines, assigned roles and timely renewals.
- **Sustainability:** recurrent costs are covered and there is basic cost visibility and planning.
- **A trust baseline:** established through routine backups and tested recovery and continuity practices.

Common mismatch patterns are evident across tiers (explaining why institutions can appear “strong” in one area yet be constrained overall).

- » **Systems without reliability:** platforms exist (LMS/SIS/email), but instability in bandwidth and power prevents routine use.
- » **Connectivity without service management:** connectivity is improved, but weak support and monitoring mean that downtime persists.
- » **Assets without sustainability:** equipment and licences are acquired through projects, but the recurrent costs and renewals are unfunded.

- » **Backups without recovery:** data copies exist, but recovery procedures and testing are inadequate, meaning services cannot be restored quickly.
- » **Local improvements without standards:** upgrades occur locally, but a lack of standards and coordination limits scale and interoperability.

5.3 Targeting Support by Tier

Use the tier system to provide targeted support and avoid one-size-fits-all programming.

Tier 1: Foundational (raise the floor)

- » Support options: foundational reliability packages; minimum operating model; minimum trust baseline; basic budgeting support for recurring costs.
- » Avoid complex systems rollouts, advanced integration or large equipment purchases without operating capacity.

Tier 2 – Emerging (stabilise and standardise)

- » Best-fit support: improvements to bandwidth adequacy; service management routines; renewal discipline; baseline security and continuity practices; shared procurement support.
- » Avoid expansion into multiple new platforms before stabilising existing ones.

Tier 3 – Developing (institutionalise and integrate)

- » Best-fit support: service level agreements (SLAs); performance reporting; recovery testing; interoperability steps (identity/data standards); cost-sharing mechanisms; and shared services participation.
- » Avoid bespoke, one-off solutions that increase complexity without improving service quality.

Tier 4 – Established (optimise and scale)

- » Best-fit support: optimisation, advanced security and governance, shared services, leadership roles, mentoring, peer learning, benchmarking and continuous improvement.
- » Avoid parallel standalone solutions that fragment the system or duplicate shared services.

System targeting implication:

As most institutions currently fall within Tiers 1–2, near-term investments should prioritise minimum viable service reliability and operating capacity, delivered at scale through shared approaches. As more institutions progress to Tiers 3–4, the focus can shift towards standards, interoperability, quality assurance and sustainability mechanisms that improve performance and reduce recurrent costs.

6 Recommendations and Sequencing

The recommendations below are organised into three time horizons and two readiness groups: Tier 1–2 (Foundational/Emerging) and Tier 3–4 (Developing/Established). These groups are supported by system-level actions that enable scale. The intention is to prioritise short-term steps that improve baseline service reliability and reduce fragmentation, while establishing a clear pathway towards managed, sustainable digital services.

- » **Tier 1–2:** Prioritise reliability, minimum operating capacity, predictable recurrent funding and a minimum trust baseline.
- » **Tier 3–4:** Prioritise service standards, integration, performance reporting, continuity testing and efficiency through shared services.
- » **System level (all tiers):** Use SomaliREN to enable pooled procurement, shared tools and services, common standards and coordinated monitoring, reducing fragmentation and accelerating progress at scale.

6.1 Priority Actions (0–6 months)

Tier 1–2: Stabilise and establish minimum service conditions

- » **Define a minimum service package** for institutional operations (connectivity for core functions, basic email and collaboration tools, and priority administrative workflows) and focus support on ensuring its reliability.

- » **Put a minimum operating model in place**, including basic support and helpdesk services, simple monitoring, asset inventory and documented routines for renewals and backups.
- » **Introduce a minimum trust baseline** for security and continuity (regular backups for critical systems and data, basic access controls, named responsibility for incident handling and simple recovery steps).
- » **Create a minimum recurrent ICT budget line** (even if modest) to cover essential recurring costs (connectivity, basic maintenance and critical subscriptions/licences).

Tier 3–4: Consolidate reliability and standardise quality

- » **Adopt basic service standards** for core services (e.g. uptime expectations, response times and escalation pathways) and begin routine performance reporting.
- » **Strengthen continuity** by documenting recovery procedures and scheduling periodic recovery testing for priority services.
- » **Clarify ownership of major systems** by appointing named system owners, training administrators and documenting configurations to reduce dependence on individuals.

System-level actions to enable scale and reduce fragmentation

- » **Agree on the tier framework** as the tool for targeting support and investment sequencing (i.e. not for ranking).
- » **Launch pooled procurement** support through SomaliREN for connectivity and common ICT goods and services, including model specifications and basic service levels.
- » **Confirm a shortlist of decisions** regarding participation rules, the minimum baseline and which services will be delivered/shared first.

6.2 Scaling Actions (6–18 months)

Tier 1–2: Transition from unreliable assets to reliable services

- » **Right-size and stabilise connectivity** relative to institutional scale including campus distribution, if applicable
- » **Institutionalise service management routines** such as ticketing/logs, scheduled maintenance, renewals calendar, vendor management and documentation
- » **Stabilise core systems** that have already been deployed (ensure consistent usage, assign system owners and strengthen user support and administrator capacity)
- » **Begin basic continuity planning** (identify priority services, define the order of restoration, validate backups and conduct simple recovery drills).

Tier 3–4: Institutionalise, integrate and improve efficiency

- » **Implement service standards and SLAs** for core services with routine monitoring and reporting (internal and/or via SomaliREN shared tools).
- » **Improve interoperability and data quality** by using a shared identity approach where feasible, establishing common data definitions and producing reports that support institutional planning.
- » **Strengthen sustainability mechanisms** through multi-year ICT planning, clearer cost visibility, cost-sharing approaches appropriate to the context and reducing unit costs through shared services.
- » **Strengthen security governance** (role-based access; stronger authentication where feasible; patching discipline; incident response routines; tested recovery).

System-level actions to enable shared services and improve standards

- » **Improve the service catalogue for SomaliREN-supported services**, including what is offered, service levels, participation requirements and costing principles
- » **Introduce common standards** (minimum security baseline, procurement specifications, minimum operating model and reporting expectations).
- » **Build shared operational support** (NOC/helpdesk functions, shared tooling, training, and playbooks) to reduce the burden on institutions and increase consistency.

6.3 Consolidation Actions (18–36 months)

Tier 1–2: Maintain progress and move into Tier 3

- » **Maintain reliability and renewals** (avoid ‘restart cycles’ by maintaining recurrent funding and operational routines).
- » Once minimum conditions are met, **expand the core service package cautiously** (prioritise services with strong operational feasibility).
- » **Formalise governance linkages** between leadership priorities, budgeting and ICT execution so that services remain stable across leadership changes.

Tier 3–4: Optimise, assure and scale advanced capability

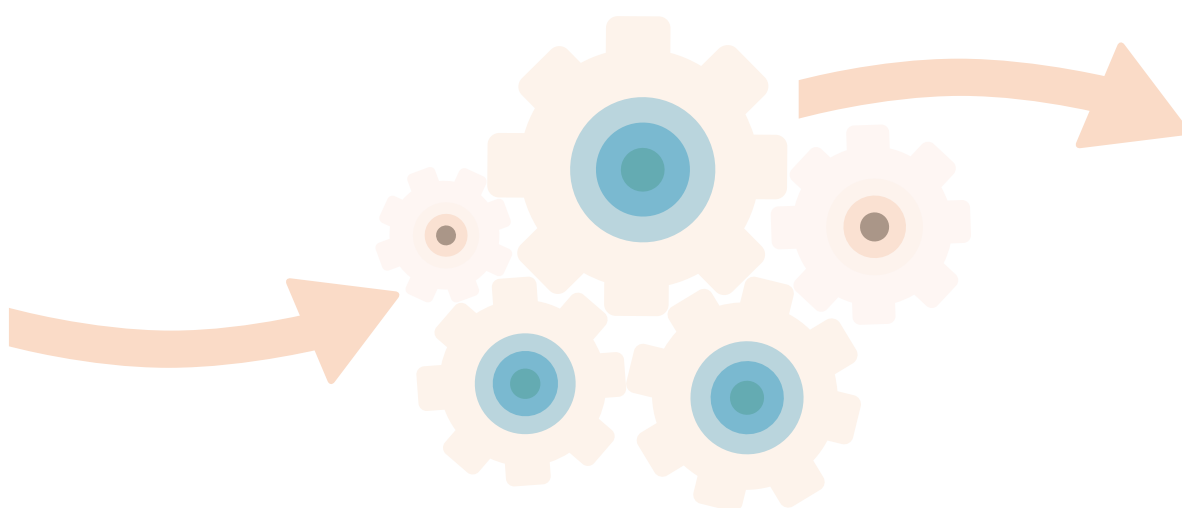
- » **Continuous improvement and assurance** through regular performance reviews, user feedback loops, planned upgrades rather than reactive replacements
- » **Stronger resilience** involving routine recovery testing, improved backup architecture and clearer incident management maturity (including sector-wide exercises where feasible)
- » **Increase efficiency through**

shared services by expanding the use of shared hosting/support and shared procurement, and by benchmarking costs and service performance

- » **Develop advanced use cases** where foundational reliability is strong, selectively scale analytics, research collaboration services and emerging technology pilots.

System-level actions (sustainability and governance)

- » **Embed tier-based planning in annual cycles** (review tier movement, update targeting and track service reliability and sustainability indicators).
- » **Formalise quality assurance processes**, including service reporting, audits and assurance checks, and compliance with the minimum trust baseline.
- » **Strengthen cost-sharing and long-term financing** to sustain shared services and reduce dependence on one-off projects.



7 Delivery and Financing

This section outlines the approach to delivery required to transition from fragmented, institution-by-institution investments to reliable, sustainable services at a systems level. The focus is on SomaliREN as the core coordination and delivery platform, the catalytic role of EARDIP, and the sustainability principles required for investments to translate into enduring services.

7.1 SomaliREN as a Delivery Platform

SomaliREN provides a practical mechanism for delivering sector-wide improvements that individual institutions cannot efficiently achieve on their own. By aggregating demand and standardising requirements, SomaliREN can help institutions to secure better value for money, improve service reliability and reduce duplication through **pooled procurement and shared services**.

Key functions of SomaliREN as a delivery platform include:

- » **Pooled procurement and contracting support:** aggregation of institutional demand for connectivity and common ICT goods/services; model specifications; clearer service levels; and improved price discipline.
- » **A shared service catalogue:** a defined set of shared services that institutions can opt into, prioritising those with the highest impact on reliability and sustainability (e.g. monitoring tools, helpdesk escalation, shared hosting options where feasible, common collaboration services and security support partnerships).
- » **Standards and participation rules:** minimum technical and operational requirements for participation (including a minimum trust baseline) to ensure that shared delivery improves quality rather than spreading risk.
- » **Performance monitoring and reporting:** basic measurement of service levels (e.g. uptime, incident response and renewal discipline) to support accountability and continuous improvement.

Participation by institutions should be linked to clear commitments, such as minimum readiness steps, cost-sharing contributions and adherence to standards. SomaliREN enables government and partners to shift from funding discrete projects to funding a delivery mechanism capable of sustaining services on a large scale.

7.2 EARDIP as a Catalytic Window

EARDIP provides a time-limited opportunity to speed up tier progression and establish sector-wide service foundations. To maximise impact and reduce fragmentation, EARDIP financing should prioritise investments that strengthen **system delivery capacity** and reduce ongoing cost pressures.

High-priority funding areas include:

- » **Shared procurement capability and frameworks:** such as contracting tools, model specifications, service level templates and procurement support that institutions can reuse.
- » **Shared operational capacity:** monitoring tools and routines; helpdesk/escalation pathways; training and playbooks; and light-touch service management support to improve reliability across institutions.
- » **Minimum trust baseline and continuity readiness:** shared incident response arrangements, baseline security controls, recovery planning/testing support and sector-level assurance practices.
- » **Targeted upgrades that unlock service reliability:** such as connectivity adequacy improvements and critical campus distribution improvements, especially when tied to standards and operating commitments.
- » **Interoperability foundations:** minimum standards for identity and core data and reporting to reduce system fragmentation over time.

In practice, EARDIP should be used to 'build the rails' for coordinated delivery, including standards, shared services, shared procurement and operating capacity, while using tiers to appropriately target institution-level support.

7.3 Sustainability Principles

Long-term success depends on viewing ICT as an ongoing service obligation rather than a series of individual projects. The following principles can help anchor sustainability:

- » **Service-first financing:** ensure that recurrent costs (connectivity, licences, maintenance, security, backups and minimum ICT staffing) are planned for and funded, not just the initial acquisition.
- » **Cost sharing should be aligned to service value:** this means defining transparent contributions for shared services (e.g. tier-sensitive contributions, enrolment or size proxies or service-based fees) in order to sustain SomaliREN-delivered functions without overburdening lower-tier institutions.
- » **Standards as a condition for scale:** shared procurement and shared services should adhere to minimum standards (service levels, security baseline, documentation, and renewal discipline) to protect quality and reduce system risk.
- » **Predictability and renewal discipline:** multi-year planning and timely renewals are essential to prevent service degradation and repeated 'restart costs'.
- » **Accountability through simple performance reporting:** track a small set of indicators that reflect service reliability and sustainability, such as uptime, incident response, renewal timeliness, backup validation/recovery testing and budget line presence.

When applied consistently, these principles can help reduce fragmentation, improve value for money and ensure that EARDIP and partner investments result in dependable services that institutions can sustain and improve over time.

8 Implementation

This section summarises the minimum implementation architecture required to deliver the recommendations on a large scale and prevent execution from becoming fragmented. It clarifies roles, establishes a light monitoring cadence

and lists priority decisions that must be confirmed, enabling the government, SomaliREN, institutions and partners to swiftly progress from agreement to delivery.

Visual 8: RACI-lite + Milestone Strip

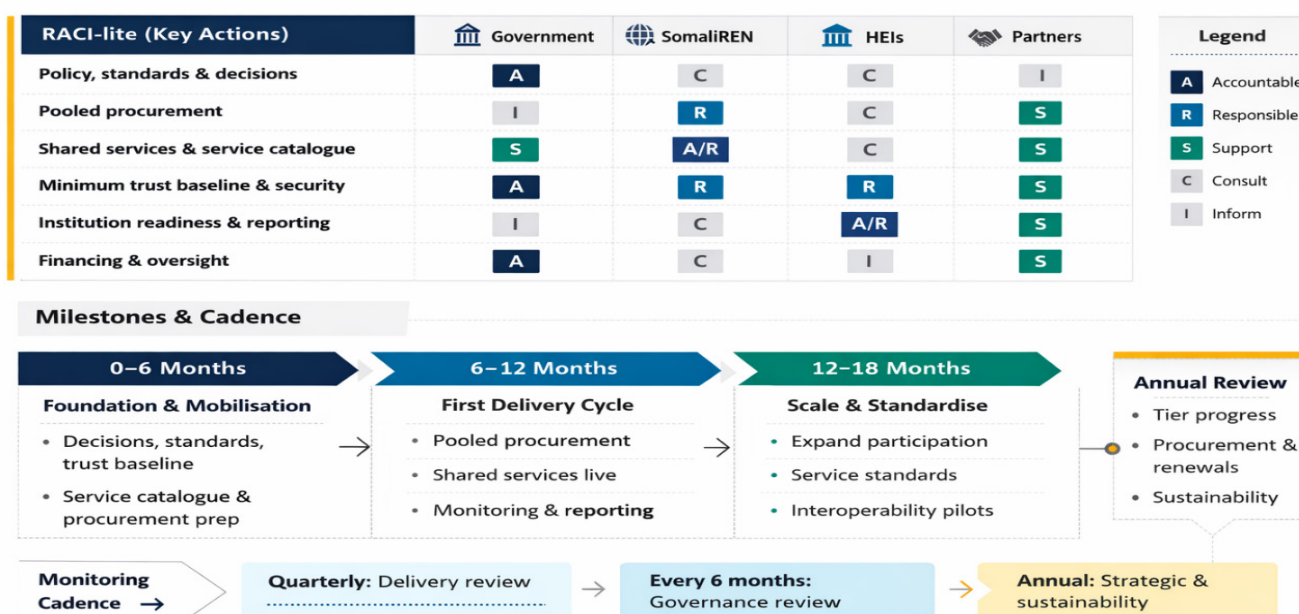


Figure 6: Implementation architecture for coordinated delivery

8.1 Roles and Responsibilities

Implementation requires a clear division of responsibilities across four groups of actors:



Government/sector leadership sets policy direction, confirms standards and participation rules, and provides oversight for system coordination and accountability



SomaliREN acts as the delivery platform for pooled procurement and shared services. It maintains the service catalogue and service standards and coordinates performance monitoring across participating institutions



Higher education institutions (HEIs) implement minimum internal readiness actions (operating routines, governance assignments, budget lines and adherence to the minimum trust baseline), participate in pooled procurement and shared services and report a small set of performance signals



Development partners (including the World Bank) finance catalytic system-level capacity (shared services, procurement frameworks and standards rollout), provide technical assistance and support monitoring and learning.

8.2 Milestones and Monitoring Cadence

A consistent but light monitoring cadence is essential to sustain momentum and ensure that investments translate into improved services over time.

Proposed milestones

- » **0–6 months (foundation and mobilisation):**
 - Confirm the tier framework and participation rules.
 - Agree the minimum trust baseline.
 - Confirm the initial service catalogue and service standards.
 - Establish governance and coordination arrangements.
 - Prepare the launch of pooled procurement and shared services (including templates, specifications and onboarding steps).
- » **6–12 months (first delivery cycle):**
 - Complete the first pooled procurement cycle
 - Deploy priority shared services for participating institutions
 - Implement baseline monitoring tools and reporting templates
 - Begin continuity improvements (e.g. backup validation and basic recovery steps) in participating institutions.
- » **12–18 months (scale and standardise):**
 - Expand participation
 - Embed service standards and routine reporting
 - Agree initial interoperability steps (e.g. minimum identity, data and reporting standards) and begin targeted pilots where feasible.

Monitoring cadence:

- » **Quarterly (delivery review):** SomaliREN and the participating institutions review the progress of implementation against the milestones, as well as any service issues that could affect continuity and any risks that require escalation.
- » **Every six months (governance review):** involving a sector steering review of standards compliance, participation, shared service performance and financing/sustainability risks. Partners align support and remove bottlenecks.
- » **Annual (strategic review):** involves a tier-based progress review and targeting update, a service catalogue refresh, and a consolidated review of the status of procurement and renewals for priority services as part of sustainability planning.

The monitoring burden should be kept to a minimum by focusing on a small number of indicators that reflect service reliability, sustainability and compliance with the minimum trust baseline.

e-Readiness Assessment Report of **Somali** **Higher Education Institutions 2026**



TCC Building, Taleh Road, Hodan District, Mogadishu, Somalia



+252 612697979



info@somaliren.org



<https://www.somaliren.org>